N^0=d'ordre : 18/2008-M/MT

République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université des Sciences et de la Technologie Houari Boumediene

Faculté de mathématiques

MEMOIRE

Présenté pour l'obtention du diplôme de MAGISTER

EN : MATHEMATIQUES

Spécialité : Algèbre et théorie des nombres

Par : MAMERI Ahmed

Sujet

Courbes Elliptiques et leurs Applications Cryptographiques

Soutenu le : 11/03/2008, devant le jury composé de:

M . BENZAGHOU Ben Ali ;	**Professeur**	**USTHB**	**Président**
M . HACHAICHI M. Salah ;	**Maître de conférences**	**USTHB**	**Directeur de thèse**
M . ZITOUNI Mohamed ;	**Professeur**	**USTHB**	**Examinateur**
M . AIDER Meziane ;	**Professeur**	**USTHB**	**Examinateur**
M . BETINA Kamal ;	**Professeur**	**USTHB**	**Examinateur**
M . HERNANE M. Ouamar ;	**Maître de conférences**	**USTHB**	**Examinateur**

Table de matières

Introduction ……1
Chapitre 1
1.1 Arithmétique sur les courbes elliptiques ……..2
1.1.1 Définitions ……2
1.1.2 Loi de groupe sur une courbe elliptique ……6
1.1.2.1 Approche géométrique de la loi de la sécante tangente……..7
1.1.2.2 Expression analytique ……10
1.2 Fonctions polynomiales et rationnelles……11
1.2.1 Définitions ……11
1.2.2 Zéros et pôles d'une fonction rationnelle ……..14
1.2.3 Diviseurs ……...18
1.2.4 Isogénies ……...20
1.2.4.1 Applications rationnelles entre courbes elliptiques ……...20
1.2.4.2 Homomorphismes ……21
1.2.4.3 Isogénie duale ……... 21
1.2.4.4 Anneau des endomorphismes d'une courbe elliptique……...22
1.2.5 Points de m-torsion ……...22
1.2.6 Les polynômes de divisions ……..29
1.2.7 L'accouplement de Weil ……..32
1 .3 Courbes elliptiques sur un corps fini…… 35
1.3.1 Théorème de Hasse ……..35
1.3.2 Compter les points d'une courbe elliptique sur un corps fini…….. 36
1.3.2.1 L'algorithme de Schoof……. 38

Chapitre 2
2. Introduction générale à la Cryptologie ……...46
2.1 Rappel des objectifs fondamentaux de la cryptographie ……46
2.1.1 Cryptographie à clé secrète ……..46
2.1.1.1 Exemples historiques ……48
2.1.1.2 Le système de Vernam, ou « one-time pad »……49
2.1.1.2 Le chiffrement à clé secrète : point de vue moderne……. 49
2.1.2 Cryptographie à clé publique ……..50
2.1.2.1 L'exponentiation modulaire ……..50
2.1.2.2 Le protocole de Diffie-Hellman ……51
2.1.2.3 L'idée de clé publique ; le système d'El Gamal ……...52
2.1.2.4 La fonction puissance : le système RSA ……...54
2.2 Génération des grands nombres premiers ……..55
2.2.1 Test de Solovay-Strassen. ……56
2.2.2 Test de Miller-Rabin ……58
2.2.3 Test AKS (*Agrawal, Kayal et Saxena*) …….. 58
2.3 Cryptosystèmes basés sur les courbes elliptiques ……... 61
2.3.1 Protocole d'échange de clé Diffie- Hellmann ……..61
2.3.2 Problème du logarithme discret ……...62
2.3.2.1 Problème Diffie- Hellmann ……...62
2.3.2.2 La méthode d'ElGamal ……65

2.3.2.3 Le système de Menezes- Vanstone ……...67
2.3.2.4 Signature électronique d'ElGamal ……67
2.3.2.5 Algorithme de signature digitale avec courbe elliptique ECDSA …… 71

Chapitre 3
3.1 Résoudre le problème du logarithme discret ……..73
3.1.1 Baby Step, Giant Step …….. 73
3.1.2 L'algorithme MOV ……..74
3.2 Choix d'une courbe elliptique pour une utilisation cryptographique ……77
3.2.1 Cas d'une courbe elliptique définie sur F_p ……77
3.2.2 Cas d'une courbe elliptique définie sur F_{2^m}. 78
3.3 Performances de ECC ……78
3.3.1 Comparaison des niveaux de sécurité …….. 78
3.3.2 Comparaison des temps de calcul ……79

Chapitre 4
4.1 Application ……..81
4.2 Langage de programmation ……81
4.3 Implémentation des différentes étapes du système ……81
4.3.1 Étape de génération d'un grand nombre premier…….. 81
4.3.2 Étape de génération de la courbe elliptique ……..81
4.3.3 Étape de calcul de nombre de points d'une courbe elliptique ……82
4.3.4 Étape de choix de la courbe elliptique ……82
4.3.5 Étape de choix de l'ensemble des paramètres ……82
4.4 les algorithmes implémentés ……82
4.4.1 Algorithme de génération de l'ensemble de paramètres ……..82
4.4.2 Algorithme de génération de la paire de clés ……...83
4.4.3 Algorithme de chiffrement ECC ……..83
4.4.4 Algorithme de déchiffrement ECC ……83
4.4.5 Algorithme de signature ECDSA ……84
4.4.6 Algorithme de vérification de signature ECDSA …… 84
4.5 Description du logiciel ……..85
4.5.1 Les menus ……85
Conclusion ……... 93
Bibliographie ……94

Notation

Dans tout ce document nous fixons $q = p^n$ où p est un nombre premier.

N, ensemble des nombres naturels

Z, ensemble des entiers relatifs

R, ensemble des nombres réels

Q, ensemble des nombres rationnels

C, ensemble des nombres complexes

$\#E = |E|$, cardinalité de l'ensemble fini E

$\lfloor x \rfloor$, plus grand entiers inférieur ou égal à x

$n \bmod m$, reste de division euclidienne d'un entier n par l'entier m

$\left(\frac{m}{n}\right)$, symbole de Jacobi de l'entier m par rapport à l'entier n

Z/lZ, anneau des entiers modulo l

F_{p^n}, corps fini à p^n éléments

$F_q[x]/(P(x))$, extension algébrique d'un corps fini F_q définie par un polynôme $P(x)$

$\overline{K}$, clôture algébrique d'un corps K

$\deg(P)$, degré d'un polynôme P

Id, application identité

$End(E)$, groupe d'endomorphismes d'un groupe E

$Ker\phi$, noyau d'un morphisme ϕ

$\phi \circ \psi$, composition de deux morphismes

$E[m]$, sous groupe de points de *m-torsion* d'une courbe elliptique E

AES, Advanced Encryption Standard

DES, Data Encryption Standard

DH, Diffie-Hellman

DHP, Diffie-Hellman Problem

DL, Discrete Logarithm

DLP, Discrete Logarithm Problem

DSA, Digital Signature Algorithm

DSS, Digital Signature Standard

ECC, Elliptic Curve Cryptography

ECDDHP, Elliptic Curve Decision Diffie-Hellman Problem

ECDH, Elliptic Curve Diffie-Hellman

ECDHP, Elliptic Curve Diffie-Hellman Problem

ECDLP, Elliptic Curve Discrete Logarithm Problem

ECDSA, Elliptic Curve Digital Signature Algorithm.

Introduction

L'intérêt suscité par les systèmes de chiffrement à clef publique, fut le point de départ d'un nouvel engouement pour la théorie des nombres et l'arithmétique dans ses aspects calculatoires. Dans ce domaine où la construction explicite sur ordinateur "d'objets mathématiques abstraits" joue un rôle prépondérant, les résultats obtenus peuvent servir aussi bien à mettre en oeuvre de nouveaux procédés qu'à montrer les faiblesses d'anciens schémas.

Les courbes elliptiques définies sur des corps finis sont un exemple parmi d'autres de ces objets. Elles ont des applications aussi bien pour construire de grands nombres premiers, pour trouver de petits facteurs premiers d'un nombre de taille arbitraire que pour permettre la construction de schémas cryptographiques très sûrs. Pour cette dernière application, l'ensemble des points $E(F_q)$ d'une courbe elliptique de la forme : $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ définie sur un corps à $q = p^n$ éléments F_q, forme un groupe fini et le calcul du nombre de points de ces courbes est une étape incontournable pour toute mise en œuvre cryptographique. Or, seule l'utilisation de courbes elliptiques d'un type particulier était dans un premier temps possible. Il s'agit essentiellement des courbes supersingulières. Cependant, ces dernières se sont avérées désastreuses car le problème du logarithme discret y est plus facile à résoudre. Rappelons que le problème du logarithme discret consiste, étant donné un élément R de sous groupe cyclique G engendré par un élément P, à trouver un élément k tel que $R = kP$.

L'objet de ce travail est de présenter les applications des courbes elliptiques à la cryptographie. Pour cela, le premier chapitre est consacré d'une part à la théorie des courbes elliptiques et aux preuves de certains résultats, d'autre part à l'algorithme de Schoof ; une méthode de comptage de points d'une courbe elliptique définie sur un corps fini, un algorithme d'une complexité polynomiale. Le deuxième chapitre est une partie purement cryptographique ; elle traite de la cryptographie traditionnelle et moderne, celle basée sur l'arithmétique modulaire et en particulier aux analogues des points précédents construits sur les courbes elliptiques définies sur un corps fini. Un troisième chapitre consacré aux différentes attaques possibles des cryptosystèmes basés sur les courbes elliptiques : les méthodes génériques et l'attaque MOV. Et en fin les performances des ECC : comparaison de ECC avec les autres systèmes à clés publiques existants. Dans le dernier chapitre nous présentons une application ; une implémentation informatique d'un ECC en langage C++.

Chapitre 1

1.1Arithmétique sur les courbes elliptiques

1.1.1 Définitions ([1], [2])

Définition 1.1. (Espace projectif). On appelle espace projectif de dimension 2 associé à un corps K et on note $P^2(K)$, l'ensemble des classes $(x:y:z)$ de la relation d'équivalence

$$\forall((x,y,z),(x',y',z')) \in (K^3\backslash\{(0,0,0)\})^2,$$

$$(x,y,z)\Re(x',y',z') \Leftrightarrow [\exists t \in K\backslash\{0\}\ (x,y,z)=(tx',ty',tz')]$$

Définition 1.2. (Polynôme homogène). Un polynôme non nul $F \in K[x,y,z]$ est homogène de degré d. S'il satisfait

$$F(\lambda x,\lambda y,\lambda z)=\lambda^d F(x,y,z), \text{ pour tout } x,y,z,\lambda \in K$$

L'ensemble des polynômes homogènes de degré d est noté par $K_d[x,y,z]$.

Définition 1.3. Une courbe algébrique plane C est une courbe de l'espace projectif $P^2(K)$ d'équation $F(x,y,z)=0$ où F est un polynôme homogène de degré d >0. Si d=1, alors C est appelée une droite ; si d =2, une conique ; si d =3, une cubique etc…, le nombre d est appelé le degré de la courbe.

Remarques.

- On peut injecter K^2 dans $P^2(K)$ de la manière suivante :

$$K^2 \rightarrow P^2(K)$$
$$(x,y) \rightarrow (x:y:1)$$

- Si $(x:y:z) \in P^2(K)$ avec $z \neq 0$, alors $(x:y:z)=(\frac{x}{z}:\frac{y}{z}:1)$ .C'est un point fini de $P^2(K)$. Par contre si $z=0$, alors diviser par z nous donne ∞ dans au moins une des coordonnées x,y. C'est pourquoi on appelle les points ayant la forme $(x:y:0)$ les points à l'infini dans $P^2(K)$.

Définition 1.4. (Courbe non singulière). La courbe C sur K est dite non singulière, si tout point de la courbe E est non singulier i.e. :

$$\forall P \in C(K),\left(\frac{\partial F}{\partial x}(p),\frac{\partial F}{\partial y}(p),\frac{\partial F}{\partial z}(p)\right) \neq (0,0,0)$$

Définition 1.5. (Courbe elliptique). Une courbe elliptique définie sur un corps K est une courbe algébrique plane, irréductible, non singulière et d'équation de Weierstrass homogène

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \ ; \ a_1, a_2, a_3, a_4, a_6 \in \mathrm{K} \qquad (1)$$

Pour alléger les notations, on peut écrire l'équation de Weierstrass (1) en coordonnées non homogènes ($x = \frac{X}{Z}$ et $y = \frac{Y}{Z}$) :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad a_1, a_2, a_3, a_4, a_6 \in \mathrm{K} \qquad (2)$$

Plus le point $(0,1,0)$ qui est le seul point à l'infini $(Z = 0)$ de la courbe E et que l'on choisit comme point distingué O.

On définit alors les quantités suivantes :

$$b_2 = a_1^2 + 4a_2,$$

$$b_4 = 2a_4 + a_1a_3,$$

$$b_6 = a_3^2 + 4a_6,$$

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$$

$$c_4 = b_2^2 - 24b_4$$

$$c_6 = -b_2^3 + 36b_2b_4 - 216b_6$$

Définition 1.6. On appelle discriminant Δ de l'équation de Weierstrass la quantité

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

Définition 1.7.(j-invariant). On appelle j-invariant de la courbe elliptique E la quantité

$$j(E) = \frac{c_4^3}{\Delta} \qquad \textbf{(4)}$$

Théorème 1.1. Si K est de caractéristique autre que 2 et 3, on peut toujours trouver une forme courte de Weierstrass, i.e. mettre E sous la forme :

$$y^2 = x^3 + ax + b \qquad (5)$$

dans ce cas on a :

$$\Delta = -16(4a^3 + 27b^2) \qquad (8)$$

$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2} \qquad (7)$$

Démonstration. Si la caractéristique de K $\neq$ 2, alors $2 \neq 0_K$. On peut donc faire le changement de variable $y \to (y - \frac{1}{2}(a_1 x + a_3))$ et on obtient :

$$y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}.$$

Si de plus la caractéristique de K $\neq$ 3, on peut faire le changement de variable $x \to (x - \frac{b_2}{12})$ pour obtenir : $y^2 = x^3 - \frac{c_4}{48}x - \frac{c_6}{864}$. D'où le résultat cherché en posant $a = -\frac{c_4}{48}$ et $b = -\frac{c_6}{864}$. □

Remarque. Dans le cas où la caractéristique de K est égale à 2 ou 3 on a, suivant j(E).

$chr(K)$	$j(E)$	E	Δ	$j(E)$
2	0	$y^2 + cy = x^3 + ax + b$	c^4	0
2	$\neq 0$	$y^2 + xy = x^3 - ax^2 + b$	a	$1/a$
3	0	$y^2 = x^3 + ax + b$	$-a^3$	0
3	$\neq 0$	$y^2 = x^3 + ax^2 + b$	$-a^3 b$	$-a^3/b$

Lemme 1.2. Soit E une courbe elliptique donnée par son équation de Weierstrass générale. E : $f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$ **(7)**

dont le discriminant est Δ et le j-invariant est $j(E)$. Le changement de variables $(x,y) \to (u^2x + r, u^3y + u^2sx + t)$ avec $u,r,s,t \in$K et $u \neq 0$ transforme l'équation précédente en : E$'$: $f'(x,y) = y^2 + a_1' xy + a_3'y - x^3 - a_2'x^2 - a_4'x - a_6' = 0$ (8)

où les coefficients sont données par

$$ua_1' = a_1 + 2s, \quad u^2a_2' = a_2 - sa_1 + 3r - s^2$$

$$u^3a_3' = a_3 + ra_1 + 2t$$

$$u^4a_4' = a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st$$

De plus $u^{12}\Delta' = \Delta$ et $j(E) = j(E')$.

Preuve. Il suffit de remplacer x *et* y par leurs nouvelles expressions pour obtenir les relations désirées. □

Proposition 1.3. Soit K un corps de caractéristique p. deux courbes elliptiques sont isomorphe sur K si et seulement si elles ont le même j-invariant.

Preuve. $(\Rightarrow)$ Par le lemme précédent.

$(\Leftarrow)$ Pour simplifier les calculs, nous allons proposer $p \neq 2,3$. Soient deux courbes $E \text{ et } E'$ ayant le même j-invariant dont les équation de Weierstrass sont données par

$$E : y^2 = x^3 + ax + b$$
$$E' : y^2 = x^3 + a'x + b'$$

Comme $j(E) = 1728\dfrac{4a^3}{4a^3 + 27b^2}$ et $j(E') = 1728\dfrac{4a'^3}{4a'^3 + 27b'^2}$ sont égaux, cela implique que $a^2a'^3 = a^3a'^2$. Cherchons des isomorphismes de la forme $(x, y) \leftarrow (u^2x, u^3y)$.

1° Si $a = 0$ *alors* $b \neq 0$ $(car\ \Delta \neq 0)$ et donc $a'' = 0$. Nous obtenons un isomorphisme en prenant $u = (\dfrac{b}{b'})^{\frac{1}{6}}$.

2° Si b = 0, alors $a \neq 0$ $(car\ \Delta \neq 0)$ et donc $b'' = 0$. Nous obtenons un isomorphisme en prenant $u = (\dfrac{a}{a'})^{\frac{1}{4}}$.

3° Si $ab \neq 0$, alors $a'b' \neq 0$. Nous obtenons un isomorphisme en prenant

$$u = (\frac{a}{a'})^{\frac{1}{4}} = (\frac{b}{b'})^{\frac{1}{6}}$$

Si $p = 2$ ou 3, la démonstration ce fait de la même façon en prenant les équations de Weierstrass correspondantes. □

Théorème 1.4. Soit E une courbe elliptique sur k, donnée par son équation de Weierstrass. Alors E est non singulière si et seulement si $\Delta \neq 0$.

Preuve.

$(\Leftarrow)$ Soit l'équation général de Weierstrass :

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

Montrons d'abord que le point à l'infini $O = (0,1,0)$ n'est jamais un point singulier.

Regardons E comme une courbe de IP^2 :

$$F(X, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 = 0.$$

Comme $\frac{\partial F}{\partial Z}(O) = 1 \neq 0, O$ n'est pas un point singulier de E.

Par l'absurde, supposons que E soit singulière en un point $P_0 = (x_0, y_0)$. Par le changement de variables $(x, y) \leftarrow (x - x_0, y - y_0)$, nous ramenons le point P_0 en (0, 0). Par le lemme 1, cette transformation ne modifie pas le discriminant (car u = 1). Nous avons alors $a_6 = f(0,0) = 0, a_4 = \frac{\partial f}{\partial x}(0,0) = 0 \; et \; a_3 = \frac{\partial f}{\partial y}(0,0) = 0$. La courbe E à pour équation : E : $f(x, y) = y^2 + a_1 xy - x^3 - a_2 x^2 = 0$

Le discriminant de cette équation est nul, ce qui contredit l'hypothèse.

$(\Rightarrow)$ Pour simplifier les calculs, nous allons supposer que $p \neq 2, 3$. Soit alors la courbe E donnée par l'équation de Weierstrass : E : $y^2 = x^3 + a_4 x + a_6$.

Si la courbe est singulière en un point $P_0 = (x_0, y_0)$, alors

$$2y_0 = 0 \Rightarrow y_0 = 0$$

$$3x_0^3 + a_4 = 0 \Rightarrow x_0^2 = -\frac{a_4}{3}.$$

Or, $P_0 = (x_0, y_0)$ est un point de la courbe, par conséquent,

$y_0^2 = 0 = x_0^3 + a_4 x_0 + a_6 = \frac{2}{3} a_4 x_0 + a_6$.

Il s'ensuit que $x_0^2 = \frac{9a_6^2}{4a_4^2} = -\frac{a_4}{3}$ et donc $\Delta = -16(4a_4^3 - 27a_6^2) = 0.$

Si $p = 2$ ou $p = 3$ la démonstration se fait de la même façon en prenant les équations de Weierstrass correspondantes. □

Exemple

K= IR, E : $y^2 = x^3 - x$ $a = -1, \; b = 0 \quad et \quad \Delta(E) = -4 \neq 0$

la courbe E n'est pas singulière.

1.1.2 Loi de groupe sur une courbe elliptique

Le plus important dans les courbes elliptiques est que les points de la courbe forment un groupe abélien [1].

Soit E/K une courbe elliptique donnée par l'équation de Weierstrass sur K. On note l'ensemble des points K-rationnels de la courbe E par E(K).

$$\text{E(K)} = \{(x, y) \in E : x, y \in K\} \cup \{O\},$$

Où O est le point à l'infini de la courbe E.

Exemple

K= $Z/5Z$, E : $y^2 = x^3 + x + 2$ $a = 1,\ b = 2$ *et* $\Delta(E) = 2 \neq 0$

Pour $E : y^2 = x^3 + x + 2$,

E(K) = $\{O,(4,0), (1,2), (1,3)\}$.

Les points K- rationnels de E sont en nombre de 4.

Proposition 1.5. Soient P et Q (non nécessairement distincts) deux points K-rationnels de la courbe elliptique E. La droite L reliant P à Q coupe la courbe E en un troisième point R.

Preuve. Comme E est irréductible, $E \cap L$ a un nombre fini de points. Soit la droite $L : aX + bY + cZ = 0$ où, par symétrie, nous supposons $c \neq 0$. Les points d'intersection de E et de L sont les racines du polynôme

$$p(X,Y) = F(X,Y,-\frac{aX + bY}{c}) \in K[X,Y]_3.$$

Notons $P_1 = (x_1, y_1, z_1)$ *et* $P_2(x_2, y_2, z_2)$ (avec éventuellement $(P_1 = P_2)$, deux points d'intersection de E avec L, alors, comme $p(x_1, y_1) = p(x_2, y_2) = 0$, il vient que

$$p(X,Y) = v(X,Y)\prod_{i=1}^{2}(b_i X - a_i Y) \quad où \quad v(X,Y) \in K[X,Y]_1.$$

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

$P_3 = (a_3, b_3, -\frac{aa_3 + bb_3}{c})$ où (a_3, b_3) est l'unique racine de $v(X,Y)$. □

Cette proposition permet de définir la loi de composition de la sécante tangente.

1.1.2.1 Approche géométrique de la loi de la sécante tangente

Soit E une courbe elliptique définie sur P^2(IR) par :

$$E : \quad Y^2Z = X^3 + aXZ^2 + bZ^3 \qquad (9)$$

Soit encore en coordonnées non homogènes (en posant $x = \frac{X}{Z}$ *et* $y = \frac{Y}{Z}$) :

$$E : \quad y^2 = x^3 + ax + b \qquad (10)$$

plus le point à l'infini $O = (0,1,0)$

On peut alors définir sur E une loi de composition $*$ dite loi de composition de la sécante tangente :

◦ Si $(P,Q) \in E^2$ *avec* $P \neq Q$, on définit $P * Q$ comme étant le troisième point d'intersection de la droite D passant par P *et* Q *avec* E

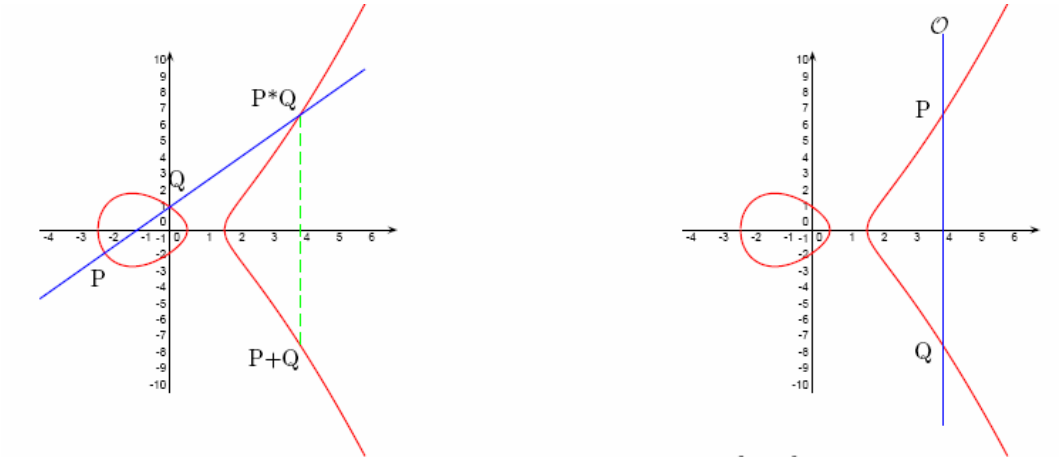


FIG. 1 Calcul de $P * Q$ dans la courbe elliptique E : $y^2 = x^3 - 4x + 2$

◦ Si $P \in E$, on définit $P * P$ comme étant le troisième point d'intersection de la droite D tangente à la courbe E en P avec E (P alors est considéré comme un point double de la courbe).

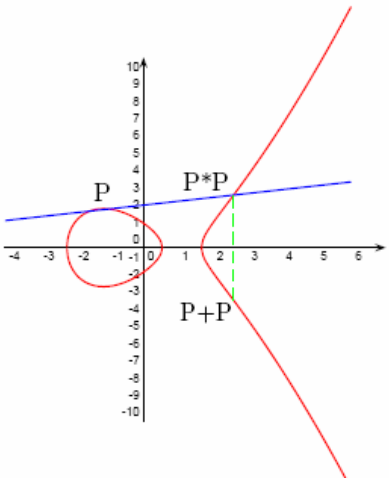


FIG. 2 Calcul de $P * P$ dans la courbe elliptique E : $y^2 = x^3 - 4x + 2$

Définition 1.8. Soit E une courbe elliptique définie sur un corps K, et soient deux points $P, Q \in E(K)$, L la droite reliant P à Q (la tangente à E si $P = Q$) et R le troisième point d'intersection de L avec E. Soit L' la parallèle à l'axe oy passant par R. On définit l'addition de deux points $P + Q \in E(K)$ comme étant le deuxième point d'intersection de L' avec E.

.**Théorème 1.6.** Soit E/K une courbe elliptique. L'ensemble $E(K)$ des points rationnels sur la courbe E, est un groupe abélien additif pour l'opération d'addition définie précédemment, avec le point à l'infini O comme élément neutre du groupe.

Preuve. Vu la définition de la loi de composition de la sécante tangente :

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

La commutativité est évidente : $P + Q = O * (P * Q) = O * (Q * P) = Q + P$.

1. O est un élément neutre, car $P + O = O * (P * O) = O * (O * p) = O + P = P$.
2. L'élément symétrique d'un élément Q est défini par : $-Q = (O * O) * Q.$

   Ce qui est bien le symétrique, car

   $Q + (-Q) = O * (Q * ((O * O) * Q)) = O * (O * O) = O + O = O$

   et

   $-Q + Q = O * (((O * O) * Q) * Q) = O * (O * O) = O + O = O$
3. Il reste à montrer l'associativité, elle est trop technique. Voir [1], Chapitre III, proposition 2.2. □

Remarque. Pour $m \in Z \; et \; P \in E(K)$, il est d'usage de noté mP la quantité égale à $\overbrace{P + P + ... + P}^{mfois}$ pour $m > 0$, à O pour $m = 0$ et à $(-m)(-p)$ pour $m < 0$. Nous définissons alors l'endomorphisme ''multiplication par un entier m'' comme étant égale

$$[m]_E : E(K) \to E(K)$$
$$P \quad \mapsto mP$$

Dans la suite nous notons $E[m]$ le noyau de $[m]_E$ défini sur $\overline{K}$, la clôture algébrique de K, c'est-à-dire

$$E[m] = \left\{(x,y) \in E(\overline{K}), [m]_E(x,y) = O\right\}.$$

1.1.2.2 Expression analytique Soit E une courbe elliptique définie par :

E : $f(x,y) = y^2 - x^3 - ax - b = 0, avec \quad 4a^3 + 27^2 \neq 0$ (11)

Proposition 1.7 Soit $P_1(x_1,y_1), P_2(x_2,y_2)$ *et* $P_3(x_3,y_3)$ trois points de E/$\{O\}$ tels que $P_1 \neq P_2$. Si $x_1 \neq x_2$ et si $P_3 = P_1 * P_2$, alors

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 \\ y_3 = \lambda(x_3 - x) + y_1 \end{cases}, \quad \text{avec } \lambda = \frac{y_1 - y_2}{x_1 - x_2}$$

Preuve. Si $x_1 \neq x_2$ alors la sécante D passant par P_1 *et* P_2 a pour pente $\lambda = \frac{y_1 - y_2}{x_1 - x_2}$.

Soit $\gamma = y_1 - \lambda x_1$. L'équation de D est alors : $y = \lambda x + \gamma$. On a alors :

$$f(x, \lambda x + \gamma) = (\lambda x + \gamma)^2 - x^3 - ax - b = -x^3 + \lambda^2 x^2 + (2\lambda\gamma - a)x + (\gamma^2 - b)$$

Or les points P_1, P_2 *et* P_3 sont racines de f car ils appartiennent à la courbe E. De plus ils appartiennent à la droite D. On doit donc avoir :

$f(x_1, \lambda x_1 + \gamma) = f(x_2, \lambda x_2 + \gamma) = f(x_3, \lambda x_3 + \gamma) = 0$.

x_1, x_2 *et* x_3 étant distincts, ce sont donc les trois racines de polynôme de degré 3 :

$$\begin{aligned} -x^3 + \lambda^2 x^2 + (2\lambda\gamma - a)x + (\gamma^2 - b) &= -(x - x_1)(x - x_2)(x - x_3) \\ &= -x^3 + (x_1 + x_2 + x_3)x^2 - (x_1x_2 + x_1x_3 + x_2x_3)x + x_1x_2x_3 \end{aligned}$$

par identification du coefficient de x^2, on obtient :

$x_3 = \lambda^2 - x_1 - x_2$ *et* $y_3 = \lambda(x_3 - x) + y_1$. □

Proposition 1.8. Soit $P_1(x_1,y_1)$ *et* $P_2(x_2,y_2)$ deux points de $E/\{O\}$. Si $x_1 = x_2$ et si $P_3 = P_1 * P_2$, alors :

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 \\ y_3 = \lambda(x_3 - x) + y_1 \end{cases} \qquad \text{Avec } \lambda = \frac{3x_1^2 + a}{2y_1}$$

Preuve. La tangente D à E en P_1 à pour pente : $\lambda = \frac{\frac{\partial f}{\partial x}(P_1)}{\frac{\partial f}{\partial y}(P_1)} = \frac{3x_1^2 + a}{2y_1}$.

Soit $\gamma = y_1 - \lambda x_1$. L'équation de D est alors : $y = \lambda x + \gamma$. Et la démonstration est identique à celle de la proposition 1.7. □

Remarque. Cette définition est encore vraie dans le cas où :

$$x_1 = x_2 \text{ et } y_1 = -y_2 \text{ avec } P_1 * P_2 = O .$$

1.2 Fonctions polynomiales et rationnelles

1.2.1 Définitions ([1], [2], [4]).

Dans la suite on considérera uniquement des courbes non singulières.

Les symboles $x \text{ et } y$ seront réservés pour les fonctions coordonnées sur la courbe elliptique E définies par $x(a,b) = a \quad et \quad y(a,b) = b.$

Si on considère des polynômes en les fonctions $x \text{ et } y$ la relation $y^2 = x^3 + Ax + B$ est automatiquement vérifiée car

$\forall\ (a,b) \in E\ y^2(a,b) = (y(a,b))^2 = b^2$ et $(x^3 + Ax + B)(a,b) = (x(a,b))^3 + Ax(a,b) + B =$

$a^3 + Aa + B \text{ cela implique } b^2 = a^3 + Aa + B \text{ d'où } y^2 = x^3 + Ax + B$.

Définition 1.9. On appelle polynôme sur E tout polynôme de $K[x, y]$. On note aussi $K[E]$ l'ensemble des polynômes sur E.

Proposition 1.9. Tout polynôme de $K[E]$ se met de la forme

$P(x, y) = u(x) + y\ v(x)$. $u, v \in K[x]$

Preuve : Soit $P = \sum_{finie} a_{ij} x^i y^j \in K[E]$

$= a_0(x) + a_1(x)y + a_2(x)y^2 + .. + a_n(x)y^n,\ a_i(x) \in K[x]$. Or $y^2 = x^3 + Ax + B$ d'où le résultat. □

Définition 1.10. Si $f(x, y) = u(x) + v(x)\ y \in K[E]$, on appelle polynôme conjugué de f le polynôme $\overline{f}\ (x, y) = u(x) - v(x)y$ et sa norme :

$\lambda(f) = f.\ \overline{f} = u^2(x) - s(x)\ v^2(x) \in K[x], \text{ ou } s(x) = x^3 + Ax + B$.

Proposition 1.10.

1. $\lambda(f.g) = \lambda(f)..\lambda(g)$

2. l'écriture $f(x, y) = u(x) + y\ v(x) \in K[E]$ est unique

3. $K[E]$ est un anneau intègre ($f, g \in K[E] \text{ avec } f.g = 0 \Rightarrow f = 0 \text{ ou } g = 0$)

Preuve.

1. $f = u + y\ v \in K[E] \text{ et } g = u_1 + y\ v_1 \in K[E]$

On a : $\overline{f.g} = \overline{f}\ .\ \overline{g}$ car $\overline{f.g} = \overline{uu_1 + (x^3 + Ax + B)vv_1 + y(uv_1 + u_1v)}$

Cela implique $\overline{f.g} = uu_1 + (x^3 + Ax + B)vv_1 - y(uv_1 + u_1v)$ (*)

D'autre part $\overline{f}.\overline{g} = (u - yv).(u_1 - yv_1) = uu_1 + (x^3 + Ax + B)vv_1 - y(uv_1 + u_1v)$ (**)

(*) et (**) impliquent $\overline{f.g} = \overline{f}.\overline{g}$. On aura donc $\lambda(f.g) = f.g\ \overline{f.g} = f.g.\overline{f}.\overline{g}$

$= f.\overline{f}\ \ g\overline{g} = \lambda(f)..\lambda(g)$

2. Supposons que $f = u + y\,v = u_1 + y\,v_1$ on va montrer que $u = u_1\ et\ v = v_1$

On a $u - u_1 + y(v - v_1) = 0$ il faut montrer que: $u - u_1 = 0\ et\ v - v_1 = 0$ et donc on se ramène au problème suivant : $u_2 + yv_2 = 0 \Rightarrow u_2 = 0\ et\ v_2 = 0$.

Soit $f = u_2 + y\,v_2\ donc\ f = 0 \Rightarrow \lambda(f) = f.\overline{f} = 0.$

Or $\lambda(f) = u^2(x) - s(x)\,v^2(x),$ avec $s(x) = x^3 + Ax + B$ d'où $u^2(x) - s(x)\,v^2(x) = 0$

Si $u_2 = 0\ alors\ v_2 = 0\quad et\ si\ \ v_2 = 0\ alors\ u_2 = 0$.

Si $u_2 \neq 0\ et\ v_2 \neq 0$ comme $d^o(u_2(x)^2)$ est pair et $d^o(s(x)\,v(x)^2)$ est impair. Alors on aura

$u^2(x) - s(x)\,v^2(x) \neq 0$ (Contradiction)

3. la preuve est facile ; il faut utilisé seulement les définitions. □

Définition 1.11. Une fonction rationnelle sur E est une classe d'équivalence de quotients $\frac{f}{g}\ \ avec\ g \neq 0$, ou $f\ et\ g$ sont des polynômes sur E, avec l'identification $\frac{f}{g} = \frac{h}{k} \Leftrightarrow f.k = g.h$. Comme polynômes sur E .i.e. $f.k - g.h \in I(P)$, ou $I(P)$ est l'idéal engendré par le polynôme irréductible $P(x, y) = y^2 - x^3 - Ax - B$.

Remarques.

1. Comme $K[E]$ est intègre, il est facile de voir que les fonctions rationnelles sur E forment un corps qu'on notera K(E), appelé corps des fonctions rationnelles sur E.

2. Puisque les polynômes sur E ont des valeurs en chaque point fini de E, les fonctions rationnelles peuvent ne pas avoir de valeur en tout point fini et peuvent avoir une valeur à l'infini en O.

3. Si r $= \frac{f}{g}$ est une fonction rationnelle sur E, avec $f = u(x) + v(x)\ et\ g = u_1(x) + v_1(x)$,

alors $r = \frac{f}{g} = \frac{f.\overline{g}}{g.\overline{g}} = \alpha(x) + y\beta(x)\ avec\ \ \alpha, \beta \in K(x)$.

Définition 1.12. Si r est une fonction rationnelle sur E et P est un point fini de E, on dit que *r* est finie en P s'il existe une représentation $r = \frac{f}{g} \in K(E)$ *avec* $g(P) \neq 0$ et on pose $r(P) = \frac{f(P)}{g(P)}$

Définition 1.13. Soit $f = u(x) + y\,v(x) \in K[E] - \{0\}$. On définit le degré de f *par* : $\deg(f) = \max(2\deg_x(u), 3 + 2\deg_x(v))$. Et si f ne dépend que de *x* on pose : $\deg(f) = \deg_x(u)$.

Lemme 1.11. Si $f \in K[E]$ *alors* $\deg(f) = \deg_x(\lambda(f))$.

Preuve. Si $f(x,y) = u(x) + y\,v(x)$, *avec* $u, v \in K[x]$

$\lambda(f) = u^2(x) - s(x)\,v^2(x) \in K[x]$ et $\deg(\lambda(f)) = \max(\deg_x(u^2(x)), \deg_x(s(x)\,v^2(x)))$

Car $\deg_x(u^2(x))$ *est pair et* $\deg_x(s(x)\,v^2(x))$ est impair $(= 3 + \deg_x(v^2))$ cela implique $\deg_x(\lambda(f)) = \max(2\deg_x(u), 3 + 2\deg_x(v))$ □

Proposition 1.12. Si $f, g \in K[E]$ *alors* $\deg(f.g) = \deg(f) + \deg(g)$

Preuve. On a $\deg(f.g) = \deg_x(\lambda(f.g)) = \deg_x(\lambda(f)\lambda(g)) = \deg_x(\lambda(f)) + \deg_x(\lambda(g)) =$ (car $\lambda(f)$ *et* $\lambda(g) \in K[x]) = \deg(f) + \deg(g)$. Cela d'après le lemme précédent. □

Définition 1.14. Supposons que $r = \frac{f}{g} \in K(E)$, une fonction rationnelle sur E

1. *Si* $\deg(f) < \deg(g)$, *On pose* $r(O) = 0$
2. Si $\deg(f) > \deg(g)$, *On pose* $r(O) = \infty$ et on dit que *r* n'est pas finie en *O*
3. Si $\deg(f) = \deg(g)$, alors :
   - $\deg(f)$ est pair, en prenant la forme canonique de f et de g, ils ont comme termes de plus haut degré $a\,x^d$ *et* $b\,x^d$ *et on pose* $r(O) = \frac{a}{b}$
   - $\deg(f)$ est impair, les termes de plus haut degré sont de la forme $a\,yx^d$ *et* byx^d et on pose $r(O) = \frac{a}{b}$.

Remarques.

1. Si $r, s \in K[E]$ sont finies en O : $r \cdot s(O) = r(O).s(O) et (r+s)(O) = r(O) + s(O$
2. Si $r \in K[E]$ *et* r n'est pas finie en P, on écrit $r(P) = \infty$

1.2.2 Zéros et pôles d'une fonction rationnelle

Définition 1.15. Soit $r \in K(E)$, on dit que r à un zéro en $P \in E$ si $r(P) = 0$ et que r à un pole en P si $r(P) = \infty$.

Théorème 1.13. Pour tout point $P \in E$, il existe $u \in K(E)$, telle que

1. $u(P) = 0$

2. $\forall r \in K(E) - \{0\}$ *on a* $r = u^d.s$ *où* $d \in Z, s \in K(E)$ finie en P *et* $s(P) \neq 0$, de plus d ne dépend pas de choix de la fonction u.

Preuve. 1. On a : $x^3 + Ax + B = (x - \omega_1)(x - \omega_2)(x - \omega_3)$

1er cas. $P = O$, si $r = \frac{f}{g} \in K(E)$ avec $r(P) = 0$, cela implique $\deg(f) < \deg(g)$, on pose

$\deg(f) - \deg(g) = d > 0$, $\deg(x) - \deg(y) = -1$

On a $\deg(y^d . f) = \deg(x^d . g)$. Car $\deg(y^d . f) = \deg(y^d) + \deg(f) = 3d + \deg(f)$

Et $\deg(x^d . g) = \deg(x^d) + \deg(g) = 2d + \deg(g)$

D'où $\deg(y^d . f) - \deg(x^d . g) = d + (\deg(f) - \deg(g)) = d - d = 0.$ Cela implique

$\frac{x^d}{y^d}(\frac{y^d}{x^d}\frac{f}{g}) = \frac{f}{g} = r$ *et si on pose* $s = \frac{y^d}{x^d}\frac{f}{g}$, *donc* $s(O) = \frac{a}{b}$ est finie et $s(O) \neq 0$

On pose $u = \frac{x}{y}$, on a donc $u(O) = 0$

Par contre si $r(O) \neq 0$, *on pose* $r = (u)^0 . r$ avec $u = \frac{x}{y}$.

2e cas. $P = (\omega_i, 0)$

ω_i est une racine de $x^3 + Ax + B$. On peut poser $P = (\omega_1, 0)$

soit $r = \frac{f}{g} \in K[E]$ et on suppose que $f(P) = 0$.

$f = u_1 + yv_1$ *et* $g = u_2 + yv_2$

$f(P) = 0 = u_1(P) + (yv_1)(p) = u_1(\omega_1, 0) + y(\omega_1, 0).v_1(\omega_1, 0) = u_1(\omega_1, 0)$

$$r = \frac{u_1 + yv_1}{u_2 + yv_2} = \frac{(x - \omega_1)u_1' + yv_1}{u_2 + yv_2} = \frac{(x - \omega_1)(x - \omega_2)(x - \omega_3)u_1' + yv_1(x - \omega_2)(x - \omega_3)}{(x - \omega_2)(x - \omega_3)u_2 + yv_2(x - \omega_2)(x - \omega_3)}$$

$$= \frac{y^2u_1' + yv_1'}{u_2' + yv_2'} = y.s_1 \quad avec \quad s_1 \in K(E).$$

Si $s_1(P)=0$, on continue : $r=y^2 s_2$ et ainsi de suite jusqu'à obtenir $r=y^d s_d$ *avec* $s_d \neq 0$

et $s_d(p)$ fini et $s_d \in K(E)$. Comme $y(\omega,0)=0$, on peut prendre $u=y$.

Si $r(P)\neq 0$ et $r(P)$ fini on peut écrire $r=y^0 r$.

Par contre si $g(P)=0$, d'après le résultat précédent on peut écrire $r=y^{-m}s_m$ avec $m>0$ *et* $s_m(P)\neq 0$

3^e cas. $P=(a,b)$ *avec* $P\neq O$ *et* $P\neq(\omega_i,0)$ *donc* $b\neq 0$

$r=\dfrac{f}{g}\in K(E)$ *et* $f(P)=0$

I) Si $\overline{f}(P)=0$ (avec $f=u_1+yv_1$ *et* $\overline{f}=u_1-yv_1$), donc $u_1(a)=v_1(a)=0$ *car* $b\neq 0$

Cela implique $f=(x-a)(u'+yv')=(x-a)f'$ et $r=(x-a)\dfrac{f'}{g}=(x-a)r_1$

Si $r_1(P)=0$, on continue jusqu'à $r=(x-a)^d r_d$, *avec* $r_d(P)\neq 0$ *et finie* $(r_d\in K(E))$,

on prend $u=x-a$ $(on\ a\ u(P)=(x-a)(a,b)=a-a=0$

II) Si $\overline{f}(P)\neq 0$, alors on a $r=\dfrac{f}{g}=\dfrac{f.\overline{f}}{g.\overline{f}}=\dfrac{u_1^2-(x^3+Ax+B)v_1^2}{(u_2+y_2)(u_{\&}-yv_1)}$

$r(P)=0\Rightarrow[u_1^2(x)-(x^3+Ax+B)v_1^2(x)](a,b)=0$

d'où $[u_1^2(x)-(x^3+Ax+B)v_1^2(x)]=(x-a)f_1(x)$, donc $r=(x-a)\dfrac{f_1(x)}{g.\overline{f}}=(x-a)s_1$

Si $s_1(P)=0, on\ continue\ jusqu'à\ r=(x-a)^d.s_d$, *avec* $s_d(P)\neq 0$ *finie* et on prend $u=x-a$

Par contre si $g(P)=0$, d'après le résultat précédent on peut écrire $r=(x-a)^{-m}s_m$ *avec* $m>0$

et $s_m(P)\neq 0$.

Il reste à montrer maintenant la dernière partie de théorème

Soit $u'\in K(E)$ *t.q.* $u'(p)=0$ *et* $\forall r\in K(E)-\{0\}, on\ a\ r=(u')^{d'}s'$, *où* $d'\in Z$ *et* $s'\in K(E)$ finie en P *et* $s'(P)\neq 0$

On a $u=(u')^{d'}s'$ car $u\in K(E)$

Soit $r\in K(E)$, alors $u^d s=((u'')^{d'})^d s=[(u')^{d'}]^d(s')^d s=(u')^{d'd}(s')^d s$

Si $d \neq d^{'}$ on a $d^{'}d - d \neq 0$ ou $d^{'}d - d = 0$

$r = (u^{'})^{d^{'}d}(s^{'})^{d}s = (u^{'})^{d^{'}}s^{'} \Rightarrow (u^{'})^{d^{'}d-d^{'}}(s^{'})^{d-1}s = 1$ (Contradiction)

$u = (u^{'})^{d_1^{'}}s^{'}$ et $u^{'} = u^{d_1}s \Rightarrow (u^{d_1}s)^{d_1^{'}}s^{'} = (u^{d_1})^{d_1^{'}}s^{d_1^{'}}s^{'} = u^{d_1d_1^{'}}s^{d_1^{'}}s^{'}$

Si $d_1d_1^{'} \neq 1$ alors $1 = u^{d_1d_1^{'}-1}s^{d_1^{'}}s^{'}$

On peut supposer que $d_1d_1^{'} - 1 > 0$ (si non prendre les inverses)

D'où 1 = 0 (contradiction)

donc $d_1d_1^{'} = 1 \Rightarrow d_1 = d_{1'}^{'} = \pm 1 \quad (car\ d_1, d_1^{'} \in Z)$

$u = u^{'}s_1^{'}, u^{'} = us_1 \Rightarrow r = u^{d}s = (u^{'}s_1^{'})^{d}s = (u^{'})^{d}(s_1^{'})^{d}s$. □

Définition 1.16. [1] Une fonction rationnelle u vérifiant le théorème précédent est appelée variable uniformisante ou uniformisante en P.

Si $r \in K(E) - \{0\}$ et $r = u^{d}s$ où u est une uniformisante en P alors l'ordre de r en P est l'entier $d \in Z$ et on écrit $ord_P r = d$

On définit la multiplicité d'un zéro comme étant l'ordre de la fonction et la multiplicité d'un pôle comme étant $-$ l'ordre.

Remarque Soit $r = a_0 + a_1x + a_2x^2 + ... + a_nx^n \in K[E], \quad alors\ ord_O r = -\deg(r) = -2n$

Car si on prend $P = O$, alors $u = \frac{x}{y}$

$r = (\frac{x}{y})^{-2n}.(\frac{x}{y})^{2n}r$ donc $ord_O r = -2n = -\deg(r)$

Théorème 1.14. Soit $r \in K(E)$ *alors* $\sum_{P \in E} ord_P r = 0$

Preuve. Il suffit de montrer le théorème pour *r* polynôme

$r = (x - a_1)(x - a_2)...(x - a_n)$, si $P \neq (a_i, b_i)$ on a $ord_P r = 0$

Si $P = (a_i, b_i)$ on a $ord_P r = l_i \geq 0$, on a $\sum_i l_i = 2n$, d'après la remarque précédente

$ord_O r = -\deg r = -2n$, d'où $\sum_{P \in E} ord_P r = 0$. □

Lemme 1.15. Une fonction rationnelle sur E et ne possédant pas de pôles fini est un polynôme

Preuve. $r = \frac{f}{g} = \frac{u + yv}{u_1 + yv_1} = a + yb, \quad a, b \in K(x)$

Il suffit de montrer que a *et* b ne possèdent pas de pôles fini (a *et* $b \in K[x]$)

$r = a + yb, \bar{r} = a - yb \Rightarrow a = \frac{1}{2}(r + \bar{r})$, r sans pole fini implique $\bar{r}$ sans pole fini donc $r + \bar{r} = 2a$ est sans pole fini d'où $2a \in K[x]$ d'où $a \in K[x]$

On a $r - a = yb$ *avec* $r - a$ sans pôle fini, donc yb est sans pôle fini donc $(yb)^2$ est sans pôle fini, or $(yb)^2 = y^2b^2 = (x^3 + Ax + B)b^2, b^2 \in K(x)$

Si b possède un pole fini en P, alors b^2 possède un pôle d'ordre 2 en P, or $(x^3 + Ax + B)b^2$ ne possède pas de pole en P donc $(x^3 + Ax + B)$ possède un zéro d'ordre 2 en P ce qui contredit l'hypothèse que $x^3 + Ax + B$ possède 3 racines distinctes. Conclusion b ne possède pas de pole fini. □

Lemme 1.16. Soit $f \in K[x]$, alors la somme des multiplicités des zéros de f est égale au degré de f.

Preuve. Soit $f \in K[E]$ de degré n, on a vu que

$\deg(f) = \deg_x \lambda(f) = \deg(f\bar{f})$. Or $\lambda(f) = (x - a_1)(x - a_2)...(x - a_n)$

Les zéros de $x - a_i$ sont les points $P_i(a_i, b_i)$ et $P_i' = (a_i, -b_i)$, donc le nombre de zéros de $\lambda(f)$ est $2n$. Puisque f *et* $\bar{f}$ ont le même nombre de zéros, on conclut que le nombre de zéros de f *est* $n = \deg(f)$. □

Lemme 1.17. Soit $f \in K[x]$, non constant. Alors f possède au moins 2zéros simples ou un zéro d'ordre 2 en des points finis de E.

Preuve. f est non constant, donc f contient la variable x, ou la variable y, donc $\deg(f) \geq 2$ et d'après le lemme précédent f possède une racine double ou 2 racines distinctes (au moins). □

Définition 1.17. Une application rationnelle F sur E est une paire (r, s), ou r *et* s sont des fonctions rationnelles sur E vérifiant la relation $s^2 = r^3 + Ar + B$.

Par convention on pose : $F(P) = O$ si r *et* s ne sont pas finis en P

Remarques.

1. Une application rationnelle $F = (r, s)$ est un point de la courbe elliptique $E : y^2 = x^3 + Ax + B$, défini sur le corps $K(E)$.

2. l'application rationnelle $F=(r,s)$ définit une fonction de E dans E en posant $F(P)=(r(P),s(P))$

On a P pôle de $r \Leftrightarrow P$ pôle de s, et on pose $F(P)=O$ si P est un pole de r.

1.2.3 Diviseurs

Définition 1.18. Soit S un ensemble, le groupe abélien libre engendré par S est l'ensemble des sommes formelles finies $G(S)=\left\{\sum_{s\in S} m(s)\ s\right\}$, où $m(s)\in Z\ et\ m(s)=0$

pour presque tous les s (*ie* $m(s)=0$ sauf pour un nombre fini de *s*)

Définition 1.19. Soit E une courbe elliptique sur un corps K, le groupe abélien libre engendré par les points de E, est appelé le groupe de diviseurs de E, on le note $Div(E)$.

Notation : on note $\langle P\rangle$ le diviseur particulier $\sum_{s\in E} m(s).s,\ avec\ m(s)=0,$ si $s\neq P$ et $m(P)=1.$

Définition 1.20. Si $\Delta=\sum_{P\in E} m(P)\langle P\rangle \in Div(E)$. On définit le degré de Δ par

$\deg\Delta=\sum_{P\in E} m(p)$ et on appelle norme de Δ le nombre $|\Delta|=\sum_{P\in E-\{O\}}|m(P)|$.

Définition 1.21. Soit r une fonction rationnelle non nulle sur E. On appelle diviseur de r le diviseur $div(r)=\sum_{P\in E} ord_P r.\langle P\rangle$

Exemple : Soit $r=x-a\ et\ P=(a,b)\in E\ avec\ b\neq 0$

On a $r(P)=x(p)-a=a-a=0\ et\ \ r(-P)=x(a,-b)-a=a-a=0\ \ (-P=(a,-b)\in E$

Si $Q\in E-\{O,P,-P\}, ord_Q r=0$. Par contre $ord_O r=-2\ et\ ord_P r=ord_{-P} r=1$

Donc $div(r)=div(x-a)=\langle P\rangle+\langle P'\rangle-2\langle O\rangle$, avec ($P'=-P$).

Définition 1.22. Un diviseur Δ est principal s'il existe une fonction rationnelle $r\in K(E)$ telle que $\Delta=div(r)$

Proposition 1.18. Si $r_1 et\ r_2$ deux fonctions rationnelles sur E, alors

$div(r_1 r_2)=div(r_1)+div(r_2)$

Preuve. $ord_P(r_1 r_2)=ord_P r_1+ord_P r_2, car\ si\ on\ a\ ord_P r_1=d\ \ \ et\ ord_P r_2=d'$.

Donc $r_1=u^d s_1\ et\ r_2=u^{d'} s_2\ avec\ s_i(p)\neq 0$ cela implique $ord_P(r_1 r_2)=u^{d+d'} s_1 s_2$

D'où $ord_P(r_1 r_2) = d + d' = ord_P r_1 + ord_P r_2$ et

$$div(r_1 r_2) = \sum_{P \in E} ord_P(r_1 r_2) = \sum_{P \in E} ord_P r_1 + ord_P r_2 = \sum_{P \in E} ord_P r_1 + \sum_{P \in E} ord_P r_2$$

$$= div(r_1) + div(r_2).$$ □

Remarque. D'après la proposition précédente, l'ensemble des diviseurs principaux est un sous groupe du groupe $Div(E)$ qu'on notera $\Pr in(E)$. On notera aussi, $Div^o(E)$, le sous groupe des diviseurs de E de degré 0 $(\forall r \in K(E), \sum_{P \in E} ord_P(r) = 0$

$donc \sum_{P \in E} ord_P r\langle P \rangle \in Div^o(E))$.

On va maintenant étudier l'ensemble des diviseurs qui sont principaux,i.e quels zéros et quels pôles peut avoir une fonction rationnelle ? cela équivaux à étudier les diviseurs qui ne sont pas principaux. Ces derniers sont représentés par les éléments du groupe $Pic(E) = Div(E) \big/ \Pr in(E)$, qu'on appelle groupe de Picard de E.

($\Delta, \Delta_1 \in Div(E), \overline{\Delta}, \overline{\Delta_1}$, leurs images dans $Pic(E)$. $\overline{\Delta} = \overline{\Delta_1} \Leftrightarrow \overline{\Delta} - \overline{\Delta_1} = \overline{\Delta - \Delta_1} = 0 \Leftrightarrow$

$\Delta - \Delta_1 \in \Pr in(E) \Leftrightarrow \Delta_1 = \Delta + l, où\ l \in \Pr in(E))$

Définition 1.23. Le groupe $Pic^o(E) = Div^o(E) \big/ \Pr in(E)$ est appelé le groupe de Picard de degré 0

Théorème 1.19. Soit $\Delta \in Div(E)$, alors il existe un diviseur $\Delta_1 \in Div(E)$ vérifiant

1^o Δ *et* Δ_1 ont la même image dans $Pic(E)$ *.i.e.* $\Delta - \Delta_1 \in \Pr in(E)$

2^o $\deg(\Delta) = \deg(\Delta_1)$

3^o $|\Delta_1| \le 1$ $(|\Delta_1| = 1 \Rightarrow \Delta_1 = \pm\langle P \rangle \pm n\langle O \rangle)$

□

Corollaire 1.20. Pour tout $\Delta \in Div(E)$, il existe un unique point $P \in E$ tel que $\Delta \sim \langle P \rangle - \langle O \rangle$

Preuve. D'après le théorème précédent, $\exists \Delta_1 \in Div^o(E)$ tel que :

$\Delta \sim \Delta_1$ et $|\Delta_1| = 1$ (on suppose que $\Delta \neq 0$) donc $\Delta_1 = \langle P \rangle - \langle O \rangle$, d'où $\Delta \sim \langle P \rangle - \langle O \rangle$.

On montre maintenant l'unicité de P : supposons que $\Delta \sim \langle Q \rangle - \langle O \rangle$ avec $Q \neq P$

$\Delta \sim \langle P \rangle - \langle O \rangle \sim \langle Q \rangle - \langle O \rangle$, donc $\langle P \rangle - \langle O \rangle - \langle Q \rangle - \langle O \rangle = div(r), r \in K(E)$

D'où $\langle P\rangle - \langle Q\rangle \sim \langle S\rangle - \langle O\rangle$ (d'après le théorème précédent), donc $\langle S\rangle - \langle O\rangle \sim div(r)$

Cela implique $\langle S\rangle - \langle O\rangle - div(r) = div(r_1)$, d'où $\langle S\rangle - \langle O\rangle = div(r) + div(r_1) = div(rr_1)$

i.e $\langle S\rangle - \langle O\rangle = div(t), t \in K(E)$ et comme $div(t) = \sum ord_P(t)\langle P\rangle = \langle S\rangle - \langle O\rangle$

$ord_S(t) = 1, ord_O(t) = -1$ *et* $ord_Q(t) = 0$; *pour* $Q \neq S, O$. Cela implique t ne possède pas de pôles finis, d'où $t \in K[E]$, mais comme $ord_S(t) = 1$ (contraction, car un polynôme non constant, possède au moins deux zéros) donc $P = Q$. □

Corollaire 1.21. L'application $\begin{array}{rcl} \sigma : Pic^o(E) & \to & E \\ classe\,\Delta & \to & P \end{array}$ est bijective

P est défini par le corollaire précèdent ($\Delta \sim \langle P\rangle - \langle O\rangle$ et P est unique

Preuve. L'application σ est surjective par construction d'après le corollaire précèdent

σ est injective car si $\sigma(classe\Delta) = \sigma(classe\Delta_1)$, pour $\Delta \sim \langle P\rangle - \langle O\rangle$ et $\Delta_1 \sim \langle Q\rangle - \langle O\rangle$, cela implique $P = Q$, d'où $\Delta \sim \Delta_1$ donc $classe\,\Delta = classe\,\Delta_1$, d'où le résultat σ est injective. □

1.2.4 Isogénies

1.2.4.1 Applications rationnelles entre courbes elliptiques

Soient E et E' deux courbes elliptiques sur un corps K algébriquement clos

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

O, l'élément neutre de E et O', l'élément neutre de E'

Définition 1.24. Une application rationnelle de E dans E' est une paire (r, s) de fonctions rationnelles sur E telles que $s^2 = r^3 + A'r + B'$.

Par convention, si on pose $F = (r, s)$

$F(P) = O' \Leftrightarrow P$ est un pole de *r* et donc de *s*.

$F(P) = \big(r(P), s(P)\big) \in E'$ car $s^2(P) = r^3(P) + A'r(P) + B'$

Lemme 1.22. soit $F : E \to E'$ une application rationnelle non constante alors, *F* est surjective.

Preuve. $F = (r, s)$, non constante implique *r* et *s* non constantes et donc il existe un pole *P* de *r* et *s* cela implique $F(P) = O'$.

Soit $Q \in E'$ et soit $\phi = F - Q, \phi$ est une application rationnelle non constante donc il existe $P \in E$ telle que $\phi(P) = O'$ i.e. il existe $P \in E$ telle que $F(P) = Q.$ i.e. F est surjective. □

1.2.4.2 Homomorphismes

Définition 1.25. Une application rationnelle $F : E \to E'$ est un homomorphisme si F est un homomorphisme de groupe. i.e. $F(P+Q) = F(P) + F(Q), \forall P, Q \in E.$

Définition 1.26. Une application rationnelle non nulle $\varphi : E \to E'$ vérifiant $\varphi(O) = O'$ est appelée isogénie. On dira alors que les deux courbes E et E' sont isogènes. C'est une relation d'équivalence.

Toute isogénie $\varphi : E \to E'$ est un homomorphisme. De plus comme φ est surjective, elle induit l'injection suivante sur les corps des fractions associés à E et E' :

$$\varphi^* : \begin{cases} K(E) \to K(E') \\ f \mapsto f \circ \varphi \end{cases}$$

φ est dite séparable ou inséparable selon la nature de l'extension $\left[K(E) : \varphi^*(K(E'))\right].$

On a alors $\deg \varphi = \deg_s \varphi \times \deg_i \varphi$ ou $\deg_s \varphi$ et $\deg_i \varphi$ sont les degrés de séparabilité et d'inséparabilité.

- $\forall S \in E'(K),\ \#\varphi^{-1}(S)$ est fini et égal à $\deg_s \varphi$. A titre d'exemple, $\deg[m] = m^2.$ pour tout entier positif $m.$

1.2.4.3 Isogénie duale Soit $\varphi : E \to E'$ une isogénie non constante définie sur $K.$ Alors il existe une unique isogénie $\hat{\varphi} : E' \to E$ tel que $\hat{\varphi} \circ \varphi = [\deg \varphi].$

$\hat{\varphi}$ est appelée isogénie duale de $\varphi.$

On suppose que $\deg \varphi = m.$ Alors on a les propriétés suivantes :

$\hat{\varphi} \circ \varphi = [m]$ sur E, $\quad \varphi \circ \hat{\varphi} = [m]$ sur E', $\quad \hat{\varphi + \psi} = \hat{\varphi} + \hat{\psi}$, $\quad \forall m \in Z, \hat{m} = m$,

$\deg \hat{\varphi} = \deg \varphi$ et $\hat{\hat{\varphi}} = \varphi.$

1.2.4.4 Anneau des endomorphismes d'une courbe elliptique

Une isogénie de E dans E est un endomorphisme. L'ensemble des endomorphismes de E est un anneau, noté $End_K(E)$. L'ensemble des endomorphismes de E définie sur $\overline{K}$ l'est aussi et est noté $End(E)$. Par exemple l'application $[m]_E$ (multiplication par m sur E) est dans $End(E)$. On a alors le théorèmes suivant :

Théorème 1.23. (voir [1])

1. $End(E)$ est un Z-module de rang 1, 2 ou 4.
2. Sur un corps fini, le rang est 2 ou 4 (on dira que la courbe est à multiplication complexe).
3. Si le rang est 4 sur un corps fini, alors la courbe est supersingulière. □

1.2.5 Points de m-torsion

Définition 1.27. Soit $m \in Z$, on appelle ensemble de *m*-torsion de E noté $E[m]$, le noyau de l'endomorphisme $[m]_E$ défini sur $\overline{K}$, c'est à dire $E[m] = \{P \in E(\overline{K}) / mP = O\}$.

1. $O \in E[m], \forall m \in Z$.
2. $E[m]$ est un sous groupe de E .

On pose $nP = (g_n, h_n)$

Théorème 1.24. $g_n et\ h_n$ sont des fonctions rationnelles sur E/K avec des pôles sur les points de $E[n]$ et $E[n]$ possède un nombre fini de points.

Preuve. Elle se fera par récurrence sur n

- Pour $n = 1$, alors $P = (x, y)$ avec $x, y \in K[E] \subset K(E)$

$E[1] = \{P \in E(\overline{K}) / 1 \cdot P = O\} = \{O\}$ est fini.

- On suppose que le théorème est vrai pour $q = 1, 2, ..., n-1$ et on vérifie qu'il est encore vrai pour $q = n$.

$nP = (n-1)P + P = (g_{n-1}, h_{n-1}) + (x, y)$.

Comme $g_{n-1} et\ h_{n-1}$ sont des fonctions rationnelles, x et y sont rationnelles aussi, donc

$g_n = -g_{n-1} - x + \left(\frac{h_{n-1} - y}{g_{n-1} - x}\right)^2, h_n = -y - \left(\frac{h_{n-1} - y}{g_{n-1} - x}\right) \cdot (g_n - x)$ Donc $g_n et\ h_n$ sont rationnelles.

C'est le cas où $(n-1)p + P \neq O_M$ où O_M : l'application rationnelle qui vaux O partout.

On va se restreindre maintenant au cas où le cardinal de E/K est infini (si non $E[n]$ est fini $E[n] \subset E$).

On sait que $E[1], E[2], ..., E[n-1]$ sont finis (hypothèse de récurrence)

1er cas : $n = k \cdot l$ avec $k > 1, l > 1$ (n, n'est pas premier) Si $P \in E[n]$ alors $kP \in E[l]$ (car $O = nP = \underbrace{kP + kP + ... + kP}_{l \text{ fois}}$). $E[l]$ et $E[k]$ sont deux sous groupe de $E[n]$ et sont finis (hypothèse de récurrence).

On a vu que $P \in E[n] \Rightarrow kP \in E[l] = \{R_1, R_2, ..., R_s\}$, cela implique qu'il existe i telle que $kP = R_i$, $1 \leq i \leq s$.

Si on montre que l'équation $kP = R_i$, possède un nombre fini de solution pour $1 \leq i \leq s$, alors, le nombre de points de $E[n]$ est fini (car ils vérifient tous l'une des équations $kP = R_i$).

Considérons l'équation $kP = R_i$ pour i fixé et soit P_0 une solution : $kP_0 = R_i$ d'où $k(P - P_0) = O$ *i.e* $P - P_0 \in E[k]$ qui est fini ($E[k] = \{Q_1, Q_2, ..., Q_t\}$) i.e $P = P_0 + Q_j$, $1 \leq j \leq t$ i.e les solutions de l'équation $kP = R_i$, qui sont de la forme $P = P_0 + Q_j$, $1 \leq j \leq t$ sont en nombre fini.

2eme cas : n est premier.

$E[2] = \{P \in E(\overline{K}) / 2 \cdot P = O\} = \{O, (w_1, 0), (w_2, 0), (w_3, 0)\}$ qui est un ensemble fini.

Pour $n > 2$ (par l'absurde) si $E[n] = E$ (infini) alors $E[2] \subset E[n] = E$ donc $n = 2$; car si $n = 2r + 1$ pour tout $P \in E[n] = E$ (par hypothèse) $nP = 2rP + P = O$

Or si $P = P_1 = (w_1, 0)$, on à $O = 2rP_1 + P_1 = r \cdot 2P_1 + P_1 = O + P_1 = P_1 = (w_1, 0)$ (contradiction $O \neq (w_1, 0)$), cela implique $E[n]$ est fini.

(g_n *et* h_n ont des pôles dans $E[n]$ car $P \in E[n] \Leftrightarrow nP = (g_n, h_n) = O$). □

Proposition 1.25. Soit p la caractéristique du corps K. Si n et p sont premiers entre eux, alors $\frac{g_n}{x}(O) = \frac{1}{n^2}$ *et* $\frac{h_n}{y}(O) = \frac{1}{n^3}, \forall n$

Preuve : elle se fera par récurrence sur n.

Pour n= 1 c'est évident ($\frac{x}{x}(O) = 1(O) = \frac{1}{1^2} = 1,\ \frac{y}{y}(O) = 1(O) = \frac{1}{1^3} = 1$).

Vérifions la proposition pour n = 2 $2P = (x, y) + (x, y) = (g_2, h_2)$ avec :

$g_2 = -(x+x) + \left(\frac{3x^2 + A}{2g}\right)^2, h_2 = -y - \left(\frac{3x^2 + A}{2y}\right)(g_2 - x)$, cela implique

$$g_2 = -2x + \frac{9x^4 + 6Ax^2 + A^2}{4y^2} = \frac{9x^4 - 8xy^2 + 6Ax^2 + A^2}{4y^2}$$

$$\frac{g_2}{x} = \frac{9x^4 - 8xy^2 + 6x^2 + A^2}{4y^2x} = \frac{9x^3}{4y^2} - 2 + \frac{6Ax^2 + A^2}{4xy^2}$$

Puisque deg ($6Ax^2 + A^2$) < deg ($4xy^2$) on aura $\frac{6Ax^2 + A^2}{4xy^2}(O) = 0$

donc : $\frac{g_2}{x}(O) = \frac{9}{4} - 2 = \frac{1}{4} = \frac{1}{2^2}$

Pour $n = 2$, on a : $\frac{h_2}{y} = -1 - \left(\frac{3x^2 + A}{4y^2}\right)(g_2 - x)$ cela implique

$$h_2 = y\frac{x^6 - 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 + A^3}{8s(x)^2}$$

$\frac{h_2}{y} = \frac{x^6 - 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 + A^3}{8(x^3 + Ax + B)^2} = \frac{\alpha}{\beta}$, $\deg(\alpha) = \deg(\beta) = 12$

d'où $\frac{h_2}{y}(O) = \frac{1}{8} = \frac{1}{2^3}$, donc la proposition est vraie pour n = 2.

On suppose que $\frac{g_q}{x}(O) = \frac{1}{q^2}$ et $\frac{h_q}{y}(O) = \frac{1}{q^3}$ pour q = 1, 2, …, n-1

Montrons que $\frac{g_n}{x}(O) = \frac{1}{n^2}$ et $\frac{h_n}{y}(O) = \frac{1}{n^3}$

On a $np = (g_n, h_n) = (n-1)P + P = (g_{n-1}, h_{n-1}) + (x, y)$

On peut voir facilement que pour n>1 on a $g_n - x \neq 0$, donc on a

$$g_n = -(g_{n-1} + x) + \left(\frac{h_{n-1} - y}{g_{n-1} - x}\right)^2 = -(g_{n-1} + x) + \frac{y^2}{x^2}\left(\frac{\frac{h_{n-1}}{y} - 1}{\frac{g_{n-1}}{x} - 1}\right)^2$$

$$\frac{g_n}{x} = -\frac{g_{n-1}}{x} - 1 + \frac{y^2}{x^3}\left(\frac{\frac{h_{n-1}}{y} - 1}{\frac{g_{n-1}}{x} - 1}\right)^2, \quad \frac{g_n}{x}(O) = -\frac{1}{(n-1)^2} - 1 + \left(\frac{\frac{1}{(n-1)^3} - 1}{\frac{1}{(n-1)^2} - 1}\right)^2 = \frac{1}{n^2}.$$

De la même manière on peut démontrer que $\frac{h_n}{y}(O) = \frac{1}{n^3}$. □

***Calculons maintenant* : ($g_n - g_m$)**

On veut déterminer le diviseur de $g_n - g_m$ et relier ce diviseur aux points de $E[k]$ pour un k approprier.

Pour calculer la multiplicité des zéros et l'ordre des pôles de $g_n - g_m$ on a besoin d'étudier la notion de dérivée. On veut définir la dérivée d'une fonction rationnelle sur E, en tenant compte de faite que $y^2 - x^3 - ax - b = 0$; i.e la dérivée de polynôme $y^2 - x^3 - ax - b$ doit être nulle.

Soit Δ une dérivation sur $K[E]$ i.e une application $\Delta : K[E] \to K[E]$ vérifiant :

1. $\Delta(F+G) = \Delta F + \Delta G, \forall F, G \in K[E]$.
2. $\Delta(F \cdot G) = \Delta F \cdot G + F \cdot \Delta G, \forall F, G \in K[E]$.
3. $\Delta(\lambda \cdot F) = \lambda \cdot \Delta F + F \cdot \Delta G, \forall \lambda \in K$.

On veut aussi que $\Delta(y^2 - x^3 - ax - b) = 0$ i.e $2y \cdot \Delta y = (3x^2 + a)\Delta x$.

On pose $\Delta x = 2y$ et $\Delta y = 3x^2 + a$

Cette dérivation se prolonge en une dérivation sur le corps des fonctions rationnelles sur E.

$\Delta : K(E) \to K(E)$ on posant $\Delta\left(\frac{f}{g}\right) = \frac{\Delta f \cdot g - f \cdot \Delta g}{g^2}$, où $f, g \in K[E]$.

Montrons d'abord que : $g_n \neq x$ (n fixé), $(nP = (g_n, h_n) \in E, (x, y) \in E)$

Si $g_n = x$ alors, $g_n(P) = x(P)$ $\forall P \in E$ i.e $1^{\text{ère}}$ composante de $nP =$ $1^{\text{ère}}$composante de P

Donc $nP = \pm P$. Cela implique $(n \pm 1)P = O, \forall P \in E$ donc $E[n-1] = E$ ou $E[n+1] = E$ i.e $E[n-1]$ ou $E[n+1]$ est infini ce qui contredit le résultat précèdent. D'où $g_n \neq x$

Remarque

Si $f \in K(E)$ est finie en P alors, Δf est finie en P.

En effet pour $f = \frac{u}{v}$, $u, v \in K[E]$ finie en $P \neq O$ et $v(P) \neq 0$

$\Delta f = \frac{v \cdot \Delta u - u\Delta v}{v^2}$ est finie en P

Si $P = O$ alors, $d^o u \leq d^o v$ cela implique $d^o(v\Delta u - u\Delta v) \leq d^o v^2$ i.e Δf est finie en P .

Proposition 1.26. Soit $f \in K(E)$. Si $ord_P(f) = d \neq 0$ est premier avec $p =$ caractéristique du corps K alors $ord_P(\Delta f) = d - 1$.

Preuve. Soit U une uniformisante en P : $f = U^d S$, S finie, non nulle en P et $U(P) = 0$

$\Delta f = \Delta(U^d S) = \Delta U^d \cdot S + U^d \Delta S = dU^{d-1} S \cdot \Delta U + U^d \Delta S) = U^{d-1}(\underbrace{d \cdot S \cdot \Delta U + U \cdot \Delta S}_{R}) =$

$= U^{d-1} R$, il suffit de montrer que est non nulle en P

1^er^cas $P = O$: $U = \frac{x}{y}$, $\Delta U = \frac{-x^3 + ax + 2b}{y^2}$ donc $\Delta U(O) = -1$ et $R(O) = d \cdot S(O) \cdot \Delta U(O)$

$= d \cdot S(O) \cdot (-1)$ cela implique que R est finie non nulle en $P = O$.

2^ème^cas $P = (w_i, 0)$: $U = y$, $\Delta U = \Delta y = 3x^2 + a$

alors, $\Delta y(P) = (3x^2 + a)(P) \neq 0$ si non w_i est une racine double de $x^3 + ax + b$ donc $R(w_i, 0) = d \cdot (3x^2 + a) \cdot S(w_i, 0)$ non nulle et finie.

3^ème^cas $P = (\alpha, \beta)$, $\beta \neq 0$: $U = x - \alpha$, $\Delta U = \Delta x = 2y$

$\Delta U(P) = 2y(P) = 2\beta \neq 0$ d'où $R(\alpha, \beta) = d \cdot 2\beta \cdot S(\alpha, \beta) \neq 0$ et finie. □

Proposition 1.27. On a $\Delta g_n = 2nh_n$ *et* $\Delta h_n = n(3g_n^2 + a)$

Preuve elle se fait par récurrence sur n

Pour $n = 1$, alors $nP = 1P = (x, y) = (g_1, h_1)$ donc $\Delta g_1 = \Delta x = 2y = 2h_1$ et

$\Delta h_1 = \Delta y = 3x^2 + a = 3g_1^2 + a$.

On suppose que la proposition est vraie pour $k = 1,2,....,n-1$ et montrons qu'elle est vraie pour n.

On a $\begin{cases} nP = (g_n, h_n), (n-1)P = (g_{n-1}, h_{n-1}), P = (x, y) \\ nP = (n-1)P + P \end{cases}$

Donc $g_n = -g_{n-1} - x + \left(\frac{h_{n-1} - y}{g_{n-1} - x}\right)^2$ $(car\ g_n - x \neq 0, \forall n)$ (*)

et $h_n = -y - \left(\frac{h_{n-1} - y}{g_{n-1} - x}\right)(g_n - x)$ (**) on a aussi $h_{n-1}^2 = g_{n-1}^3 + ag_{n-1} + b$ et

$\Delta h_{n-1} = (n-1)(3g_{n-1}^2 + a)$ et $\Delta g_{n-1} = 2(n-1)h_{n-1}$ (hypothèse de récurrence).

En dérivant (*) et (**) on obtient le résultat. □

Lemme 1.28. Soit $P, Q \in E$ et soit U une uniformisante en P. Alors la fonction $T_Q(U)$ définie par $(T_Q(U))(R) = U(R+Q), \forall R \in E$ est une uniformisante en $P - Q$. □

Notation. Soit $E[n] = \{P_1, P_2, ..., P_s\}$ (fini) on note $\langle E[n] \rangle$ le diviseur $\langle P_1 \rangle + ... + \langle P_s \rangle$

Théorème 1.29. On suppose que $m > n > 0$ et que $m, n, m-n$ *et* $m+n$ sont tous premiers avec la caractéristique p du corps K. Alors :

$$div(g_m - g_n) = \langle E[m+n] \rangle + \langle E[m-n] \rangle - 2\langle E[m] \rangle - 2\langle E[n] \rangle \qquad (1)$$

Preuve. 1/ $P \in E[m] \cap E[n]$

$mP = O$ et $nP = O$ donc $(m+n)P = O$ et $(m-n)P = 0$. i.e $P \in E[m+n]$ et $P \in E[m-n]$

Cela implique le coefficient de $\langle P \rangle$ dans le 2ème membre de (1) est $+1+1-2-2 = -2$; il suffit dans ce cas de vérifier que l'ordre de $g_m - g_n$ en P est -2 ($ord_P(g_m - g_n) = -2$).

On a $O \in E[m] \cap E[n] \cap E[m+n] \cap E[m-n]$, donc il faut d'abord vérifier que $ord_O(g_m - g_n) = -2$

Rappelons que $\frac{g_m}{x}(O) = \frac{1}{m^2}$ et $\frac{g_n}{x}(O) = \frac{1}{n^2}$ donc $\frac{g_m - g_n}{x}(O) = \frac{m^2 - n^2}{m^2 n^2}$ or d'après les hypothèses $m^2 - n^2 = (m+n)(m-n) \neq 0$ car ($m-n$ *et* $m+n$ sont premier avec p) cela implique $ord_O(g_m - g_n) = -2$.

Si $P \in E[m]$ alors $mP = O$ et donc $\forall Q \in E$, $m(P+Q) = mP + mQ = mQ$ i.e

$(g_m(P+Q), h_m(P+q)) = (g_m(Q), h_m(Q))$ cela implique $g_m(P+Q) = g_m(Q)$. Or

$g_m(P+Q) = (T_P(g_m))(Q)$ donc $(T_P(g_m))(Q) = g_m(Q)$ d'où $(T_P(g_m)) = g_m$

Or si U désigne l'uniformisante en O, le lemme précédent entraîne que $T_P(U)$ est une uniformisante en $O - P = -P$ qui appartient à $E[m]$ ($E[m]$ un s-groupe) cela implique :

$$\left(g_m - g_n = U^{-2}S, P = O, U = \frac{x}{y}, \quad alors\ g_m - g_n = T_P(g_m - g_n) = [T_P(U)]^{-2} T_P(S)\right)$$

ce qui termine la démonstration.

2/ $P \in E[m]$ *et* $P \notin E[n]$.

D'où $P \notin E[m+n]$ et $P \notin E[m-n]$ sinon par exemple $(m+n)P = O$ et $mP = O$ implique $nP = O$ donc $P \in E[n]$ (contradiction).

Et donc le coefficient de $\langle P \rangle$ dans le 2ème membre de (1) est -2 et en refait le raisonnement précédent.

3/ $P \notin E[m]$ *et* $P \notin E[n]$ donc $mP \neq O$ et $nP \neq O$ il y'a trois cas à étudier : $P \in E[m-n]$ et $P \notin E[m+n]$, $P \in E[m+n]$ et $P \notin E[m-n]$, $P \in E[m+n]$ et $P \in E[m-n]$

*cas où $P \in E[m-n]$ et $P \notin E[m+n]$

Dans les trois cas on a $g_m(P) = g_n(P)$ (c'est facile de le voir).

Le coefficient de $\langle P \rangle$ dans le 2ème membre de (1) est +1, donc il faut vérifier que $g_m - g_n$ possède un zéro d'ordre +1 en P, pour cela il suffira de vérifier que $\Delta(g_m - g_n)(P) \neq 0$ $((g_m - g_n)(P) = 0)$ i.e $ord_P(g_m - g_n) = 1$.

On a : $\Delta(g_m - g_n) = \Delta g_m - \Delta g_n = 2mh_m - 2nh_n$ cela implique :

$\Delta(g_m - g_n)(P) = 2mh_m(P) - 2nh_n(P)$. Or $P \in E[m-n]$ donc $mP = nP$ i.e $(g_m(P), h_m(P)) = (g_n(P), h_n(P))$ d'où $h_m(P) = h_n(P)$ i.e $\Delta(g_m - g_n)(P) = 2(\text{m-n})\, h_m(P)$.

Comme par hypothèse $(m-n)$ est premier à p, $2(m-n) \neq 0$, donc, il reste à vérifier que $h_m(P) \neq 0$ pour terminer la démonstration.

On a $P \notin E[m+n]$ donc $(m+n)P \neq O$ i.e $mP \neq -nP$ i.e $h_m(P) \neq -h_n(P)$ (car $g_m(P) = g_n(P)$) et comme $h_m(P) = h_n(P)$ alors, $2h_m(P) \neq 0$ d'où $h_m(P) \neq 0$.

Les autre cas se démontrent de la même manière. □

Corollaire 1.30. Si n est premier avec, p alors $E[n]$ possède n^2 éléments i.e $E[n] \cong Z/nZ \oplus Z/nZ$.

Preuve.

On note d_n le degré de diviseur $\langle E[n] \rangle$, on a $\deg(div(g_m - g_n)) = 0$ (déjà vu) et le degré du 2ème membre de (1) = $d_{m-n} + d_{m-n} - 2d_m - 2d_n$ d'où

$d_{m-n} + d_{m-n} - 2d_m - 2d_n = 0$ or $d_n =$ cardinal de $E[n]$ donc il suffit de vérifier que $d_n = n^2$

Par récurrence sur n.

$d_1 = \deg(\langle E[1]\rangle) = \deg(\langle O\rangle) = 1 = 1^2$

$d_2 = \deg(\langle E[2]\rangle) = \deg(\langle O\rangle + \langle (w_1,0)\rangle + \langle (w_2,0)\rangle + \langle (w_3,0)\rangle) = 4 = 2^2$

On suppose que $d_k = k^2, k = 1,2,...,n-1$.

Or $d_{i+j} + d_{i-j} - 2d_i - 2d_j = 0$ pour $i > j$.

Pour $i = n-1,\ j = 1$ alors, $i - j = n-2$ donc

$d_n = d_{i+j} = -d_{i-j} + 2d_i + 2d_j = -(n-2)^2 + 2 + 2(n-1)^2 = n^2$ □

1.2.6 Les polynômes de divisions

On veut définir un polynôme ψ_n dont le diviseur est $\langle E[n]\rangle$. On rappelle qu'un diviseur $D = \sum_{P\in E} n_P \langle P\rangle$ est principal si est seulement si $\deg(D) = 0$ et $\sum_{P\in E} n_P P = 0$ i.e on doit avoir $\sum_{P\in E[n]} P = O$ (Rappel : $\langle E[n]\rangle = \sum_{P\in E[n]} 1\cdot P$ n'est pas principal à cause de $\deg\langle E[n]\rangle = n^2$ lorsque n est premier à p).

Mais comme le cardinal de $E[n] = n^2$, on doit prendre $\langle E[n]\rangle - n^2\langle O\rangle$ pour avoir un degré égal à 0. Pour montrer que $\langle E[n]\rangle - n^2\langle O\rangle$ est principal, il suffit de vérifier que

$$\sum_{P\in E[n]} P - n^2 O = O \text{ ou bien } \sum_{P\in E[n]} P = O.$$

- Si $p \in E[n]$ alors $-p \in E[n]$ (car : $E[n]$ est un sous groupe)
- Si $P \neq O$ et $P \neq (w_i,0)$ pour $i = 1,2,3$ alors $P \neq -P$

Or

$$\sum_{P\in E[n]} P = O + (w_1,0) + (w_2,0) + (w_3,0) + \sum_{\substack{P\in E[n]\\ P\neq -P}} P$$

Mais comme $p \in E[n]$ et $P \neq -P$ implique $-p \in E[n]$ donc $\sum_{\substack{P\in E[n]\\ P\neq -P}} P = O$, il reste donc à vérifier que $(w_1,0) + (w_2,0) + (w_3,0) = O$, mais cette relation est triviale (trois points alignés de la courbe E leur somme égale O).

Remarque. Si $(w_i,0) \in E[n]$ pour i fixé. Alors les deux autres points sont encore dans $E[n]$.

En effet si $n = 2r+1$ $n \cdot (w_i, 0) = O$ cela implique $(2r+1) \cdot (w_i, 0) = O$, mais comme $2 \cdot (w_i, 0) = O$ alors $(w_i, 0) = O$ contradiction donc n est pair $(n = 2q)$. Cela implique $(w_i, 0) \in E[n], \forall i$.

Conclusion. On vient de voir que si

1. l'un des points $(w_i, 0) \in E[n]$ alors les deux autres aussi. Donc

$$\sum_{P \in E[n]} P = O + (w_1, 0) + (w_2, 0) + (w_3, 0) + \sum_{\substack{P \in E[n] \\ P \neq -P}} P = O$$

2. aucun des points $(w_i, 0)$ n'appartient à $E[n]$ alors

$$\sum_{P \in E[n]} P = O + \sum_{\substack{P \in E[n] \\ P \neq -P}} P = O$$

ainsi le diviseur $\langle E[n] \rangle - n^2 \langle O \rangle$ est principal.

Remarque importante.

Soit $f, g \in K(E)$. Si les coefficients des termes dominants de f et g sont égaux et si $div(f) = div(g)$, alors $f = g$.

(Il suffit d'utiliser les définitions).

Définition 1.28. Le polynôme ψ_n est l'unique polynôme dont le diviseur est $\langle E[n] \rangle - n^2 \langle O \rangle$ et dont le coefficient du terme dominant est n.

Proposition 1.31. Le polynôme ψ_n satisfait la relation suivante :

$$\psi_n^2 = n^2 \prod_{p \in E[n] - \{O\}} (x - x(P)) \qquad (*)$$

Preuve.

On a $div\,\psi_n^2 = 2div\,\psi_n$ donc on doit montrer que $div[n^2 \prod_{p \in E[n]-\{O\}} (x - x(P))] = 2div(\psi_n)$.

Le deuxième membre de (*) est un polynome en x de degré $n^2 - 1$ (car si $P \in E[n]$ alors $-P \in E[n]$) donc il admet $\frac{n^2 - 1}{2}$ racines, chacune d'ordre 2 et son diviseur

$$div[n^2 \prod_{p \in E[n]-\{O\}} (x - x(P))] = 2 \cdot [\sum_{\substack{1 \le i \le n^2 - 1 \\ P \in E[n] - \{O\}}} \langle P_i \rangle - (n^2 - 1)\langle O \rangle] = 2 \cdot [\sum_{\substack{1 \le i \le n^2 \\ P \in E[n]}} \langle P_i \rangle - n^2 \langle O \rangle] =$$

$$2[\langle E[n] \rangle - n^2 \langle O \rangle] = 2div(\psi_n). \qquad \square$$

Théorème 1.32. Si $m > n > 0$ alors $g_m - g_n = -\frac{\psi_{m+n}\psi_{m-n}}{\psi_m^2\psi_n^2}$.

Preuve. On a : $mP = \left(g_m(P), h_m(P)\right)$, le terme dominat de $g_m - g_n$ est $\frac{1}{m^2} - \frac{1}{n^2} \neq 0$ et

le terme dominant de $\frac{\psi_{m+n}\psi_{m-n}}{\psi_m^2\psi_n^2}$ est $-\frac{m+n}{m^2}\frac{m-n}{n^2} = -\frac{m^2-n^2}{m^2n^2} = \frac{1}{m^2} - \frac{1}{n^2}$

D'après la remarque précédente, il reste à vérifier que $div\,(-\frac{\psi_{m+n}\psi_{m-n}}{\psi_m^2\psi_n^2}) = div\,(g_m - g_n)$.

On a déjà vu que $div(g_m - g_n) = \langle E[m+n]\rangle + \langle E[m-n]\rangle - 2\langle E[m]\rangle - 2\langle E[n]\rangle$ (1)

D'autre part $div\,-\frac{\psi_{m+n}\psi_{m-n}}{\psi_m^2\psi_n^2} = div(\psi_{n+m}\psi_{m-n}) - 2(div(\psi_m\psi_n))$

$= div(\psi_{n+m}) + div(\psi_{m-n}) - 2div(\psi_m) - 2div(\psi_n)$

$= \langle E[m+n]\rangle - (m+n)^2\langle O\rangle + \langle E[m-n]\rangle - (m-n)^2\langle O\rangle$

$-2\langle E[m]\rangle - 2m^2\langle O\rangle - 2\langle E[n]\rangle - 2n^2\langle O\rangle$

$= \langle E[m+n]\rangle + \langle E[m-n]\rangle - 2\langle E[m]\rangle - 2\langle E[n]\rangle = div(g_m - g_n).$ □

Corollaire 1.33. Pour tout $P \in E$, $g_m(P) = x(P) - \frac{\psi_{m+1}(P)\psi_{m-1}(P)}{\psi_m^2(P)}$.

Preuve. On prend $n = 1$ dans le théorème précédent, on a donc :

$g_m - g_1 = -\frac{\psi_{m+1}\psi_{m-1}}{\psi_m^2\psi_1^2}$, $g_1 = x$ d'où $g_m = x - \frac{\psi_{m+1}\psi_{m-1}}{\psi_m^2\psi_1^2}$, il reste à vérifier que

$\psi_1^2 = 1$, on a $E[1] = \{O\}$ or $\psi_1^2 = 1^2 \prod_{p \in E[1]-\{O\}=\phi}(x - x(P)) = 1$.

Théorème 1.34. les polynômes de division $\Psi_m \in Z[x, y]$ satisfont les relations suivantes :

1) $\Psi_0 = 0$, 2) $\Psi_1 = 1$,

3) $\Psi_2 = 2y$, 4) $\Psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2$

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

6) $\psi_n^2\psi_{m+1}\psi_{m-1} - \psi_m^2\psi_{n+1}\psi_{n-1} = \psi_{m+n}\psi_{m-n}$, *pour* $m > n > 0$

7) $\Psi_{2k+1} = \Psi_{k+2}\Psi_k^3 - \Psi_{k-1}\Psi_{k+1}^3, k \geq 2$

8) $\Psi_{2k} = (2y)^{-1}\Psi_k(\Psi_{k+2}\Psi_{k-1}^2 - \Psi_{k-2}\Psi_{k+1}^2), k \geq 2$

Preuve.

1) $\psi_0 = 0$ par convention, 2) $\psi_1^2 = 1$ (déjà vu)

3) on a $\psi_2^2 = 2^2 \prod_{p \in E[2]-\{O\}} (x - x(P)) = 4(x - w_1)(x - w_2)(x - w_3) = 4y^2$

D'où $\psi_2 = 2y$.

4) $g_2 - g_1 = -\frac{\psi_3 \psi_1}{\psi_2^2 \psi_1^2}(*)$, or $g_2(P) = \frac{x^4 - 2ax^2 - 8bx + a^2}{4(x^3 + ax + b)}$, $g_1 = x, \psi_1 = 1, \psi_2 = 2y$

On remplace tous ces résultats dans (*) on trouve le résultat escompté.

6) on a $(g_m - g_n). = (g_m - g_1) - (g_n - g_1)$

D'où $-\frac{\psi_{m+n}\psi_{m-n}}{\psi_m^2 \psi_n^2} = -\frac{\psi_{m+1}\psi_{m-1}}{\psi_m^2 \psi_1^2} + \frac{\psi_{n+1}\psi_{n-1}}{\psi_n^2 \psi_1^2} = -\frac{\psi_n^2 \psi_{m+1}\psi_{m-1} - \psi_m^2 \psi_{n+1}\psi_{n-1}}{\psi_m^2 \psi_n^2}$

Cela implique : $\psi_n^2 \psi_{m+1}\psi_{m-1} - \psi_m^2 \psi_{n+1}\psi_{n-1} = \psi_{m+n}\psi_{m-n}$, *pour* $m > n > 0$

7) dans l'équation (6) si on prend $m = k+1$ *et* $n = k-1$ on obtient le résultat.

8) dans l'équation (6) si on prend $m = k+1$ *et* $n = k$ on obtient le résultat. □

1.2.7 L'accouplement de Weil

Définition 1.29. Soit un corps K et Soit n un nombre entier qui n'est pas divisible par la caractéristique de K. On pose :

$$\mu_n(\overline{K}) = \left\{x \in \overline{K} : x^n = 1\right\},$$

le groupe des racines $n^{ème}$ de l'unité dans $\overline{K}$. Puisque la caractéristique de K ne divise pas n, l'équation $x^n = 1$ n'a pas de racines multiples. Ainsi μ_n est cyclique d'ordre n.

Un générateur ς de μ_n est appelé une racine primitive $n^{ème}$ de l'unité.

Soit E/K une courbe elliptique. Pour cette section nous fixons un entier $m \geq 2$, premier avec $p = chac(K)$ si $p \succ 0$. On rappelle aussi que $\sum n_i \langle P_i \rangle$ est le diviseur d'une fonction rationnelle si et seulement si $\sum n_i = 0$ et $\sum n_i P_i = O$.

Soit $T \in E[m]$. Alors il existe une fonction $f \in \overline{K}(E)$ telle que

$$div(f) = m\langle T \rangle - m\langle O \rangle.$$

Pour $T' \in E$ avec $mT' = T$, il existe aussi une fonction $g \in \overline{K}(E)$ qui satisfait

$$div(g) = \sum_{R \in E(m)} (T' + R) - (R).$$

(Noté que $\#E[m] = m^2$ et $m^2 T' = O$).

On peut vérifier immédiatement que les fonctions $f \circ [m]$ et g^m ont le même diviseur, donc $f \circ [m] = g^m$ ou $f' \circ [m] = g^m$ avec $f' = \lambda \cdot f$, $\lambda \in \overline{K}^*$, on peut supposer que

$$f \circ [m] = g^m.$$

Maintenant supposons que $S \in E[m]$ est un autre point de *m*-torsion (le cas $S = T$ est autorisé). Alors pour tout point $X \in E(K)$,

$$g(X + S)^m = f(mX + mS) = f(mX) = g(X)^m.$$

de la l'accouplement de Weil est défini par

$$e_m : E[m] \times E[m] \to \mu_m ; (S,T) \mapsto \frac{g(X+S)}{g(X)}$$

Théorème 1.35. Soit E une courbe elliptique définie sur un corps K et soit un entier *m* positif tel que la caractéristique de k premier à *m*. alors il existe une application

$$e_m : E[m] \times E[m] \to \mu_m,$$

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

1. e_m est bilinéaire, c'est-à-dire

   $e_m(S_1 + S_2, T) = e_m(S_1, T) e_m(S_2, T)$ et $e_m(S, T_1 + T_2) = e_m(S, T_1) e_m(S, T_2)$

   pour tous $S, S_1, S_2, T, T_1, T_2 \in E[m]$.
2. $e_m(T, T) = 1$ pour tout $T \in E[m]$.
3. $e_m(S, T) = e_m(S, T)^{-1}$ pour tout $S, T \in E[m]$, *i.e.* e_m est antisymétrique.
4. e_m est non dégénéré, c'est-à-dire que si $e_m(S, T) = 1$ pour tout $S \in E[m]$ alors $S = O$ et si $e_m(S, T) = 1$ pour tout $T \in E[m]$ alors $T = O$.

Preuve.

1. Par définition :

$$e_m(S_1 + S_2, T) = \frac{g(X + S_1 + S_2) \cdot g(X + S_1)}{g(X + S_1) \cdot g(X)} = e_m(S_1, T) e_m(S_2, T).$$

Pour la deuxième égalité, soient $f_3, f_3, f_3, g_3, g_3, g_3$, 6 fonctions rationnelles définies comme si- dessus pour les points $T_1, T_2, T_1 + T_2$. Choisir $h \in \overline{K}(E)$ tel que

$$div(h) = (T_1 + T_2) - (T_1) - (T_2) + (O).$$

Alors

$$div(f_3 / f_1 f_2) = mdiv(h),$$

ainsi

$$f_3 = cf_1 f_2 h^m \text{ pour un } c \in \overline{K}^{\bullet}$$

Si on compose par l'application multiplication par *m* on trouve

$$f_3 \circ [m] = cf_1 f_2 (h^m \circ [m]).$$

ensuite on utilisant le résultat

$$f_i \circ [m] = g_i^m$$

puis on prend la racine m^{th} des deux membres on trouve

$$g_3 = c' g_1 g_2 (h \circ [m]).$$

et maintenant on peut écrire :

$$e_m(S, T_1 + T_2) = \frac{g_3(X+S)}{g_3(X)} = \frac{g_1(X+S)g_2(X+S)h([m]X + [m]S)}{g_1(X)g_2(X)h([m]X)} = e_m(S, T_1)e_m(S, T_2)$$

D'où le résultat.
2. Utilisé la propriété 1 pour $e_m(S+T, S+T)$ et montrer que $e_m(T, T) = 1, \forall T \in E[m]$.
Pour la preuve des propriétés 3. et 4. Regarder [1] chapitre III. Proposition 8.1. □

Corollaire 1.36. Si les deux points T_1, T_2 forme une base de $E[m]$. Alors $e_m(T_1, T_2)$ est une racine n^{eme} de l'unité de plus $E[n] \subset E(K), alors, \mu_m \subset K^{\bullet}$ [1]. □

1 .3 Courbes elliptiques sur un corps fini

1.3.1 Théorème de Hasse ([1], [2], [11], [13], [14]).

Cardinalité :

Contrairement aux autres corps, notons tout d'abord que toute courbe elliptique E définie sur un corps fini F_q est à multiplication complexe puisque on peut montrer que l'endomorphisme Frobenius de $End(E)$ défini comme suit est distinct de $[m]_E$ pour tout entier m.

Définition 1.30. Soit E une courbe elliptique définie sur un corps fini F_q de caractéristique p.

Alors, l'endomorphisme de Frobenius de E est défini par

$$\phi : \begin{cases} E(\overline{F}_q) \to E(\overline{F}_q) \\ (x, y) \mapsto (x^q, y^q) \end{cases}$$
$$et \quad \phi(O) = O$$

Théorème 1.37. Le polynôme caractéristique de Frobenius ϕ est :

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

Où t est défini par :

$$\#E(F_q) = q + 1 - t \text{ et vérifie de plus } |t| \le 2\sqrt{q}.$$

On va donner un esquisse de démonstration de ce théorème, pour pouvoir mettre en évidence l'importante formule pour calculer le nombre N de points d'une courbe elliptique grâce à la trace t de son Frobenius : $N = q + 1 - t$. C'est cette formule qu'on utilisera par la suite pour calculer le nombre de points d'une courbe elliptique puisque calculer N revient à calculer t.

***Preuve* :** On rappelle que pour une isogénie $\varphi : E \to E'$, $\#Ker\varphi$ divise $\deg\varphi$, φ est séparable si et seulement si $\#Ker\varphi = \deg\varphi$, et φ est purement inséparable si et seulement si $\#Ker\varphi = 1$. Donc ϕ est purement inséparable, et de degré p.

On a aussi l'endomorphisme de Frobenius $\phi : (x, y) \mapsto (x^q, y^q)$ (toujours inséparable de degré q [1]). L'ensemble de points invariants par ϕ est égal à

$$\left\{(x, y) \in E(\overline{F}_q) / x^q = x, y^q = y\right\} = E(F_q).$$

Autrement dit $Ker(1-\phi) = E(F_q)$ dans $End(E)$.

De plus $1-\phi$ est séparable, c'est-à-dire $\#Ker(1-\phi) = N = \deg(1-\phi).$

On considère donc $N = \deg(1-\phi),$ comme un endomorphisme de E, et on a donc dans $End(E)$ l'égalité :

$$N = (1-\hat{\phi})\,(1-\phi) = (\hat{1}-\hat{\phi})(1-\phi) = (1-\hat{\phi})(1-\phi) = 1-(\underbrace{\phi+\hat{\phi}}_{t}) + \underbrace{\phi\hat{\phi}}_{q}$$

où *t* est la trace de Frobenius, qui appartient à Z. On a donc dans Z : $N = 1+q-t.$

Montrons que : $|t| \le 2\sqrt{q}$.

On sait qu'on peut identifier ϕ à un élément d'un corps quadratique imaginaire. Donc $\hat{\phi} = \overline{\phi}$ et ϕ vérifie l'équation quadratique $\phi^2 - t\phi + q = 0$ (tout nombre quadratique θ vérifie l'équation $\theta^2 - Tr(\theta)\theta + N(\theta) = 0).$ Le discriminant de l'équation est donc négatif, i.e. $t^2 \le 4q,$ ce qui démontre le théorème. □

Remarques.

1. Le théorème de Hasse ne nous permet pas de déterminer le nombre de points d'une courbe elliptique, mais il nous permet d'avoir un intervalle de taille $4\sqrt{q}$ où l'on peut le chercher.
2. Compter le nombre de points K- rationnels d'une courbe elliptique E définie sur un corps finis K est un problème par fois très difficile.

1.3.2 Compter les points d'une courbe elliptique sur un corps fini

Il est très important de connaître $\#E(F_q)$ pour les méthodes de cryptages utilisant les courbes elliptiques. Dans cette partie nous allons montrer qu'il est facile de calculer l'ordre d'une courbe $E(F_{q^n})$ si nous connaissons son ordre pour $E(F_q)$. Ensuite nous allons donnée un algorithme qui nous permet de calculer $\#E(F_p)$ pour *p* premier [20] [22], [23].

Théorème 1.38. Soit $\#E(F_q) = q+1-a$. Posons $X^2 - ax + q = (X-\alpha)(X-\beta),$ où $\alpha, \beta \in \overline{F_q}.$ Alors $\#E(F_{q^n}) = q^n + 1 - (\alpha^n + \beta^n)$, pour tout $n \ge 1.$

Preuve. Commençons par montrer que $\alpha^n + \beta^n$ est un nombre entier.

Posons :

$s_n = \alpha^n + \beta^n$, alors $s_0 = 2, s_1 = a$.

Montrons que

$$s_{n+1} = as_n - qs_{n-1}, \qquad \text{pour tout } n \geq 1.$$

En effet, en multipliant la relation $\alpha^2 - a\alpha + q = 0$ par α^{n-1} nous obtenons

$$\alpha^{n+1} = a\alpha^n - q\alpha^{n-1}.$$

Nous faisons de même pour β et nous trouvons

$$\beta^{n+1} = a\beta^n - q\beta^{n-1}.$$

En additionnant ces deux égalités ensembles nous avons bien

$$s_{n+1} = as_n - qs_{n-1}$$

Posons : $f(X) = (X^n - \alpha^n)(X^n - \beta^n) = X^{2n} - (\alpha^n + \beta^n)X^n + q^n$.

Alors $X^2 - ax + q = (X - \alpha)(X - \beta)$, divise $f(X)$ car α et β sont des racines de f. Ainsi, il existe un polynôme $Q \in Z[X]$ tel que

$$f(X) = Q(X)\ (X^2 - ax + q).$$

Et donc, $(\phi_q^n)^2 - (\alpha^n + \beta^n)\phi_q^n + q = Q(\phi_q)(\phi_q^2 - a\phi_q + q) = 0$

comme endomorphisme de E.

De plus, remarquons que : $\phi_q^n = \phi_{q^n}$.

Par le théorème (1.37) Il n'y a qu'un unique nombre entier k qui satisfait

$$\phi_{q^n}^2 - k\phi_{q^n} + q^n = 0$$

et ce k est donné par $k = q^n + 1 - \#E(F_{q^n})$. Ainsi $\#E(F_{q^n}) = q^n + 1 - (\alpha^n + \beta^n)$ □

Exemple. Considérons la courbe elliptique $E : y^2 = x^3 + 2$ définie sur F_7,

$$E(F_7) = \{O, (0,3), (0,4), (3,1), (3,6), (5,1), (5,6), (6,1), (6,6)\}.$$

Ainsi $E(F_7) = 9$ et $a = 7 + 1 - 9 = -1$ et nous avons le polynôme suivant

$$X^2 + X + 7 = (X - \frac{-1 + \sqrt{-27}}{2})(X - \frac{-1 - \sqrt{-27}}{2}).$$

Nous pouvons donc calculer la cardinalité de tout groupe $E(F_{7^n})$. Par exemple :

$$\left(\frac{-1+\sqrt{-27}}{2}\right)^{60}+\left(\frac{-1-\sqrt{-27}}{2}\right)^{60}=180498585261198848060064 98,$$

et donc $\#E(F_{7^{60}}) = 7^{60}+1-180498585261198848060064 98$

$= 508021860739623365322188179602357975652549718829504.$

Grâce à ce théorème nous pouvons très vite calculer la cardinalité d'un groupe $E(F_{q^n})$ du moment que nous connaissons $\#E(F_q)$.

1.3.2.1 L'algorithme de Schoof

Nous allons maintenant présenter un algorithme dû à René Schoof [11], [13], [14] qui permet de calculer $E(F_p)$ pour un grand nombre premier p. Sa complexité est $O(\ln^8 p)$ [17], ainsi nous pourrons calculer $E(F_{p^n})$ grâce au théorème précèdent.

Soit $E: y^2 = x^3 + Ax + B$ une courbe elliptique définie sur F_p avec p un nombre premier et soit $a = p+1-E(F_p)$. L'idée de cet algorithme est de déterminer $a \bmod l_i$ pour de petits nombres premiers l.

Par le théorème de Hasse nous avons $p+1-2\sqrt{p} < \#E(F_p) < p+1+2\sqrt{p}$

i.e. $|a| < 2\sqrt{p}$. Il suffit donc de prendre tous les k premiers nombres premiers l_i de manière à avoir $\prod_{i=1}^{k} l_i > 4\sqrt{p}$.

Pour pouvoir déterminer $\#E(F_p)$ de manière unique grâce au théorème Chinois. Notons S l'ensemble de ces premiers. On remarque que puisque p est premier grand, les premiers l_i sont petits par apport à p et $l_i \neq p$.

Nous allons maintenant voir comment déterminer $a \bmod l_i$ pour les différents $l_i \in S$.

Cas $l = 2$:

$\#E(F_p) \equiv 0 \pmod 2$ ça veut dire que l'ordre du groupe est pair, sinon son ordre est impair. Nous savons que les seuls éléments d'ordre 2 de $E(F_p)$ sont de la forme (e,0) avec $e \in F_p$, i.e. e est une racine de $x^3 + Ax + B$ et donc $p+1-a \equiv 0 \pmod 2$ ce qui veut die que $a \equiv 0 \pmod 2$.

Si $x^3 + Ax + B$ n'a pas de racines dans F_p, alors $\#E(F_p) \equiv 1 \pmod 2$ et donc

$$a \equiv 1 (\mathrm{mod}\, 2).$$

Pour déterminer si $x^3 + Ax + B$ possède des racines dans F_p, il suffit de rappeler que les éléments de F_p sont exactement les racines de $x^p - x.$ Ainsi $x^3 + Ax + B$ a une racine dans F_p si et seulement s'il a une racine en commun avec $x^p - x,$ i.e. si et seulement si

$$\mathrm{PGCD}\,(x^3 + Ax + B, x^p - x.) \neq 1$$

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

$$[x] \equiv x^p \ (\mathrm{mod}\, x^3 + Ax + B)$$

et d'utiliser le résultat suivant :

$$\mathrm{PGCD}\,([x] - x, x^3 + Ax + B) = \mathrm{PGCD}\,(x^3 + Ax + B, x^p - x.).$$

Ceci termine le cas $l = 2$.

Cas $l \neq 2$:

Pour déterminer $a\ (\mathrm{mod}\, l_i)$, il suffit d'examiner quelle relation du type $\Phi_p^2 - k\Phi_p + p$ peut avoir lieu sur $E[l_i]$.

On aura alors $\mathrm{k} \equiv a\ (\mathrm{mod}\, l_i)$.

Pour les polynômes de division $\Psi_m \in Z[x, y, A, B]$ définis par

$$\Psi_0 = 0, \Psi_1 = 1, \Psi_2 = 2y, \Psi_3 = 3x^3 + 6Ax^2 + 12Bx - A^2$$
$$\Psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3)$$
$$\Psi_{2m+1} = \Psi_{m+2}\Psi_m^3 - \Psi_{m-1}\Psi_{m+1}^3, m \geq 2$$
$$\Psi_{2m} = (2y)^{-1}\Psi_m(\Psi_{m+2}\Psi_{m-1}^2 - \Psi_{m-2}\Psi_{m+1}^2), m \geq 2$$

nous allons énoncer la proposition suivante :

Proposition 1.39.

1. Si n est impair, alors $\Psi_n \in Z[x, y^2, A, B]$
2. Si n est un nombre impair, alors le degré de $\Psi_n \in Z[x]$ est égale à $(n^2-1)/2$.
3. Soient $(x, y) \in E(\overline{F}_p)$ *et* $n \in N$, alors $(x, y) \in E[n] \Leftrightarrow \Psi_n(x) = 0$

Soit $l \in S$ avec $l \neq 2$. Soit $(x, y) \in E(F_p) \bigcap E(l).$ Alors

$(x^{p^2}, y^{p^2}) + p.(x, y) = a(x^p, y^p)$ *et* $\Psi_l(x) = 0$. □

La deuxième équation permet de travailler modulo Ψ_l dans tout ce qui suit. Soit $p_l \in [-l/2, l/2]$ tel que $p_l \equiv p \pmod{l}$. Comme $(x, y) \in E[l]$, nous avons encore $p.(x, y) = p_l.(x, y)$ et donc $(x^{p^2}, y^{p^2}) + p_l.(x, y) = a(x^p, y^p)$.

Ceci nous permet de travailler avec des valeurs plus petites. Puisque (x^p, y^p) est aussi d'ordre l (car Φ_p est un endomorphisme), la relation ci-dessus détermine $a \pmod{l}$. L'idée est de calculer tous les termes de cette expression excepté a, puis de déterminer a pour que cette relation soit satisfaite. Notons que si cette relation est satisfaite pou un point $(x, y) \in E[l]$, alors nous avons déterminer $a \bmod l$ et donc elle sera vraie pour tout $(x, y) \in E[l]$.

1er cas : supposons tout d'abord que $(x^{p^2}, y^{p^2}) \neq \pm p_l.(x, y)$ pour $(x, y) \in E[l]$.

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

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

Pour j un entier. Nous avons $x' = \left(\dfrac{y^{p^2} - y_{p_l}}{x^{p^2} - x_{p_l}} \right)^2 - x^{p^2} - x_{p_l}$.

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

$$\left(y^{p^2} - y\right)^2 = y^2 \left(y^{p^2-1} - 1\right)^2 = (x^3 + Ax + B) \left((x^3 + Ax + B)^{p^2-1/2} - 1\right)^2$$

Il en va de même pour x_{p_l}. Nous pouvons donc exprimer x' comme une fonction rationnelle de x. Nous cherchons j de telle manière à avoir

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

Regardons tout d'abord la première coordonnée. Nous avons $(x, y) \in E[l]$, avec $(x', y') = \pm\ (x_j^p, y_j^p)$. si et seulement si $x' = x_j^p$. Nous avons dit plus haut que si cette relation est vraie pour un point de $E[l]$, alors elle est vraie pour tout point de $E[l]$.

Puisque les racines de ψ_l sont les première coordonnées des points finis de $E[l]$, ceci implique que

$$x' - x_j^p \equiv 0 \pmod{\psi_l}.$$

Il faut aussi se rendre compte que les racines de ψ_l sont simples. En effet, il y a l^2-1 points finis d'ordre l, car $E[l] \cong \mathrm{Z}/l\mathrm{Z} \oplus \mathrm{Z}/l\mathrm{Z}$ que nous avons démontrer.

Il y a donc $(l^2-1)/2$ points de $E[l]$ ayant la première coordonnée distincte des autres, puisque si $(x,y) \in E[l]$ alors $(x,-y) = -(x,y) \in E[l]$. De plus, le degré de ψ_l est $(l^2-1)/2$, donc ψ_l n'a que des racines simples. Ainsi $\psi_l \mid x' - x^p$. Nous calculons donc $\left(x^p\right)_j$ pour $1 \le j \le (l-1)/2$ jusqu'a ce que $x' - x_j^p \equiv 0 (\mathrm{mod}\psi_l)$ soit satisfait.

Supposons maintenant que nous ayons trouvé un tel j. Alors

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

Pour déterminer le signe de a il nous faut regarder y'. Les expressions y'/y et y_j^p/y sont des fonctions en x

Si

$$(y' - y_j^p)/y \equiv 0 \ (\mathrm{mod}\psi_l),$$

$$a \equiv j \ (\mathrm{mod}\, l).$$

Si non, nous avons

$$(y' - y_j^p)/y \equiv 0 \ (\mathrm{mod}\, l)$$

et donc

$$a \equiv j \ (\mathrm{mod}\, l).$$

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

$$\phi_p^2(x,y) = -\,p.(x,y),$$

alors $aP = (\phi_p^2 + p)(P) = O$ pour tout $P \in E[l]$. Ainsi $a \equiv 0 \ (\mathrm{mod}\, l)$.

Si

$$\phi_p^2(x,y) = \left(x^{p^2}, y^{p^2}\right) = p.(x,y),$$

alors

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

autrement dit $a^2 p.(x,y) = a^2\phi_p^2(x,y) = (2p)^2(x,y),$

Ainsi, $a^2 p \equiv 4p^2 \pmod{l}$, i.e $p \equiv a^2(2^{-1})^2 \pmod{l}$, ce qui veut dire que p est un carré $\bmod l$. Posons $w^2 \equiv p \pmod{l}$. Nous avons

$$(\phi_p - w)(\phi_p + w)(x, y) = \phi_p^2(x, y) = O$$

pour tout point $(x, y) \in E[l]$. Soit $P \in E[l]$, alors soit $(\phi_p - w)(P) = O$, et donc

$$\phi_p(P) = wP,$$

soit $(\phi_p - w)(P) = P'$ est un point fini avec

$$(\phi_p + w)(P') = O.$$

Dans tous les cas, il existe un point $P \in E[l]$ avec

$$\phi_p(P) = \pm wP.$$

Supposons qu'il existe un point $P \in E[l]$ tel que $\phi_p(P) = wP$. Alors

$$O = (\phi_p^2 - a\phi_p + p)(P) = (p - a\,w + p)(P),$$

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

$$a \equiv 2w \pmod{l}.$$

De même manière, s'il existe P tel que $\phi_p(P) \equiv -wP$, alors

$$a \equiv -2w \pmod{l}.$$

Ainsi si $\phi_p^2(x, y) = p.(x, y)$ nous avons forcément que p est un carré modulo l. Nous procédons donc ainsi, nous regardons si p est un carré modulo l en calculant le symbole de Legendre $\left(\frac{p}{l}\right)$ qui est assez facile à calculer.

Si p n'est pas un carré modulo l alors nous somme forcément dans le cas

$$\phi_p^2(x, y) = -p.(x, y)$$

qui a été traité plus haut. Si nous avons que p est un carré modulo l, il faut regarder s'il existe un point $P \in E[l]$ tel que $\phi_p(P) = \pm wP$ où $w^2 = p$. Pour le savoir, il suffit de calculer PGCD (numérateur $(x^p - x_w), \psi_l)$.

Si ce PGCD est différent de 1, alors il existe un tel point (x, y) qui est dans $E[l]$ tel que $\phi_p(x, y) = \pm w(x, y)$. Pour déterminer le signe, il nous faut encore calculer

$$\text{PGCD (numérateur}\,(y^p - y_w)/y), \psi_l).$$

S'il est différent de 1, alors $a \equiv 2w \pmod{l}$. Si non $a \equiv -2w \pmod{l}$.

Si PGCD (numérateur $(x^p - x_w), \psi_l) = 1$, alors nous nous retrouvons dans le cas $\phi_p^2(P) = -pP$ et donc $a \equiv 0 \pmod{l}$.

Remarque. Ici nous calculons les pgcd et nous regardons pas si nous avons $0 \pmod{\psi_l}$ parce que ce ne sont pas tous les points de $E[l]$ qui satisfont $\phi_p(P) = wP$ et donc nous voulons juste voir s'il y a une racine en commun.

En résumé : l'algorithme de Schoof se déroule ainsi. Soit une courbe elliptique E, d'équation $y^2 = x^3 + Ax + b$ définie sur F_p, nous voulons calculer $\#E(F_p) = p + 1 - a$.

1. Soit S l'ensemble défini plus haut.
2. Si $l = 2$, alors $a \equiv 0 \pmod{2}$ si et seulement si PGCD $(x^3 + Ax + b, x^p - x) \neq 1$.
3. pour chaque nombre premier $l \in S$ avec $l \neq 2$, faire ce qui suit.
   (a) Posons $p_l \equiv p \pmod{l}$ avec $p_l < l/2$.
   (b) Calculer x', la première coordonnée de
   $$(x', y') = (x^{p^2}, y^{p^2}) + p_l.(x, y) \pmod{\psi_l}$$
   (c) Pour $j = 1, \ldots (l-1)/2$, faire ce qui suit.
      i. Calculer x_j, la première coordonnée de
      $$(x_j, y_j) = j(x, y).$$
      ii. Si $x' - x_j^p \equiv 0 \pmod{\psi_l}$, aller à l'étape (iii). Sinon, essayer la prochaine valeur de j à l'étape (c). Si toutes les valeurs de $1 \leq j \leq (l-1)/2$ ont été essayées aller à l'étape (d).
      iii. Calculer y' et y_j. Si $(y' - y_j)/y \equiv 0 \pmod{\psi_l}$. Alors $a \equiv j \pmod{l}$. Sinon, $a \equiv -j \pmod{l}$.
   (d) Si toutes les valeurs $j = 1, \ldots (l-1)/2$, ont été essayées sans succès, posons : $w^2 \equiv p \pmod{l}$.
   Si p n'est pas un carré modulo l, alors $a \equiv 0 \pmod{l}$.

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

4.Connaissant $a \pmod{l}$ pour chaque $l \in S$, nous pouvons calculer $a \bmod \prod_{l \in S} l$

par le théorème chinois. Choisir la valeur de a qui satisfait cette congruence et telle que $|a| \leq 2\sqrt{p}$. Alors $\#E(F_p) = p + 1 - a$

Remarque. Les polynômes avec lesquels nous travaillons, par exemple x^p ou x^{p^2}, ne sont pas utilisés tels quels dans la pratique mais réduit modulo ψ_l avec $l \in S$, ce qui nous permet de travailler avec des polynômes ayant un degré qui n'est pas trop grand.

m	courbe	Factorisation de $\#E_a(F_{2^m})$
101	E_1	$2 \cdot 1267650600228230886142808508011$
103	E_0	$2^2 \cdot 2535301200456459535862530067069$
107	E_0	$2^2 \cdot 405648192073033356043634890378 09$
107	E_1	$2 \cdot 81129638414606692182851032212511$
109	E_1	$2 \cdot 32451855365842670148744865646 1467$
113	E_1	$2 \cdot 51922968585348276278967038334675 07$
131	E_0	$2^2 \cdot 68056473384187692693232012949340998 5129$
163	E_1	$2 \cdot 58460065493236116728147417535984483483291185740 63$
233	E_0	$2^2 \cdot 34508731733952818937173779311385127605709409888622 5212/$ 6328087024741343
239	E_0	$2^2 \cdot 22085588309729804119791218759286481494821656132170 98488/$ 87480219215362213
277	E_0	$2^2 \cdot 60708402882054033466233184588234965832575110498 7865/$ $08764884175561891622165064650683$
283	E_0	$2^2 \cdot 38853377844514581418389238136470378132848117337/$ $93061324295874997529815829704422603873$
283	E_1	$2 \cdot 77706755689029162836778476272940756265696312448309935/$ $21422749282851602622232822777663$
311	E_1	$2 \cdot 20859248397665137523388883849312032369167036350717111 66/$ $73989121858491635472665429482533830 2183$
331	E_1	$2 \cdot 21872507247830119243725022271176213653531694308932276 43/$ $44701030671135871258677658859434350525561430 3$
347	E_1	$2 \cdot 14334366349937946947567630595638043379978531182301756 57/$ $28537420307240763803325774115493723193900257029311$
349	E_0	$2^2 \cdot 28668732699875893895135261191276086759957062364603514 78/$ $84067443354153078762511899035960651549018775044323$
359	E_1	$2 \cdot 58713564569345830697237014919733425684392063722707996 68/$ $11081824609485917244124494882365172478748165648998663$
409	E_0	$2^2 \cdot 33052798439512429947595765401638551991420234148214060 96/$ $42324395022880711289249191050673258457777458014096366590 6/$ 17731358671
571	E_0	$2^2 \cdot 19322687615086291723476759454659936721494636648532174 99/$ $32861762572575957114478021226813397852270671183470671280/$ $08253514612736749740666173119296824216170925035557336852/$ 76673

Table 1.1 Courbes elliptiques de Koblitz

$E_a : y^2 + xy = x^3 + ax^2 + 1, a \in F_2$ et $\#E_a(F_{2^m})$, $m \in [100,600]$

Chapitre 2

2. Introduction générale à la Cryptologie

La cryptologie se compose de deux activités opposées, complémentaires et étroitement liées : la cryptographie qui cherche à construire des système cryptographiques, ou cryptosystèmes, garantissant une certaine sécurité à un ensemble d'informations, en les transformant par une opération de chiffrement ou de signature. La cryptanalyse qui cherche à déjouer de tels systèmes. Tout cryptographe cherche à imaginer toutes les attaques possibles susceptibles de casser son nouveau système.

L'art de la cryptographie date de plusieurs siècles, et son utilisation a surtout été militaire ou diplomatique, beaucoup plus rarement commerciale ou privée. Aujourd'hui cependant, en raison de la multiplication des calculateurs électroniques, des réseaux qui les relient et des données en tout genre qui y transitent, en raison de la facilité et de la modicité du coût des communications même les plus lointaines, les besoins de sécurité se font de plus en plus sentir à tous les niveaux, et c'est pourquoi la cryptologie a connu un essor considérable. Un nombre croissant de secteurs économiques sont concernés par les applications de la cryptologie. Le développement des cartes à puces, le commerce électronique, la téléphonie mobile et l'armement sont des exemples non exhaustifs. Plus généralement, la sécurité des systèmes informatiques repose sur des protocoles cryptographiques de plus en plus complexes [5].

2.1 Rappel des objectifs fondamentaux de la cryptographie

La cryptographie répond à déférents besoins :

La confidentialité le message crypter doit rester secret, ne peut être décrypté par un tiers.

L'authentification assurance de l'authenticité, notamment de l'expéditeur ou de l'origine.

L'intégrité assurance que le message n'a pas été modifiée durant la transmission.

La non répudiation l'expéditeur ne peut pas nier d'avoir envoyé le message.

2.1.1 Cryptographie à clé secrète

La cryptographie traite de la transmission confidentielle de données. C'est l'étude de méthodes permettant de transmettre des messages sous forme déguisée, de telle sorte que, seuls les destinataires autorisés soient capables de les lire. Le message à envoyer est appelé message ou texte en clair et sous sa forme déguisée, message chiffré (même s'il n'est pas

représenté sous forme de chiffres), ou cryptogramme. Une fonction cryptographique, ou de chiffrement, est donc la donnée d'une transformation, en générale bijective.

$$f : M \to C$$

où M représente l'ensemble des messages en clair, et C l'ensemble des messages chiffrés. La transformation f^{-1} est la transformation de déchiffrement.

L'histoire a montré que chaque fois qu'une fonction cryptographique f est destinée à être utilisée un nombre important de fois, il devient de plus en plus difficile de la maintenir complètement secrète. Il est donc souhaitable de pouvoir changer régulièrement de fonction *f*. A' cette fin ; on définit un système cryptographique, ou de chiffrement, ou encore un chiffre comme étant une famille finie

$$F = (f_k)_{k \in K}$$

de fonctions cryptographiques chacune étant paramétrée par un paramètre *k*, appelé clé.

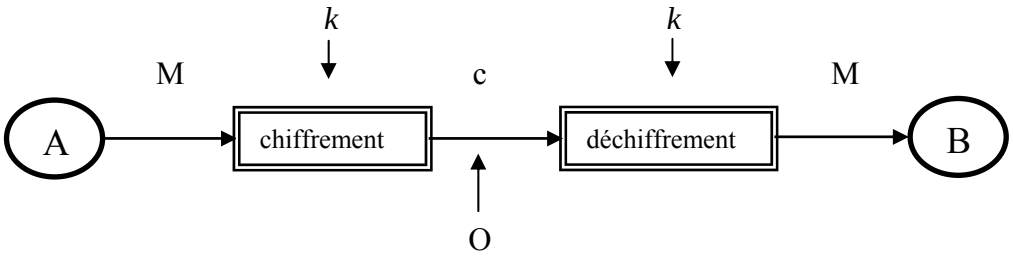


Figure. 1 .

La figure. 1 .illustre le contexte type. Deux entités, expéditeur et destinataire que l'on appelle Alice et Bob, c'est la coutume, communiquant en présence d'un observateur ou cryptanalyste Oscar. Le but du cryptanalyste est de décrypter le cryptogramme transmis C, c'est-à-dire d'en déduire le message émis M. Idéalement, il souhaitera trouver la clé *k* et la transformation f_k.

Si le système cryptographique *F* est utilisé sur une grande échelle, il n'est pas raisonnable de le considérer comme complètement secret. Pour cette raison on supposera qu'Oscar connaît entièrement le système de chiffrement *F,* il ne sait pas, par contre, laquelle des transformations f_k est utilisée. En d'autres termes il lui manque juste la clé

secrète k : c'est le principe de Kerckhoffs (1835-1903) [5]. Si le système est suffisamment bien conçu, le secret de la seule clé k suffit à assurer la confidentialité d'un message.

2.1.1.1 Exemples historiques

1- ***Chiffrement par décalage*** (*ou de Jules César*). Le message chiffré se déduit du message en clair par un décalage circulaire des lettres de l'alphabet. On peut considérer que l'ensemble des messages chiffrés C est l'alphabet latin. L'ensemble des clés est :

$$K = \{0,1,\ldots 25\}$$

Si l'on utilise un décalage de quatre lettres de l'alphabet, le texte en clair.

« *Tests statistiques* » Se transforme en le texte chiffré. « *xiwxw wxexmwxmuyiw* »

Suétone rapporte que Jules césar utilisait systématiquement la clé $k = 3$ dans sa correspondance avec ses proches. Notons que le principe de Kerckhoffs n'est pas respecté dans ce cas.

2- *Chiffrement par substitution*. L'ensemble des messages en clair et l'ensemble des messages chiffrés sont les mêmes que précédemment ; mais on augmente l'ensemble des clés. Plutôt que de se restreindre aux décalages circulaires on autorise toute permutation de l'alphabet. Le nombre de clés possibles égale donc $\# K = 26!$.

Si la clé est $$k = \begin{pmatrix} abcdefghigklmnopqrstuvwxyz \\ jteziawuyndpbsofmgxcqlvkhr \end{pmatrix}$$

Alors le texte en clair : « *tests statistiques* »

se transforme en le texte chiffré : « *cixcx xcjcyxcymqix* »

3- *Chiffrement par permutation* : (la terminologie cryptographique traditionnelle est « *transposition* »). Dans ce cas on ne modifié pas les symboles du texte en clair, mais on les permute, le texte en clair est d'abord découpé en blocs de n symboles appartenant à Σ.

Par exemple, Σ peut être l'alphabet latin augmenté du symbole blanc. On aura $M = C = \Sigma^n$ et chaque clé k est une permutation de $\{1,2,\ldots n\}$.

On chiffre par la transformation : $M \to C$, $(m_1, m_2, ..., m_n) \mapsto (m_{i1}, m_{i2}, ..., m_{in})$

Soit $n = 5$ et la clé $k =$ 3 5 2 1 4 . le texte en clair : « *tests statistiques +bbb* »

se transforme en texte chiffré : « *ssett aitstiutsqbbseb* »

Remarque.

Notons dés maintenant que dans ces systèmes la connaissance de la clé k est censée rendre facile le calcul, tant de la fonction de chiffrement f, que la transformation de

déchiffrement f^{-1}. C'est une caractéristique des systèmes cryptographiques traditionnels où à clé secrète[24] :en parle encore de déchiffrement symétrique.

Les systèmes ci-dessus sont bien peu résistants, le chiffrement par décalage utilise un ensemble de clés trop petit. Le cryptanalyste n'a qu'à essayer successivement toutes les clés possibles pour retrouver le message en clair à partir du message chiffré. Le chiffrement par substitution d'un texte écrit dans une langue naturelle ne résiste pas à une analyse de fréquences. Par exemple en « Français », la lettre la plus fréquente est « E ».

Retenons que pour rendre la tâche du cryptanalyste plus difficile, il est important de concevoir des systèmes tels que le texte chiffré ait un aspect aléatoire, même si le message en clair correspondant ne l'est pas.

2.1.1.2 Le système de Vernam, ou « one-time pad »

Le système de Vernam (1926) [24], ou « one-timepad », fonctionne de la manière suivante. Les messages, tant en clair que chiffrés, s'écrivent dans un même alphabet Σ,que l'on représente par Z_m (ou $m = \#\Sigma$). Un message de n symboles m = $\{x_1,x_2, \ldots x_n\}$, se chiffre par la transformation f_k, $f_k : M = Z_m^n \to C = Z_m^n; (x_1,...,x_n) \mapsto (y_1,...,y_n)$

avec : $y_i = x_i + k_i \bmod n$

Le n-uple k =(k_1, k_2, … k_n) constitue la clé de la transformation et il est choisi aléatoirement dans Z^n_m. En particulier, cela veut dire que si un nouveau message est envoyé, un nouveau n-uple k est utilisé comme clé et que pour chaque message, émetteur et récepteur partagent autant de symboles de clé que de symboles qu'il souhaite se transmettre : (un n-upl k n'est jamais sciemment réutilisé, d'où l'appellation « one-time ». Ce système peut être considéré comme l'aboutissement de la cryptographie traditionnelle.

2.1.1.2 Le chiffrement à clé secrète : point de vue moderne

Le « one-time pad » assure une sécurité inconditionnelle, car il ne préjuge pas de la puissance de calcul du cryptanalyste qui peut être illimitée. A partir de là une notion de sécurité calculatoire apparaît. En effet, une sécurité inconditionnelle impose de manier des clés très longues, ce qui n'est pas praticable pour la plupart des applications. On utilisera donc des clés courtes et le cryptanalyste aura en théorie tous les éléments pour clé ou message en clair. Cependant, s'il n'a pas la puissance de calcul pour le faire, il n'aboutira pas.

Les algorithmes à clé secrète peuvent être classés en deux catégories. Certains opèrent sur le message en clair un bit à la fois, ceux-ci sont appelés algorithmes de chiffrement en

continu ou par flot qui sont directement issus du système de Vernam. L'idée est tout simplement de remplacer la suite aléatoire constituant la clé par une suite pseudo-aléatoire, engendrée de manière déterministe par une clé courte , et de chiffrement par blocs qui agit globalement sur des ensembles de *n* symboles, en général des bits. Autrement dit, la fonction de chiffrement est de la forme : $f_k : \{0,1\}^n \rightarrow \{0,1\}^n$, le paramètre *k* représente la clé secrète. On peut citer comme exemples d'algorithmes de chiffrement par blocs le DES, AES [24].

2.1.2 Cryptographie à clé publique

Les algorithmes de chiffrement à clé publique sont conçus de telle manière que : La clé de chiffrement soit différente de la clé de déchiffrement. De plus, la clé de déchiffrement ne peut pas être calculée (du moins en un temps raisonnable) à partir de la clé de chiffrement. De tels algorithmes sont appelés « à clé publique » parce que la clé de chiffrement peut être rendue publique : n'importe qui peut utiliser la clé de chiffrement pour chiffrer un message mais seul celui qui possède la clé de déchiffrement peut déchiffré le message chiffré résultant. Dans de tels systèmes, la clé de chiffrement est appelée clé publique et la clé de déchiffrement est appelée clé privée (ou secrète). Par fois, les messages seront chiffrés avec la clé privée et déchiffrés avec la clé publique, une telle technique est utilisée pour signatures numériques. On peut citer comme exemple l'algorithme de chiffrement et signature RSA, ECC [17].

2.1.2.1 L'exponentiation modulaire

Il s'agit de passer maintenant à des candidats concrets. Une fonction considérée comme difficilement inversible est l'exponentiation modulo un nombre premier *p*. On l'appelle souvent *exponentielle discrète* ou *modulaire*. La fonction est construite ainsi : on se donne un grand nombre premier *p* et un nombre α primitif modulo *p* et on définit

$$\begin{aligned} Z_p^* &\rightarrow Z_p^* \\ x &\mapsto f(x) = \alpha^x \end{aligned}$$

où α est choisi de préférence primitif pour que f soit bijective. Tout les algorithme connus pour inverser cette fonction. C'est-à-dire calculer le logarithme discret, nécessitent un temps de calcul no polynomial en log *p* (le nombre de chiffres de *p*) et prohibitif en pratique lorsque *p* est un nombre de plus de quelques centaines de bits.

Remarques.

1. L'exponentiation peut être réalisée en moins de $\lceil 2\log p \rceil$ multiplications modulo p ; en procédant par élévations au carré successive.
2. Pour fabriquer réellement une fonction exponentielle de type ci-dessus, il faut trouver un grand nombre premier p et un élément primitif α modulo p. signalons que l'on ne connaît pas d'algorithme polynomial permettant de trouver un élément primitif modulo un nombre premier p quelconque. Cependant, si l'on connaît la factorisation de $p-1$ on peut tester si un nombre α est primitif en l'élevant à la puissance d pour tous les diviseurs d de $p-1=\#Z_p^*$: au bout de quelques tentatives, on trouvera presque sûrement un élément primitif. Il est tout à fait praticable de fabriquer un grand nombre premier p dont on connaisse la factorisation de $p-1$.

2.1.2.2 Le protocole de Diffie-Hellman

La cryptographie moderne, fondée donc sur les fonction à sens unique, à connu son véritable début lors de la parution en 1976 de l'article de Diffie-Hellman « New directions in cryptography ». Les auteurs y résolvent, grâce à l'exponentielle discrète, un problème de partage de secret considéré jusqu'alors comme insoluble. Le problème est le suivant : Alice et Bob ne disposent pour communiquer que d'un canal non sûr, c'est-à-dire non protégé des écoutes indiscrètes. Ils souhaitent, cependant, communiquer de manière confidentielle. Il leur faut se mettre d'accord publiquement sur un procédé de communication assurant la confidentialité. Si l'on accepte que cette confidentialité ne soit garantie que par limitation de la puissance de calcul adverse, ce problème admet une solution très simple et très ingénieuse [7].

Il suffit qu'Alice et Bob se mettent d'accord sur un nombre secret *S* qui leur servira, par exemple, de clé pour un système de chiffrement traditionnel. Il faut, bien entendu, ne pas transmettre *S* sur le canal, ni transmettre d'informations permettant d'en déduire *S*. Voici la solution proposée. Alice et Bob commencent par se mettre d'accord publiquement (sur le canal) sur un grand nombre premier *p,* et une racine primitive modulo *p*, soit α. Alice choisit secrètement et aléatoirement un nombre *a*, qu'elle gardera pour elle seule. Mais elle transmet à Bob, et à qui veut l'entendre, le nombre $\alpha^a \bmod p$. Bob choisit de

même un nombre secret *b* et transmet α^b. Alice et Bob décident ensuite que leur secret commun sera

$$S = \alpha^{ab} \bmod p.$$

Alice accède à *S* en élevant α^b à la puissance son nombre secret *a*. de même Bob élève α^a à la puissance *b.* on ne voit pas comment, à partir des seules indications transmises publiquement, $(p, \alpha, \alpha^a, \alpha^b)$, obtenir α^{ab} sans calculer un logarithme discret modulo *p*, ou faire un quelconque calcul d'une complexité démesurée.

Remarques.

1. La sécurité du système est calculatoire. Elle repose sur deux hypothèses.
   - La puissance de calcul de l'adversaire est limitée.
   - Avec une puissance de calcul et un temps limités, il n'est pas possible d'inverser la fonction exponentielle, ni de trouver α^{ab} à partir de $(p, \alpha, \alpha^a, \alpha^b)$.
2. Deux propriétés de l'exponentielle sont en fait utilisées : la difficulté de l'inverser et la commutativité de l'exponentiation

$$(\alpha^a)^b = (\alpha^b)^a.$$

2.1.2.3 L'idée de clé publique ; le système d'El Gamal

Le protocole de Diffie-Hellman a ouvert la voie à toute une série d'algorithmes cryptographiques nouveaux. Un des premiers concepts à émerger est celui de système de chiffrement à clé publique. L'idée est de rompre la symétrie du chiffrement et de déchiffrement. Dans un système traditionnel, la connaissance de la fonction de chiffrement f implique la connaissance de la fonction de déchiffrement f^{-1}. Mais connaître une fonction, dans notre contexte, veut dire disposer d'un algorithme efficace pour la calculer. Or, nous avons vu que dans certains cas on ne sait pas transformer un algorithme efficace qui calcule f en un algorithme efficace qui calcule f^{-1}. Si l'on peut en outre donner au destinataire un algorithme secret qui calcule f^{-1}, alors il n'y a plus besoin de garder secrète la fonction de chiffrement f (ou plutôt l'algorithme qui la calcule). On a alors réalisé un système dit « a clé publique » ou « asymétrique » : seul le destinataire possède le secret permettant de déchiffrer. C'est le gros avantage d'une telle stratégie : plus besoin de se préoccuper d'un partage de secret, toujours délicat.

Remarque. On dit parfois d'une telle transformation f qu'elle est à sens unique et à porte dérobée. En l'absence d'un certain secret elle est effectivement difficile à inverser. Avec le secret l'inversion est facile.

Passons à la réalisation concrète. Nous commençons par le système à clé publique d'El-Gamel, qui n'est pas le premier à être apparu historiquement, mais qui est fondé sur l'exponentielle et qui, conceptuellement, se rapproche le plus du protocole de Diffie-Hellman.

Le destinataire potentiel, Bob, possède deux clés :

- une clé secrète, soit un nombre *s*
- une clé publique, soit un nombre premier *p,* un entier α primitif modulo *p*, et l'entier modulo *p* donné par $y = \alpha^s$.

Chiffrement. Toute personne souhaitant envoyer un message M à Bob doit disposer d'un moyen de connaître les éléments de sa clé publique.

Pour chiffrer le message $M \in Z_p^*$, on procède ainsi : on tire au hasard un nombre *k* modulo *p*, et l'on calcule

$$C_1 = \alpha^k \bmod p \quad \text{et} \quad C_2 = M\, y^k \bmod p.$$

Le message chiffré est le couple

$$(C_1, C_2)$$

Pour décrypter, c'est-à-dire recouvrer M sans la clé secrète, il faut découvrir y^k. On peut chercher l'exposant k, mais pour cela on ne dispose que de $C_1 = \alpha^k$, et l'on est confronté au calcul de logarithme discret.

Déchiffrement. Par contre, si l'on est le destinataire légitime du message, et que l'on dispose de la clé secrète *s*, on trouve y^k par le calcul

$$y^k = \alpha^{sk} = C_1^s \bmod p.$$

Le message M est donc donné par

$$M = \frac{C_2}{C_1^s} \bmod p.$$

Soulignons encore une fois la dissymétrie du protocole. Si Alice et Bob veulent communiquer de manière confidentielle, chacun utilisera pour chiffrer son message la clé publique de l'autre. Pour déchiffrer, chacun utilise sa propre clé.

Remarques.

1. la fonction de chiffrement $f : M \to C$ n'est pas à proprement parler une fonction puisqu'à un message en clair M correspond potentiellement plusieurs cryptogrammes images. On continuera tout de même à parler de fonction. Ou de fonction à sens unique dans ce cas.
2. un défaut de système d'El Gamal est que le message chiffré est deux fois plus long que le message original. En contrepartie. L'introduction de l'aléa *k* est plutôt un avantage : le message M chiffré deux fois à des moment différents se traduira par des cryptogrammes différents.

2.1.2.4 La fonction puissance : le système RSA

Le premier système à clé publique solide à avoir été inventé, et le plus utilisé, est le système RSA (Rivest, Shamir, Adleman)[9]. Il est fondé sur la difficulté de factoriser des grands nombres, et la fonction à sens unique utilisée est une fonction puissance. En voici le principe.

La clé secrète est constituée de deux grands nombres premiers *p* et *q.* et d'un entier d tel que $ed \equiv 1 \bmod \varphi(n)$, où φ est la fonction indicatrice d'Euler.

La clé publique est constituée du produit $n = pq$, ainsi que de l'entier *e*.

Le chiffrement d'un message, représenté par un entier M modulo *n,* se fait par la transformation

$$M \mapsto M^e \bmod n.$$

Le déchiffrement il faut savoir calculer la fonction réciproque.
Or celle-ci est tout simplement :

$$X \mapsto X^d \bmod n$$

où *d* est l'inverse de *e* modulo $\varphi(n)$, i.e.

$$ed \equiv 1 \bmod \varphi(n).$$

En effet, rappelons que d'après le théorème de Fermat-Euler, si M est inversible modulo *n*, alors

$$M^{\varphi(n)} \equiv 1 \bmod n$$

on a donc :

$$\begin{aligned}(M^e)^d &= M^{ed} \\ &= M \bmod n.\end{aligned}$$

2.2 Génération des grands nombres premiers

Dans la mise en œuvre du chiffrement des systèmes cryptographiques à clé publique, il faut engendrer de grands nombres premiers ‘’nombres premiers aléatoires’’. En pratique, on fabrique des nombres aléatoires et l'on teste leur primalité jusqu'à l'obtention d'un nombre premier. On utilise comme test un algorithme polynomial probabiliste de Monte Carlo tel l'algorithme de Solovay-Strassen, Miller-Rabin [5] ou un algorithme polynomial déterministe tel l'algorithme AKS [26], que l'on présente dans cette section. Ces algorithmes sont rapides (un nombre n peut être testé en un temps polynomial).

Définition 2.1 Un ***algorithme de Monte Carlo positif*** est un algorithme probabiliste qui résout un problème de décision tel que toute réponse positive est toujours correcte, mais pour lequel une réponse négative peut être incorrecte. Un ***algorithme de Monte Carlo négatif*** se définit de la même manière. On dit qu'un *algorithme de Monte Carlo négatif* à une probabilité d'erreur de ε si pour chaque question dont la réponse devrait être positive, l'algorithme donne une réponse négative avec une probabilité au plus ε.

Avant de commencer la description des tests de primalité. Mentionnons tout d'abord que le nombre moyen de choix qu'il faut effectuer avant de tirer effectivement un nombre premier[24] est tout à fait acceptable. Cela est affirmé par le théorème des nombres premiers, qui donne la densité de l'ensemble des nombres premiers inférieurs à un nombre donné.

Théorème 2.1 Le nombre de nombres premiers inférieurs à x est noté $\pi(x)$, vérifie

$$\pi(x) \approx \frac{x}{\ln(x)}.$$

De plus on peut démonter que cet équivalent est approché relativement rapidement ; ceci veut dire que si l'on choisit au hasard des entiers de 500 bits, on accrochera un nombre premier au bout d'environ 350 tentatives en moyenne. □

Théorème 2.2 Pour un réel x donné l'estimation :

$$\#\left\{r \le x : q, r \ \textit{premiers}; q \,|\, r-1; q \ge x^{1/2+\delta}\right\} \ge c_\delta \frac{x}{\ln(x)} \quad \text{est vérifiée pour } \delta = 0{,}1687 > 1/6.$$

La chasse au plus grand δ s'ouvrit en 1969 avec Morris Goldfeld [27] qui obtint $\delta \approx 12$, et ce conclut, jusqu'à présent, en 1985 avec Etienne Fouvry [28] avec pour valeur de $\delta = 0.1687 > 1/6$. Tous ces travaux utilisaient des méthodes profondes de la théorie analytique des nombres qui se développèrent avec le grand crible d'Enrico Bombieri. □

Identités remarquables

Les tests de primalité **Solovay-Strassen, Miller-Rabin et *AKS*** sont fondés sur les deux identités suivantes (Fermat et Fermat généralisé), valable pour les nombres premiers.

Proposition 2.3 Soient $a \in Z$ *et* $n \in N, n \geq 2,$ *tels que* $a \wedge n = 1.$

1- Si n est premier impair, alors, $a^n \equiv a \bmod n$

2- n est premier si, et seulement si, $(X+a)^n \equiv X^n + a \bmod n$

Preuve. Supposons que n est premier. Pour tout $i \in [1, n-1]$, $iC_n^i = nC_{n-1}^{i-1}$ donc n divise iC_n^i.

Comme n est premier avec i, n divise C_n^i en vertu du théorème de Gauss. Or, le coefficient de X^i dans le polynôme $(X+a)^n$ étant $C_n^i a^{n-i}$, il se trouve divisible par n, si bien que $(X+a)^n \equiv X^n + a \bmod n$.

Réciproquement, supposons que l'on ait $(X+a)^n \equiv X^n + a \bmod n$.

Soit d un diviseur strict de n : $1 \leq d < n.$ On a : $dC_n^d = nC_{n-1}^{d-1} \equiv 0 \bmod n$ d'après l'identité puisque a est premier à n. Regardons maintenant les résidus des $C_{n-1}^i \bmod n.$

Pour $i = 1, C_{n-1}^1 = n-1 \equiv -1 \bmod n.$ Or, d'après la formule de Pascal, $C_{n-1}^i + C_{n-1}^{i+1} = C_n^{i+1}$, donc $C_{n-1}^{i+1} \equiv -C_{n-1}^i \bmod n.$ Il s'ensuit par une récurrence immédiate que $C_{n-1}^i \equiv (-1)^i \bmod n$ pour tout $1 \leq i \leq n-1$, et $\frac{n}{d} C_{n-1}^{d-1} \equiv \frac{n}{d}(-1)^{d-1} \equiv 0 \bmod n,$ ce qui n'est pas possible que si $d = 1.$ Donc n est premier. (l'identité 1 est plus facile à démontrer). □

L'avantage de ce résultat est qu'il donne une caractérisation complète des nombres premiers, cependant le calcul des puissances d'un polynôme modulo *p* nécessite beaucoup de temps car il faut calculer tous les coefficients.

2.2.1 Test de Solovay-Strassen. Choisir a au hasard. Calculer $a^{n-1/2} \bmod n$, puis le symbole de Jacobi $(\frac{a}{n})$. L'entier n satisfait au test si $a^{n-1/2} \equiv (\frac{a}{n}) \bmod n.$ (1.1)

Rappelons que le théorème d'Euler affirme que si n est premier, alors il satisfait au test pour tout $a \neq 0 \bmod n$. Rappelons par ailleurs que la loi de la réciprocité quadratique permet de calculer efficacement le symbole de Jacobi $(\frac{a}{n})$. Rappelons aussi que l'application $x \mapsto (\frac{x}{n})$ est un morphisme du groupe $(Z_n^*, \times)$ sur le groupe $\{-1, 1\}$, de même

que l'application $x \mapsto a^{n-1/2}$. Pour un n donné, l'ensemble des a vérifiant (1.1) est donc un sous groupe G_n de Z_n^*.

Si n est premier, il passe le test pour tous les $a \neq 0 \bmod n$, autrement dit $G_n = Z_n^*$.

Proposition 2.4 Si n n'est pas premier, alors $G_n \neq Z_n^*$.

Autrement dit, Si n n'est pas premier, il existe au moins un $a \in Z_n^*$ qui ne vérifie pas (1.1),(ne passe pas le test), et dans ce cas il yen a forcément $\varphi(n)/2$ puisque G_n est un sous groupe de Z_n^*. On peut donc énoncer :

Corollaire 2.5 Si n n'est pas premier, et si a est choisi aléatoirement dans Z_n^*, alors la probabilité que n satisfasse le test de Solovay-Strassen (1.1) est inférieure à $1/2$.

On a donc une probabilité $\geq 1 - 1/2^r$ de déceler en r applications du test la non primalité d'un quelconque entier n.

Preuve de la proposition2.4. Supposons que $G_n = Z_n^*$, et montrons que n est premier. Tout d'abord montrons que n n'a pas de facteur carré.

Soit p un diviseur premier de n et p^t la plus grande puissance de p divisant n. D'après le théorème de Gauss, il existe un générateur g *de* Z_q^*, $q = p^t$, et d'après le théorème chinois il existe un $a \in Z_n^*$ tel que

$$a \equiv g \bmod q \quad \text{et} \quad a \equiv 1 \bmod n/q.$$

Un tel a est d'ordre $\varphi(q)$ dans Z_n^*. Par ailleurs, si $G_n = Z_n^*$, on a $a^{n-1} = 1$ dans Z_n, donc $\varphi(p^t) = p^{t-1}(p-1)$ divise $n-1$. On en déduit que $t = 1$, si non p diviserait à la fois n et $n-1$. qui sont premiers entre eux.

Si n n'est pas premier, sa décomposition en facteur premier est de la forme $n = p_1 \ldots p_k$. D'après le théorème chinois, il existe un a non résidu quadratique modulo p_1 et tel que $a \equiv 1 \bmod n/p_1$. On a donc, par définition du symbole de Jacobi,

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{n/p_1}\right) \equiv -1 \bmod n.$$

Or si a passe le test (1.1) on a $a^{n-1/2} \equiv -1 \bmod n$. Mais cela implique $a^{n-1/2} \equiv -1 \bmod n/p_1$, qui contredit $a \equiv 1 \bmod n/p_1$. □

2.2.2 Test de Miller-Rabin

Le test de Miller-Rabin est un raffinement du test de Solovay-Strassen qui se fonde sur la remarque suivante.

Si $a^{n-1/2} \equiv 1 \bmod n$, et si $(n-1)/2$ est encore pair, alors $a^{n-1/4}$ est une racine de $1 \bmod n$, et vaut donc 1 ou -1 dans le cas où n est premier.

Plus généralement, si on examine les racines successives de $1 \bmod n$ du $a^{(n-1)/2}, a^{(n-1)/4}, \ldots, a^{(n-1)/2^s}$ tant que si possible, i.e. jusqu'au premier s tel que $a^{(n-1)/2^s}$ est impair, alors, si n est premier, la première racine différente de 1 que l'on obtient doit être -1. Cette constatation mène au test suivant.

Déroulement du test. Choisir a au hasard. Ecrire $n-1 = 2^s t$, avec t impair. Evaluer

$$a^t, a^{2t}, a^{4t}, \ldots, a^{2^{s-1}t} = a^{\frac{n-1}{2}} \bmod n. \qquad (1.2)$$

L'entier n satisfait au test si tous les entiers modulo n de la liste (1.2) égalent 1 ou bien si l'un d'entre eux égale -1.

Ce test est véritablement une amélioration du test de Solovay-Strassen.

Proposition 2.6. Si n n'est pas premier, et si a est choisi aléatoirement dans Z_n^*, alors la probabilité que n satisfasse le test de Miller-Rabin est inférieure à $1/4$.

Une preuve de cette proposition est donnée dans [24]. □

2.2.3 Test AKS (*Agrawal, Kayal et Saxena*)

L'identité de Fermat généralisé fournit donc un critère très simple de primalité : étant donné un nombre n, il suffit de choisir un entier a premier avec n puis de vérifier si la congruence est satisfaite. Cependant, cela prend un temps en $O(n)$ puisqu'il s'agit d'évaluer n coefficients dans le pire des cas.

Un moyen simple de réduire le nombre de coefficients est d'évaluer les deux membres de la congruence modulo un polynôme de la forme $X^r - 1$ pour un entier r plus petit que n bien choisi. En d'autres termes, il s'agit de vérifier si la congruence $(X+a)^n \equiv X^n + a$ est vraie dans l'anneau $\frac{Z/nZ[X]}{(X^r-1)Z/nZ[X]}$.

D'après la proposition précédente, il est immédiat de constater que tous les nombres n premiers satisfont cette équation pour tout *a* et pour tout *r*. Le problème est qu'il existe

aussi des nombres composés qui vérifient l'identité pour quelques valeurs de *a* et de *r*. Par exemple, le troisième nombre de CARMICHAEL, $n = 1729 = 7 \cdot 13 \cdot 19$, vérifie la congruence pour $a = 5$ et $r = 3$.

Comment trouver alors un nombre r tel que si l'équation est vérifiée pour plusieurs nombres a déterminés, alors n est premier ?

Théorème 2.8 (Agrawal-Kayal-Saxena). Soient $n, s, q, r \in N$, qui vérifient $s \le n, q, r$ premiers, $q \mid r-1$, $n^{(r-1)/q} \neq 0,1 \bmod r$ *et* $\binom{q+s-1}{s} \ge n^{2\lfloor \sqrt{r} \rfloor}$.

Si pour tout $a, 1 \le a < s$, on a

(i) a est relativement premier avec n et

(ii) $(X+a)^n \equiv X^n + a \bmod (X^r - 1, n)$, dans l'anneau des polynômes $Z[X]$ alors, n est une puissance d'un nombre premier.

Pour atteindre notre but nous devons permettre à s et r de croître au plus de façon polynomial en log *n*. On commence par montrer ce qui en principe est possible. Posons $s = \theta q$, avec un facteur θ fixé. La formule de Stirling donne la relation asymptotique $\log \binom{q+s-1}{s} \approx c_\theta^{-1} q$.

En conséquence, les conditions du théorème nécessitent l'estimation asymptotique $q \ge 2c_\theta \lfloor \sqrt{r} \rfloor \cdot \log n$.

Pour n grand, cela ne peut arriver essentiellement que s'il existe une infinité de nombres premiers r tels que $r-1$ à un facteur premier q qui vérifie $q \ge r^{1/2+\delta}$. Ainsi on se retrouve confronté à un problème bien étudié en théorie analytique des nombres (proposition 1. 2).

Esquisse de la preuve. Soit *p* un facteur premier de n qui vérifie déjà $p^{(r-1)/q} \neq 0,1 \bmod r$

Nous montrons que si (i) et (ii) sont vérifiés pour tout $a, 1 \le a < s,$ alors le nombre n est une puissance de *p*.

Pour faire cela on considère des produits de la forme $t = n^i p^j$ avec $0 \le i, j \le \lfloor \sqrt{r} \rfloor$. Le principe de Dirichlet donne deux paires distinctes (i_1, j_1) et (i_2, j_2) d'exposants tels que $t_1 = n^{i_1} p^{j_1} \equiv n^{i_2} p^{j_2} = t_2 \bmod r$. Le but est maintenant de prouver qu'en fait $t_1 = t_2$ et que donc $n = p^l$ pour un certain l.

D'après le petit théorème de Fermat, il suit de (ii) que pour tout $1 \le a \le p$ et $\mu = 1, 2$

$$(X+a)^{t_\mu} \equiv X^{t_\mu} + a \bmod (X^r - 1, p). \qquad (*)$$

comme $t_1 \equiv t_2 \bmod r$, $X^r - 1$ divise la différence $X^{t_1} - X^{t_2}$, ce qui entraîne finalement, d'après (*), que $(X+a)^{t_1} \equiv (X+a)^{t_2} \bmod (X^r - 1, p)$.

Donc $(g)^{t_1} = g^{t_2}$ pour tout $g \in G$, si G représente le sous groupe multiplicatif engendrer par les facteurs linéaires $(\varsigma_r - a)$ dans le corps cyclotomique sur Z/pZ obtenu par adjonction des *r*-ième racines de l'unité ς_r. En prenant un élément primitif g, c'est-à-dire un élément d'ordre $\#G$, on montre que $\#G \mid (t_1 - t_2)$.

Par ailleurs, d'après la condition (i), et comme $p^{(r-1)/q} \neq 0,1 \bmod r$ le groupe G a par un peut de combinatoire et de théorie élémentaire des polynômes cyclotomiques au moins $\binom{q+s-1}{s}$ éléments. Donc d'après l'hypothèse sur les coefficients du binôme

$|t_1 - t_2| < n^{\lfloor\sqrt{r}\rfloor} p^{\lfloor\sqrt{r}\rfloor} \leq n^{2\lfloor\sqrt{r}\rfloor} \leq \binom{q+s-1}{s} \leq \#G$ d'où l'on déduit l'égalité désirée $t_1 = t_2$. □

Algorithme AKS. **1**. *Décide si* $n = b^k$ $b, k \in N$. *Si c'est le cas va au point 5.*

2. *Choisis* (q, r, s) *satisfaisant les hypothèses du théorème (1.8).*

3. *Pour* $a = 1, \ldots, s-1$ *fait ce qui suit :*

(i) *si a divise n, va au point 5.*

(ii) *Si* $(X+a)^n \neq X^n + a \bmod (X^r - 1, n)$ *va au point 5.*

4. *n est premier, c'est fini.*

5. *n est composé, c'est fini.*

2.3 Cryptosystèmes basés sur les courbes elliptiques

Nous allons présenter trois cryptosystèmes basés sur les courbes elliptiques. Mais commençons par rappeler les différents types de cryptosystèmes. Il en existe principalement deux types [17], [21] :

- Les systèmes à clé publique ou cryptosystèmes asymétriques : la clé pour chiffrer le message est connue par tout le monde mais ne permet pas d'en déduire la clé qui permet de déchiffrer le message. Cette clé-ci n'est connue que par le destinataire. Par exemple le RSA est un tel cryptosystème.
- Les systèmes à clé privée ou cryptosystème symétriques : dans ce cas les correspondants se mettent d'accord sur une clé secrète que seul eux connaissent. Il leur faut alors un moyen sûr pour s'échanger la clé. Par exemple le protocole de Diffie- Hellmann, que nous allons présenter ci-dessous, permet d'échanger une clé en toute sécurité.

2.3.1 Protocole d'échange de clé Diffie- Hellmann

Alice et Bob veulent avoir une clé en commun pour s'échanger des données en toute sécurité. Supposons que leur seul moyen de communication soit public. Un des moyens de sécuriser leurs données est qu'ils établissent une clé privée entre eux. La méthode Diffie-Hellmann [17] permet justement de faire cela (en général on utilise cette méthode avec des groupes F_q^*, mais nous présentons cette méthode adaptée pour les courbes elliptiques).

1. Alice et Bob choisissent une courbe elliptique E définie sur un corps fini F_q tel que le logarithme discret soit difficile à résoudre. Ils choisissent aussi un point $P \in E(F_q)$ tel que le sous groupe généré par P ait un ordre de grande taille.

   (En général, la courbe E et le point P sont choisis de manière à ce que l'ordre soit un grand nombre premier.)
2. Alice choisit un nombre entier secret a, calcule $P_a = aP$ et envoie P_a à Bob.
3. Bob choisit un nombre entier secret b, calcule $P_b = bP$ et envoie P_b à Alice.
4. Alice calcule $aP_b = abP$.
5. Bob calcule $bP_a = baP = abP$.

6. Alice et Bob utilise une méthode quelconque connue pour extraire une clé secrète de abP. Par exemple, ils peuvent utiliser les derniers 256 bits de la première coordonnée de abP comme clé, ou il peuvent hacher une des coordonnées de abP avec une fonction de hachage pour laquelle ils se sont mis d'accord.

2.3.2 Problème du logarithme discret

Commençons par définir ce qu'est le problème du logarithme discret dans un groupe G quelconque.

Définition 2.2 Soient G un groupe et $g \in G$. Le problème du logarithme discret dans g en base g est, pour $y \in G$ donné, de trouver un entier x tel que

$$g^x = y \quad (xg = y \text{ si G est noté additivement})$$

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

$$Q = xP$$

si un tel x existe.

Nous parlerons plus spécialement du problème du logarithme discret dans la section qui suit.

Revenons au protocole de Diffie- Hellmann. Les seuls informations qu'un espion peut connaître sont la courbe E, le corps F_q et les points P, aP, bP. Ainsi s'il veut pouvoir connaître la clé secrète, l'espion doit résoudre le problème suivant :

2.3.2.1 Problème Diffie- Hellmann

Connaissons P, aP, bP des points de $E(F_q)$, peut-on trouver abP?

Si l'espion peut résoudre le problème du logarithme discret sur $E(F_q)$, alors il peut résoudre le problème de Diffie- Hellmann. Actuellement, on ne connaît pas de moyens de trouver abP sans d'abord résoudre le problème du logarithme discret.

Problème de décision de Diffie- Hellmann

Connaissant P, aP, bP des points de $E(F_q)$ et un point $Q \in F_q$, peut-on déterminer si

$$Q = abP?$$

Autrement dit, si quelqu'un fournit à l'espion un point Q en lui affirmant qu'il est égal à abP, l'espion a-t-il un moyen de vérifier si l'information est correcte ?

Le problème de Diffie- Hellmann et le problème de décision de Diffie- Hellmann peuvent être posés pour des groupes arbitraires. Pour les courbes elliptiques, l'accouplement de Weil peut être utilisé pour résoudre le problème de décision de Diffie-Hellmann dans certains cas. Voyons ceci.

Résolution du problème de Diffie- Hellmann pour une famille de courbes elliptique

Lemme 2.7 Soit q une puissance d'un nombre premier impair et $q \equiv 2 (\mathrm{mod}\, 3)$ et b un carré de F_q^*. Considérons la courbe supersingulière $E : y^2 = x^3 + b.$ Soit $w \in \overline{F_q}$ une racine cubique primitive de l'unité. Remarquons que $w \notin F_q$ puisque l'ordre de F_q^* est $q-1$ qui n'est pas un multiple de 3. Définissons l'application

$$B : E \to E$$
$$(x, y) \to (wx, y)$$
$$O \to O$$

Pour $(x, y) \in E(F_q)$, nous avons bien $(wx, y) \in E(F_q)$.

Preuve. On peut vérifier que cette application est un homomorphisme (En appliquant seulement la définition). Mais nous pouvons voir que B est bijective. En effet w^{-1} est aussi une racine cubique primitive de l'unité et l'application $(w^{-1}x, y) \to (x, y)$ est l'inverse de B. □

Lemme 2.8 Soit $P \in E$ un point d'ordre *n*. Alors $B(P)$ est aussi d'ordre *n* car B est un isomorphisme. Supposons que 3 ne divise pas *n*. Si $P \in E(F_q)$ est d'ordre *n* avec $E : y^2 = x^3 + b, b \in F_q$ un carré, alors $e_n(P, B(P))$ est une racine primitive $n^{ème}$ de l'unité.

Preuve. Commençons par montrer que P et $B(P)$ forment une base de $E[n]$. Soient u, v des nombres entiers tels que

$$uP = vB(P)$$

Alors

$$B(vP) = vB(P) = uP \in E(F_q).$$

Si $vP = O,$ alors $uP = O$ et donc $u \equiv 0 \ (\mathrm{mod}\, n)$. Si $vP \neq O,$ écrivons $vP = (x, y)$ avec $x, y \in F_q.$ Alors

$$(wx, y) = B(vP) \in E(F_q).$$

Puisque $w \notin F_q$, nous devons avoir $x = 0$. Ainsi $vP = (0, \pm\sqrt{b})$ qui est d'ordre 3. Ceci est impossible puisque, par hypothèse, 3 ne divise pas *n.* Ceci implique que les seules relations $uP = vB(P)$ sont $u, v \equiv 0 \pmod{n}$, et donc P et $B(P)$ forment une base de $E[n]$. Par le corollaire (1.36) $e_n(P, B(P))$ est une racine primitive $n^{ème}$ de l'unité.

Supposons maintenant que nous connaissons P, aP, bP, Q et nous voulons savoir si $Q = abP$.

Lemme 2.9 Soit E une courbe elliptique définie sur F_q et $P, Q \in E(F_q)$ tel que N est l'ordre de P et $PGCD(N, q) = 1$. Il existe un entier k tel que $Q = kP$ si et seulement si $Q \in E[N]$ et $e_N(P, Q) = 1$.

Preuve. Supposons que $Q = kP$, alors $N \cdot Q = kN \cdot P = O$. De plus,

$$e_N(P, Q) = e_N(P, P)^k = 1^k = 1.$$

Réciproquement, Si $NQ = O$, alors $Q \in E[N]$. Puisque $PGCD(N, q) = 1$, nous avons $E[N] = Z/NZ \oplus Z/NZ$.

Soit $R \in E[N]$ un point tel que $\{P, R\}$ soit une base de $E[n]$. Alors il existe des entier a, b tels que

$$Q = aP + bR$$

Par le corollaire (1.36) $e_N(P, R) = \varsigma$, une racine primitive $N^{ème}$ de l'unité. Ainsi, puisque $e_N(P, Q) = 1$, nous obtenons

$$1 = e_N(P, Q) = e_N(P, P)^a . e_N(P, P)^a = e_N(P, R)^b = \varsigma^b.$$

Ce qui implique que $b \equiv 0 \pmod{N}$, donc $bR = O$. Ainsi, $Q = aP$.

Ce lemme nous permet de savoir si Q est un multiple de P.

Si $e_n(P, Q) \neq 1$, alors Q n'est pas un multiple de P.

Si $e_n(P, Q) = 1$ (n est l'ordre de P) alors il existe un entier t tel que $Q = tP$. Remarquons tout d'abord que

$$e_n(abP, B(P)) = e_n(aP, B(bP)).$$

Alors

$$ab \equiv t \pmod{n} \Rightarrow tP = Q = abP \Rightarrow e_n(Q, B(P)) = e_n(aP, B(bP)).$$

Supposons que 3 ne divise pas *n*. Alors $e_n(aP, B(bP))$. est une racine primitive $n^{ème}$ de l'unité par le lemme (6.2) Supposons aussi que $e_n(Q, B(P)) = e_n(aP, B(bP))$. Alors

$$e_n(aP, B(bP)) = e_n(abP, B(P))$$
$$\Rightarrow e_n(P, B(P))^t = e_n(P, B(P))^{ab}$$
$$\Rightarrow e_n(P, B(P))^{t-ab} = 1$$
$$\Rightarrow t - ab \equiv 0 \pmod{n}.$$

Ces implications viennent du fait que e_n est bilinéaire et du fait que $e_n(P, B(P))$ une racine primitive $n^{ème}$ de l'unité.

En résumé, si 3 ne divise pas *n,* nous avons

$$Q = abP \Leftrightarrow ab \equiv t \pmod{n} \Leftrightarrow e_n(aP, bB(P)) = e_n(Q, B(P)).$$

Ceci résout le problème de décision de Diffie-Hellmann dans ce cas puisque P, Q, aP, bP sont des informations que l'espion connaît et $e_n(aP, B(bP))$ est calculable. Remarquons que nous n'avons jamais dû résoudre le problème du logarithme discret, il nous a juste fallu calculer l'accouplement de Weil.

2.3.2.2 La méthode d'ElGamal

Alice veut envoyer un message secret à Bob. Tout d'abord Bob fabrique une clé puplique de la manière suivante. Il choisit une courbe elliptique E définie sur un corps fini F_q de telle manière que le problème du logarithme discret soit plus difficile à résoudre sur $E(F_q)$ que sur F_q [21], [15]. Il choisit aussi un point P sur E tel que l'ordre de P soit un grand nombre premier. Il choisit un entier secret *s* et calcule $B = sP$. La courbe E, le corps fini F_q, et les points P et B sont la clé publique de Bob. La clé secrète de Bob est *s.* pour envoyer le message, Alice fait comme suit :

1. Elle télécharge la clé publique de Bob.
2. Elle transforme son message en un point $M \in E(F_q)$.
3. Elle choisit un nombre entier secret k et calcule $M_1 = kP$.

4. Elle calcule $M_2 = M + kB$.
5. Elle envoie M_1 et M_2 à Bob.

Bob déchiffre le message en calculant

$$M = M_2 - sM_1.$$

Nous avons cette égalité parce que

$$M_2 - sM_1 = (M + kB) - s(kP) = M + ksP - skP = M.$$

Un espion connaît la clé publique et les points M_1 et M_2. Si l'espion savait résoudre le problème du logarithme discret, il pourrait utiliser P et B pour trouver s et ainsi calculer $M_2 - sM_1$. L'espion pourrait aussi utiliser P et M_1 pour trouver k et calculer

$$M = M_2 - kB.$$

Actuellement, on ne connaît pas de moyen plus rapide pour retrouver le message initial en sachant que ce qui est rendu public du système de cryptage. Donc, a priori, la fiabilité de ce genre de cryptosystèmes dépend fortement des progrès fait en matière du logarithme discret.

Remarque. Il est important qu'Alice utilise, à chaque fois qu'elle envoie un message crypté à Bob avec la même clé, un k différent. En effet, si elle utilise le même k pour deux messages différents M et M', alors $M_1 = M_1'$. Un espion ayant intercepté les deux messages cryptés s'en apercevra et pourra calculer

$$M_2' - M_2 = M' - kB - (M - kB) = M' - M.$$

Supposons que pour une raison quelconque le message M soit rendu public dés que l'information n'est plus d'actualité, alors l'espion calculera sans peine M' qui vaut $M + M_2' - M_2$.

En théorie pas de problème, mais en pratique on a deux ennuis. Premièrement, les messages en clair sont des éléments de $E(F_q)$, il nous faut donc pré coder chaque message en un point de la courbe, ce qui n'est pas très commode. Deuxièmement, un cryptosystème est un couple de points, et chaque point est un couple d'éléments de F_q pour spécifier le message chiffré. Le cryptogramme est au moins quatre fois plus long que le message en clair, alors qu'il n'est que deux fois plus long dans le système

d'ElGamal originel. Pour ce débarrasser de ces inconvénients, Menezes et Vanstone ont proposé la variante suivante, plus adaptée à l'exponentielle elliptique.

2.3.2.3 Le système de Menezes- Vanstone

Les données publiques sont : la courbe E , F_q et les points P et $B = sP$. L'entier s est la clé secrète de Bob. Jusqu'ici, pas de changement. Par contre, chaque message en clair M est un couple $M = (M_1, M_2)$ d'éléments de F_q [24], [17].

Chiffrement. Alice un entier k aléatoire, calcule $k.P$ et $k.B = (x, y)$. On fait l'hypothèse que chacune des coordonnées x et y est non nulle dans F_q, l'événement contraire se produisant avec une probabilité négligeable. Le message chiffré est le couple $C = (C_1, C_2)$ où :

$C_1 = k \cdot P$ est un point de $E(F_q)$

$C_2 = (M_1 x, M_2, y)$ est un couple d'éléments de F_q

Déchiffrement. Pour déchiffrer il suffit de calculer $(x, y) = s \cdot C_1 = s \cdot k \cdot P$ à l'aide de la clé secrète, puis on obtient (M_1, M_2) à partir de C_2 en divisant par x et par y.

Cette fois-ci, on constate que le cryptogramme C n'est que deux fois plus long que le message en clair.

2.3.2.4 Signature électronique d'ElGamal

Il nous reste un problème. Comment prouver à Bob le message à bien été envoyé par Alice ? En effet, nous ne somme pas sûrs de l'authenticité du message. Un imposteur ou un espion pourrait très bien se faire passer pou Alice en créant lui-même un système de clés privées et publiques et dire que se sont les clés d'Alice. L'idée est de joindre au message une signature électronique, l'équivalent d'autographe dans le monde physique, qui certifie au destinataire l'identité de l'expéditeur.

Nous allons présenter un modèle de signature basé sur les courbes elliptiques et réputé difficilement falsifiable ; ce modèle utilise les fonction de hachages [17], nous allons donc commencer par donner la définition de ces fonctions.

Définition 2.3 Soient G et G' des ensembles quelconques, par exemple, pour ce qui va suivre $G = E(F_q)$. Une fonction de hachage H est une fonction

$$H : G \to G'$$

telle que l'image par H de n'importe quel élément (grande longueur) est un élément ayant une longueur plus petite, par exemple, de 160 bits. De plus, elle doit satisfaire les propriétés suivantes :

1. Pour un nombre *n* donné, $H(n)$ se calcule très rapidement.
2. Pour un nombre *y* donné, il est très difficile de trouver un nombre *n* tel que
$$H(n) = y$$
3. Il est très difficile de trouver deux nombres distincts n_1 et n_2 tels que
$$H(n_1) = H(n_2).$$
(Dans ce cas, on dit que H est fortement sans collisions).

Remarque. Les conditions 2 et 3 empêchent un espion de falsifier la signature. Il existe plusieurs bonnes fonctions de hachages. Par exemple, la fonction MD5 est une fonction de hachage inventée par Ron Rivest. Elle donne des ''hachés'' de 128 bits. Des faiblesses ont été trouvées et son utilisation se raréfié. Une autre fonction de hachage est la fonction SHA1. Elle renvoie une empreinte de 160 bits. C'est l'un des algorithmes les plus utilisés avec le MD5.

Supposons donc qu'Alice envie un message à Bob et qu'elle veuille signer électroniquement son message. Si elle utilise la signature ElGamal voici comment elle doit s'y prendre.

Alice doit tout d'abord créer une clé publique. Pour cela, elle choisit une courbe elliptique E définie sur un corps fini F_q, de manière que le problème du logarithme discret soit difficile à résoudre sur $E(F_q)$. Elle choisit aussi un point $A \in E(F_q)$, tel que l'ordre *n* de A est un grand nombre premier[24], [19]. De plus, elle choisit un nombre secret *a* et calcule $B=aA$. Finalement, Alice choisie deux fonctions, une fonction de hachage $H : N \to N$ et une fonction

$$f : E(F_q) \to Z.$$

Par exemple, si q est un nombre premier, elle peut prendre $f(x, y) = x \pmod q$. La fonction *f* doit avoir les propriétés suivantes :

- La cardinalité de $f(E(F_q))$ doit être grande.
- Un élément de l'image de f n'a q'un petit nombre d'antécédents. Par exemple, pour $f(x,y) = x \pmod q$, il y a au plus deux point qui ont pour image *x*.

L'information publique d'Alice est (E, F_q, A, B, H, f). Elle garde secret le nombre *a*. L'ordre *n* de *A* n'est pas forcément gardé secret, n'entrave pas la sécurité du système. Pour signer son document, Alice fait comme suit :

1. Elle représente son document sous forme d'un nombre entier *m* et le hache, c'est-à-dire calcule H(*m*) (*n* étant un grand nombre premier, $H(m) \le n$).
2. Elle choisit un nombre entier *k* avec PGCD(*k*,*n*) = 1 et calcule
$$R = kA.$$
3. Elle calcule $s \equiv k^{-1}(H(m) - a \cdot f(R)) \pmod n.$

Le message signer est (m, s, R).

Pour vérifier l'authenticité de la signature d'Alice, Bob procède comme de la manière suivante :

1. Il télécharge l'information publique d'Alice.
2. Il calcule
$$V_1 = f(R)B + sR \text{ et } V_2 = H(m)A$$
3. Si $V_1 = V_2$ alors la signature est valide.

Montrons tout d'abord que si la signature est valide, alors $V_1 = V_2$.

$$\begin{aligned} V_1 &= f(R)B + sR \\ &= f(R)aA + (k^{-1}(H(m) - af(R)) + zn)kA \\ &= f(R)aA + (H(m) - af(R))A \\ &= H(m)A \\ &= V_2, \end{aligned}$$

où *z* est un nombre entier et nous utilisons le fait que l'ordre de *A* est *n*. C'est pour cela que nous définissons *s* modulo *n*.

En fait, $V_1 = V_2$ n'implique pas forcément que la signature soit valide mais il est très difficile de trouver un nombre s' tel que

$$f(R)B + s'R = H(m)A$$

sans connaître ni *a,* ni *k*. C'est l'utilisation de la fonction de hachage qui nous garantit ceci.

Nous allons donner deux exemples où l'on peut falsifier la signature si nous n'utilisons pas la fonction de hachage, i.e que nous utilisons *m* tel quel.

Exemple 1. Supposons que nous signons un message avec une signature ElGamal sans utiliser une fonction de hachage. Le message signé est (m,s,R) comme ci-dessus, à ceci près que $s \equiv k^{-1}(m-af(R)) \pmod{n}$. Soit *h* un nombre entier tel que $PGCD(h,n)=1$. Supposons que $PGCD(f(R),n)=1$ et posons

$$\begin{aligned} R' &= hR, \\ S' &\equiv s(f(R')f(R)^{-1}h^{-1} \pmod{n}, \\ m' &\equiv mf(R')f(R)^{-1} \pmod{n}. \end{aligned}$$

Alors (m',s',R') est une signature valide. En effet,

$$\begin{aligned} V_1 &= f(R')B + s'R' \\ &= f(R')aA + sf(R')f(R)^{-1}kA \\ &= f(R')aA + k^{-1}(m-af(R))f(R')f(R)^{-1}kA \\ &= mf(R')f(R)^{-1}A \\ &= m'A \\ &= V_2. \end{aligned}$$

Donc dans ce cas, il suffit que $PGCD(f(R),n)=1$, pour qu'il soit possible de falsifier la signature. Par contre si Alice utilise une fonction de hachage il est très difficile de trouver un nombre m' tel que

$$H(m') = H(m)f(R')f(R) \pmod{n},$$

Par la propriété 2 des fonction de hachage.

Exemple 2. Utilisons les mêmes notations que pour la signature ElGamal. Soient *u,v* deux entiers tels que $PGCD(u,v)=1$ et $R=uA+vB$. Posons $s' \equiv -v'f(R) \pmod{n}$ et $m' \equiv su \pmod{n}$. Alors (m',s',R') est une signature valide. En effet

$$\begin{aligned} V_1 &= f(R)B + s'R = f(R)B + (-v^{-1})f(R)R = f(R)v^{-1}(R-uA) - v^{-1}f(R)R \\ &= -f(R)v^{-1}uA = s'uA = m'A \\ &= V_2. \end{aligned}$$

Pour falsifier le message, il suffit de trouver un *v* tel que $PGCD(u,v)=1$.

Là encore, si Alice utilise une fonction de hachage, cette méthode ne fonctionne pas. Il faudrait pour cela trouver un nombre m' tel que $H(m') \equiv s'u \pmod{n}$ ce qui est très difficile à cause de la propriété 2 des fonctions de hachages.

Remarque. Dans la signature ElGamal, l'équation de vérification

$$f(R)B + sR = mA$$

Requiert trois calculs d'un multiple d'un point. C'est la partie la plus coûteuse de l'algorithme. Il existe une variante de cette méthode qui ne fait que deux tels calculs. Voyons cette méthode.

2.3.2.5 Algorithme de signature digitale avec courbe elliptique ECDSA

Comme avant, Alice veut signer un message *m* qu'elle envoie à Bob. Pour cela, Alice choisit une courbe elliptique E définie sur un corps fini F_q telle que

$$\#E(F_q) = f \cdot r$$

où *r* est un grand nombre premier et f un petit nombre entier (généralement 1, 2 ou 4) et une fonction de hachage *H.* Elle choisit un point de base $B \in E(F_q)$ ayant pour ordre *r* et un nombre entier secret *a.* Elle calcule $Q = aG$ et rend public

$$(F_q, E, r, B, Q, H).$$

Pour signer le message *m,* Alice fait ce qui suit.

1. Elle choisit un nombre entier *k* tel que $1 \le k \le r$ et calcule $R = kB = (x, y).$
2. Elle calcule $s \equiv k^{-1}(H(m) + ax) \pmod{r}.$

Le document signé est

$$(m, s, R).$$

Pour vérifier l'authenticité de la signature Bob fait ceci.

1. Il calcule $u_1 \equiv s^{-1}H(m) \pmod{r}$ et $u_2 \equiv s^{-1}x \pmod{r}.$
2. Il calcule $V = u_1B + u_2Q.$
3. Si $V = R,$ la signature est valide.

Si le message est valide alors nous avons bien :

$$\begin{aligned} V &= u_1 B + u_2 Q \\ &= s^{-1} H(m) B + s^{-1} xQ \\ &= s^{-1} (H(m) B + xaB) \\ &= kB \\ &= R. \end{aligned}$$

Pour cette méthode aussi Alice doit choisir E tel que le problème de logarithme discret soit difficile à résoudre dans $E(F_q)$.

Ici, il ne faut calculer que deux fois un multiple d'un point de la courbe.

Voici une liste de quelques standards utilisant les courbes elliptiques

Standard	Année	Appellation	
ANSI X9.62 ANSI X9.63	1999 2001	elliptic curve digital signature algorithm Key agreement and key transport	
FIPS 186-2	2000	Digital signature standard (DSS)	
IEEE 1363-2000	2000	Standard specifications for public-key cryptography	
ISO/IEC 15946-1 ISO/IEC 15946-2 ISO/IEC 15946-3	2002 2002 2002	Techniques based on elliptic curves–Part 1: General Part 2: Digital signatures Part 3: Key establishment	
SEC 1 SEC 2	2000 2000	Elliptic curve cryptography Recommended elliptic curve domain parameters	

Tableau 2.1 Standards utilisant les courbes elliptiques.

Chapitre 3

3.1 Résoudre le problème du logarithme discret

Nous allons, dans ce chapitre, traiter le problème du logarithme discret. Nous présenterons plusieurs méthodes qui permettent, dans certains cas, de résoudre ce problème. En effet, puisque le cryptage des messages avec des courbes elliptiques se base sur la difficulté de résoudre le problème de logarithme discret en un temps raisonnable généralement, il est important de savoir dans quels cas nous pouvons le résoudre rapidement pour éviter ces cas là. Nous parlerons plus précisément du Baby Step, Giant Step qui est apparemment l'un des algorithmes les plus efficaces ; mais nous parlerons aussi de l'algorithme MOV [8], [17], [18] qui ramène le problème au cas du logarithme discret dans F_{p^n} pour un certain nombre premier p.On termine ce chapitre par une comparaison de ECC aux deux autres cryptosystèmes à clé publique les plus utilisés.

3.1.1 Baby Step, Giant Step

Cette méthode, développée par D. Shanks, fait environ $\sqrt{N}$ pas et stocke environ $\sqrt{N}$ donnée. C'est pourquoi elle ne fonctionne bien que pour des N de taille modérée.

Par commodité, dans ce paragraphe, nous exposons la méthode de Baby Step, Giant Step pour un groupe de la forme $E(F_q)$ avec E une courbe elliptique sur F_q mais elle est valable pour un groupe quelconque.

Nous supposerons qu'il existe un nombre entier k tel que $Q = kP$ avec $P, Q \in E(F_q)$ et que N , l'ordre de E , est connu.

L'algorithme se déroule comme suit :

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

Nous allons maintenant voir pourquoi cet algorithme fonctionne. Puisque $m^2 > N$, nous avons $0 \le k < m^2$. Ecrivons $k = k_0 + mk_1$, ainsi $k \equiv k_0 (\mathrm{mod}\, m)$ avec $0 \le k_0 \le m.$ et $k_1 = (k - k_0)/m$ et donc $0 \le k_1 \le m.$ Posons $i = k_0$ et $j = k_1$, nous obtenons donc

$$Q - k_1 mP = kP - k_1 mP = k_0 P$$

est la relation voulue.

Le point iP est calculé en ajoutant P (''baby step'') à $(i-1)P$. L point $Q - jmP$ est trouvé en ajoutant $-mP$ (''giant step'') à $Q - (j-1)mP$.

Remarquons que nous ne devons pas connaître l'ordre exact de $E(F_q)$. Nous devons juste connaître une borne supérieure de N. Ainsi pour une courbe elliptique définie sur un corps fini F_q, nous pouvons prendre un m tel que :

$m^2 \ge q + 1 + 2\sqrt{q}$ par le théorème de Hasse.

Exemple. Soit $G = E(F_{41})$, où E est donnée par : $y^2 = x^3 + 2x + 1$

Soient $P = (0,1)$ et $Q = (30,40).$ Par le théorème de Hasse, nous savons que l'ordre de G est au plus 56, posons $m = 8$. Les points iP pour $0 \le i \le 7$ sont

$$(0,1), (1,39), (8,23), (38,38), (23,23), (20,28), (26,9).$$

Calculons $Q - jmP$ pour $j = 0,1,2 \ldots$on trouve $(30,40), (9,25), (26,9), \ldots$

où nous nous arrêtons puisque le troisième point correspond à $7P$. Nous avons donc $Q = (7 + 2.8)P = 23P$ et nous trouvons $k = 23.$

3.1.2 L'Algorithme MOV

Nous allons, maintenant, présenter un algorithme spécifique pour résoudre le problème du logarithme discret dans le cas des courbe elliptique, contrairement à l'algorithme précédent qui peut être utilisé sur un groupe quelconque.

Le MOV, développé par Menezes, Okamoto et vanstone, utilise l'accouplement de Weil pour transformer un problème de logarithme discret dans $E(F_q)$ en un problème de logarithme discret dans $F_{q^m}^*$ pour un certain entier m. Puisque le problème de logarithme discret sur un corps fini peut être résolu par la méthode du calcul d'index, il peut être résolu plus vite sur $F_{q^m}^*$ que sur $E(F_q)$ tant que $\# F_{q^m}^*$ n'est pas beaucoup plus grand que $\# F_q^*$.

En fait, l'entier m de $E(F_{q^m})$ peut très bien être grand, auquel cas le problème du logarithme discret dans le groupe $F_{q^m}^*$, qui est d'ordre $q^m - 1$, est aussi difficile à résoudre que le problème du logarithme discret dans $E(F_q)$, qui a un ordre d'environ q, par le théorème de Hasse. Par contre, pour une courbe supersingulière, nous pouvons en général prendre $m = 2$, comme nous allons le montrer par la suite.

Soit E une courbe elliptique définie sur F_q. Soient $P, Q \in E(F_q)$ et N l'ordre de P. Supposons que

$$\text{PGCD } (q, N) = 1.$$

Nous cherchons un entier k tel que $Q = kP$. Le lemme (6.3) nous permet de voir si un tel k existe.

Puisque tout point de $E[N]$ a ses coordonnées dans $\overline{F_q} = \bigcup_{j \geq 1} F_{q^j}$, il existe un m tel que $E[N] \subset E(F_{q^m})$. Le groupe μ_N des racines $N^{ème}$ de l'unité est alors continu dans F_{q^m}.

L'algorithme MOV se déroule ainsi.

1. *Choisir un point* $T \in E(F_{q^m})$.
2. *Calculer* M *, l'ordre de T.*
3. *Soit* $d = PGCD(M, N)$. *Posons* $T_1 = (M/d)T$, *l'ordre de* T_1 *est* d. *Celui-ci divise* N *, ainsi* $T_1 \in E(N)$.
4. *Calculer* $\varsigma_1 = e_N(P, T_1)$ *et* $\varsigma_2 = e_N(Q, T_1)$. *Donc* ς_1 *et* ς_2 *sont dans* $\mu_d \subseteq \mu_N \subseteq F_{q^m}^*$. *En effet,*

$$1 = e_N(P, O) = e_N(P, dT_1) = e_N(P, T_1)^d = \varsigma_1^d,$$

idem pour ς_2.

5. *Résoudre le problème du logarithme discret pour*

$$\varsigma_2 = \varsigma_1^k$$

dans $F_{q^m}^*$. *Nous trouvons* $k \pmod d$.

6. *Recommencer avec des points* T *choisis au hasard jusqu'à ce que nous ayons* $PGCD(M, N) = N$. *Ceci détermine* $k \pmod d$.

Remarque. A priori, on pourrait penser que le cas $d = 1$ apparaisse très fréquemment. En réalité, il se passe le contraire. Voyons pourquoi.

Rappelons que

$$E(F_{q^m}) \cong Z/n_1 Z \oplus Z/n_2 Z$$

Pour des entiers n_1, n_2 tels que n_1 divise n_2. Ainsi N divise n_2, puisque n_2 est l'ordre le plus grand possible pour un élément du groupe $E(F_{q^m})$. Soient B_1 et B_2 des points d'ordres n_1, n_2 respectivement tels qu'ils engendrent $E(F_{q^m})$. Nous pouvons donc écrire

$$T = a_1 B_1 + a_2 B_2.$$

Soit $l^e \mid N$ avec l premier. Donc $l^f \mid n_2$ avec $f \geq e$. Si l ne divise pas a_2, alors $l^f \mid M$, l'ordre de T.

En effet, $$O = M\,T = Ma_1 B_1 + Ma_2 B_2,$$

puisque B_1, B_2 engendre $E(F_{q^m})$, cela implique que $Ma_1 B_1 = Ma_2 B_2 = O$ et donc que $n_2 \mid Ma_2$, de plus l ne divise pas a_2 et $l^f \mid n_2$, donc $l^f \mid M$. Ainsi $l^e \mid d$, avec $d = PGCD(M, N)$.

La probabilité que l ne divise pas a_2 est de $1 - 1/l$, et donc la probabilité que $d \neq 1$ est au moins $1 - 1/l$. Ainsi, après avoir choisi plusieurs T différents nous devrions trouver un $d \neq 1$, et après quelques itérations de l'algorithme trouver k.

Montrons maintenant que dans le cas d'une courbe elliptique supersingulière nous pouvons, en général, prendre $m = 2$.

Soit E une courbe elliptique définie sur F_q, où q est la puissance d'un nombre premier p. Alors $\#E(F_q) = q + 1 - a$,

où a est un entier. Rappelons qu'une courbe E est appelée supersingulière si $a \equiv 0 (\mathrm{mod}\ p)$. Nous savons aussi …… que ceci est équivalent à $a = 0$ lorsque $q \geq 5$ et q est premier.

Proposition 3.1 Soit E une courbe elliptique sur F_q et supposons que $a = 0$, i.e. E est supersingulière. Soit N un nombre positif premier à p où $q = p^j$. S'il existe un point $P \in E(F_q)$ d'ordre N, alors $E[N] \subseteq E(F_{q^2})$. □

3.2 Choix d'une courbe elliptique pour une utilisation cryptographique

Dans ce paragraphe nous allons parler sur les conditions de sécurité qu'on impose sur une courbe elliptique pour une éventuelle utilisation cryptographique [25]. Pour cela on présente deux cas. Le premier est celui de $q = p$ un grand nombre premier et le deuxième cas lorsque la courbe elliptique est définie sur un corps fini de caractéristique égale à 2.

3.2.1 Cas d'une courbe elliptique définie sur F_p

Soit $q = p$ un nombre premier $p \geq 5$, une courbe elliptique sur F_p est une paire $E = (a,b) \in F_p^2$ tel que $4a^3 + 27b^2 \neq 0$. Un point $P \in E$ est une solution $(x, y) \in \overline{F}_p^2$ ou le point à l'infini O. Les points $(x, y) \in E$ avec $x, y \in F_p$ au quel on rajoute O forme un groupe pour l'addition, il est noté $E(F_p)$: l'ensemble de points rationnels sur F_p.

La sécurité de système cryptographique dans lequel $E(F_p)$ est utilisé est basé sur la difficulté de résoudre le problème de logarithme discret dans le sous-groupe d'ordre r dans $E(F_p)$. Pour cela la communauté cryptographique recommande que le groupe $E(F_p)$ doit satisfaire les conditions suivantes :

1. $\left|E(F_p)\right| = k \cdot r$ avec $r > 2^{160}$ un nombre premier et k un entier positif.
2. le nombre premier r et p sont différents.
3. l'ordre de p dans le groupe multiplicatif $F_r^\times$ de F_r est de moins B, avec $B \geq 20$.

La première condition exclue l'application des algorithme générique pour résoudre le problème de logarithme discret dans $E(F_p)$. La deuxième condition évite que la courbe E soit une courbe à anomalie dont le problème de logarithme discret est plus facile à résoudre. La dernière condition exclue l'attaque de MOV, et l'attaque de Frey, Ruck [17]. Les deux attaque réduisent le problème de logarithme discret dans $E(F_p)$ à un problème de logarithme discret dans une extension finie de F_p. Le degré de cette extension est au moins l'ordre de p dans $F_r^\times$.

Remarque. De préférence prendre k le plus petit qui soit possible (en pratique on prend $k \leq 4$). Il est à noté que la robustesse du système est indépendante de k .

1	$\left\|E(F_p)\right\| = k \cdot r$ avec r premier et $k \le 4$).
2	$P \neq r$
3	$p^s \neq 1 \bmod r, 1 \le s < 20$

Table 3.1 Conditions de sécurité sur groupe $E(F_p)$

Source : NIST recommended Key sizes

3.2.2 Cas d'une courbe elliptique définie sur F_{2^m}.

Dans cette section on prend $q = 2^m$. Une courbe elliptique sur F_{2^m} est une paire $E = (a,b) \in F_{2^m}^2$, $4a^3 + 27b^2 \neq 0$. Un point $P \in E$ est une solution $(x,y) \in \overline{F}_{2^m}^2$ de $y^2 + xy = x^3 + ax^2 + b$ ou le point à l'infini O. De même les points $(x,y) \in E$ avec $x, y \in F_{2^m}$ au quel on rajoute O forme un groupe pour l'addition, il est noté $E(F_{2^m})$: l'ensemble de points rationnels sur F_{2^m}.

Les conditions de sécurité sur $E(F_{2^m})$ sont similaires à celles de la section précédente. Ils sont présentés sur le tableau suivant :

(E1)	$\left\|E(F_{2^m})\right\| = k \cdot r$ avec r premier et $k \le 4$).
(E2)	m est premier
(E3)	$2^{ms} \neq 1 \bmod r, 1 \le s < 20$

Table 3.2 Conditions de sécurité sur groupe $E(F_{2^m})$

Source : NIST recommended Key sizes

3.3 Performances de ECC

Pour mieux évaluer l'efficacité de ECC, il est nécessaire d'établir des comparaisons avec les systèmes RSA et DSA. Ces comparaisons vont porter essentiellement sur les niveaux de sécurité atteints et sur le temps de calcul et de la vérification de la signature propres à chaque système.

3.3.1 Comparaison des niveaux de sécurité

Le tableau suivant, élaboré par RSA Laboratories, donne une estimation des ressources nécessaires pour casser les trois systèmes ECC, RSA et DSA pour différentes tailles de clé.

RSA/DSA **Taille des clés**	**ECC** **Taille des clés**	**Année MIPS**	**Rapport** **des tailles des clés**
512	106	10^4	5 :1
768	132	10^8	6 :1
1024	160	10^{11}	7 :1
2048	210	10^{20}	10 :1
21000	600	10^{73}	35 :1

Source : NIST recommended Key sizes

Comme la puissance de calcul des machines augmente très rapidement, les tailles des clés doivent augmenter si on veut garder le même niveau de sécurité. Mais le tableau précédent prouve que ceci est irréalisable avec RSA pour des applications disposant de ressources limitées, c'est pourquoi un ECC semble être idéal dans ces cas.

Remarque.

En implémentant un algorithme de factorisation (cribles linéaires) avec de nouvelles ressources en hardware, A. Shamir estime que l'on peut casser une clé RSA de 512 bits en 10 minutes pour 10 000 $, et 1024 bits en moins d'une année pour 10 millions de $.

3.3.2 Comparaison des temps de calcul

Pour mieux évaluer l'efficacité des ECC, on va comparer les temps de calcul en millisecondes pour une signature et une vérification de signature pour le schéma ECDSA (dérivé du DSA, utilisant les courbes elliptiques) aux temps correspondants pour RSA et DSA sur trois différentes plates-formes.

Les temps de calcul sont en millisecondes.

Algorithme	RSA			DSA			ECDSA		
Tailles des clés	680 bits	1368 bits	2704 bits	680 bits	1368 bits	2704 bits	112 bits	bits 160	224 bits
Signature	10	45	270	10	20	80	5	5	25
vérification	0	2	8	10	30	110	25	75	95

Tableau 3.3 Pentium III 900 Mhz avec 256 M de RAM**.**

Source : NIST recommended Keey sizes

On remarque que le temps de calcul que nécessite la signature ECDSA est très court par apport à celui de RSA et de DSA. Par contre la vérification d'une signature ECDSA est très élevé par rapport à celui de RSA, *tout en restant très inférieur à la seconde*, mais on peut le réduire considérablement en opérant quelques modifications au niveau du hardware. On peut également améliorer les performances de ECC on optimisant le choix des paramètres qui interviennent dans l'implémentation de ECDSA.

Chapitre 4

4.1 Application

Ce chapitre est consacré à l'application. Nous parlerons tout d'abord du choix du langage, puis de l'implémentation des différentes étapes du système. Quelques algorithmes implémentés seront présentés puis nous terminerons par une description du logiciel.

4.2 Langage de programmation

Pour réaliser notre système nous avons choisi le langage C++ sous l'environnement Borland C^{++} Builder et qui tourne sous le système d'exploitation Windows XP. Ce choix a été motivé par le fait que ce langage supporte la manipulation aisée et efficace des corps finis de grandes caractéristiques en faisant appel à la librairie MIRACL. De plus, C^{++} permet une programmation modulaire, par l'utilisation des unités qui peuvent être compilées séparément et indépendamment du programme qui les utilise et il possède une bibliothèque des composants très riche.

4.3 Implémentation des différentes étapes du système

4.3.1 Étape de génération d'un grand nombre premier

En pratique, on fabrique des nombres aléatoires et l'on teste leur primalité jusqu'à l'obtention d'un nombre premier. On utilise comme test : un algorithme polynomial probabiliste de Monte Carlo tel l'algorithme Miller-Rabin ou un algorithme polynomial déterministe tel l'algorithme AKS. Mais de préférence utilisé une hybridation des deux tests de la façon suivante :

- Générer un nombre pseudo premier, en utilisant le test de Miller-Rabin pour une probabilité fixée α .
- Tester sa primalité en utilisant l'algorithme AKS.

4.3.2 Étape de génération de la courbe elliptique

Une fois que le nombre premier *p* est généré, on définit le corps fini $K = F_p$. Maintenant on peut générer une courbe elliptique $E : y^2 = x^3 + ax + b.$ définie par le couple (a, b) de la manière suivante :

- Choisir au hasard deux nombres entiers $a, b \bmod p$.
- Vérifier que $-(27b^2 + 4a^3) \neq 0 \bmod p$.

4.3.3 Étape de calcul de nombre de points d'une courbe elliptique

Le calcul de la cardinalité de l'ensemble de points rationnels $\#E(F_p)$ d'une courbe elliptique définie sur un corps fini à p éléments est un préalable incontournable à toute mise en œuvre cryptographique.

- Utiliser l'algorithme de Schoof ou l'algorithme SEA (Schoof, Elkies et Atkin) dont la complexité est polynomiale.

4.3.4 Étape de choix de la courbe elliptique

Pour une utilisation cryptographique, le choix de la courbe elliptique est lié à la difficulté de résoudre le problème du logarithme discret dans un sous groupe de $E(F_p)$.

- Vérifier que $\#E(F_p) = n.h$, avec $n > 2^{160}$ premier et $1 \le h \le 4$.
- Vérifier que $n \bmod p \neq 0$.
- Vérifier que $p^i \bmod n \neq 1$ pour $1 \le i \le 20$.

4.3.5 Étape de choix de l'ensemble des paramètres

L'ensemble des paramètres $D = (p,(a,b),P,n,h)$, est les données qu'on affiche publiquement dans un annuaire par exemple. Cet ensemble est indispensable dans toute procédure de chiffrement ou de signature.

4.4 les algorithmes implémentés

4.4.1 Algorithme de génération de l'ensemble de paramètres

Input : le corps F_p, un entier $160 \le l \le \lfloor \log_2 p \rfloor$ et $2^l \ge 4\sqrt{p}$ qui fixe le niveau de sécurité.

Output : l'ensemble des paramètres $D = (p, E_{a,b}, P, n, h)$.

1. choisir au hasard deux entiers $a, b \bmod p$.
2. vérifier que $-(27b^2 + 4a^3) \neq 0 \bmod p$. Si non aller à l'étape 1.
3. calculer $\#E(F_p) = N$.
4. vérifier que $N = nh$, avec $n > 2^{160}$ premier et $1 \le h \le 4$. Si non aller à l'étape 1.
5. vérifier que $p^i - 1 \bmod n \neq 0$ pour $1 \le i \le 20$ et $n \neq p$. Si non aller à l'étape 1.
6. choisir au hasard un point fini $P' \in E(F_p)$ et calculer $P = hP'$. Vérifier que $P \neq O$. Si non recommencer.
7. retourner : $(p, E_{a,b}, P, n, h)$.

4.4.2 Algorithme de génération de la paire de clés

Input : l'ensemble des paramètres $D = (p, E_{a,b}, P, n, h)$.

Output : une clé publique Q et une clé privée d.

1. choisir au hasard un entier d tel que $1 < d \leq n-1$.
2. calculer $Q = dP$.
3. retourner : (Q, d).

4.4.3 Algorithme de chiffrement ECC

Input : l'ensemble des paramètres $D = (p, E_{a,b}, P, n, h)$, la clé publique Q et le message $m = (m_1, m_2) \in F_p^* \times F_p^*$.

Output : un cryptogramme (C_1, C_2).

1. choisir au hasard un entier k (secret) tel que $1 < k \leq n-1$.
2. calculer $C_1 = kP$ et $(x, y) = kQ$. Vérifier que $x, y \bmod p \neq 0$. Si non aller à l'étape 1.
3. calculer $u = m_1 x$ et $v = m_2 y$. Soit $C_2 = (u, v)$.
4. retourner : (C_1, C_2).

4.4.4 Algorithme de déchiffrement ECC

Input : l'ensemble des paramètres $D = (p, E_{a,b}, P, n, h)$, la clé privée d et le cryptogramme (C_1, C_2).

Output : le message en clair $m = (m_1, m_2)$.

1. calculer $(x, y) = dC_1$.
2. calculer $m_1 = u \cdot x^{-1} \bmod p$ et $m_2 = v \cdot y^{-1} \bmod p$.
3. retourner : (m_1, m_2).

4.4.5 Algorithme de signature ECDSA

Input : l'ensemble des paramètres $D = (p, E_{a,b}, P, n, h)$, la clé privée d, une fonction de hachage H et le message m.

Output : signature (r, s).

1. choisir au hasard un entier k (secret) tel que $1 < k \leq n-1$.
2. calculer $kP = (x_1, y_1)$
3. calculer $r = x_1 \bmod n$. Vérifier que $r \neq 0$. Si non aller à l'étape 1.
4. calculer $e = H(m)$.
5. calculer $s = k^{-1}(e + dr) \bmod n$. Vérifier que $s \neq 0$. Si non aller à l'étape 1.
6. retourner : (r, s).

4.4.6 Algorithme de vérification de signature ECDSA

In put : l'ensemble des paramètres $D = (p, E_{a,b}, P, n, h)$, la clé publique Q, une fonction de hachage H, le message m et la signature (r, s).

Out put : accepter ou rejeter la signature.

1. vérifier que $1 \leq r, s \leq n-1$. Si non, retourne ''rejeter'' la signature.
2. calculer $e = H(m)$.
3. calculer $w = s^{-1} \bmod n$.
4. calculer $u_1 = e \cdot w \bmod n$ et $u_2 = r \cdot w \bmod n$.
5. calculer $X = u_1 P + u_2 Q$.
6. Si $X = O$, retourne ''rejeter'' la signature.
7. soit $X = (x_1, x_2)$. Calculer $v = x_1 \bmod n$.
8. si $v = r$. Alors, retourne ''accepter'' la signature.

   Si non, retourne ''rejeter'' la signature.

4.5 Description du logiciel

L'application que nous avons réalisée est composée d'une interface principale graphique conviviale, elle est dotée d'une :

- **Barre de menus :** elle propose quatre menus différents comportant diverses commandes.
- **Barre de boutons de raccourcis :** elle reprend les éléments les plus utiles des menus.

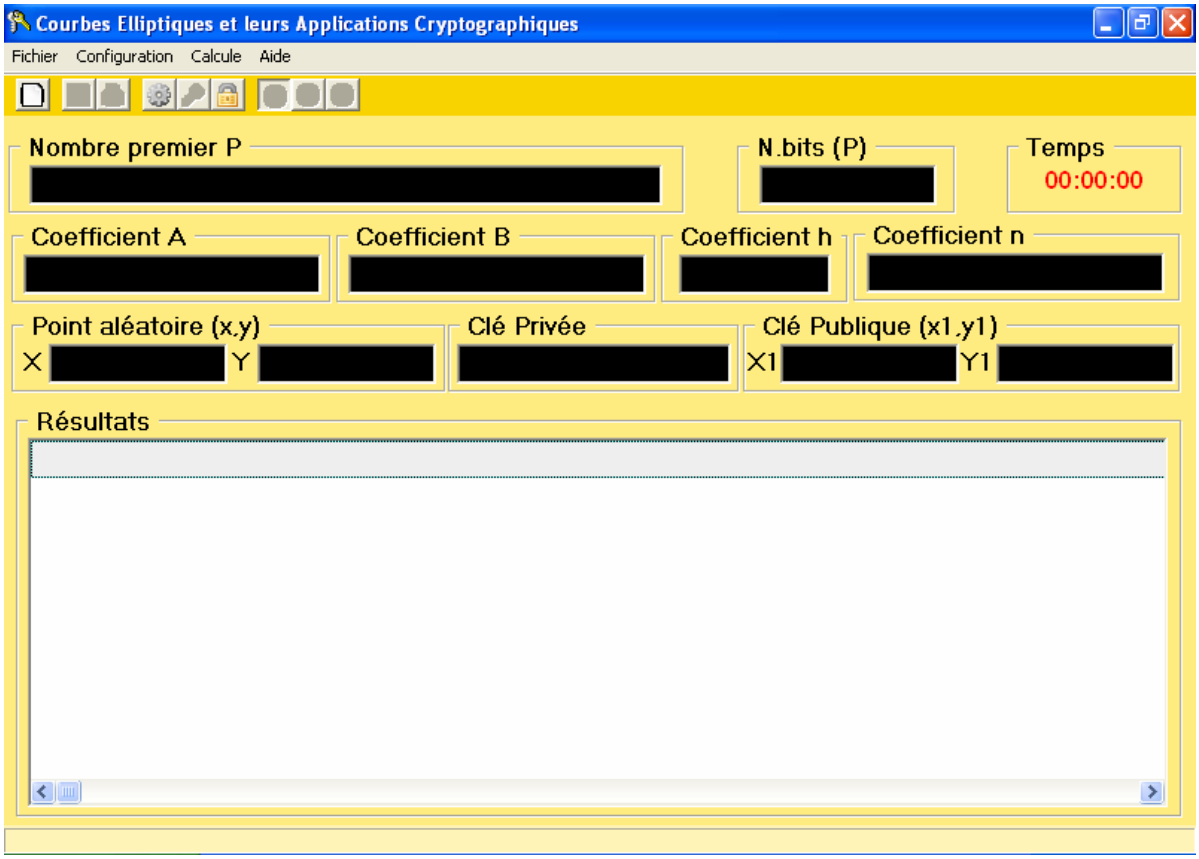


Fig.4.1: Interface principale

4.5.1 Les menus

a. Menu Fichier

Fig.4.2 : menu Fichier

Ce menu permet :

- Nouveau : l'initialisation de l'application
- Enregistrer: l'enregistrement de domaine des paramètres.
- Imprimer : l'impression.
- Quitter : de quitter l'application.

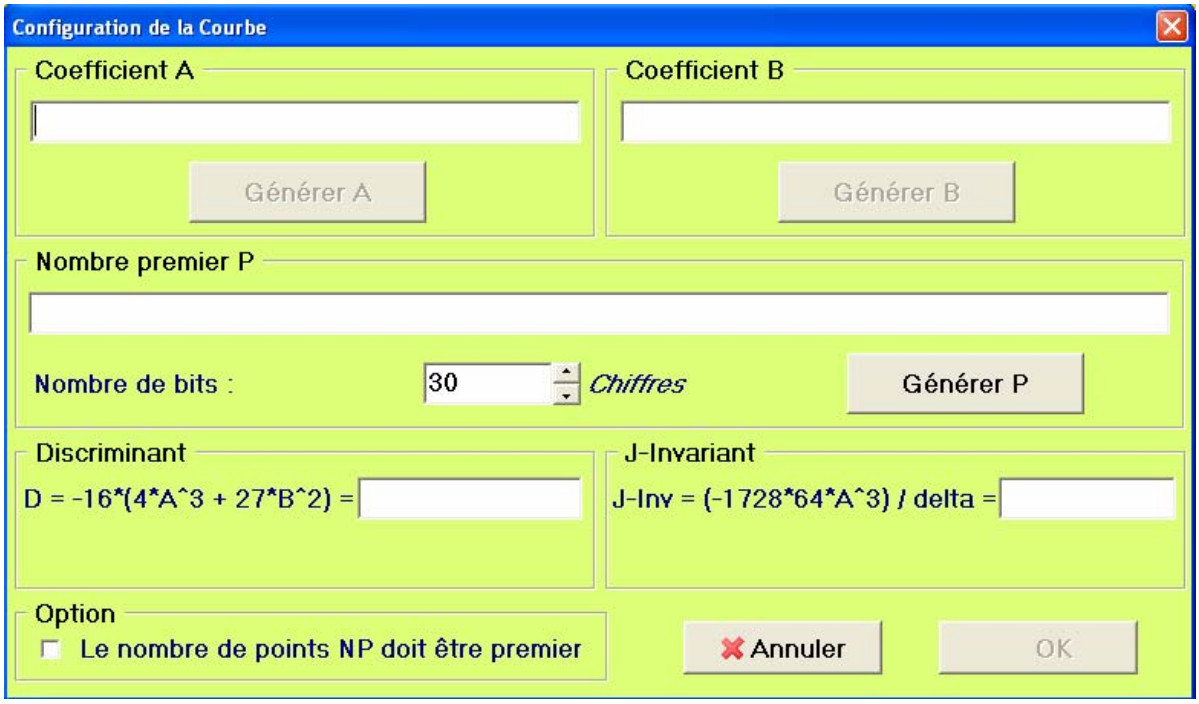
b. menu Configuration

Fig.4.3 : menu Configuration

Ce menu permet :

- Paramètres : de générer aléatoirement les paramètres de départ.
- Générer les clés : la génération des clés (publique/privée)
- Chiffrer/ déchiffrer : de chiffrer et de déchiffrer les messages.

En cliquant sur le bouton paramètre, une boite de dialogue s'affiche. Il suffit maintenant de cliquer sur le bouton générer *p* (voir Fig.4 .4).



,

Fig.4.4 : boite de dialogue ''paramètres''

Une fois que le grand nombre premier p est générer, on clique sur les boutons générer A et générer B pour définir une courbe elliptique qui nous permet d'initialiser l'application (voir Fig.4.5).

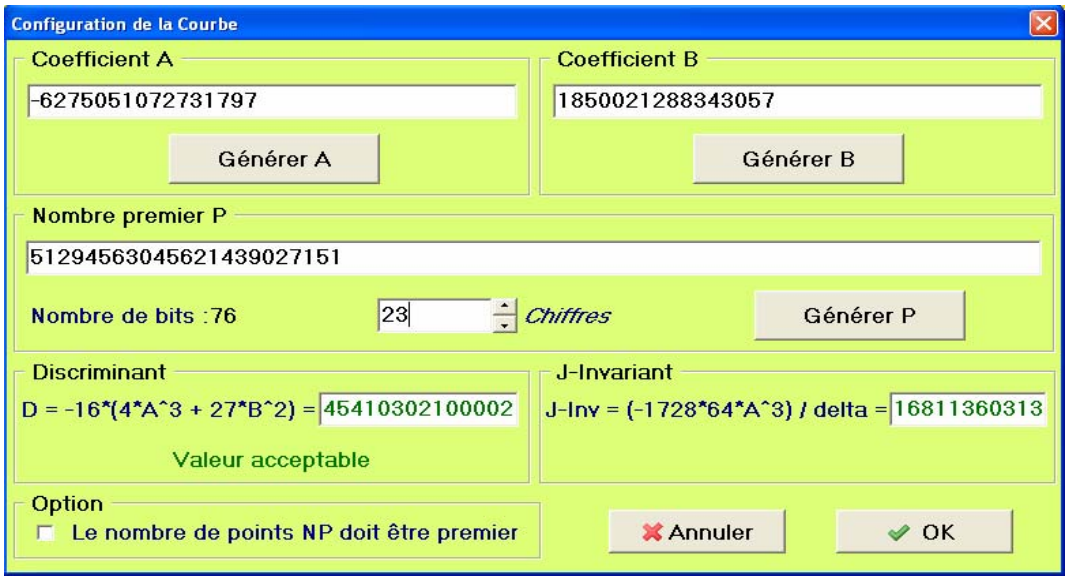


Fig.4.5 : boite de dialogue ''paramètres''

Un simple clique sur le bouton OK, les paramètres A, B, p seront affichés sur l'interface principale.

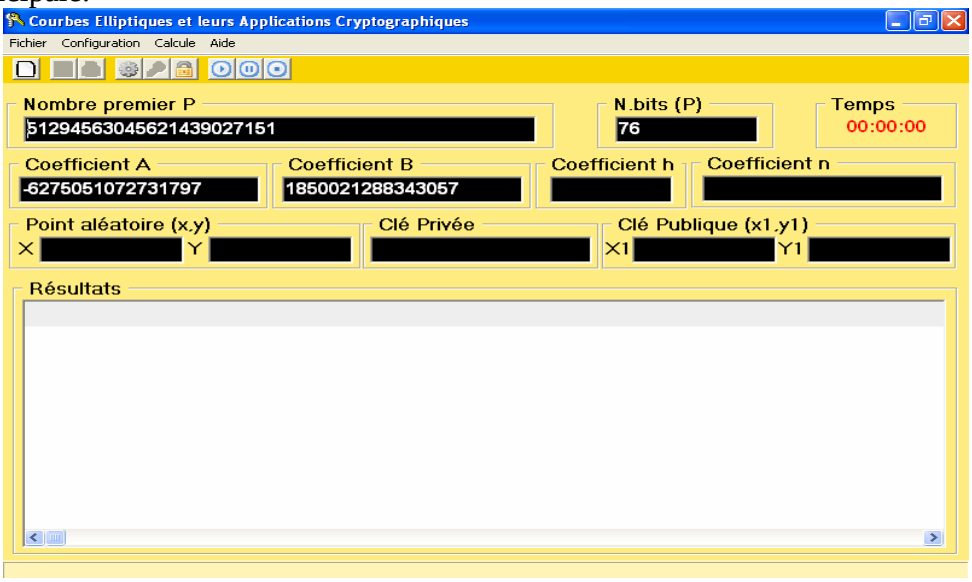


Fig.4.6

c. menu calcule

Ce menu permet :

- Commencer : de lancer l'algorithme de calcul de nombre de points.
- Suspendre : suspendre le calcul (avoir une pause)
- Arrêter : interrompre le calcul.

Fig.4.7 : menu calcule

C'est le menu qui constitue le cœur du logiciel, il nous permet de calculer le nombre de points d'une courbe elliptique bien choisie (voir Fig.4.8 et Fig.4.9). Cliquer sur la commende '' commencer'' de menu calcule.

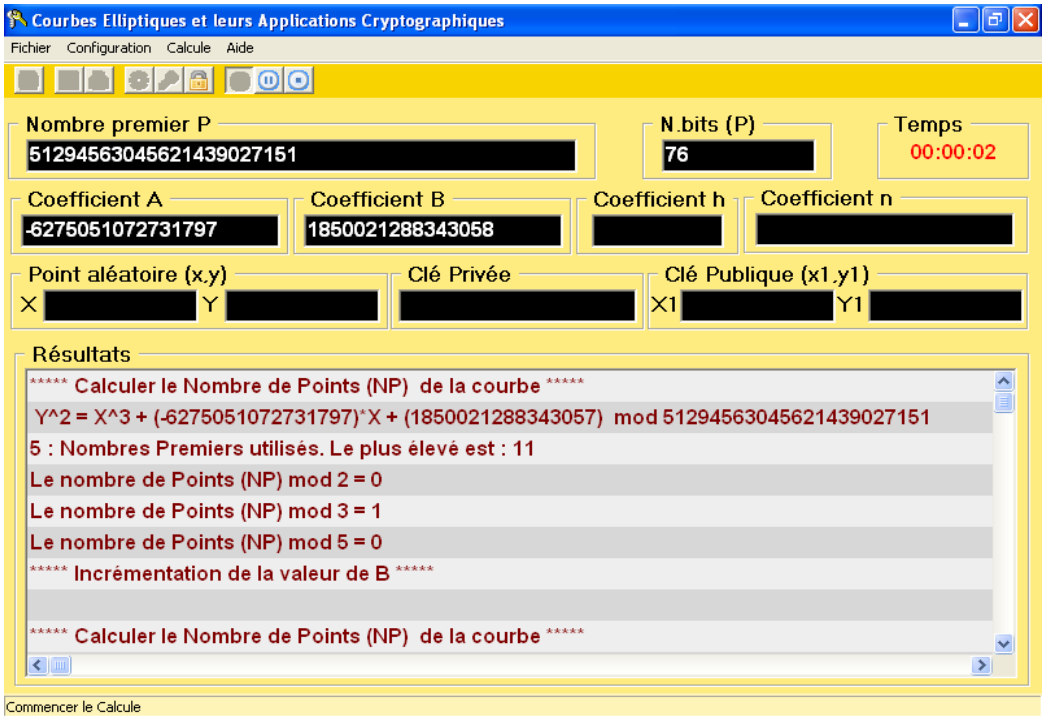


Fig.4.8

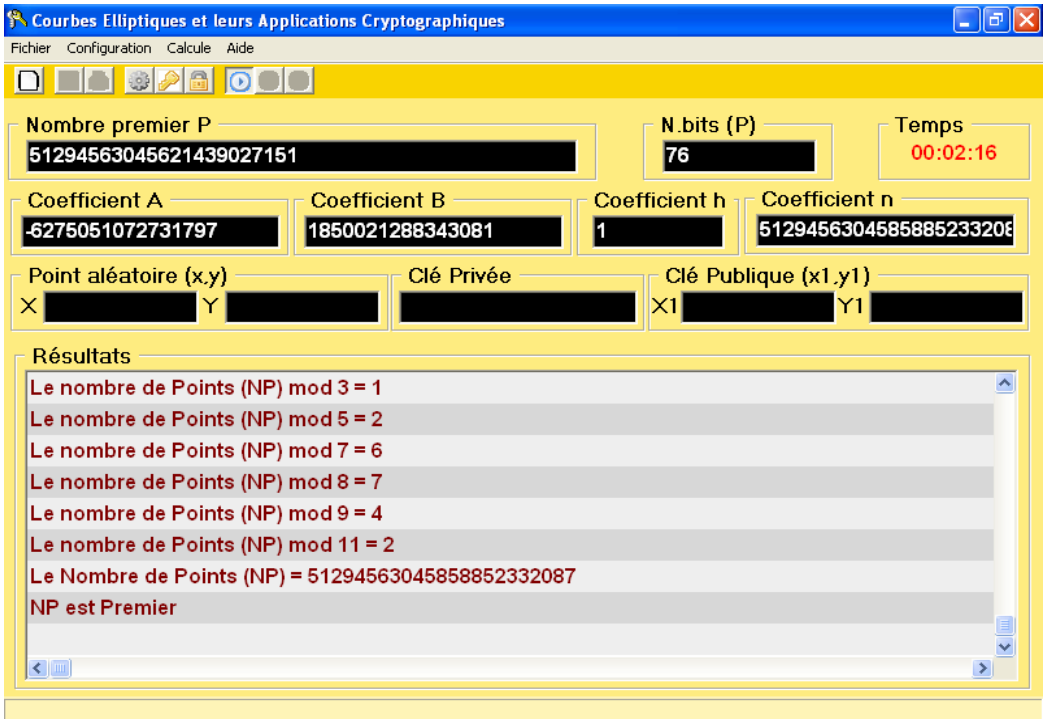


Fig.4.9

Une fois que le nombre de points est calculé, on clique sur la commande ‘’générer les clés’’, la clé privée et la clé publique s’afficheront (voir Fig.4.10).

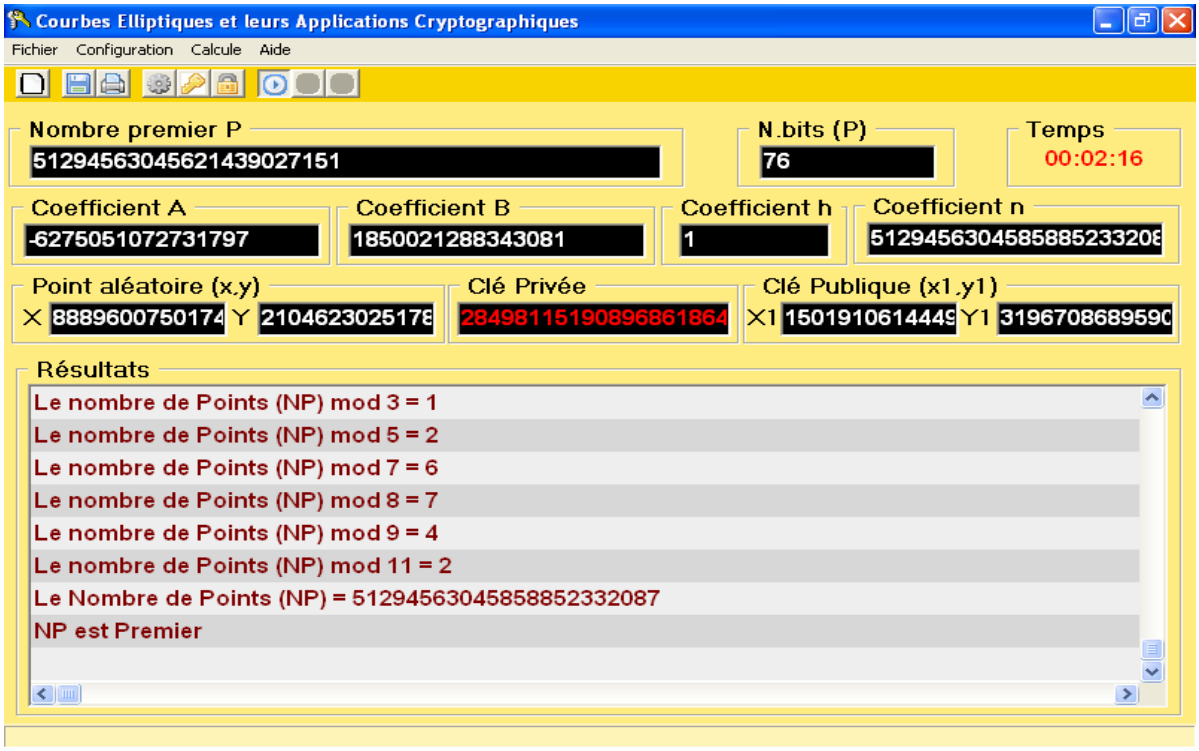


Fig.4.10

Cliquer sur la commande ‘’enregistrer’’. Le domaine des paramètres, la clé publique et la clé privée seront enregistrés automatiquement sur un fichier clés, toute en gardant la clé privée secrète.

Maintenant, nous somme en mesure d’envoyer des messages cryptés à toute personne propriétaire d’une clé publique donnée.

Pour entamer la procédure de chiffrement :
Cliquer sur la commande ‘’chiffrer/déchiffrer’’, une boite de dialogue s’affiche (voir Fig.4.11).
Incérer le texte clair dans la zone ‘’message en clair’’ (voir Fig.4.12).

Fig.4.11

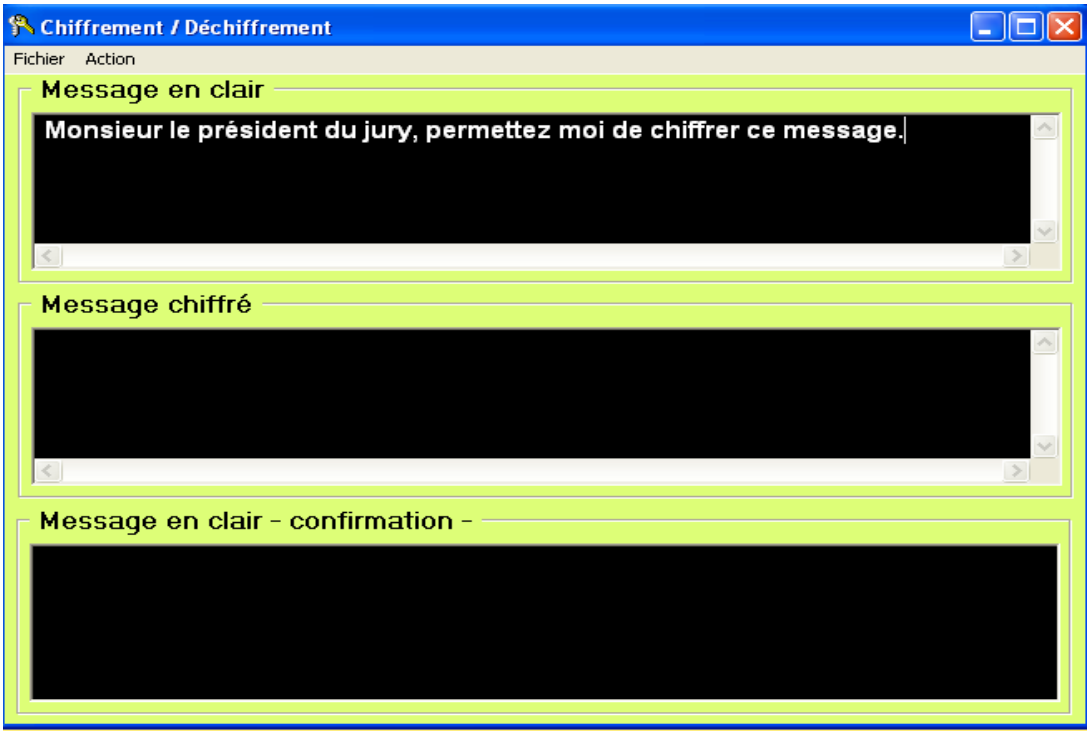


Fig.4.12

Ensuite cliquer sur le sous menu ‘’Fichier’’ et sélectionner le domaine des paramètres ainsi que la clé publique du destinataire (voir Fig.4.13).

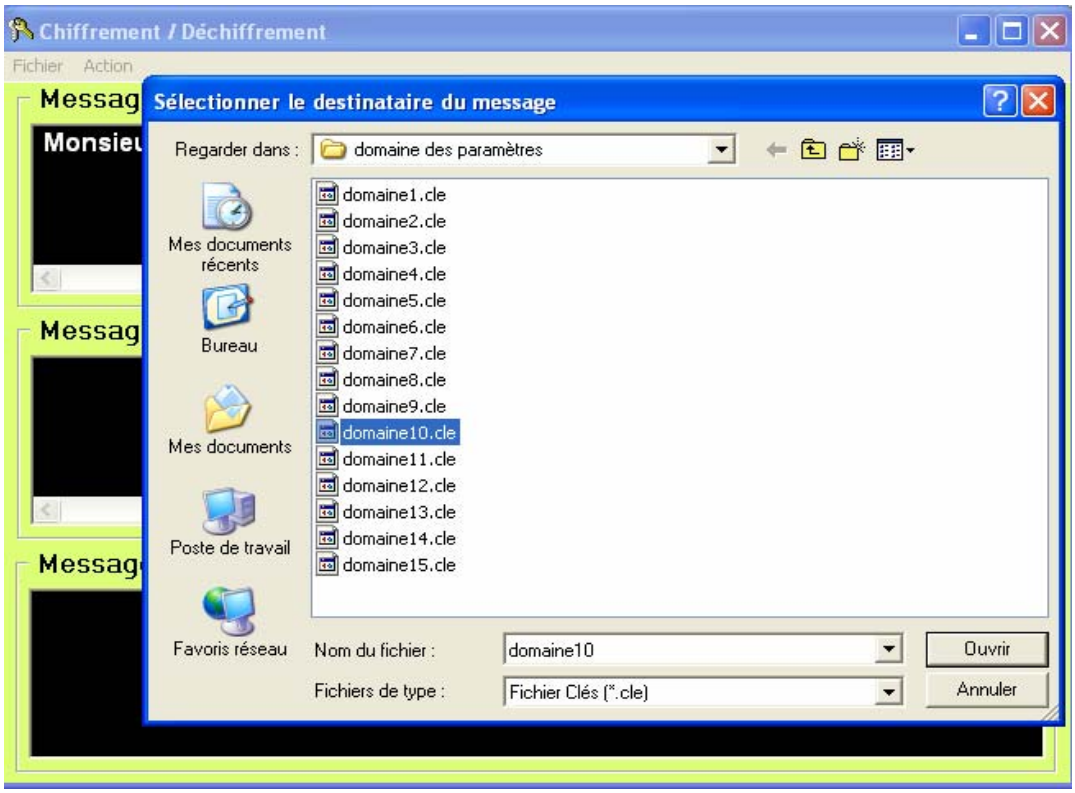


Fig.4.13

Enfin, cliquer sur le sous menu ‘’Action’’ puis sélectionner ‘’chiffrer’’ pour chiffrer un message ou ‘’déchiffrer’’ pour déchiffrer un message (voir Fig.4.14 et Fig.4.15).

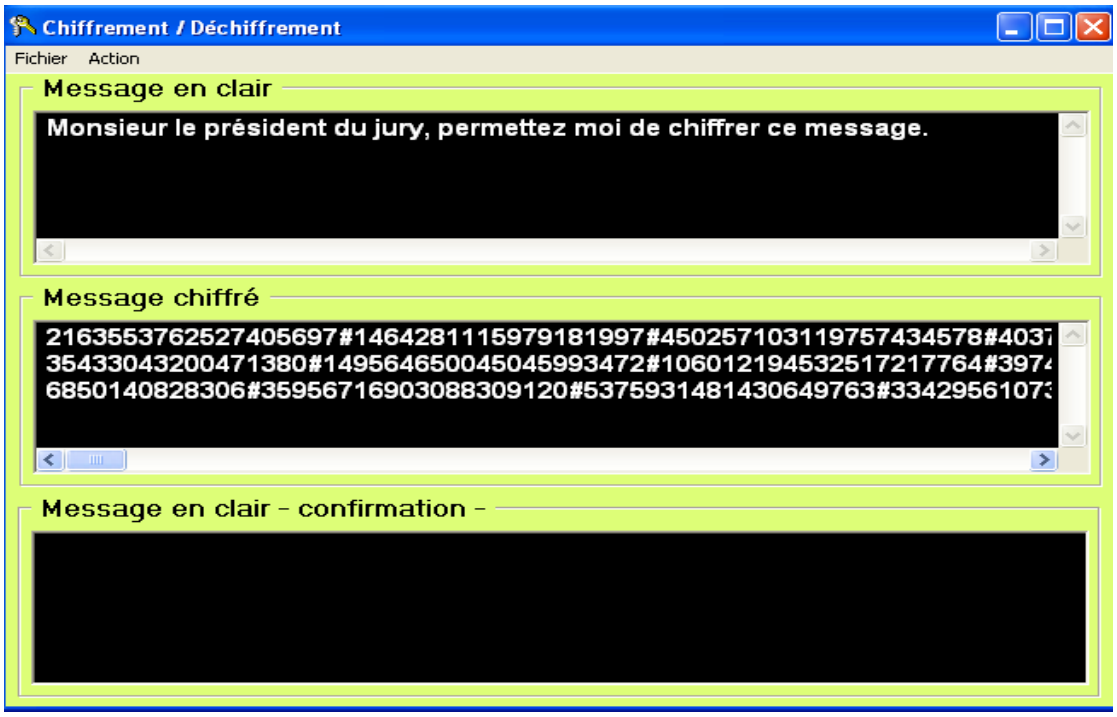


Fig.4.14

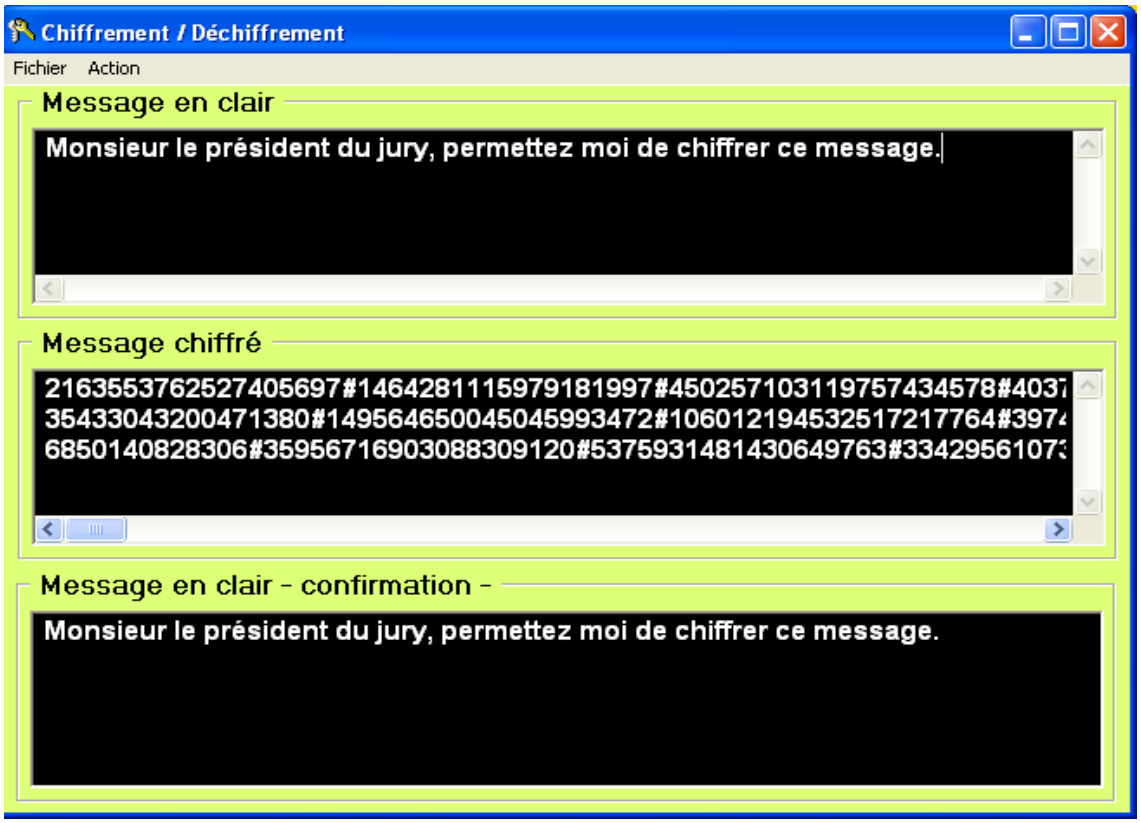

Chiffrement / Déchiffrement
Fichier Action
Message en clair
Monsieur le président du jury, permettez moi de chiffrer ce message.
Message chiffré
216355376252740569 7#14642811159791819 97#450257103119757434578#403
354330432004713 80#14956465004504599 3472#106012194532517217764#397
685014082830 6#359567169030883091 20#537593148143064976 3#3342956107
Message en clair - confirmation -
Monsieur le président du jury, permettez moi de chiffrer ce message.

Fig.4.15

Conclusion

Ce travail nous a permis d'améliorer nos connaissances en la théorie des courbes elliptiques, de voire concrètement la façon dont elles sont utilisées en cryptographie et dans quelles conditions elles offrent une meilleure sécurité. D'autre part, savoir pourquoi dans un monde dominé par la cryptographie RSA, ces dernières deviennent à terme une alternative crédible en particulier dans le domaine de la miniaturisation.

En effet, le RSA est actuellement le système de cryptographie à clé publique le plus utilisé. Néanmoins, nous avons déjà vu que les courbes elliptiques présentaient un certain nombre d'avantages que nous allons expliciter.

Tous ces avantages sont basés sur la différence de complexité pour résoudre les problèmes mathématiques sous-jacents. D'un coté la factorisation (et donc RSA) peut être effectuée à l'aide d'algorithmes sous-exponentiels tandis que de l'autre coté seuls des algorithmes exponentiels permettent de résoudre le problème du logarithme discret sur une courbe elliptique. Cela à pour première conséquence que les clés sont plus courtes avec ECC qu'avec RSA. Typiquement, actuellement une clé inviolable doit avoir 1024 bits pour RSA contre 163 pour ECC. Mais le phénomène le plus remarquable est que cette différence de taille de clé va aller en s'amplifiant avec le temps du fait de la différence de complexité.

Ainsi les premières applications des courbes elliptiques ont été conçues pour des environnements restreints (PDA, téléphones mobiles, cartes à puces,…) qui ont peu de puissance de calcul (par exemple, traiter du 1024 bits avec un processeur 8 bits demande une multiprécision lourde) et surtout peu de mémoire disponible.

Plus précisément on ne peut pas vraiment dire que ECC soit toujours plus efficace que RSA. En effet, dans la pratique courante, on observe que ECC est beaucoup plus rapide que RSA pour déchiffrer ou signer un message (facteur 4 à 20) c'est-à-dire opérations privées alors que pour chiffrer ou vérifier une signature (opérations publiques), RSA est beaucoup plus rapide. En fait ECC met à peu près le même temps pour tout alors que RSA est beaucoup plus déséquilibré. Cela est dû au fait qu'avec RSA les gens choisissent en général $e = 3$ comme exposant publique (bien que ce soit reconnu que c'est une faille majeure de RSA). Par contre les opérations privées sont beaucoup plus longues car elles utilisent cette fois comme exposant l'inverse de $e \bmod (p-1)(q-1)$ qui lui pèse bien ces 1024 bits. Pour finir, il est intéressant de noter que la génération de clé (trouver deux nombres premiers pour RSA, trouver un point sur la courbe pour ECC) est beaucoup plus rapide pour ECC.

Bibliographies

[1] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer,1986.

[2] I.R. Shafarevich. Basic algebraic geometry. Springer 1977

[3] H. Cohen. A Course in computational algebraic number theory. Springer 1993

[4] L.C. Washington. Elliptic curves number theory and cryptography. Champman and Hall/CRC, 2003

[5] Douglas Stinson. Cryptographie théorie et pratique. I.T.P France, Paris, 1986

[6] N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48(177) :203–209, January 1987.

[7] N. Koblitz. Primality of the number of points on an elliptic curve over a finite field. *Pacific Journal of Mathematics*, 131(1) :157–165, 1988.

[8] N. Koblitz. Elliptic curve implementation of zero-knowledge blobs. *Journal of Cryptology*, 4(3) :207–213,1991

[9] L. M. Adleman, R. L. Rivest, and A. Shamir. A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM*, 21(2) :120–126, 1978.

[10] A. O. L. Atkin. The number of points on an elliptic curve modulo a prime, 1988. Email on the Number Theory Mailing List.

[11] A. O. L. Atkin. The number of points on an elliptic curve modulo a prime, 1991. Email on the Number Theory Mailing List.

[12] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comp.*, 61(203) :29–68, July1993

[13] E. W. Howe. On the group orders of elliptic curves over finite fields. *Compositio Mathematica*, 85 :229–247,1993

[14] D. Husemöller. *Elliptic curves*, volume 111 of *Graduate Texts in Mathematics*. Springer, 1987.

[15] G. J. Lay and H. G. Zimmer. Constructing elliptic curves with given group order over large finite fields. In L. Adleman and M.-D. Huang, editors, *ANTS-I*, volume 877 of *Lecture Notes in Comput. Sci.*, pages 250–263. Springer-Verlag, 1994. 1st Algorithmic Number Theory Symposium - Cornell University, May 6-9, 1994.

[16] D. H. Lehmer. Euclid's algorithm for large numbers. *American Mathematical Monthly*, 45 :227–233, 1938.

[17] A. Menezes, T. Okamoto, and S. A. Vanstone. Reducing elliptic curves logarithms to logarithms in a finite field. *IEEE TIT*, 39(5) :1639–1646, 1993.

[18] A. Menezes and S. A. Vanstone. The implementation of elliptic curve cryptosystems. In J. Seberry and J. Pieprzyk, editors, *Advances in Cryptology*, number 453 in Lecture Notes in Comput. Sci., pages 2–13.
Springer–Verlag, 1990. Proceedings Auscrypt '90, Sysdney (Australia), January 1990.

[19] A. J. Menezes. *Elliptic curve public key cryptosystems*. Kluwer Academic Publishers, 1993.

[20] A. J. Menezes, S. A. Vanstone, and R. J. Zuccherato. Counting points on elliptic curves over F_{2^m}. *Math. Comp.*, 60(201) :407–420, January 1993.

[21] V. Miller. Use of elliptic curves in cryptography. In A. M. Odlyzko, editor, *Advances in Cryptology*, volume 263 of *Lecture Notes in Comput. Sci.*, pages 417–426. Springer-Verlag, 1987. Proceedings Crypto '86, Santa Barbara (USA), August11–15, 1986.

[22] R. Schoof. Nonsingular plane cubic curves over finite fields. *J. Combin. Theory Ser.*, 46 :183–211, 1987.

[23] R. Schoof. Counting points on elliptic curves over finite fields. *J. Théor. Nombres Bordeaux*, 7 :219–254,
1995. Available at http://www.emath.fr/Maths/Jtnb/jtnb1995-1.html.

[24] Gilles Zemor, cours de cryptographie Paris : Cassini 2000.

[25] H. Babier. How to find elliptic curve groups of prime order. Technical raport, Darmstadt university of technology, 2002.

[26] M. Agrawal, N. Kyal, and N. Sexina. Prime is in P. available via WWW from http://www.cse.iitk.ac.in/primality.pdf, August 2002.

[27] Etienne Foury, Théorème de Brun-Titchmarsh; application au théorème de Fermat, Invent. Math. 79, 383-407, 1985.

[28] Morris Goldfeld, On the number of primes p for which $p + a$ has a large prime factor, Mathématika 16, pp. 23-27, 1969.