UNIVERSITE ASSANE SECK DE ZIGUINCHOR

UFR DES SCIENCES ET TECHNOLOGIES

DEPARTEMENT DE MATHEMATIQUES

Mémoire de Master

DOMAINE	:	Sciences et Technologies
MENTION	:	Mathématiques et Applications
SPÉCIALITÉ	:	Mathématiques Pures
OPTION	:	Géométrie Algébrique

Thème :

Problème du Logarithme Discret

Présenté par : Raymond DIATTA

Sous la direction de : Professeur Oumar SALL

Devant le jury ci-après :

Prénom(s) et Nom	**Grade**	**Qualité**	**Établissement**
Marie Salomon SAMBOU	Professeur titulaire	Président du jury	UASZ
Amoussou Thomas GUEDENON	Professeur assimilé	Examinateur	UASZ
Daouda Niang DIATTA	Maître de conférences	Examinateur	UASZ
Moussa FALL	Maître de conférences	Examinateur	UASZ
Oumar SALL	Professeur titulaire	Directeur	UASZ

Année universitaire 2019-2020

Problème du Logarithme Discret

Raymond DIATTA

30 janvier 2021

Table des matières

Remerciements

La réalisation de ce mémoire a été possible grâce au concours de plusieurs personnes à qui je voudrais témoigner toute ma gratitude.

Je voudrais tout d'abord adresser toute ma reconnaissance au directeur de ce mémoire, Monsieur Oumar SALL, pour l'encadrement dont j'ai bénéficié de sa part tout au long de ce travail. Je le remercie pour sa disponibilité, ses remarques pertinentes et enrichissantes, ses recadrages et surtout ses judicieux conseils, qui ont contribué à alimenter ma réflexion.

Je suis honoré par la présence de Monsieur Marie Salomon SAMBOU qui a accepté de présider le jury de mon mémoire et je le remercie sincèrement.

Je souhaite remercier Monsieur Oumar SALL, Monsieur Marie Salomon SAMBOU, Monsieur Amoussou Thomas GUEDENON, Monsieur Daouda Niang DIATTA et Monsieur Moussa FALL pour avoir accepté de faire parti du jury.

Mes remerciements vont à l'endroit de tous les professeurs du département de mathématiques de l'Université Assance SECK de Ziguinchor, pour la qualité de l'enseignement qu'ils nous ont dispensé.

Je remercie Monsieur Moussa FALL et Monsieur Eramane BODIAN pour avoir accepté de faire une relecture de mon mémoire et pour leurs pertinentes suggestions.

Je dédie un merci particulier à Souhaibou SAMBOU, à Moustapha CAMARA, à Papa BADIANE, à Nestor DJINTELBE, à Abdoulaye DIOUF, à Pape Modou SARR, à Marcel Sihintoé BADIANE, à Agack Alain DIEDHIOU pour leurs suggestions remarquables sur plusieurs points dans ce mémoire, pour leurs encouragements et leurs conseils pratiques tout au long de ce travail.

Je dédie également un merci particulier à mon ami Souleymane BA qui m'a aidé dans l'implémentation des algorithmes de la partie annexe.

Je tiens à témoigner toute ma reconnaissance à la Sœur Montserrat DAUSA PLANS pour son aide durant tout mon cursus scolaire depuis le collège Saint Joseph de Brin jusqu'à l'obtention de mon baccalauréat.

Je remercie tous les gens qui m'ont aidé moralement, intellectuellement et financièrement de près ou de loin à réaliser ce travail. Je n'oublie pas : Madeleine DIATTA, Pathé BA, Bienvenu Paul Alain NDIAYE.

Notations et Abréviations

min	Minimum
i.e.	C'est-à-dire
$\nmid$	Ne divise pas
$[\![ ]\!], [\![[\![$	Intervalles d'entiers
$\overline{\mathbf{K}}$	clôture algébrique de $\mathbf{K}$
■	Marque la fin d'une preuve
PLD	Problème du Logarithme Discret

Introduction

Etymologiquement, le mot cryptographie [1] provient du grec : **kruptos** (*Caché*) et **graphein** (*écrire*). Le cryptographe essaie donc de mettre en place des systèmes cryptographiques ou cryptosystèmes, fiables pour chiffrer (ou sécuriser) des messages circulant dans un réseau de communication. De son côté, le cryptanalyste [2] tente de disséquer le système utilisé afin de trouver des failles et d'obtenir une information à partir du message codé, appelé cryptogramme. *Cryptographie* et *Cryptanalyse* font tous deux partie du domaine général qu'est *la cryptologie : la science du secret.*

Après plusieurs lectures d'articles tels que : le rapport de *Aude LE GLUHER*, les articles de *Christophe Delaunay et de Vanessa Vitse sur le site Images des Mathématiques* (www.images.math.cnrs.fr) qui parlent de la *cryptanalyse*, discipline dont l'objectif est de retrouver le sens d'un message crypté sans en être le destinataire, nous a motivé à s'intéresser au problème mathématique dit du **logarithme discret**. Ce dernier est en effet sous-jacent à la cryptanalyse de nombreux cryptosystèmes et en particulier à la cryptanalyse sur courbes elliptiques.

Ce travail est structuré en trois chapitres :
Le premier chapitre de ce travail rassemble *les notions fondamentales* pour la bonne compréhension du sujet proprement dit.
Le second chapitre se rapporte à la *présentation du problème du logarithme discret dans les groupes multiplicatifs et quelques méthodes de résolution de ce problème qui sont : la recherche exhaustive, l'algorithme Baby-Steps/Giant-Steps et l'algorithme de Pohlig-Hellman.*
Le troisième et dernier chapitre aborde *le problème du logarithme dicret sur les courbes elliptiques* avec comme méthode de résolution : *l'algorithme MOV.*

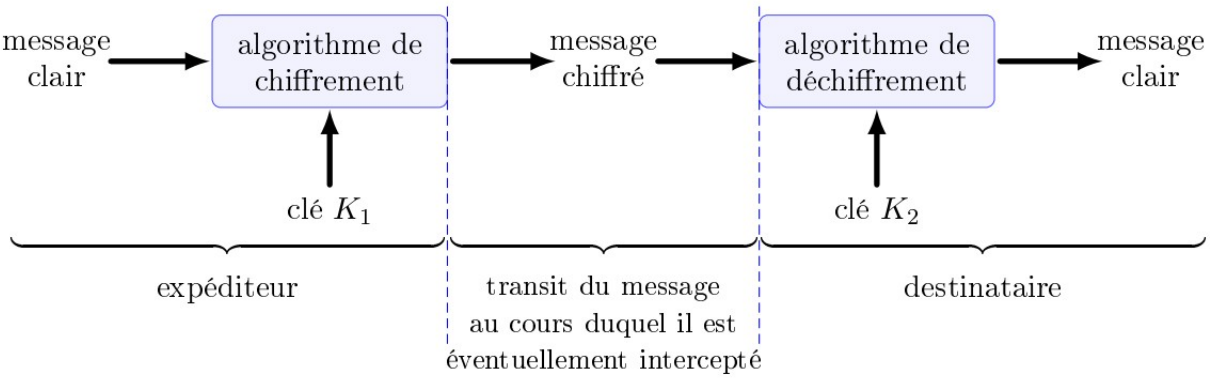
Certains résultats du premier chapitre ne sont pas démontrés ici. Une partie implémentation et quelques résultats se trouvent en annexe. Les codes ont été implémentés en langage python.

1. C'est une branche qui regroupe l'ensemble des méthodes qui permettent de chiffrer et de déchiffrer un texte en clair afin de le rendre incompréhensible pour quiconque n'est en possesion de la clé à utiliser pour le déchiffrer.

2. Un cryptanalyste est un spécialiste de la cryptanalyse. La cryptanalyse est l'art de révéler les textes en clair qui ont fait l'objet d'un chiffrement sans connaître la clé utilisé pour chiffrer le texte en clair.

VOCABULAIRE CRYPTOGRAPHIQUE

Dans tout ce travail, un message ou un texte sera qualifié de *clair* avant traitement cryptographique et est dit *chiffré* après traitement cryptographique. Un *chiffre* est un couple formé d'un algorithme, c'est-à-dire un procédé de cryptage général et d'une *clé*, paramètre spécifiant un algorithme de chiffrement. Selon le principe de Kerckhoffs [3] : la sécurité d'un système de cryptage ne repose que sur le secret de la clé.
Traditionnellement, l'expéditeur de message chiffré se nomme Alice, le destinataire Bob et l'adversaire qui souhaite déchiffrer le message Eve (Eve est souvent appelé *l'homme du milieu* (HDM) ou *man-in-the-middle*). Si Alice et Bob souhaitent échanger un message sans que celui-ci soit compréhensible par Eve, ils procèdent de la manière suivante :



Dans *la cryptographie (à clé) symétrique* [4], $K_1 = K_2$; dans *la cryptographie (à clé) asymétrique* [5], $K_1 \neq K_2$.

NB : Le gros inconvénient de la cryptographie symétrique est qu'avant d'échanger un secret, Alice et Bob doivent déjà en partager un : ils doivent s'être mis d'accord sur une clé. C'est pourquoi les chiffres utilisés en pratique, tels que RSA, sont asymétriques. Ici, nous ne travaillerons qu'avec des chiffres asymétriques.

3. C'est le principe qui exprime que la sécurité d'un cryptosystème ne doit reposer que sur le secret de la clef. Autrement dit, tous les autres paramètres doivent être supposés publiquement connus.

4. Aussi appelée *cryptographie à clé secrète*, c'est la cryptographie qui utilise la même clé pour les processus de codage et de décodage ; cette clé est le plus souvent appelée "secrète" (en opposition à "privée") car toute la sécurité de l'ensemble est directement liée au fait que cette clé n'est connue que par l'expéditeur et le destinataire.

5. Par opposition à la cryptographie symétrie, dans la cryptographie asymétrique la clé qui sert au chiffrement est différente de celle qui sert à déchiffrer. Dans ce cas, on parlera de clé privée et de clé publique. Ces deux clés sont intimement liées par une fonction mathématique complexe.

Chapitre 1

Prérequis

1.1 Division Euclidienne et PGCD

1.1.1 Divisibilité et division euclidienne

Défnition 1.1.1

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{Z}^\star$. On dit que b divise a et on note $b \mid a$ s'il existe $q \in \mathbb{Z}$ tel que :

$$a = bq.$$

Théorème 1.1.1 (Division Euclidienne)

Soient $a \in \mathbb{Z}$ et $b \in \mathbb{N}^\star$. Il existe des entiers q, $r \in \mathbb{Z}$ tels que :

$$a = bq + r \text{ et } 0 \leq r < b$$

De plus q et r sont uniques.

Terminologie : q est le quotient et r est le reste.
Nous avons donc l'équivalence : $r = 0$ si et seulement si b divise a.

1.1.2 PGCD de deux entiers

Défnition 1.1.2

Soient a et $b \in \mathbb{Z}$, deux entiers non tous les deux nuls. Le plus grand entier qui divise à la fois a et b s'appelle le plus grand commun diviseur de a et de b. On le note $PGCD\,(a, b)$.

1.1.3 Algorithme d'Euclide

Lemme 1.1.1

Soient a, $b \in \mathbb{N}^\star$. Écrivons la division euclidienne $a = bq + r$. Alors

$$\boxed{PGCD\ (\ a,\ b\ ) = PGCD\ (\ b,\ r\ )}$$

En fait on a même $PGCD\,(a,b) = PGCD\,(b, a-qb)$ pour tout $q \in \mathbb{Z}$. Mais pour optimiser l'algorithme d'Euclide on applique le lemme avec q le quotient.

Preuve:

Nous allons montrer que les diviseurs de a et de b sont exactement les mêmes que les diviseurs de b et r. Cela impliquera le résultat car les plus grands diviseurs seront bien sûr les mêmes.

- Soit d un diviseur de a et de b. Alors d divise b donc aussi bq, en plus d divise a donc d divise $a - bq = r$.
- Soit d un diviseur de b et de r. Alors d divise aussi $bq + r = a$.

■

Algorithme d'Euclide :
On souhaite calculer le $PGCD$ de a, $b \in \mathbb{N}^\star$. On peut supposer $a \geq b$. On calcule des divisions euclidiennes successives. Le PGCD sera le dernier reste non nul.

- division de a par b, $a = bq_1 + r_1$. Par le **lemme** 1.1.1, $PGCD(a,b) = PGCD(b, r_1)$ et si $r_1 = 0$ alors $PGCD(a,b) = b$ sinon on continue :
- $b = r_1 q_2 + r_2$, $PGCD(a,b) = PGCD(b, r_1) = PGCD(r_1, r_2)$,
- $r1 = r_2 q_3 + r_3$, $PGCD(a,b) = PGCD(r_2, r_3)$,

  $\vdots$
- $r_{k-2} = r_{k-1} q_k + r_k$, $PGCD(a,b) = PGCD(r_{k-1}, r_k)$,
- $r_{k-1} = r_k q_k + 0$, $PGCD(a,b) = PGCD(r_k, 0) = r_k$.

Comme à chaque étape le reste est plus petit que le quotient on sait que $0 \leq r_{i+1} < r_i$. Ainsi l'algorithme se termine car nous sommes sûrs d'obtenir un reste nul, les restes formant une suite décroissante d'entiers positifs ou nuls : $b > r_1 > r_2 > \cdots \geq 0$.

Exemple 1.1.1

Calculons le $PGCD$ de $a = 600$ et $b = 124$.

$$\begin{array}{rcrcrcr} 600 & = & 124 & \times & 4 & + & 104 \\ 124 & = & 104 & \times & 1 & + & 20 \\ 104 & = & 20 & \times & 5 & + & 4 \\ 20 & = & 4 & \times & 5 & + & 0 \end{array}$$

Ainsi $PGCD(600, 124) = 4$.

Voici un deuxième exemple :

Exemple 1.1.2

Calculons $PGCD(9945, 3003)$.

$$\begin{array}{rcrcrcr} 9945 & = & 3003 & \times & 3 & + & 936 \\ 3003 & = & 936 & \times & 3 & + & 195 \\ 936 & = & 195 & \times & 4 & + & 156 \\ 195 & = & 156 & \times & 1 & + & 39 \\ 156 & = & 39 & \times & 4 & + & 0 \end{array}$$

Ainsi $PGCD(9945, 3003) = 39$.

1.1.4 Nombres premiers entre-eux

Défnition 1.1.3

Deux entiers a, b sont premiers entre-eux si $PGCD(a, b) = 1$.

1.2 Théorème de Bézout

1.2.1 Théorème de Bézout

Théorème 1.2.1 ***(Théorème de Bézout)***

Soient a, b des entiers. Il existe des entiers u, v tels que :

$$au + bv = PGCD(a, b)$$

Preuve:

La preuve découle de l'algorithme d'Euclide. Les entiers u, v ne sont pas uniques. Les entiers u, v sont appelés : **coefficients de Bézout**. Ils s'obtiennent en « remontant » l'algorithme d'Euclide.

■

1.2.2 Corollaires du théorème de Bézout

Corollaire 1.2.1

Soient a, $b \in \mathbb{Z}$ et $d \in \mathbb{Z}^*$.
Si $d \mid a$ et $d \mid b$ alors $d \mid PGCD(a, b)$.

Preuve:

Soient a, $b \in \mathbb{Z}$. D'après le **théorème de Bézout**1.2.1, il existe u, $v \in \mathbb{Z}$ tels que $PGCD(a, b) = au + bv$.
Comme $d \mid au$ et $d \mid bv$ donc $d \mid au + bv$. Par le théorème de Bézout $d \mid PGCD(a, b)$.

■

Exemple 1.2.1

$4 \mid 16$ *et* $4 \mid 24$ *donc* 4 *doit diviser* $PGCD(16, 24)$ *qui effectivement vaut* 8.

Corollaire 1.2.2

Soient a, b deux entiers. a et b sont premiers entre-eux si et seulement s'il existe u, $v \in \mathbb{Z}$ tels que :

$$au + bv = 1$$

Preuve:

La condition nécessaire est une conséquence du théorème de Bézout.
Pour **la condition suffisante** on suppose qu'il existe u, v tels que $au + bv = 1$. Comme $PGCD(a, b) \mid a$ alors $PGCD(a, b) \mid au$.
De même $PGCD(a, b) \mid bv$. Donc $PGCD(a, b) \mid au + bv = 1$. Donc $PGCD(a, b) = 1$.

■

Corollaire 1.2.3 (Lemme de Gauss)

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

$$\textit{Si } a \mid bc \textit{ et } PGCD(a,b) = 1 \textit{ alors } a \mid c$$

Preuve:

Comme $PGCD(a,b) = 1$ alors il existe u, $v \in \mathbb{Z}$ tels que $au + bv = 1$. On multiplie cette égalité par c pour obtenir $acu + bcv = c$. Mais $a \mid acu$ et par hypothèse $a \mid bcv$ donc a divise $acu + bcv = c$.

■

Exemple 1.2.2

si $4 \mid 7 \times c$, *et comme* 4 *et* 7 *sont premiers entre-eux, alors* $4 \mid c$.

1.3 Nombres premiers

Les nombres premiers sont en quelque sorte les briques élémentaires des entiers : tout entier s'écrit comme produit de nombres premiers.

1.3.1 Une infinité de nombres premiers

Défnition 1.3.1

Un nombre premier p est un entier $n \geq 2$ dont les seuls diviseurs positifs sont 1 *et* p.

Exemple 1.3.1

2, 3, 5, 7, 11 *sont premiers,* $4 = 2 \times 2$, $6 = 2 \times 3$, $8 = 2 \times 4$ *ne sont pas premiers.*

Lemme 1.3.1

Tout entier $n \geq 2$ admet un diviseur qui est un nombre premier.

Preuve:

Soit $\mathcal{D}$ l'ensemble des diviseurs de n qui sont ≥ 2 :

$$\mathcal{D} = \{k \geq 2 \text{ où } k|n\}.$$

L'ensemble $\mathcal{D}$ est non vide (car $n \in \mathcal{D}$), notons alors $p = \min \mathcal{D}$.
Supposons, par l'absurde, que p ne soit pas un nombre premier, alors p admet un diviseur q tel que $1 < q < p$ mais alors q est aussi un diviseur de n et donc $q \in \mathcal{D}$ avec $q < p$. Ce qui donne une contradiction car p est le minimum.
Conclusion : p est un nombre premier. Et comme $p \in \mathcal{D}$, p divise n.

■

Proposition 1.3.1

Il existe une infinité de nombres premiers.

1.3.2 Eratosthène et Euclide

Comment trouver les nombres premiers ?
Le **crible d'Eratosthène** permet de trouver les premiers nombres premiers. Pour cela on écrit les premiers entiers : pour notre exemple de 2 à 25.

2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

Rappelons-nous qu'un diviseur positif d'un entier n est inférieur ou égal à n. Donc 2 ne peut avoir comme diviseurs que 1 et 2 et est donc premier. On entoure 2. Ensuite on raye (ici en grisé) tous les multiples suivants de 2 qui ne seront donc pas premiers (car divisible par 2) :

2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

Le premier nombre restant de la liste est 3 et est nécessairement premier : il n'est pas divisible par un diviseur plus petit (sinon il serait rayé). On entoure 3 et on raye tous les multiples de 3 $(6, 9, 12, \cdots)$.

2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

Le premier nombre restant est 5 et est donc premier. On raye les multiples de 5.

2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

7 est donc premier, on raye les multiples de 7 (ici pas de nouveaux nombres à barrer). Ainsi de suite : 11, 13, 17, 19, 23 sont premiers.

2 3 4 5 6 7 8 9 10 11 13 12 14 15 16 17 18 19 20 21 22 23

Test de primalité :
Si un nombre n n'est pas premier alors un de ses facteurs est $\leq \sqrt{n}$.
En effet si $n = a \times b$ avec $a, b \geq 2$ alors $a \leq \sqrt{n}$ ou $b \leq \sqrt{n}$.
Par exemple pour tester si un nombre ≤ 100 est premier il suffit de tester les diviseurs ≤ 10. Et comme il suffit de tester les diviseurs premiers, il suffit en fait de tester la divisibilité par 2, 3, 5 et 7.
Exemple : 89 n'est pas divisible par 2, 3, 5, 7 et est donc un nombre premier.

Proposition 1.3.2 ***(Lemme d'Euclide).***
Soit p un nombre premier. Si $p \mid ab$ alors $p \mid a$ ou $p \mid b$.

1.3.3 Décomposition en facteurs premiers

Théorème 1.3.1

Soit $n \geq 2$ un entier. Il existe des nombres premiers $p_1 < p_2 < \cdots < p_r$ et des exposants entiers $\alpha_1, \alpha_2, \cdots, \alpha_r \geq 1$ tels que :

$$n = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \cdots \times p_r^{\alpha_r}.$$

De plus les p_i et les α_i, $i \in \{1, \cdots, r\}$ sont uniques.

Exemple 1.3.2

$24 = 2^3 \times 3$ est la décomposition en facteurs premiers. Par contre $36 = 2^2 \times 9$ n'est pas la décomposition en facteurs premiers, c'est $2^2 \times 3^2$.

Remarque 1.3.1

La principale raison pour laquelle on choisit de dire que 1 n'est pas un nombre premier, c'est que sinon il n'y aurait plus unicité de la décomposition : $24 = 2^3 \times 3 = 1 \times 2^3 \times 3 = 1^2 \times 2^3 \times 3 = \cdots$

Exemple 1.3.3

$$504 = 2^3 \times 3^2 \times 7, \quad 300 = 2^2 \times 3 \times 5^2$$

Pour calculer le PGCD on réécrit ces décompositions :

$$504 = 2^3 \times 3^2 \times 5^0 \times 7^1, \quad 300 = 2^2 \times 3^1 \times 5^2 \times 7^0.$$

Le PGCD est le nombre obtenu en prenant chacun des facteurs affecté de son plus petit exposant :

$$PGCD(504, 300) = 2^2 \times 3^1 \times 5^0 \times 7^0 = 12.$$

1.4 Congruences

Défnition 1.4.1

Soit $n \geq 2$ un entier. On dit que a est congru à b modulo n, si n divise $b - a$. On note alors

$$a \equiv b \bmod n \ .$$

On note aussi parfois $a = b \bmod n$ ou $a \equiv b[n]$.
Une autre formulation est :

$$\boxed{a \equiv b \bmod n \Leftrightarrow \exists k \in \mathbb{Z} : a = b + kn.}$$

On remarque que n divise a si et seulement si $a \equiv 0 \bmod n$.

Remarque 1.4.1

Pour trouver un « bon » représentant de $a \bmod n$ on peut aussi faire la division euclidienne de a par n :
$a = bn + r$ alors $a \equiv r \bmod n$ et $0 \leq r < n$.

1.4.1 Théorème des restes chinois

Le théorème des restes chinois dit que nous pouvons résoudre de manière unique chaque paire de congruences ayant des modules premiers entre-eux.

Théorème 1.4.1

Soient m et n deux entiers positifs premiers entre-eux. Pour tous a et b, la paire de congruences :

$$x \equiv a \bmod m,\ x \equiv b \bmod n$$

a une solution, et cette solution est unique modulo mn.

Preuve:

Cf [3]

■

Exemple 1.4.1

Les équations de congruences $x \equiv 6 \bmod 9$ et $x \equiv 4 \bmod 11$ sont valables lorsque $x = 15$, et plus généralement lorsque $x \equiv 15 \bmod 99$, et ils ne sont pas valables pour les autres x. Le modulo 99 est 9×11.

Extension à plus de deux congruences :

Théorème 1.4.2

Soit un entier $r \geq 2$; $m_1, m_2, \cdots, m_r$ des entiers différents de zéro qui sont deux-à-deux premiers entre-eux i.e. $PGCD(m_i, m_j) = 1$ pour $i \neq j$. Alors, pour tous entiers $a_1, a_2, \cdots, a_r$, le système de congruences

$$x \equiv a_1 \bmod m_1, x \equiv a_2 \bmod m_2, \cdots, x \equiv a_r \bmod m_r,$$

a une solution, et cette solution est unique modulo $m_1 m_2 \cdots m_r$.

Preuve:

Montrons d'abord l'existence d'une solution. Ensuite, nous montrerons que cette solution est unique modulo $m_1 m_2 \cdots m_r$.

Existence de la solution :

Prouvons l'existence d'une solution par récurrence :

- Le cas $r = 2$ est le **théorème**1.4.1, qui a déjà été prouvé.
- Supposons que c'est vrai à l'étape $r > 2$. i.e.
  $$x \equiv a_1 \bmod m_1, x \equiv a_2 \bmod m_2, \cdots, x \equiv a_r \bmod m_r,$$
  a une solution.
- Démontrons que c'est vrai à l'étape $r + 1$.
  Considérons un système de congruences simultanées avec $r + 1$ modules deux-à-deux premiers entre-eux :
  $$x \equiv a_1 \bmod m_1, \cdots, x \equiv a_r \bmod m_r, x \equiv a_{r+1} \bmod m_{r+1},$$
  où $PGCD(m_i, m_j) = 1$ pour tout $i \neq j$ et les $a_i \in \mathbb{Z}, \forall i \in \{1, 2, \cdots, r + 1\}$.
  Par hypothèse, il y a une solution b aux r premières équations de congruences, i.e.
  $$b \equiv a_1 \bmod m_1, b \equiv a_2 \bmod m_2, \cdots, b \equiv a_r \bmod m_r.$$
  Considérons maintenant le système de deux équations de congruences
  $$x \equiv b \bmod m_1 m_2 \cdots m_r, x \equiv a_{r+1} \bmod m_{r+1} \qquad (2)$$

Comme $PGCD(m_i, m_{r+1}) = 1\ \forall i \in \{1, 2, \cdots, r\}$, on a $PGCD(m_1 m_2 \cdots m_r, m_{r+1}) = 1$, donc les deux modules de l'équation **(2)** sont premiers entre-eux. Puis par le cas de deux équations de congruences, à savoir le **théorème**1.4.1, il existe une solution à **(2)**, appelons la c. Comme $c \equiv b \bmod m_1 m_2 \cdots m_r$, on a $c \equiv b \bmod m_i\ \forall i \in \{1, 2, \cdots, r\}$.
Par hypothèse on a $b \equiv a_i \bmod m_i\ \forall i \in \{1, 2, \cdots, r\}$. Donc $c \equiv a_i \bmod m_i\ \forall i \in \{1, 2, \cdots, r\}$.
Comme $c \equiv a_{r+1} \bmod m_{r+1}$, alors c satisfait les $r+1$ équations de congruences données.
Ceci conclut l'étape $r+1$. Donc une solution existe.

Unicité de la solution :
Si $x = c$ et $x = c'$ satisfont tous les deux

$$x \equiv a_1 \bmod m_1\,;\, x \equiv a_2 \bmod m_2, \cdots, x \equiv a_r \bmod m_r\,;$$

alors on a $c \equiv c' \bmod m_i\ \forall i \in \{1, 2, \cdots, r\}$, donc $m_i \mid (c - c')$ pour $\forall i \in \{1, 2, \cdots, r\}$. Puisque les m_i sont deux à deux premiers entre-eux, leur produit $m_1 m_2 \cdots m_r$ divise $c - c'$, ce qui signifie que $c \equiv c' \bmod m_1 m_2 \cdots m_r$. Cela montre que toutes les solutions au système d'équations de congruences sont les même modulo $m_1 m_2 \cdots m_r$.

■

1.5 Groupe

Défnition 1.5.1

Un groupe $(G, \star)$ est un ensemble G auquel est associé une opération $(\star)$ (la loi de composition) vérifiant les quatre propriétés suivantes :

1. *pour tous $x, y \in G$, $x \star y \in G$ ($\star$ est une loi de composition interne)*
2. *pour tous $x, y, z \in G$, $(x \star y) \star z = x \star (y \star z)$ (la loi est associative)*
3. *il existe $e \in G$ tel que $\forall x \in G$, $x \star e = x$ et $e \star x = x$ (e est l'élément neutre)*
4. *pour tout $x \in G$ il existe $x^{-1} \in G$ tel que $x \star x^{-1} = x^{-1} \star x = e$ (x est le symétrique de x et est noté x^{-1})*
   Si de plus l'opération vérifie :
   pour tous $x, y \in G$ on a
   $$x \star y = y \star x$$
   on dit que G est un groupe commutatif (ou abélien).

1.5.0.1 Ordre

Défnition 1.5.2

L'ordre d'un élément g d'un groupe G est le plus petit entier $t > 0$ noté $Ord(g, G)$ ou $Ord(g)$ tel que $g^t = e$ où e est l'élément neutre du groupe G.

Remarque 1.5.1

Si G est fini alors l'ordre du groupe G est le cardinal de G.

1.5.1 Le groupe $\mathbb{Z}/n\mathbb{Z}$

Soit $n \geq 1$, $\mathbb{Z}/n\mathbb{Z}$ est l'ensemble :

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}\}$$

où $\overline{p}$ désigne la classe d'équivalence de p modulo n.
Autrement dit :

$$\boxed{\overline{p} = \overline{q} \Leftrightarrow p \equiv q \bmod n}$$

ou encore $\overline{p} = \overline{q} \Leftrightarrow \exists k \in \mathbb{Z}$, $p = q + kn$.
On définit une addition sur $\mathbb{Z}/n\mathbb{Z}$ par :

$$\boxed{\overline{p} + \overline{q} = \overline{p+q}}$$

Par exemple dans $\mathbb{Z}/60\mathbb{Z}$, on a $\overline{31} + \overline{46} = \overline{31+46} = \overline{77} = \overline{17}$.
Cette addition est bien définie :
En effet si $\overline{p'} = \overline{p}$ et $\overline{q'} = \overline{q}$ alors $\overline{p'} \equiv \overline{p} \bmod n$, $\overline{q'} \equiv \overline{q} \bmod n$ et donc $p' + q' \equiv p + q \bmod n$.
Donc $\overline{p'+q'} = \overline{p+q}$. Donc on a aussi $\overline{p'} + \overline{q'} = \overline{p} + \overline{q}$. Nous avons montré que l'addition est indépendante du choix des représentants.

Proposition 1.5.1

$(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe commutatif.

1.5.1.1 Groupes cycliques

Défnition 1.5.3

Un groupe $(G, \star)$ est dit monogène si $(G, \star)$ est engendré par un seul élément.
i.e.
S'il existe un élément $a \in G$ tel que : Pour tout $x \in G$, il existe $k \in \mathbb{Z}$ tel que $x = \underbrace{a \star \cdots \star a}_{k \text{ fois}}$.

Défnition 1.5.4

Un groupe $(G, \star)$ est dit cyclique si $(G, \star)$ est monogène et de cardinal fini.

Exemple 1.5.1

Le groupe $(\mathbb{Z}/n\mathbb{Z}, +)$ est un groupe cyclique.
En effet, il est engendré par $a = \overline{1}$, car tout élément k s'écrit :

$$\overline{k} = \underbrace{\overline{1} + \overline{1} + \cdots + \overline{1}}_{k \text{ fois}} = k \cdot \overline{1}$$

Voici un résultat intéressant : il n'existe, à isomorphisme près, qu'un seul groupe cyclique à n éléments, c'est $\mathbb{Z}/n\mathbb{Z}$.

Théorème 1.5.1

Si $(G, \star)$ un groupe cyclique de cardinal n, alors $(G, \star)$ est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$.

Chapitre 2

Le Problème du Logarithme Discret dans les groupes multiplicatifs

Le logarithme discret est un objet mathématique utilisé en cryptologie. C'est l'analogue du logarithme réel qui est la réciproque de l'exponentielle, mais dans un groupe cyclique G.

Le logarithme discret est utilisé pour la cryptographie à clé publique, typiquement dans l'échange de clés Diffie-Hellman et le chiffrement El Gamal. La raison est que, pour un certain nombre de groupes, on ne connait pas d'algorithme efficace pour le calcul du logarithme discret, alors que celui de la réciproque, l'exponentiation, se réalise en un nombre de multiplications logarithmiques en la taille de l'argument.

2.1 Le problème du logarithme discret

Soit G un groupe cyclique d'ordre n engendré par $g \in G$, i.e.

$$G = \{g^0, g, g^2, \cdots, g^{n-1}\}$$

et $g^n = g^0 = 1$, le neutre de G. On suppose également que les opérations dans G se font rapidement (comme une multiplication d'entiers). Une situation typique est de considérer le groupe $G = (\mathbb{Z}/p\mathbb{Z})^\times$ des éléments inversibles modulo p où p est un nombre premier.

Exemple 2.1.1

Prenons $G = (\mathbb{Z}/11\mathbb{Z})^\times$. On a donc :

$$G = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}, \overline{7}, \overline{8}, \overline{9}, \overline{10}\}.$$

Le groupe G est cyclique engendré par exemple, par $g = \overline{2} \in G$. On peut donc réécrire les éléments de G :

$$G = \{\underset{\overline{1}}{g^0}, \underset{\overline{2}}{g^1}, \underset{\overline{4}}{g^2}, \underset{\overline{8}}{g^3}, \underset{\overline{5}}{g^4}, \underset{\overline{10}}{g^5}, \underset{\overline{9}}{g^6}, \underset{\overline{7}}{g^7}, \underset{\overline{3}}{g^8}, \underset{\overline{6}}{g^9}\}.$$

et on retrouve bien tous les éléments de G comme des puissances de $\overline{2}$.

Dans l'exemple précédent, connaissant G, g et un entier $l > 0$, il est facile de calculer g^l dans G. En revanche, pour la réciproque c'est pas évident.
L'exemple2.1.2 illustre cela.

Facile, Difficile :

Un cryptosystème à clef publique s'appuie sur une fonction dite à sens unique. Essentiellement, il s'agit d'une fonction f telle que :

- il est facile d'évaluer $f(x)$ lorsqu'on connaît x dans l'espace de définition de f ;
- connaissant un y dans l'espace d'arrivée, il est difficile de trouver un x tel que $f(x) = y$.

Exemple 2.1.2

1. $3^5 = 3 \times 3 \times 3 \times 3 \times 3 = 243$ *(ce que fait n'importe quelle calculatrice, et même un humain). Par contre, il est beaucoup plus difficile de faire l'opération inverse (retrouver* 3^5 *à partir de* 243*), surtout lorsque les nombres utilisés sont très grands comme dans l'exemple suivant :*
2. *Un logiciel spécialisé comme le logiciel PARI-GP (disponible sur pari.math.u-bordeaux.fr) calcule très rapidement le résultat de* 25488756^{1521} *(un nombre énorme, à* 193 *chiffres). Par contre, il lui est impossible de retrouver* 25488756^{1521} *à partir de ce nombre dans une durée raisonnable : c'est un problème du logarithme discret.*

Défnition 2.1.1 (Problème du logarithme discret)

Soit $(G, \cdot)$ un groupe cyclique. Soient g un générateur de G et h un élément de G. Le problème du logarithme discret consiste à trouver un entier x tel que $\underbrace{g \cdot g \cdot \ldots \cdot g}_{x \text{ fois}} = h$. *Cet entier x est appelé logarithme de h en base g et est noté* $\log_g(h)$.

Remarque 2.1.1

- *La façon dont est posé le problème garantit l'existence de x. C'est généralement sous cette forme qu'on le rencontre en cryptanalyse. Souvent, on trouve même le problème sous cette forme :*

  Soit p un nombre premier, g un générateur de $(\mathbb{Z}/p\mathbb{Z})^\times$ et h un élément de $(\mathbb{Z}/p\mathbb{Z})^\times$.

  Trouver un exposant x tel que $g^x \equiv h \bmod p$.

- *À l'inverse, on trouve des versions plus larges du PLD comme telle :*

  Soit $(G, \cdot)$ un groupe. Soient h et g deux éléments de G. Trouver, s'il existe, un entier x tel que $\underbrace{g \cdot g \cdot \ldots \cdot g}_{x \text{ fois}} = h$

- *Le logarithme discret en base g est défini modulo l'ordre de g.*

Remarque 2.1.2

Dans le groupe $(\mathbb{Z}/p\mathbb{Z}, +)$ où p est un nombre premier. Soit g un générateur de $\mathbb{Z}/p\mathbb{Z}$ et h un de ses éléments. Trouver x tel que $x \cdot g = h \bmod p$ *est simple : il suffit de calculer l'inverse de g modulo p. Le PLD n'est donc pas toujours un problème difficile.*

2.2 Protocoles d'échange de clé à base du problème du logarithme discret

2.2.1 Protocole de Diffie-Hellman

L'échange de clés Diffie-Hellman, du nom de ses auteurs Whitfield Diffie et Martin Hellman, est une méthode publiée en 1976, par laquelle deux agents, nommés par convention Alice et Bob, peuvent se mettre d'accord sur un nombre (qu'ils peuvent utiliser comme clé pour chiffrer la conversation suivante) sans qu'un troisième agent appelé Ève puisse découvrir le nombre, même en ayant écouté tous leurs échanges. Cette idée valut en 2015 aux deux auteurs le prix Turing [1]

Supposons qu'Alice et Bob veulent partager une clé privée, mais ils vont échanger des informations en utilisant un réseau non sécurisé (où le message est éventuellement intercepté par l'homme du milieu i.e. Eve). Alors

1. Alice choisit un groupe cyclique $(G, \cdot)$ et g un générateur de G. Le groupe G et g sont publics.
2. Alice choisit $a \in \mathbb{N}$ et Bob choisit $b \in \mathbb{N}$.
3. Alice calcul $A_0 = g^a$ et Bob fait $B_0 = g^b$.
4. Alice envoie A_0 à Bob et Bob envoie B_0 à Alice.
5. Alice calcule $A_1 = B_0^a$ et Bob calcule $B_1 = A_0^b$.

Et les valeurs A_1 et B_1 sont les clés privées. En fait, on voit que

$$A_1 = g^{ab} = B_1$$

alors à la fin, Alice et Bob partagent la même valeur.

Dans cette procédure, les valeurs g, A_0, B_0 et le groupe $(G, \cdot)$ sont connus par tous (car on a supposé que la chaine de communication n'était pas sûre). Alors, quelqu'un peut essayer de résoudre le PLD $g^x = A_0$ (ou $g^x = B_0$) et après utiliser a (ou b) pour trouver la clé $A_1 = A_0^b$ (ou B_0^a).

2.2.2 Protocole ElGamal

Le protocole ElGamal est une extension du protocole de Diffie-Hellman tout comme plusieurs autres protocoles qui permettent l'échange de messages. Ce protocole est inventé par Taher Elgamal en 1984.

Supposons que Bob veut envoyer un message m à Alice par un réseau non sécurisé (où le message est éventuellement intercepté par l'homme du milieu i.e. Eve). Avec cet algorithme, il peut envoyer m de la manière suivante :

1. Le prix Turing ou ACM Turing Award, en hommage à Alan Turing (1912-1954), est attribué tous les ans depuis 1966 à une personne sélectionnée pour sa contribution de nature technique faite à la communauté informatique. Les contributions doivent être d'une importance technique majeure et durable dans le domaine informatique.

1. Alice choisit un groupe cyclique $(G, \cdot)$ et g un générateur de G. La valeur g est publique.
2. Alice choisit une clé privée $a \in \mathbb{N}$
3. Alice calcule la clé publique A, où $A = g^a$
4. Bob choisit une valeur aléatoire k, calcule

$$B_0 = g^k$$

et

$$B_1 = mA^k$$

et envoie le couple (B_0, B_1) à Alice.

5. Alice calcule $A_0 = B_0^a$ (qui est égal à g^{ak}) et A_0^{-1}.
Ainsi, elle fait

$$B_1 \cdot A_0^{-1} = (mA^k)(A_0^{-1}) = (mg^{ak})(g^{ak})^{-1} = m$$

et réussit à trouver le message m.

2.3 Méthodes de résolution du problème du logarithme discret

Soit $(G, .)$ un groupe cyclique d'ordre n engendré par g et soit $h \in G$. On cherche donc $x \in \mathbb{Z}$ tel que $y = g^x$.

2.3.1 Recherche exhaustive

Cette recherche aussi appellée la *méthode naïve*, consiste à calculer g^i pour tout i appartenant à $\{1, 2, 3, \ldots, Ord(g)\}$ et voir quelle valeur de i satisfait $g^i = h$.
On peut commencer en voyant si g et h sont égaux, s'ils ne le sont pas, on mutiplie g par lui-même, en obtenant g^2 et on le compare avec h. S'ils sont encore différents, on multiplie g^2 par g pour obtenir g^3 et on compare cette valeur avec h. On continue ainsi jusqu'à trouver la réponse.
Notons que dans le pire cas on va faire un nombre de multiplications égal à l'ordre de g.

2.3.2 Méthode Baby-Steps/Giant-Steps

L'algorithme *Baby-steps/Giant-steps* permet de résoudre le problème du logarithme discret dans un groupe cyclique quelconque. Il est dû à Daniel Shanks en 1971.
Dans cette section, on améliore la complexité de résolution d'un PLD dans un groupe cyclique quelconque.

Algorithme 2.3.1

Soit G un groupe cyclique engendré par g (avec $Ord(g) = N \geq 2$) et h un élément de G. L'algorithme suivant résout le PLD $g^x = h$:

1. *Calculer $n = \lfloor \sqrt{N} \rfloor + 1$ où $\lfloor \sqrt{N} \rfloor$ désigne l'entier naturel immédiatement inférieur ou égal à $\sqrt{N}$.*
2. *Calculer les deux listes :*
$$\begin{cases} {g^r}_{0 \leq r < n} : & e, g^1, g^2, g^3, \ldots, g^n \text{ Ce sont les pas de bébé (Baby-Steps)} \\ {hg^{-qn}}_{0 \leq q \leq n} : & hg^0, hg^{-n}, hg^{-2n}, \ldots, hg^{-n^2} \quad \text{Ce sont les pas de géant (Geant-Steps)} \end{cases}$$
3. *Trouver un élément commun à ces deux listes, i.e. trouver $(i, j) \in [\![1, t]\!]^2$ tel que $g^i = hg^{-nj}$.*
4. *Calculer $i + nj$. C'est une solution du PLD.*

Preuve:

Prouvons l'existence d'une collision :
Il suffit de montrer qu'il existe toujours un élément commun à la liste des *pas de bébé* et à celle des *pas de géant*. Comme G est engendré par g et $h \in G$, il existe $x \in \mathbb{N}$ tel que $h = g^x$.
Par division euclidienne, il existe $q \in \mathbb{N}$ et $r \in [\![1, n[\![$ tels que $x = nq + r$.
Donc
$$h = g^{nq+r} \qquad (1)$$
Comme $x < N$ et $n > \sqrt{N}$, on a $q = \frac{x-r}{n} < \frac{N}{n} < n$.
L'équation (1) peut donc en effet se réécrire :
$$g^r = hg^{-nq} \quad \text{avec} \quad 0 \leq r < n \quad \text{et} \quad 0 \leq q < n$$
■

Exemple 2.3.1

Pour illustrer le fonctionnement de cet algorithme, considérons l'exemple suivant :
Soient $p = 59$, $G = ((\mathbb{Z}/p\mathbb{Z})^\times, \cdot)$, $g = 2$ et $h = 7$. On essaye de trouver x tel que $g^x = h$ avec cet algorithme.
Comme $G =< g >$, on a $Ord(g) = Ord(G) = p - 1 = 58$, donc $N = 58$.

1. *Calculons $n = 1 + \lfloor \sqrt{N} \rfloor = 7 + 1 = 8$*
2. *Calculons les deux listes :*
   - *Calcul de la première liste :*
   $$\{g^r \bmod 59\}_{0 \leq r < n} : 1, 2, 4, 8, 16, 32, 5, 10. \quad \text{Ce sont les pas de bébé.}$$
   - *Calcul de la deuxième liste :*
   On calcule g^{-n} : on sait que $g^{-1} = 30$, $gg^{-1} \equiv 60 \equiv 1 \bmod 59$. Et comme $30^8 \equiv 3 \bmod 59$, on a $g^{-n} = 3$.
   Ainsi, on calcule chaque élément de la deuxième liste et on essaye de trouver une collision :
   $$\{hg^{-nq} \bmod 59\}_{0 \leq q < n} : 7, 21, 4. \quad \text{Ce sont les pas de géant.}$$
3. *Identification de l'élément en commun :*
   On s'arrête à $hg^{-n2} \equiv 4 \bmod 59$, car 4 est dans la première liste. Ainsi, on a trouvé :
   $$g^2 \equiv 4 \equiv hg^{-2n} \bmod 59.$$
4. *La solution :*
   Une solution est $x = 2 + 2n = 2 + 2 \cdot 8 = 18$.
   En fait, on peut vérifier que $2^{18} \equiv (2^6)^3 \equiv 5^3 \equiv 7 \bmod 59$.

2.3.3 Méthode de Pohlig-Hellman

L'algorithme de *Pohlig-Hellman* est un algorithme pour résoudre le PLD. Il divise un PLD en sous-problèmes (tous des PLD aussi) et utilise ensuite les résultats de ces sous-problèmes pour construire la solution.
On cherche toujours à résoudre le PLD $g^x = h$ dans un groupe cyclique quelconque. Ici, on cherche à tirer parti de la connaissance d'une factorisation de l'ordre N de g.

Algorithme 2.3.2 (De Pohlig-Hellman)

Soit G un groupe cyclique engendré par g (avec $Ord(g) = \prod_{i=1}^{t} q_i^{e_i}$) dans lequel on sait résoudre le PLD pour tout élément d'ordre q^e où e est un entier et q est un nombre premier. Soit h, un élément de G. Alors l'algorithme suivant résout le PLD $g^x = h$.

1. *Pour tout $i \in [\![1, t]\!]$, calculer $g_i = g^{\frac{N}{q_i^{e_i}}}$ et $h_i = h^{\frac{N}{q_i^{e_i}}}$*
2. *Par hypothèse, pour tout $i \in [\![1, t]\!]$, on sait calculer une solution y^i du PLD $g_i^y = h_i$.*
3. *Grâce au **théorème des restes chinois**1.4.2, on peut calculer une solution du système de congruences $\mathcal{S} = \{x \equiv y_i \bmod q_i^{e_i}\}$. L'entier x est solution du PLD initial.*

Preuve:

Montrons que x est effectivement solution du PLD $g^x = h$.
Comme x est solution de $\mathcal{S}$ pour tout $i \in [\![1, t]\!]$, il existe $z_i \in \mathbb{Z}$ tel que $x = y_i + q_i^{e_i} z_i$.
$g^x = h \Leftrightarrow \forall i \in [\![1, t]\!]$, $(g^x)^{\frac{N}{q_i^{e_i}}} = h^{\frac{N}{q_i^{e_i}}}$.
Ces égalités se réécrivent : pour tout $i \in [\![1, t]\!]$,

$$\frac{N}{q_i^{e_i}} \times x \equiv \frac{N}{q_i^{e_i}} \times \log_g(h) \bmod N \qquad (2)$$

D'autre part, comme $PGCD\left(\left(\frac{N}{q_i^{e_i}}\right)_{i\in[\![1,t]\!]}\right) = 1$, d'après le **théorème de Bézout**1.2.1, il existe des entiers $(c_i)_{i\in[\![1,t]\!]}$ tels que $\sum_{i=1}^{t} c_i \frac{N}{q_i^{e_i}} = 1$.
En multipliant les congruences (2) par c_i et en sommant toutes les congruences obtenues on aboutit à :

$$\sum_{i=1}^{t} c_i \frac{N}{q_i^{e_i}} \times x \equiv \sum_{i=1}^{t} c_i \frac{N}{q_i^{e_i}} \times \log_g(h) \bmod N$$

puis à $x \equiv \log_g(h) \bmod N$ comme attendu.

■

Exemple 2.3.2

Soient $G = ((\mathbb{Z}/19\mathbb{Z})^\times, \cdot)$ un groupe, $g = 2$ et $h = 9$ deux éléments de ce groupe.
On va résoudre le PLD $g^x = h$.
Avant, notons que l'ordre du groupe est $N = 18$ et peut être écrit comme $N = 3^2 \cdot 2$ (facteurs premiers) et que dans cette section on va faire les calculs modulo 19.

1. *Calculons g_i pour $i \in [\![1,2]\!]$*
   $g_1 = g^{\frac{N}{3^2}} = g^2 = 4$ *et* $h_1 = h^2 = 81 = 5$.
   $g_2 = g^{\frac{N}{2}} = g^9 = 2^9 = 18$ *et* $h_2 = h^9 = 9^9 = 1$.
2. *Maintenant, on résolvons ces deux sous-problèmes :*
   $g_1^{x_1} = h_1$ *: On écrit* $x_1 = a_0 + a_1 3$ *et on trouve* a_0*, la solution du PLD* $(g_1^{\frac{N}{3}})^{a_0} = h_1^{\frac{N}{3}} \Leftrightarrow 11^{a_0} = 7 \Rightarrow a_0 = 2$.
   Et on trouve a_1 *en résolvant le PLD suivant :*
   $$\begin{aligned} g_1^{a_1 3 \frac{N}{3^2}} = h_1^{\frac{N}{3^2}} g_1^{-a_0 \frac{N}{3^2}} &\Leftrightarrow (4^6)^{a_1} = 5^2 (4)^{-2\cdot 2} \\ &\Leftrightarrow (4^6)^{a_1} = 5^2 4^{-4} \\ &\Leftrightarrow 4^4 (4^6)^{a_1} = 5^2 \end{aligned}$$
   qui donne $a_1 = 2$.
   Alors $x_1 = a_0 + a_1 3 = 2 + 2.3 = 2 + 6 = 8$.
   $g_2^{x_2} = h_2$ *: en résolvant ce PLD, on trouve* $x_2 = 2$
3. *Ainsi, utilisons* ***l'extension du théorème des Restes Chinois****1.4.2 pour calculer* x *tel que* $x = 8 \bmod 3^2$ *et* $x = 2 \bmod 2$*, il vient* $x = 26 \bmod 3^2.2$.
   - *On peut vérifier que*
   $$g^{26} = 2^{26} = (2^5)^4 \cdot 2^6 = (13)^4 \cdot 2^6 = (4) \cdot 2^6 = 9 = h.$$
   Donc cette solution est correcte.

Chapitre 3

Problème du Logarithme Discret sur les courbes elliptiques

Ce chapitre a pour objectif de comprendre d'un point de vue théorique l'algorithme **MOV** (*Menezes, Okamoto* et *Vanstone*) qui permet de calculer le logarithme discret sur une courbe elliptique.

3.1 Courbes elliptiques et fonctions rationnelles

Dans cette section, $\mathbf{K}$ désigne un corps algébriquement clos de caractéristique différente de deux et trois.

3.1.1 Définition d'une courbe elliptique

Défnition 3.1.1

On définit une courbe affine plane comme étant le lieu des points d'annulation d'un polynôme en deux variables de $\mathbf{K}[\mathbf{X}, \mathbf{Y}]$. *De même on définit une courbe projective plane comme étant le lieu des points d'annulation d'un polynôme homogène en trois variables de* $\mathbf{K}[\mathbf{X}, \mathbf{Y}, \mathbf{Z}]$.

Défnition 3.1.2

Soit $\mathcal{C}$ *une courbe affine plane associée au polynôme* $P \in \mathbf{K}[\mathbf{X}, \mathbf{Y}]$. *On dit que* $\mathcal{C}$ *est une courbe lisse si elle admet une unique tangente en tout point.*

Défnition 3.1.3 *:*

Une courbe elliptique sur $\mathbf{K}$ *est l'ensemble des points du plan projectif* $P^2(K)$ *dont les coordonnées homogènes* $[x : y : z]$ *vérifient l'équation :*

$$y^2z = x^3 + axz^2 + bz^3$$

où a *et* b *sont des éléments de* $\mathbf{K}$ *tels que* $4a^3 + 27b^2 \neq 0$.

Remarque 3.1.1

Intéressons nous aux points sur la droite à l'infini d'une courbe elliptique. Soit P un tel point et $[x : y : 0]$ ses coordonnées homogènes. Ces dernières doivent vérifier l'équation $x^3 = 0$. Par intégrité de $\mathbf{K}$, on a donc $x = 0$. De plus, comme $[0 : 0 : 0]$ n'est pas un point du plan projectif, on a nécessairement $y \neq$. En divisant les coordonnées de P par y, on obtient finalement qu'un seul point d'une courbe elliptique qui se situe sur la droite à l'infini : celui de coordonnées homogènes $[0 : 1 : 0]$. D'où la "définition" suivante que l'on choisit souvent pour décrire une courbe elliptique.

Défnition 3.1.4 (Courbe elliptique)

Une courbe elliptique est l'ensemble des points d'une courbe plane affine définie par un polynôme de $\mathbf{K}[\mathbf{X}, \mathbf{Y}]$ du type $Y^2 - X^3 - aX - b$ où a et b vérifient $4a^3 + 27b^2 \neq 0$, auquel on ajoute le point à l'infini, noté par la suite P_∞ et tel que :

$$P_\infty = \bigcap_{a \in \mathbf{K}} \{X - a = 0\}$$

Remarques 3.1.2

- *La définition de P_∞ signifie plus simplement que ce point est arbitrairement considéré comme le point d'intersection de toutes les droites verticales de $\mathbf{K^2}$.*
- *Soit P un point d'une courbe elliptique $\mathcal{E}$ différent de P_∞ de coordonnées (x_p, y_p). On dit que P est ordinaire si $y_P \neq 0$ et spécial sinon. Comme $\mathbf{K}$ est algébriquement clos et que $\mathcal{E}$ est une courbe elliptique, il existe $(\alpha, \beta, \gamma) \in \mathbf{K^3}$ tel que $X^3 + aX + b = (X - \alpha)(X - \beta)(X - \gamma)$. Les seuls points spéciaux sont donc ceux de coordonnées $(\alpha, 0), (\beta, 0)$ et $(\gamma, 0)$. La **proposition** 3.1.1 montre que α, β et γ sont en fait deux à deux distincts.*

Proposition 3.1.1

Soient a et b deux éléments de $\mathbf{K}$. Soit $\mathcal{C}$ une courbe affine plane définie par le polynôme $P = X^3 + aX + b - Y^2$. Alors, $\mathcal{C}$ est lisse si et seulement si $4a^3 + 27b^2 \neq 0$. En particulier, une courbe elliptique est lisse.

Preuve:

On montre d'abord que $Y = X^3 + aX + b$ n'a pas de racine multiple si et seulement si $4a^3 + 27b^2 \neq 0$.

En effet :

$X^3 + aX + b$ admet une racine multiple
$\Leftrightarrow$ $X^3 + aX + b$ et $3X^2 + a$ ont même racine commune
$\Leftrightarrow$ $\exists \alpha \in \mathbf{K}$ tel que $X - \alpha \mid X^3 + aX + b$ et $X - \alpha \mid 3X^2 + a$
$\Leftrightarrow$ $\exists \alpha \in \mathbf{K}$ tel que $X - \alpha \mid PGCD(X^3 + aX + b, 3X^2 + a)$
$\Leftrightarrow$ $(a = 0$ et $\exists \alpha$ tel que $X - \alpha \mid b)$ ou $(a \neq 0$ et $\exists \alpha$ tel que $X - \alpha \mid \frac{27b^2 + 4a^3}{4a^2})$
$\Leftrightarrow$ $(a = 0$ et $b = 0)$ ou $(a \neq 0$ et $27b^2 + 4a^3 = 0)$
$\Leftrightarrow$ $27b^2 + 4a^3 = 0$

Ce qui conclut la preuve par contraposée. ■

Notation :

Soit $\mathcal{E}$ une courbe elliptique. En cryptographie, on ne s'intéresse qu'aux points de $\mathcal{E}$ ayant des coordonnées appartenant à un corps fini $\mathbf{F}_p$ où p est premier. On désigne l'ensemble de ces points par $\mathcal{E}(\mathbf{F}_p)$.

3.1.2 Fonctions polynomiales sur une courbe elliptique :

Dans cette section et les sections suivantes de la deuxième partie, $\mathcal{E}$ est une courbe elliptique sur $\mathbf{K}$ décrite par l'équation : $Y^3 = X^2 + aX + b$.

Défnition 3.1.5 (anneau de coordonnées)

L'anneau de coordonnées de la courbe elliptique $\mathcal{E}$ est l'anneau quotient $\dfrac{\mathbf{K}[\mathbf{X},\mathbf{Y}]}{(Y^2 - X^3 - aX - b)}$.
On le note $\mathbf{K}[\mathcal{E}]$ et tout élément de cet anneau est appelé fonction polynomiale sur $\mathcal{E}$.

Remarque 3.1.3

Tout élément G de $\mathbf{K}[\mathcal{E}]$ peut s'écrire sous la forme dite réduite $G(X,Y) = P(X)+YQ(X)$ avec $(P,Q) \in \mathbf{K}[\mathbf{X}]$ en remplaçant successivement Y^2 par $X^3 + aX + b$. Cette écriture est unique.

Proposition 3.1.2

Soit $G \in \mathbf{K}[\mathcal{E}] \setminus \{0\}$. Alors G admet un nombre fini de zéros.

Preuve:

Introduisons tout d'abord quelques notions. La remarque précédente assure l'existence de $(P,Q) \in \mathbf{K}[\mathbf{X}]$ tels que $G = P + YQ$. On appelle conjugué de G l'objet suivant : $\overline{G} = P - YQ$.
On appelle alors norme de G, notée $n(G)$ le polynôme suivant :

$$n(G) = G\overline{G} = P(X)^2 - Y^2Q(X)^2 = P(X)^2 - (X^3 + aX + b)Q(X)^2$$

La norme de G est donc un élément de $\mathbf{K}[X]$.
Soit dès lors (α,β) un zéro de G. On a donc $P(\alpha) + \beta Q(\alpha) = 0$. Alors,

$$\begin{aligned} n(G)(\alpha) &= P(\alpha)^2 - (\alpha^3 + a\alpha + b)Q(\alpha)^2 \\ &= \beta^2 Q(\alpha)^2 - \beta^2 Q(\alpha)^2 \\ &= 0 \end{aligned}$$

Donc α est racine de $n(G)$. On en déduit que toute abscisse d'un zéro de G est un zéro de $n(G)$ qui en a un nombre fini. D'où le résultat.

■

Défnition 3.1.6

Soit $G \in \mathbf{K}[\mathcal{E}]$. On appelle degré de G, noté $deg_{\mathcal{E}}(G)$, le degré au sens habituel de la norme de G. Autrement dit, $deg_{\mathcal{E}}(G) = deg(n(G))$.
Par exemple, pour tout $k \in \mathbb{N}$, $\begin{cases} deg_{\mathcal{E}}(X^k) = 2k \\ deg_{\mathcal{E}}(Y^k) = 3k \end{cases}$

3.1.3 Fonctions rationnelles sur une courbe elliptique $\mathcal{E}$

Défnition 3.1.7 (Fonction rationnelle)

Soit $\mathcal{E}$ une courbe elliptique de sorte que l'anneau $\mathbf{K}[\mathcal{E}]$ soit ingère. Le corps des fractions de l'anneau $\mathbf{K}[\mathcal{E}]$ est appelé corps des fonctions rationnelles sur $\mathcal{E}$; il est noté $\mathbf{K}(\mathcal{E})$. Un élément de $\mathbf{K}(\mathcal{E})$ est appelé fonction rationnelle sur $\mathbf{K}[\mathcal{E}]$.

Lemme 3.1.1

Le polynôme $P = Y^2 - X^3 - aX - b$ décrivant la courbe elliptique $\mathcal{E}$ est irréductible dans $\mathbf{K}[\mathbf{X}, \mathbf{Y}]$.

Preuve:

cf [5]

■

Défnition 3.1.8 (Point régulier et pôle)

Soit P un point de $\mathcal{E}$ différent de P_∞. Soit $R \in \mathbf{K}(\mathcal{E})$. Le point P est régulier pour R s'il existe un représentant $\frac{G}{H}$ de R tel que $H(P) \neq 0$. Sinon, on dit que P est un pôle de R.

Défnition 3.1.9 (Valeur d'une fonction rationnelle en un point de $\mathcal{E}$)

$R \in \mathbf{K}(\mathcal{E})$ et $P \in \mathcal{E}$. La valeur de R en P est :

- *$R(P)$ si P est régulier*
- *$+\infty$ si P est un pôle*
- *Si $P = P_\infty$ et $\frac{G}{H}$ est un représentant de R, notons a (resp. b) le coefficient le plus haut degré de G (resp. H). Cette valeur vaut :* $\begin{cases} 0 & si \quad deg_{\mathcal{E}}(G) < deg_{\mathcal{E}}(H) \\ +\infty & si \quad deg_{\mathcal{E}}(G) > deg_{\mathcal{E}}(H) \\ \frac{a}{b} & si \quad deg_{\mathcal{E}}(G) = deg_{\mathcal{E}}(H) \end{cases}$

Proposition 3.1.3

Toute fonction rationnelle sur $\mathcal{E}$ admet un nombre fini de zéros et de pôles.

Preuve:

On reprend en les adaptant les arguments de 3.1.2.

■

Remarque 3.1.4

Une fonction rationnelle n'ayant ni zéros ni pôles est constante.

3.1.4 Uniformisantes

Défnition 3.1.10 (Uniformisante)

Soit P un point de $\mathcal{E}$. Une uniformisante en P est une fonction rationnelle u telle que :

$$\begin{cases} u(P) = 0 \\ \forall g \in \mathbf{K}(\mathcal{E}) \setminus \{0\}, \exists d \in \mathbb{N} \quad r \in \mathbf{K}(\mathcal{E}) \quad dont \quad P \quad n'est\ ni\ zéro\ ni\ pôle\ tel\ que \quad g = u^d r \end{cases}$$

Proposition 3.1.4

L'entier d dont il est question dans la précédente définition est indépendant de l'uniformisante.

Preuve:

Soit $P \in \mathcal{E}$ et u et v deux uniformisantes en P . Alors, il existe $(e, f) \in \mathbb{N}$ et $(r, s) \in \mathbf{K}(\mathcal{E})$ tels que P n'est ni zéro ni pôle de r ou de s tels que $u = v^e r$ et $v = u^f s$.
On a donc $u = u^{ef} s^e r$ puis $1 = u^{ef-1} s^e r$. On évalue cette dernière égalité en P. Comme $u(P) = 0$, on a nécessairement $ef - 1 = 0$. Comme e et f sont des entiers naturels, $e = f = 1$.
Soit désormais $g \in \mathbf{K}(\mathcal{E})$ dont l'ordre en P relativement à u est d. On a $g = u^d t$ où P n'est ni zéro ni pôle de t. Par le point précédent, $g = (vr)^d t = v^d r^d t$. Comme P n'est ni zéro ni pôle de $r^d t$, l'ordre de g en P relativement à v est aussi d.

■

Défnition 3.1.11 (Ordre d'une fonction en un point)

Soit P un point de $\mathcal{E}$ et g un élément de $\mathbf{K}(\mathcal{E})$. Soit u une uniformisante en P. Alors il existe $d \in \mathbb{Z}$ et $r \in \mathbf{K}(\mathcal{E})$ dont P n'est ni zéro ni pôle tels que $g = u^d r$. L'entier d est appelé ordre de g en P et est noté $ord_P(g)$.

Remarques 3.1.5 –

- *La **proposition**3.1.4 assure la bonne définition de l'ordre.*
- *Si P n'est ni un zéro ni un pôle, pour toute fonction rationnelle f, $ord_P(f) = 0$.*

Proposition 3.1.5

Tout point P d'une courbe elliptique admet une uniformisante. Plus précisément :

- *Si $P = (x_P, y_P)$ est un point ordinaire, $X - x_P$ est une uniformisante en P.*
- *Si P est un point spécial, Y est une uniformisante en P.*
- *Si $P = P_\infty$, $\frac{X}{Y}$ est une uniformisante en P.*

Preuve:

cf [5]

■

3.2 Les diviseurs

Dans cette section, K désigne un corps algébriquement clos de caractéristique différente de deux et trois et $\mathcal{E}$ une courbe elliptique sur K décrite par l'équation $Y^2 = X^3 + aX + b$. Cette partie requiert la connaissance du fonctionnement de la loi + sur les points de $\mathcal{E}$; loi décrite aux **paragraphes**3.3.1.1 et 3.3.1.2.

Défnition 3.2.1 (Diviseur)

Un diviseur D sur $\mathcal{E}$ est une somme formelle de points appartenant à $\mathcal{E}$:

$$D = \sum_{P \in \mathcal{E}} a_p P$$

où les a_p sont des entiers presque tous nuls.
L'ensemble des diviseurs sur $\mathcal{E}$ est noté $Div(\mathcal{E})$.

On définit une loi de composition interne, notée + sur $Div(\mathcal{E})$ qui en fait clairement un groupe commutatif.
Si $D = \sum_{P \in \mathcal{C}} a_p P$ et $D' = \sum_{P \in \mathcal{E}} a'_p P$ sont deux diviseurs sur $\mathcal{E}$, on a :

$$(D + D') = \sum_{P \in \mathcal{E}} (a_p + a'_p) P$$

Défnition 3.2.2 (Degré d'un diviseur)

Soit $D = \sum_{P \in \mathcal{E}} a_P P$ un diviseur de $\mathcal{E}$.
Le degré de D est l'entier $\sum_{P \in \mathcal{E}} a_P$, noté $deg(D)$.
La fonction $deg : \mathcal{E} \longrightarrow \mathbb{Z}$ est un morphisme de groupes dont le noyau est noté $Div^0(E)$.

3.2.1 Diviseur d'une fonction

Défnition 3.2.3

Soit f une fonction rationnelle non nulle. Par définition le diviseur de f est $Div(f) = \sum_{P \in \mathcal{E}} ord_P(f)P$.

Remarque 3.2.1

*Cet objet est bien un diviseur au sens précédent car f a un nombre fini de zéros et de pôles par la **proposition**3.1.3.*

Proposition 3.2.1

Pour toutes fonctions rationnelles r et s, $Div(rs) = Div(r) + Div(s)$ et $Div(\frac{r}{s}) = Div(r) - Div(s)$.

Preuve:

Cf [9]

■

Proposition 3.2.2

Deux fonctions non nulles ont même diviseur si et seulement si elles sont proportionnelles.

Preuve:

Si f et g sont proportionnelles elles ont mêmes zéros et mêmes pôles donc ont le même diviseur. Réciproquement, si elles ont même diviseur alors $Div(\frac{f}{g}) = Div(f) - Div(g) = 0$. La fonction $\frac{f}{g}$ n'a donc ni zéro ni pôle : elle est constante.

■

Défnition 3.2.4 (Diviseur principal)

Un diviseur D est dit principal s'il existe une fonction rationnelle f telle que $D = Div(f)$. On note $Princ(\mathcal{E})$ l'ensemble des diviseurs principaux.

Défnition 3.2.5 (Relation d'équivalence sur $Div(\mathcal{E})$)

On introduit une relation d'équivalence $\sim$ sur $Div(\mathcal{E})$. Soit D_1 et D_2 deux diviseurs.

$$D_1 \sim D_2 \Leftrightarrow D_1 - D_2 \quad \textit{est un diviseur principal}$$

Théorème 3.2.1 *(Caractérisation des diviseurs principaux)*

Un diviseur est principal si et seulement si son degré est nul.

Preuve:

Cf [9]

■

Lemme 3.2.1

Soit P_1 et P_2 deux points de $\mathcal{E}$. Alors il existe $g \in \mathbf{K}(\mathcal{E})$ tel que : $(P_1) + (P_2) = (P_1 + P_2) + (P_\infty) + Div(g)$.

Preuve:

Procédons par cas :

- Si P_1 ou P_2 est le point à l'infini, la fonction 1 convient puisque $Div(g) = 0$.
- Si $P_1 = -P_2$, notons x_1 l'abscisse commune de P_1 et P_2. On a alors $Div(X - x_1) = (P_1) + (P_2) - 2(P_\infty)$. Donc $(P_1) + (P_2) = 2(P_\infty) + Div(g)$ avec $g = X - x_1$.
- Si $P_1 \neq P_2$, considérons la droite $\mathcal{D}$ passant par P_1 et P_2 décrite par le polynôme $\alpha X + \beta Y + \gamma$. Notons $P_3 = (x_3, y_3)$ le troisième point d'intersection de $\mathcal{E}$ et $\mathcal{D}$.
  Comme $P_1 \neq P_2$, β est différent de 0 donc $deg_{\mathcal{E}}(\alpha X + \beta Y + \gamma) = 3$ et donc P_∞ est d'ordre 3.
  On a donc $Div(\alpha X + \beta Y + \gamma) = (P_1) + (P_2) + (P_3) - 3(P_\infty)$.
  D'autre part, $Div(X - x_3) = (P_3) + (-P_3) - 2(P_\infty)$. Donc

$$Div\left(\frac{\alpha X + \beta Y + \gamma}{X - x_3}\right) = (P_1) + (P_2) - (-P_3) - (P_\infty)$$

  Comme $P_1 + P_2 = -P_3$, en prenant $g = \frac{\alpha X + \beta Y + \gamma}{X - x_3}$, on obtient le résultat attendu.
- Si $P_1 = P_2$, on reprend le raisonnement précédent avec la tangente à $\mathcal{E}$ en P_1.

■

Corollaire 3.2.1

Soit D un diviseur de degré nul. Alors il existe $P \in \mathbf{K}(\mathcal{E})$ tel que $D \sim (P) - (P_\infty)$.

Preuve:

Par le **lemme**3.2.1, en regroupant les termes de D ayant des coefficients de meme signe, il est possible de remplacer deux points par leur somme quitte à rajouter un multiple de P_∞ ou le diviseur d'une fonction. On aboutit donc soit à $D \sim (P) - (Q) + n(P_\infty)$ soit à $D \sim (P) + n(P_\infty)$ soit à $D \sim -(P) + n(P_\infty)$ avec $n \in \mathbb{Z}$.

- Dans le premier cas, comme $deg(D) = 0$, $n = 0$
  Aussi
  Comme $Div(X - x_Q) = (Q) + (-Q) - 2P_\infty$, on a :

$$\begin{aligned} D &\sim D + Div(X - x_Q) \\ &\sim (P) + (-Q) - 2(P_\infty) \\ &\sim (P - Q) - (P_\infty) \quad \text{par le } \mathbf{lemme}\ 3.2.1 \end{aligned}$$

- Dans le deuxième cas, comme $deg(D) = 0$, on a $n = 1$. D'où le résultat.
- Dans le dernier cas, comme $deg(D) = 0$, on a $n = 1$.
  Comme $Div(X - x_p) = (P) + (-P) - 2P_\infty$, on a :

$$\begin{aligned} D &\sim D + Div(X - x_p) \\ &\sim (-P) - (P_\infty) \end{aligned}$$

■

3.3 Cryptographie elliptique

Dans cette section, **K** désigne un corps algébriquement clos de caractéristique différente de deux et trois et $\mathcal{E}$ une courbe elliptique sur **K** décrite par l'équation $Y^2 = X^3 + aX + b$.

3.3.1 Loi de groupe sur une courbe elliptique

On définit une loi interne sur $\mathcal{E}$, notée + qui fait de $(\mathcal{E}, +)$ un groupe commutatif. Les illustrations s'appuient sur la courbe d'équation $Y^2 = X^3 + 3X + 3$.

Théorème 3.3.1 (Théorème de Bézout)

Soient $\mathcal{E}$ une courbe elliptique et $\mathcal{D}$ une droite definies sur un corps **K**. *Si $\mathcal{E}$ a au moins deux points d'intersection (comptés avec leur multiplicité) avec la droite $\mathcal{D}$, alors $\mathcal{E}$ a exactement trois points d'intersection (compté avec leur multiplicité) avec la droite $\mathcal{D}$.*

Preuve:

Cf [7]

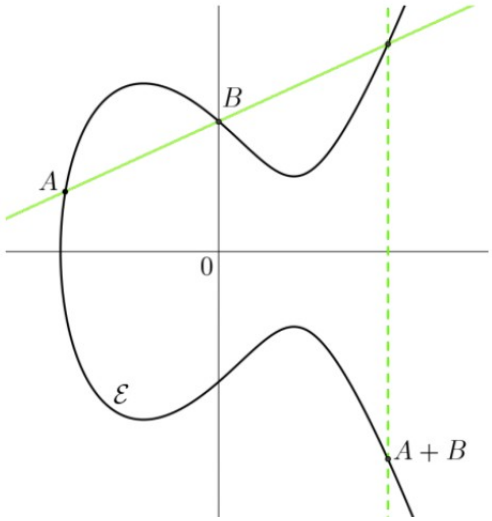
■

3.3.1.1 Considérations géométriques

Soient A et B deux points de $\mathcal{E}$. On note $\mathcal{D}$ la droite passant par A et B, en considérant que cette droite est la tangente à $\mathcal{E}$ en A si $A = B$. On peut toujours considérer cette droite :

- si $A \neq B$, il existe une unique droite projective passant par A et B
- si $A = B$, la tangente à $\mathcal{E}$ en A existe bien car $\mathcal{E}$ est lisse par définition

Comme **K** est algébriquement clos (au besoin, on se place sur la clôture algébrique de **K**) on peut utiliser le **théorème de Bézout**3.3.1. Ce dernier assure alors que $\mathcal{E}$ et $\mathcal{D}$, de degrés respectifs 3 et 1, s'intersectent en exactement 3 points.
Deux d'entre eux sont A et B. On définit la somme de A et B comme étant le symétrique du troisième par rapport à l'axe des abscisses. La figure ci-dessous illustre le propos.



3.3.1.2 Algorithme d'addition de deux points

Soient A et B deux points de $\mathcal{E}$. On cherche à calculer les coordonnées de $A + B = C$. Bien qu'il faille se placer dans le plan projectif pour assurer l'existence de C on calcule ici les coordonnées affines de C plutôt que ses coordonnées projectives : il suffit de traiter le cas particulier du point à l'infini à part. Les coordonnées de C sont :

- Si $A = P_\infty$ alors $C = B$.
- Si $B = P_\infty$ alors $C = A$.
- Sinon, on peut noter (x_A, y_A) les coordonnées de A et (x_B, y_B) celles de B.
  1. Si $x_A = x_B$ et $y_A = -y_B$ (A et B sont opposés), alors $C = P_\infty$.
  2. Sinon, on peut calculer le coefficient directeur λ de la droite joignant A et B puis les coordonnées (x_C, y_C) de C. On obtient :

$$\lambda = \begin{cases} \frac{y_B - y_A}{x_B - x_A} & \text{si} \quad A \neq B \\ \frac{3x_A^2 + a}{2y_A} & \text{si} \quad A = B \end{cases}$$

$$Puis \quad \begin{cases} x_C = & \lambda^2 - x_A - x_B \\ y_C = & \lambda(x_A - x_C) - y_A \end{cases}$$

3.3.1.3 Cette loi munit $\mathcal{E}$ d'une structure de groupe commutatif

Théorème 3.3.2

$(\mathcal{E}, +)$ est un groupe commutatif dont l'élément neutre est P_∞.

Preuve:

On démontre ici tous les axiomes sauf l'associativité
La loi est interne par le **théorème de Bézout**3.3.1.
P_∞ est un neutre pour $+$
Soit $P \in \mathcal{E}$. Si $P = P_\infty$ alors P est son propre opposé. Sinon, on peut écrire les coordonnées de P sous la forme (x_P, y_P) et le point $\tilde{P}$ de coordonnées $(x_P, -y_P)$ est l'opposé de P.
En effet la droite $(P\tilde{P})$ est verticale donc intersecte $\mathcal{E}$ en P_∞ dont l'opposé est aussi P_∞.
Donc $P + \tilde{P} = P_\infty$.
Enfin, la commutativité est claire puisque la droite passant par deux points A et B de $\mathcal{E}$ est la même que celle passant par B et A.

■

La suite de cette section est consacrée à la preuve de l'associativité de la loi

Lemme 3.3.1

Soit $A = \begin{pmatrix} a_1 & b_1 \\ a_2 & b_2 \\ a_3 & b_3 \\ a_4 & b_4 \end{pmatrix}$ *une matrice de* $\mathbf{M}_{4,2}(\mathbf{K})$ *dont les lignes sont deux à deux indépendantes. Alors, pour tous polynômes P et Q premiers entre eux de $\mathbf{K}[X]$ tels qu'il existe quatre polynômes*

U_1, U_2, U_3 et U_4 de $\mathbf{K}[X]$ tel que :

$$\begin{cases} a_1P + b_1Q = U_1^2 \\ a_2P + b_2Q = U_2^2 \\ a_3P + b_3Q = U_3^2 \\ a_4P + b_4Q = U_4^2 \end{cases}$$

on a : P et Q sont constants.

Preuve:

Procédons par l'absurde.
On choisit dès lors P et Q vérifiant les hypothèses et dont l'un des deux n'est pas constant ; il est loisible de supposer $M = max(deg(P), deg(Q)) > 0$ minimal.
Le but est de construire une matrice B vérifiant les mêmes hypothèses que A et telle que les polynômes U_1 et U_2 donnés par hypothèse jouent le rôle de P et Q avec la matrice B. Les deux égalités $a_1P + b_1Q = U_1^2$ et $a_2P + b_2Q = U_2^2$ assurant que $M = max(deg(U_1), deg(U_2)) \leq \frac{1}{2}M$, la minimalité de M sera contredite.

- Remarquons que pour tout couple (i, j) de $[\![1, 4]\!]$ tel que $i \neq j$, U_i et U_j n'ont pas de racine commune. Sinon il existerait $s \in \mathbf{K}$ tel que $U_i(x) = U_j(x) = 0$. Alors, les égalités $a_iP(x) + b_iQ(x) = 0$ et $a_jP(x) + b_jQ(x) = 0$ assurent l'existence d'une racine commune à P et Q ce qui contredit $P \wedge Q = 1$.
- Comme la famille $\{(a_1, b_1), (a_2, b_2)\}$ est libre dans $\mathbf{K}^2$, c'en est une base. Donc il existe $(\overline{\alpha}, \overline{\beta}, \overline{\gamma}, \overline{\delta}) \in \mathbf{K}^4$ tel que

  $$\begin{cases} (a_3, b_3) = \overline{\alpha}(a_1, b_1) + \overline{\beta}(a_2, b_2) \\ (a_4, b_4) = \overline{\gamma}(a_1, b_1) + \overline{\delta}(a_2, b_2) \end{cases}$$

  Comme $\mathbf{K}$ est algébriquement clos, il existe $(\alpha, \beta) \in \mathbf{K}^2$ tel que $\alpha^2 = \overline{\alpha}$ et $\beta^2 = -\overline{\beta}$. Un rapide calcule montre alors que $U_3^2 = (\alpha U_1 + \beta U_2)(\alpha U_1 - \beta U_2)$. De même, il existe $(\gamma, \delta) \in \mathbf{K}^2$ tel que $U_4^2 = (\gamma U_1 + \delta U_2)(\gamma U_1 - \delta U_2)$.
  Le premier point garantit que α, β, γ et δ sont différents de 0.
- Notons $B = \begin{pmatrix} \alpha & \beta \\ \alpha & -\beta \\ \gamma & \delta \\ \gamma & -\delta \end{pmatrix}$. L'hypothèse de non constance de P ou Q ainsi que l'absence de racine commune à U_3 et U_4 permet de montrer que les lignes de B sont deux-à-deux indépendantes.
- Les polynômes $\alpha U_1 + \beta U_2$ et $\alpha U_1 - \beta U_2$ n'ont pas de racine commune sinon, U_1 et U_2 ont une racine commune ce qui contredit le premier point. Cette observation et le fait que $U_3^2 = (\alpha U_1 + \beta U_2)(\alpha U_1 - \beta U_2)$ assurent que $\alpha U_1 + \beta U_2$ et $\alpha U_1 - \beta U_2$ sont des carrés. De même, $(\gamma U_1 + \delta U_2)$ et $(\gamma U_1 - \delta U_2)$ sont des carrés.
- **Conclusion** : la matrice B et les polynômes U_1 et U_2 vérifient les hypothèses du **lemme**3.3.1 et invalident la minimalité de M.

■

Lemme 3.3.2

On rappelle que $\mathcal{E}$ est une courbe elliptique décrite par l'équation $Y^2 = X^3 + aX + b$. Soit T une indéterminée. Alors il n'existe pas de fonctions rationnelles R et S de $\mathbf{K}[T]$ non constantes et telles que $S(T)^2 = R(T)^3 + aR(T) + b$.

Preuve:

Supposons par l'absurde qu'il existe $(P_1, P_2) \in \mathbf{K}[X]$(resp. Q_1, Q_2) n'ayant pas de racine commune et tel que $R(T) = \frac{P_1(T)}{P_2(T)}$ est non constant (resp. $S(T) = \frac{Q_1(T)}{Q_2(T)}$ est non constant). On aurait alors

$$Q_1(T)^2 P_2(T)^3 = \left(P_1(T)^3 + aP_1(T)P_2(T)^2 + bP_2(T)^3\right) Q_2(T)^2 \qquad (3)$$

Comme Q_1 et Q_2 n'ont pas de racine commune et comme $\mathbf{K}$ est algébriquement clos, $Q_1^2 \wedge Q_2^2 = 1$. Comme $Q_2^2 \mid Q_1^2 P_2^3$, par le **lemme de Gauss**1.2.3, $Q_2^2 \mid P_2^3$. On montre de même que $P_2^3 \mid Q_2^2$. Les polynômes P_2^3 et Q_2^2 sont donc associés. On peut les supposer égaux et simplifier l'égalité (3) en

$$Q_1^2 = P_1^3 + aP_1P_2^2 + bP_2^3 \qquad (4)$$

Comme $\mathbf{K}$ est algébriquement clos et que $\mathcal{E}$ est une courbe elliptique, il existe $(e_1, e_2, e_3) \in \mathbf{K}^3$ deux à deux distincts tel que $X^3 + aX + b = (X - e_1)(X - e_2(X - e_3)$. Cette égalité associée à l'égalité (4) donne

$$Q_1^2 = (P_1 - e_1P_2)(P_1 - e_2P_2)(P_1 - e_3P_2) \qquad (5)$$

Or, on montre facilement par l'absurde que pour tout $(i, j) \in [\![1, 3]\!]^2$ tel que $i \neq j$, $P_1 - e_iP_2$ et $P_1 - e_jP_2$ n'ont pas de racine commune. Cette observation associée au fait que $\prod_{i=1}^{3}(P_1 - e_iP_2)$ est le carré du polynôme Q_1 par (5) assure que pour tout $i \in [\![1, 3]\!]$, $P_1 - e_jP_2$ est le carré d'un polynôme.

Considérons dès lors la matrice $A = \begin{pmatrix} 1 & -e_1 \\ 1 & -e_2 \\ 1 & -e_3 \\ 0 & 1 \end{pmatrix}$ dont les lignes sont deux à deux indépendantes. Cette matrice et les polynômes P_1 et P_2 entrent dans les hypothèses du **lemme**3.3.1. On en déduit que P_1 et P_2 sont constants puis que R l'est aussi ce qui est une contradiction. ■

Lemme 3.3.3

Soient P et Q deux points de $\mathcal{E}$. Supposons qu'il existe $h \in \mathbf{K}(\mathcal{E})$ telle que $(P) - (Q) = Div(h)$. Alors $P = Q$.

Preuve:

Par l'absurde, $P \neq Q$.

- Remarquons d'abord que pour tout $c \in \mathbf{K}$, $h - c$ a un unique pôle simple en Q puisque Q est pôle simple de H par hypothèse.
- Soit $f \in \mathbf{K}(\mathcal{E})$.
  Si $ord_Q(f) = 0$, observons $\prod_{R \in \mathcal{E}} (h(X, Y) - h(R))^{ord_R(f)}$. Cette fonction a les mêmes zéros que f. De plus, les pôles de g sont ceux des $h - h(R)$ où R décrit $\mathcal{E}$. Le premier point assure que le seul pôle de g est Q. Enfin, ce pôle est de même ordre que dans f puisque

$ord_Q(g) = \sum_{R \in \mathcal{E}} ord_R(f) = deg(Div(f)) = 0$ par le **théorème**3.2.1.
On en déduit que f et g ont même diviseur donc qu'elles sont proportionnelles par la **proposition**3.2.2. Donc f est une fraction rationnelle en h.
Si Q est zéro ou pôle de f, on applique le raisonnement précédent à $f \times h^{ord_Q(f)}$ qui n'a ni zéro ni pôle en Q. On conclut à nouveau que f est une fraction rationnelle en h.

- On a montré : $\forall f \in \mathcal{E}$ est une fraction rationnelle en h. En particulier, X et Y sont des fonctions rationnelles en h. C'est impossible par le **lemme**3.3.2.

■

Théorème 3.3.3

La loi + induite sur $\mathcal{E}$ est associative.

Preuve:

L'objectif est de montrer que $\mathcal{E}$ est en bijection avec le groupe $\frac{Div^0(\mathcal{E})}{Princ(\mathcal{E})}$.
Pour tout $D \in Div^0(\mathcal{E})$, on note $[D]$ la classe de D modulo les diviseurs principaux.
On montre que $\phi : \begin{cases} \mathcal{E} & \to & \frac{Div^0(\mathcal{E})}{Princ(\mathcal{E})} \\ P & \longmapsto & [(P) - (P_\infty)] \end{cases}$ est une bijection.
Prouvons donc que : $\forall D \in Div^0(\mathcal{E})$, $\exists! P \in \mathcal{E}$ tel que $D - (P) + (P_\infty)$ est principal.

Existence :
Soient $D \in Div^0(\mathcal{E})$. Comme $deg(D) = 0$, le **corollaire**3.2.1 assure qu'il existe $P \in \mathcal{E}$ tel que $D \sim (P) - (P_\infty)$.

Unicité :
Soit P et Q deux points de $\mathcal{E}$ tels que $(P) - (P_\infty) \sim (Q) - (P_\infty)$. Alors $(P) - (Q)$ est un diviseur principal et le **lemme**3.3.3 assure que $P = Q$.
On montre à présent que $(P, Q) \in \mathcal{E}$, $\varphi(P + Q) = \varphi(P) + \varphi(Q)$.
Si $P = Q = P_\infty$, $\varphi(P_\infty) = [(P_\infty) - (P_\infty)] = 0 = \varphi(P_\infty) + \varphi(P_\infty)$.
Si $P = -Q$, $\varphi(P + Q) = \varphi(P_\infty) = 0$. D'autre part,

$$\begin{array}{rcll} \varphi(P) + \varphi(Q) & = & [(P) - (P_\infty)] + [(-P) - (P_\infty)] & \\ & = & [(P) + (-P_\infty) - 2(P_\infty)] & \\ & = & [(P - P) + (P_\infty) + Div(g) - 2(P_\infty)] & \text{où} \quad g \in \mathbf{K}(\mathcal{E}) \\ & = & [Div(g)] & \\ & = & 0 & \end{array}$$

Sinon, notons L le polynôme décrivant la droite $\mathcal{D}$ passant par P et Q (éventuellement la tangente à $\mathcal{E}$ en P si $P = Q$), R le troisième point d'intersection entre $\mathcal{D}$ et $\mathcal{E}$, et V le polynôme décrivant la droite verticale passant par R. On a :

$$\begin{cases} Div(L) = (P) + (Q) + (R) - 3(P_\infty) \\ Div(V) = (R) + (-R) + (R) - 2(P_\infty) \end{cases}$$

Comme $Div(\frac{L}{V}) = (P) + (Q) - (P + Q) - (P_\infty)$ est principal,$(P) + (Q) - (P + Q) - (P_\infty) \sim 0$.
Donc il existe $g \in \mathbf{K}(\mathcal{E})$ tel que $(P) + (Q) - (P + Q) - (P_\infty) = Div(g)$. On réécrit cette égalité

sous la forme : $(P)-(P_\infty)+(Q)-(P_\infty)=(P+Q)-(P_\infty)$. En passant aux classes d'équivalence modulo $Princ(\mathcal{E})$, on obtient :

$$[(P)-(P_\infty)]+[(Q)-(P_\infty)]=[(P+Q)-(P_\infty)]$$

c'est-à-dire $\varphi(P)+\varphi(Q)=\varphi(P+Q)$.
Le quotient $\frac{Div^0(\mathcal{E})}{Princ(\mathcal{E})}$ est un groupe : l'addition y est donc associative. Comme l'opération + sur $\mathcal{E}$ lui est isomorphe, + est également associative. Cela conclut la preuve du fait que $(\mathcal{E},+)$ est un groupe.

■

3.3.2 Comment crypter un message avec une courbe elliptique

Soit p un nombre premier. Alors $(\mathcal{E}(\mathbf{F}_p),+)$ est un groupe fini. On peut utiliser ce groupe pour chiffrer et déchiffrer des messages via le cryptosystème suivant dit cryptosystème à clé publique de ElGamal sur courbe elliptique.

- Données publiques : un entier premier p, une courbe elliptique $\mathcal{E}$ sur $\mathbf{F}_p$ et un point P de $\mathcal{E}(\mathbf{F}_p)$.
- Création de la clé d'Alice : Alice choisit un entier n_A, qui sera sa clé privée. Puis elle calcule et diffuse le point $Q_A=n_AP$ qui sera sa clé publique.
- Chiffrement d'un message : Connaissant Q_A, Bob souhaite envoyer un message clair $M\in\mathcal{E}(\mathbf{F}_p)$. Pour ce faire, il choisit une clé éphémère $k\in\mathbb{N}$; puis il calcule $C_1=kP$ et $C_2=M+kQ_A$. Il envoie enfin le message chiffré (C_1,C_2).
- Déchiffrement du message : Alice calcule $C_2-n_AC_1=M+kn_AP-n_AkP=M$ et retrouve le message clair.

Une façon pour Eve de déchiffrer un message est de retrouver la clé privée d'Alice connaissant P et Q_A. Il lui faut alors résoudre l'équation en x suivante : $xP=Q_A$. C'est un calcul de logarithme discret.

3.4 L'algorithme MOV

L'objet mathématique qui permet de transférer le logarithme discret d'une courbe elliptique vers un corps fini s'appelle un couplage. C'est l'équivalent pour les groupes des applications bilinéaires non dégénérées. Les couplages mathématiques permettent de construire une fonction à sens unique avec trappe. Cependant, les couplages ont d'abord été utilisés en cryptanalyse pour ramener le problème du logarithme discret depuis les courbes elliptiques à celui des corps finis, pour lequel on connaît des algorithmes sous-exponentiels tels que : *l'algorithme MOV* du nom de ses auteurs *Menezes, Okamoto et Vanstone* créé en 1993. Nous parlerons beaucoup plus en détail de cet algorithme dans la suite.

Dans cette section, $\mathbf{K}$ désigne un corps de caractéristique différente de deux et trois. On en considère la clôture algébrique au besoin. $\mathcal{E}$ une courbe elliptique sur $\mathbf{K}$ décrite par l'équation $Y^2=X^3+aX+b$.

3.4.1 Points de n-torsion

Défnition 3.4.1 (Groupe de n-torsion)

Soit n un élément de $\mathbb{N}$. Le groupe de n-torsion de $\mathcal{E}$, noté $\mathcal{E}[n]$, est l'ensemble de points $\{P \in \mathcal{E} | nP = P_\infty\}$.

Proposition 3.4.1

Soit $n \in \mathbb{N}$. Alors $\mathcal{E}[n]$ est isomorphe à $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. En particulier, le cardinal de $\mathcal{E}[n]$ est n^2.

Preuve:

Cf [1]

■

3.4.2 Couplage de Weil

3.4.2.1 Première définition

Cette première définition du couplage de Weil permet d'en montrer facilement les propriétés.

Notation : Soit $n \in \mathbb{N}$. On note $[n] : \left\{ \begin{array}{ccc} \mathcal{E} & \longrightarrow & \mathcal{E} \\ P & \longmapsto & nP \end{array} \right.$

Lemme 3.4.1

Soient $n \in \mathbb{N}$ et $T \in \mathcal{E}[n]$ tel qu'il existe T_0 tel que $nT_0 = T$. Les diviseurs $n(T) - n(T_0)$ et $D_T = \sum_{P|nP=T} (P) - \sum_{P \in \mathcal{E}[n]} (P)$ sont principaux.

Preuve:

Comme le diviseur $n(T) - n(T_0)$ a pour degré 0 et somme P_∞, il est principal par le **théorème**3.2.1. Donc il existe $f_T \in \mathbf{K}(\mathcal{E})$ tel que $Div(f_T) = n(T) - n(T_0)$.
Pour D_T, remarquons que $\{P \in \mathcal{E} \mid nP = T\} = \{P \in \mathcal{E} \mid \exists R \in \mathcal{E}[n] : P = R + T_0\}$. On en déduit que $deg(D_T) = 0$. De plus,

$$\begin{array}{rcl} Som(D_T) & = & \sum_{P \in \mathcal{E}[n]} (P + T_0) - \sum_{P \in \mathcal{E}[n]} P \\ & = & \sum_{P \in \mathcal{E}[n]} T_0 \\ & = & n^2 T_0 \quad \text{par la } \textbf{proposition}3.4.1 \\ & = & nT = P_\infty \end{array}$$

Donc D_T est aussi principal et il existe $g_T \in \mathbf{K}(\mathcal{E})$ tel que $D_T = Div(g_T)$.

■

Proposition 3.4.2

On reprend les notations du lemme précédent.
Alors $Div(f_T \circ [n]) = Div(g_T^n)$.

Preuve:

Esquisse de démonstration :
On montre que les zéros et pôles de $f_T \circ [n]$ et g_T^n sont les mêmes. Comme elles sont définies à une constante multiplicative près, on peut même supposer que $f_T \circ [n] = g_T^n$.

■

Défnition 3.4.2 (Couplage de Weil)

Soit $P \in \mathcal{E}$. On appelle couplage (ou appariement) de Weil l'application suivante :

$$e_n : \begin{cases} \mathcal{E}[n] \times \mathcal{E}[n] & \longrightarrow & U_n = \{x \in \overline{\mathbf{K}} \mid x^n = 1\} \\ (S,T) & \longmapsto & \frac{g_T(P+S)}{g_T(P)} \end{cases} \quad \text{où } P \text{ est un élément de } \mathcal{E}.$$

Preuve:

La définition de e_n résulte des notions sur les morphismes sur $\mathcal{E}$ et les isogénies que nous n'avons pas le temps de développer ici.

Le fait que e_n est à valeurs dans $\mathbf{U}_n$ est en revanche clair puisque, pour tout $S \in \mathcal{E}[n]$, pour tout $P \in \mathcal{E}$, on a :

$$g_T(P+S)^n = f_T(nP+nS) = f_T(nP) = g_T(P)^n$$

■

Le couplage de Weil e_n vérifie les propriétés suivantes qui résultent des notions d'isogénies :

1. Bilinéarité : $\forall (R,S,T) \in \mathcal{E}[n]$, $\begin{cases} e_n(R+S,T) = e_n(R,T)e_n(S,T) \\ e_n(R,T+S) = e_n(R,T)e_n(R,S) \end{cases}$
2. e_n est non dégénérée :
   Soit $S \in \mathcal{E}[n]$. Si pour tout $T \in \mathcal{E}[n]$ on a $e_n(S,T) = 1$ alors $S = P_\infty$.
   De même, soit $T \in \mathcal{E}[n]$. Si pour tout $S \in \mathcal{E}[n]$ on a $e_n(S,T) = 1$ alors $T = P_\infty$.
3. e_n est normale : $\forall T \in \mathcal{E}[n]$, $e_n(T,T) = 1$.
4. e_n est antisymétrique : $\forall (S,T) \in \mathcal{E}[n]$. $e_n(S,T) = \frac{1}{e_n(T,S)}$

3.4.2.2 Seconde définition

Défnition 3.4.3 *(Seconde définition du couplage de Weil)*

Soient $n \in \mathbb{N}$ et S et T deux éléments distincts de $\mathcal{E}[n]$. On note f_T(resp. f_S) une fonction de $\mathbf{K}(\mathcal{E})$ dont le diviseur est $n(T) - n(P_\infty)$ (resp. $n(S) - n(P_\infty)$). Ces fonctions ont même degré et sont définies à une constante multiplicative près : on les choisit de telle sorte que $\frac{f_T}{f_S}(P_\infty) = 1$ (on dit alors que f_T et f_S sont normalisées).
Si f_T et f_S sont normalisées alors $e_n(S,T) = (-1)^n \frac{f_T(S)}{f_S(T)}$.

Algorithme 3.4.1 *(Calcul du couplage de Weil)*

Pour calculer $e_n(T,S)$ il suffit, selon la dernière définition, de savoir calculer $f_S(T)$ (et $f_T(S)$ par le même procédé) où S et T sont des éléments de $\mathcal{E}[n]$.
Pour tout $i \in [\![1,t]\!]$, on note D_i le diviseur $i(S) - (iS) - (i-1)(P_\infty)$. Il est principal donc est le diviseur d'une fonction f_I de $\mathbf{K}(\mathcal{E})$. Pour $i = n$, en particulier $D_n = n(S) - (nS) - (n-1)(P_\infty) = n(S) - n(P_\infty) = Div(f_S)$. On peut donc supposer $f_n = f_S$.
L'idée est de calculer par récurrence les $f_i(T)$ pour obtenir $f_S(T)$.

Lemme 3.4.2

Soit $S \in \mathcal{E}[n]$ et $(i,j) \in \mathbb{N}^{*2}$

- *Si* $(i+j)S = P_\infty$ *alors* $f_{i+j} = f_i f_j \frac{l}{d}$ *où* l *est le polynôme décrivant la droite passant par* iS *et* jS *et* d *est celui décrivant la droite verticale qui passe par* $(i+j)S$.
- *Si* $(i+j)S = P_\infty$ *alors* $f_{i+j} = f_i f_j d$ *où* d *est le polynôme décrivant la droite verticale passant par* iS *et* jS.

Preuve:

- Si $(i+j)S \neq P_\infty$, il suffit de montrer que $Div(f_{i+j}) = Div(f_i)+Div(f_j)+Div(f_l)-Div(f_d)$. Or, par un rapide calcul n'utilisant que la définition des f_i, on trouve que ces deux quantités sont égales à $(i+j)(S) - ((i+j)S) - (i+j-1)(P_\infty)$ ce qui conclut.
- Si $(i+j)S = P_\infty$, il suffit de montrer que $Div(f_{i+j}) = Div(f_i) + Div(f_j) + Div(d)$. Un calcul similaire montre que ces deux quantités sont égales à $(i+j)S - (i+j)P_\infty$.

On commence donc par calculer $f_1 = 1$. Puis on obtient f_n en construisant n par une chaîne d'additions ; c'est-à-dire qu'on construit une suite $i_0 = 1 < i_1 < \cdots < i_l = n$ telle que $\forall j \geq 1, \exists a, b < j$ tel que $i_j = i_a + i_b$.

■

Remarques 3.4.1

- *Pour que le calcul aboutisse,* T *ne doit pas être un zéro d'une droite verticale passant par un point* kS *(annulation du dénominateur). Mais, s'il existe* k *tel que* T *est sur la droite verticale passant par* kS *alors* $T = \pm kS$. *Dans ce cas,* $e_n(S,T) = e_n(S, \pm kS) = e_n(S,S)^{\pm k} = 1$
- *Pour obtenir des fonctions normalisées, il suffit de rendre les* f_i *unitaires. Pour ce faire, il suffit d'écrire les droites verticales sous la forme* $X - x_P$ *et les autres sous la forme* $Y + aX + b$.

3.4.2.3 Une application du couplage de Weil : l'algorithme MOV

Défnition 3.4.4 *(Racine n-ième primitive de l'unité)*

Une racine n-ième primitive de l'unité dans un corps $\mathbf{K}$ *est un élément* $x \in \mathbf{K}^\times$ *tel que* $x^n = 1$ *et* x *est d'ordre exactement* n *dans* $\mathbf{K}^\times$.

Proposition 3.4.3

Soit $n \in \mathbb{N}$. *Soient* P *et* S *deux points de* $\mathcal{E}[n]$. *Alors,* (P,S) *est une base de* $\mathcal{E}[n]$ *si et seulement si* $\rho = e_n(P,S)$ *est une racine n-ième primitive de l'unité.*

Preuve:

Supposons que (P,S) est une base de $\mathcal{E}[n]$. Soit $d \in \mathbb{N}$ tel que $\rho^d = 1$. On a déjà $d \leq n$. Il suffit donc de montrer que $n \mid d$ pour conclure que ρ engendre U_n.
Soit $R \in \mathcal{E}[n]$. Comme (P,S) est une base de $\mathcal{E}[n]$, il existe $(a,b) \in \mathbb{Z}$ tel que $R = aP + bS$. Donc

$$e_n(R, dS) = e_n(aP + bS, dS) = e_n(P,S)^{da} e_n(S,S)^{db} = 1$$

Comme e_n est non dégénérée, cela implique que $dS = P_\infty$ donc que l'ordre de S (à savoir n puisque S engendre une groupe isomorphe à $\mathbb{Z}/n\mathbb{Z}$) divise d.
Réciproquement, si ρ est une racine n-ième primitive de l'unité, on montre que P et S sont d'ordre n.

■

Proposition 3.4.4

Soient p un nombre premier et S un élément de $\mathcal{E}[n]$. On note k l'entier tel que $\overline{\mathbf{F}_p} = \mathbf{F}_{q^k}$ et $U_n = \{x \in \mathbf{F}_{q^k} \mid x^n = 1\}$. Alors, $h_S : \begin{cases} \mathcal{E}[n] & \longrightarrow & U_n \\ R & \longmapsto & e_n(R,S) \end{cases}$ est un isomorphisme de groupes.

Preuve:

La bilinéarité de e_n implique que h_S est un morphisme. La proposition3.4.3 garantit la bijection.
■

Le but est d'utiliser cette bijection de façon à ramener le calcul d'un logarithme discret dans $\mathcal{E}$ à un calcul de logarithme discret dans $\mathbf{F}_{q^k}$, corps dans lequel on a des algorithmes efficaces.

Algorithme 3.4.2 *Algorithme MOV (Menezes, Okamoto et Vanstone)*

Entrée : *un point P d'ordre n dans $\mathcal{E}(\mathbf{F}_q)$ et un point Q appartenant au sous groupe de $\mathcal{E}[n]$ engendré par P.*
Sortie : *Un entier l tel que $lP = Q$.*

1. *On détermine un entier k tel que $\mathcal{E}[n] \subset \mathcal{E}(\mathbf{F}_{q^k})$.*
2. *On choisit $S \in \mathcal{E}(\mathbf{F}_{q^k})$ tel que (P,S) est une base de e_n (par exemple, on choisit S au hasard dans $\mathcal{E}[n]$ jusqu'à ce que (P,S) soit une base de $\mathcal{E}[n]$).*
3. *On calcule $\alpha = e_n(P,S)$ et $\beta = e_n(Q,S)$.*
4. *Dans $\mathbf{F}^{\times}_{q^k}$, on calcule un logarithme l de β en base α.*

Preuve:

On montre que l est bien un logarithme de Q en base P. On sait qu'il existe $j \in \mathbb{N}$ tel que $Q = jP$ et que l'algorithme MOV trouve un entier l tel que $e_n(P,S)^l = e_n(Q,S)$. Donc

$$e_n(P,S)^l = e_n(Q,S) = e_n(jP,S) = e_n(P,S)^j$$

Donc $e_n(P,S)^{l-j} = 1$. Or, $e_n(P,S)$ est une racine primitive de l'unité (puisque (P,S) est une base de $\mathcal{E}[n]$). Donc $l \equiv j \bmod n$ ce qui conclut.
■

Remarques 3.4.2

- *Ni la complexité de cet algorithme, ni le calcul effectif de k dans la première étape n'ont été étudiés.*
- *Plus l'entier k est petit, plus le calcul de logarithme discret dans $\mathbf{F}^{\times}_{q^k}$ est facile. Pour que le PLD sur une courbe elliptique soit compliqué, il faut donc éviter les courbes pour lesquelles k est petit.*

Conclusion

L'objectif de ce mémoire était d'une part de présenter *le problème du Logarithme Discret dans les groupes multiplicatifs* et de donner quelques *méthodes de résolution dudit problème*. D'autre part, d'aborder ce problème sur *les courbes elliptiques* en s'appuyant théoriquement sur *l'algorithme MOV qui est une méthode de résolution du Problème du Logarithme Discret sur courbes elliptiques*. Toutes les deux parties de cet objectif ont été remplies. L'algorithme MOV n'a pas été implémenté car plusieurs outils permettant l'implémentation dudit algorithme ne sont pas abordés dans ce mémoire.

Cependant, il existe d'autres algorithmes permettant de résoudre le problème du logarithme discret sur courbes elliptiques. Parmi ces algorithmes, on peut citer : *l'algorithme Tate*, créé en 1994 par Frey et Ruck, un an après l'apparition de *l'algorithme MOV*.

La suite logique de ce travail serait de déterminer des courbes bien couplées résistantes à ces attaques et éventuellement développer un autre cadre où des couplages peuvent être définis.

Bibliographie

[1] BLAKE Ian F. , SEROUSSI G. et SMART Nigel P. , (1999) , Elliptic Curves in Cryptography , ISBN : 0521653746

[2] BUCHMANN Johannes A. , (2006) , Introduction à la cryptographie , ISBN13 : 9782100496228 , (262) pages.

[3] CONRAD. K. , THE CHINESE REMAINDER THEOREM, (11) pages , dispoinble sur https ://kconrad.math.uconn.edu/blurbs/ugradnumthy/crt.pdf

[4] DELAUNAY C. , (2015) , LE PROBLEME DU LOGARITHME DISCRET EN CRYPTOGRAPHIE , disponible sur https ://images.math.cnrs.fr/Le-probleme-du-logarithme-discret-en-cryptographie

[5] LE GLUHER. A. , (2015) , Problème du logarithme discret appliqué à la cryptanalyse sur courbes elliptiques : ALGORITHME MOV , (30) pages , disponible sur : http ://perso.eleves.ens-rennes.fr/people/Aude.Legluher/fr/rapportl3.pdf

[6] LIMA. V. , 31 janvier 2013 , Algorithmes de cryptographie et le problème du logarithmes discret , (13) pages , disponible sur : https ://lucianolarrossa.com/wp-content/uploads/2013/03/rapport.pdf

[7] MIMRAM. S. , (2006) , Courbes elliptiques et factorisation (version détallée) , (25) pages , disponible sur : http ://www.lix.polytechnique.fr/Labo/Samuel.Mimram/docs/prepa/tipe-ecc.pdf

[8] VITSE V. , (2013) , Des corps, des couplages, des messages codés et des logarithmes discrets, disponible sur https ://images.math.cnrs.fr/Des-corps-des-courbes-des-2407

[9] WALLENBORN. Lars A. , (2010) , Elliptic Curves, Divisors and Lines , (27) pages , disponible sur : https ://www.wallenborn.net/download/Talk-Algebraic-Methods-in-Computation-Complexity-Elliptic-Curves-Divisors-and-Lines.pdf

[10] ZEMOR. G. , (2001) , Cours de cryptographie , ISBN13 : 9782842250201 , (228) pages.

Annexe : Implémentation des algorithmes du chapitre 2

1. **Prérequis pour l'implémentation des algorithmes**

Algorithme d'Euclide et théorème des restes chinois :

```
#Entree = Deux entiers naturels non nuls .
#Sortie = Le plus grand diviseur commun a ces deux entiers .
def pgcd(a, b):
    aa = max(a, b)
    bb = min(a, b)
   while aa % bb!= 0:
      aa, bb = bb, aa % bb
   return bb


#Entree = Deux entiers naturels eventuellement nuls, a et b.
#Sortie = Le couple d'entiers de Bezout (u , v) (dans cet ordre)
#tel que au+bv = pgcd (a, b ).
def bezout (a, b):
    r_0 = max(a, b)
    r_1 = min(a, b)
    u_0 = 1
    u_1 = 0
    v_0 = 0
    v_1 = 1
    while r_1!= 0:
        q = r_0/r_1
        r_0, r_1 = r_1, r_0 - q*r_1
        u_0, u_1 = u_1, u_0 - q*u_1
        v_0, v_1 = v_1, v_0 - q*v_1
    if  (a == 0 or b == 0):
         u_0, v_0 = 1, 1
    elif a % b == 0:
         u_0 = 1
         v_0 = -a/b +1
    elif b % a ==0:
         u_0 = -b/a +1
```

```
        v_0 = 1
    if a >= b:
       return u_0, v_0
    else:
       return v_0, u_0


#Entree = Un entier a et un nombre premier p.
#Sortie = Un representant de la classe de l'inverse de la classe
#de a modulo p.
def inv(a, p):
aa = a % p
u, v = bezout(aa, p)
return u


#Entree = Une liste l et un entier n.
#Sortie = La liste l privee des n premiers elements.
def enleve(l, n):
    return l[n:]


#Entree = Deux couples d'entiers tels que m et n sont premiers-
#entre eux.
#Sortie = Une solution x de systeme : x = a mod n; x = b mod m.
def th_chinois_2((a, n), (b, m)):
    u, v = bezout(n, m)
    return (b*n*u + a*m*v)%(nm)


#Entree = Une liste de couples (a_i, m_i) telle que
#les m_i sont deux a deux premiers entre-eux.
#Sortie = La solution x du systeme de congruences x = a_i mod
#m_i qui se trouve entre 0 et le produit des m_i.
def th_ chinois(l):
    while len(l) != 2:
        M = l[0][1]*l[1][1]
        c = th_chinois_2( l[0], l[1]) % M
        l = enleve(l, 2)
        l = [(c, M)]+l
    return th_chinois_2(l[0], l[1])
```

2. **Recherche Exhaustive**

```
import math

import time


# On calcule g^i pour tout i appartenant à [1, p]

def exhaustive_discret_logarithm(g, h, p):

    k = 1

    for i in range(1, p):

        print("L'indice de l'élément actuel: %d" % i)

        k = (k * g) % p

        if (k == h):

            return i

 # Ca signifie que x n'est pas trouvable
   return -1


g = int(input("Entrez la valeur de g: "))

h = int(input("Entrez la valeur de h: "))

p = int(input("Entrez la valeur de p: "))

start = time.perf_counter_ns()

x = exhaustive_discret_logarithm(g, h, p)

end = time.perf_counter_ns()

print("time: %dns, x: %d" % (end - start, x))
```

Résultats:

```
Avec g = 2, h = 7, p = 59.
On a x = 18 en 951650600 ns = 0,9516506 s

avec g = 12569, h = 1254, p = 10007
On a x = 2784 en  6728493300 ns = 6,7284933 s


Avec g = 1255, h = 598435, p = 800011
On a x = 417915 en 214554682700 ns = 214,5546827 s = 3,575911378 min
```

3. **Baby-steps /Giant-steps**

```
import math

import time


#Entree = (g : un entier), (A: un entier naturel), (N: un entier
#naturel)
#Sortie = Le resultat de g^A modulo N par exponentiation rapide.
def sqm(g, A, n):
    if A == 0:
        return 1
    elif A % 2 == 0:
       b = sqm(g, A//2, n)
        return (b*b) % n
    else:
        b = sqm(g, A//2, n)
        return (b*b*g) % n


#Entree = Deux listes l1 et l2.
#Sortie = Les indices dans l1 et l2 d'un element commun aux deux.
def collision2(l1, l2):
    s1, s2 = set(l1), set(l2)
    l = list(s1 & s2)
    c = l[0]
    return l1.index(c), l2.index(c)


#Entree = Un nombre premier p et deux entiers non nuls modulo p,
#g et h tels qu'il existe une solution a l'equation g^x = h mod p.
#Sortie = Une solution x de l'equation g^x = h mod p
#Methode = Baby step-giant step.
def bs_gs(g, h, p):
    n = int(math.sqrt(p-1))+1
    bs = [0]*(n+1)
    gs = [0]*(n+1)
    bs[0] = 1
    gs[0] = h
    inverse = sqm(inv(g, p), n, p)
    for k in range(1, n+1):
        bs[k] = (bs[k-1]*g)%p
        gs[k] = (gs[k-1]*inverse)%p
        i, j = collision2(bs, gs )
return (i + n*j)
```

Résultats:

Avec g = 2, h = 7, p = 59.
On a x = 18 en 134700 ns = 0,0001347 s

avec g = 12569, h = 1254, p = 10007
On a x = 2784 en 2425100 ns = 0,0024251 s

Avec g = 1255, h = 598434, p = 800011
On a x = 417915 en 149965100 ns = 0,1499651 s

4. **Pohlig-Hellman**

```
import math

import time


#Entree = Un entier relatif x et un entier naturel n.
#Sortie = x^n par exponentiation rapide.
def power(x, n ):
    if n == 0:
       return 1
    elif n % 2 == 0:
         b = power(x, n//2)
         return b*b
    else :
         b = power(x, n//2)
         return b*b*x


#Entree = Un entier premier p; deux entiers non nuls modulo p:
#g et h tels que l'equation g^x = h mod p admet une solution et
#N = ordre de g dans Z/pZ*
#Sortie = un entier x tel que g^x = h mod p
#Methode = Pohlig Hellman en se ramenant a resoudre le PLD pour
#des elements d'ordre une PUISSANCE d'un nombre premier.
def ph(g, h, p, N):
    facteurs = fact(N)
    l = [ ]
    for cle in facteurs.keys( ):
        m_i = power(cle, facteurs[cle])
        a_i = bs_gs2(sqm(g, N//m_i, p), sqm(h, N//m_i, p), p)
        l = l + [(a_i, m_i)]
    if len(l)>= 2:
       return th_chinois(l)
    else :
       return l[0][0] #Si il n'y a qu'un facteur premier dans N
```

L'algorithme Pohlig-Hellman n'a pas pu être compiler à cause de quelques erreurs qui n'ont pas pu être rectifier. Toutefois parmi les trois méthodes vu dans le chapitre 2, la méthode de Pohlig-Hellman est la plus efficace pour résoudre le PLD dans les groupes multiplicatifs. La méthode de la Recherche Exhaustive est la plus lente parmi les trois.