Université Assane SECK de Ziguinchor

UFR : Sciences et Technologies
Département de Mathématiques

Mémoire de Master

Domaine : Sciences et Technologies
Mention : Mathématiques et Applications
Spécialité : Mathématiques Pures
Option : Géométrie algébrique
Sujet de mémoire :

Factorisation des entiers à l'aide des courbes elliptiques

Présenté par Yaya COULIBALY
Sous la direction de
Professeur Oumar SALL, Université Assane SECK de Ziguinchor
Mémoire soutenu le Vendredi 13 Mai 2022 à l'Université Assane SECK de Ziguinchor devant le jury

Prénoms et Nom	Grade	Jury	Établissement
Marie Salomon SAMBOU	Professeur Titulaire	Président	UASZ
Oumar SALL	Professeur Titulaire	Directeur	UASZ
Amoussou Thomas GUEDENON	Professeur assimilé	Examinateur	UASZ
Daouda Niang DIATTA	Maître de conférences Titulaire	Examinateur	UASZ
Moussa FALL	Maître de conférences assimilé	Examinateur	UASZ

Remerciements

Je voudrais tout d'abord exprimer toute ma reconnaissance à mon directeur de mémoire Monsieur Oumar SALL, professeur à l'Université Assane SECK de Ziguinchor qui m'a donné la chance de travailler avec lui. Je le remercie pour ses remarques scientifiques constructives et ses grandes qualités humaines.

Je voudrais remercier aussi le docteur Moussa FALL pour sa disponibilité, ses qualités scientifiques et ses conseils.

Je tiens à remercier très sincèrement Monsieur Marie Salomon SAMBOU, professeur à l'Université Assane SECK de Ziguinchor pour avoir accepté d'être président du jury et aussi pour l'opportunité qu'il m'a offerte de pouvoir exposer mon travail dans son groupe de recherche en analyse et géométrie complexe et pour l'intérêt qu'il a manifesté à mes travaux.

Je tiens à remercier Messieurs Thomas GUEDENON, professeur assimilé et Daouda Niang DIATTA, docteur à l'Université Assane SECK de Ziguinchor pour avoir accepté d'être membres du jury.

Qu'il me soit permis également de remercier tous les enseignants du département de mathématiques, sans oublier l'ensemble des étudiants des départements de mathématiques et informatique. Mes remerciements vont aussi à tous ceux qui ont contribué de près ou de loin à la réalisation de ce travail.

Je profite de cette occasion pour remercier, Messieurs Souhaibou SAMBOU, Sény DIATTA, Nestor DJINTELBE et madame Winnie Ossete INGOBA, docteurs à l'Université Assane SECK de Ziguinchor et remercier aussi

mes prédécesseurs, Pape Modou SARR, Moustapha CAMARA, Kang-Rang Seth KOUMLA, Coura KANE et Papa BADIANE pour l'aide et l'amitié qu'ils m'ont apportées, ainsi que pour des échanges et discussions autour des mathématiques.

Je ne saurais terminer sans remercier ma famille et mes amis, qui ont tous aidé à façonner mon chemin et qui m'ont aidé à arriver où j'en suis, pour m'avoir motivé et encouragé. Merci à mes parents qui ont fait tant de sacrifices pour moi. Merci à mes frères et soeurs pour leur soutien permanent, tant financier que moral. Merci à tous mes amis, en particulier Abdarhamane BA, Awa BARRY, Azize MANGA, Abdoulaye SAGNA, Daouda DIACK, Alioune BA, Mamadou Korca BA, Amadou SEYDI, Fatou DIENG, Diénaba SAMB, Seydil Diamil DIOUF, Saliou DIAW, Mamadou Nazir DIALLO, Boubacar DIOP, Sadioba SAMATE, Idrissa DIALLO, Ibrahima HOTTE, Abdou DIA, Moustapha NOMOKHO et Younousse TOURE, pour divers services qu'ils m'ont rendus ; je leur adresse à tous un joyeux salut amical.

Table des Matières

Introduction

Par référence à ses nombreuses applications dans d'autres domaines des mathématiques, la géométrie algébrique est considérée aujourd'hui comme l'une des discilplines les plus utiles et les plus belles des mathématiques.
La géométrie algébrique s'intèresse à l'étude des ensembles algébriques, c'est-à-dire ceux définis par l'annulation d'une famille de polynômes. Son origine remonte à Descartes et de nombreux autres mathématiciens : Abel, Riemann, Poincaré, Noether, l'école italienne avec Severi. Plus recemment Weil, Zariski et Chevally s'y sont illustrés. Dans les années $1950-1960$ la géométrie algébrique a connu un développement considérable et a subi un bouleversement gigantesque sous l'impulsion de J.P. Serre et surtout de A.Grothendieck.
L'objectif de ce mémoire est d'étudier un problème de géométrie algébrique d'apparence simple, mais dont la résolution fait appel à des notions non evidentes.
L'exemple choisi est la factorisation des entiers à l'aide des courbes elliptiques.
Une courbe elliptique est une cubique, irréductible, non singulière donnée par une équation de Weierstrass définie dans le plan projectif. Dans ce document, on parlera plus spécifiquement de courbe elliptique, définie sur un corps commutatif quelconque. Puis définir une courbe elliptique sur un corps particulier de caractéristique différente de 2 et de 3. La méthodologie utilisée pour cette étude est basée sur une approche comprenant trois chapitres structurés de la maniére suivante :
Le chapitre 1 : intitulé "Préliminaires" regroupe les notions de bases utiles dans les chapitres suivants. Les résultats sont souvent sans démonstration, mais illustrés par des exemples et par des remarques pour faciliter la compréhension aux lecteurs moins familiarisés avec ces théories.
Le chapitre 2 : intitulé "Méthode de LENSTRA" qui est une des parties fondementales du sujet présente une approche permettant de reconnaitre

certaines courbes adaptées à la factorisation des entiers. La reconnaissance de certaines courbes elliptiques ont un regain d'intérêt avec l'arrivée de la cryptographie moderne comme le "RSA".
Le chapitre 3 : intitulé "Autres méthodes" dans cette partie, on s'intèresse aux méthodes de factorisation qui ne font pas recours aux courbes elliptiques comme par exemple : la méthode p-1 de POLLARD, la méthode de FERMAT ...
Nous avons présenté à la fin quelques exemples d'applications pouvant intéresser des chercheurs dans le domaine à travers plusieurs branches des mathématiques.

Chapitre 1

Préliminaires

On désignera par $\mathbb{K}$ un corps commutatif (sauf mention expresse du contraire). Les définitions, les propositions et les théorèmes cités dans ce chapitre font référence aux travaux dans [1] et [2].

1.1 Division euclidienne

Définition 1.1.1. *La division euclidienne d'un nombre entier a par un nombre entier non nul b, consiste à déterminer un couple d'entiers (q, r) tel que $a = bq + r$ où $0 \leq r < |b|$. Les entiers a, b, q et r sont appelés respectivement dividende, diviseur, quotient et reste.*

Définition 1.1.2. *Lorsque le reste de la division de a par b est nul, on dit que a est un multiple de b ou que b est un diviseur de a, ou encore que a est divisible par b.*
Dans ce cas on note $b \mid a$.

Exemple 1.1.3.
$3|21$ *car* $21 = 3 \times 7$.

1.1.1 Plus grand commun diviseur de deux entiers

Définition 1.1.4. *Soient a et b deux entiers non tous nuls. Le plus grand entier qui divise à la fois a et b s'appelle le plus grand commun diviseur de a et b et se note* pgcd(a, b).

Lemme 1.1.5. *(*d'EUCLIDE)
Soient a, b, q *et* r *des entiers avec* $0 \leqslant r < |b|$.
Si $a = bq + r$ *alors* $\mathrm{pgcd(a, b)} = \mathrm{pgcd(b, r)}$.

Ce lemme nous permet de définir l'algorithme d'EUCLIDE suivant.

1.1.2 Algorithme d'EUCLIDE

Soient a et b deux entiers naturels non nuls tels que $b < a$.
• Si b divise a, alors il existe un entier q tel que $a = bq$ et $\mathrm{pgcd(a, b)} = \mathrm{b}$.
• Si b ne divise pas a, alors il existe un couple d'entiers (q, r) tel que $a = bq + r$ avec $0 \leqslant r < b$ et $\mathrm{pgcd(a, b)} = \mathrm{pgcd(b, r)}$.
On pose $r_0 = a$ et $r_1 = b$ et tant que r_i est non nul, on effectue les divisions euclidiennes successives suivantes :

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2 \ \ avec \ \ 0 \leqslant r_2 < r_1 \\
r_1 &= r_2 q_2 + r_3 \ \ avec \ \ 0 \leqslant r_3 < r_2 \\
&\vdots \\
r_{k-2} &= r_{k-1} q_{k-1} + r_k \ \ avec \ \ 0 \leqslant r_k < r_{k-1} \\
r_{k-1} &= r_k q_k + r_{k+1} \ \ avec \ \ 0 \leqslant r_{k+1} < r_k.
\end{aligned}$$

D'après le lemme d'EUCLIDE, pour tout $k > 0$, on a :

$$\mathrm{pgcd(a, b)} = \mathrm{pgcd(r_k, r_{k+1})}$$

avec $r_{k+1} = 0$.
La suite des restes $(r_2, r_3, \ldots,)$ étant une suite strictement décroissante d'entiers positifs, on obtient nécessairement un reste nul au bout d'un nombre fini k de divisions.
Soit r_n le dernier reste non nul.
On a $r_{n+1} = 0$ ce qui signifie que $\mathrm{pgcd(a, b)} = \mathrm{pgcd(r_n, 0)} = \mathrm{r_n}$.

Exemple 1.1.6.

$$\begin{aligned}
182 &= 143 \times 1 + 39 \\
143 &= 39 \times 3 + 26 \\
39 &= 26 \times 1 + 13 \\
26 &= 13 \times 2 + 0.
\end{aligned}$$

D'après le lemme d'EUCLIDE le dernier reste non nul est 13, donc le

$$\text{pgcd}(182, 143) = 13.$$

1.1.3 Nombre premier

Définition 1.1.7. *Soit p un nombre entier supérieur ou égal 2. On dit que p est premier si, ses seuls diviseurs sont 1 et lui même.*

Exemple 1.1.8.
$2, 67, 97$ *sont des nombres premiers.*

Définition 1.1.9. *Deux entiers n et m sont dits premiers entre eux si leur diviseur commun est 1, autrement dit leur* $\text{pgcd(n, m)} = 1$.

Théorème 1.1.10. *(*Théorème de BEZOUT)
Un entier d supérieur ou égal 1 est pgcd(a, b) si et seulement si, il existe deux entiers u et v tels que $au + bv = d$.

Les entiers u et v sont appelés coefficients de BEZOUT ; ils ne sont pas uniques et s'obtiennent en remontant l'algorithme d'EUCLIDE.

Corollaire 1.1.11. *(*Identité de BEZOUT)
Les entiers a et b sont premiers entre eux si et seulement si, il existe deux entiers u et v tels que $au + bv = 1$.

1.1.4 Congruence

Définition 1.1.12. *Soit n un entier naturel non nul.*
Deux entiers a et b sont dits congrus modulo n si n divise $a - b$, c'est- à- dire

$$a = b + kn, \quad k \in \mathbb{Z}$$

et on note :

$$a \equiv b\ [n] \text{ ou } a \equiv b \pmod{n}.$$

Dans la suite, nous utiliserons la relation $a \equiv b\ [n]$.

Exemple 1.1.13.
$11 \equiv 5[3]$ *car* $11 - 5 = 6$ *est un multiple de* 3.

Définition 1.1.14. *Deux entiers a et b sont dits associés ou inverses modulo n si, leur produit ab est congru à 1 modulo n.*

Propriétés 1.1.15.
Soit n entier naturel non nul.
Soient a, b, a' et b' des entiers tels que $a \equiv b\ [n]$ et $a' \equiv b'\ [n]$. Alors on a :

- $a + a' \equiv (b + b')\ [n]$
- $a - a' \equiv (b - b')\ [n]$
- $a \times a' \equiv (b \times\ b')\ [n]$
- $a^p \equiv b^p\ [n],\ p \in \mathbb{N}^*$

.

Proposition 1.1.16.
Soient a et b des entiers.
• *Si r est le reste de la division euclidienne de a par n, alors $a \equiv r[n]$.*
• *$a \equiv b[n]$ si et seulement si, ils ont le même reste dans la division euclidienne par n.*

1.1.5 Décomposition d'un nombre en facteurs premiers

Définition 1.1.17. *On appelle décomposition d'un nombre x en facteurs premiers la formule*

$$x = \prod_{i=1}^{n} p_i^{\alpha_i}$$

telle que p_i parcourt l'ensemble des nombres premiers et α_i des entiers strictement positifs.

Remarque 1.1.18. *La décomposition d'un nombre en facteurs premiers est unique (à permutations près).*

Exemple 1.1.19. $100 = 2 \times 2 \times 5 \times 5 = 2^2 \times 5^2 = 5^2 \times 2^2$.

Définition 1.1.20. *Un diviseur non trivial d'un entier naturel n est un entier naturel diviseur de n mais distinct de n et de 1 (qui sont ses diviseurs triviaux).*

Exemple 1.1.21. *Les diviseurs non triviaux de 45 sont $3, 5, 9$ et 15.*

1.2 Variétés affines

1.2.1 Ensembles algébriques affines

Définition 1.2.1. *On appelle espace affine de dimension n, et on note $\mathbb{A}^n(\mathbb{K})$ ou encore $\mathbb{A}^n$ (s'il n'y a pas risque de confusion sur $\mathbb{K}$), l'ensemble $\mathbb{K}^n$, produit cartésien itéré n fois du corps $\mathbb{K}$.*

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

Définition 1.2.2. *Soit S une partie quelconque de $\mathbb{K}[X_1, \dots X_n]$.*
On note $\mathcal{V}(S)$ la partie de $\mathbb{A}^n$ définie par :

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

L'ensemble $\mathcal{V}(S)$ est l'ensemble algébrique affine défini par S.
On remarque que $\mathcal{V}(S)$ est l'ensemble des zéros communs à tous les polynômes de S.

Si de plus S est une partie finie de $\mathbb{K}[X_1, \dots X_n]$, $S = \{P_1, ...P_r\}$, on note $\mathcal{V}(P_1, \dots P_r)$ au lieu de $\mathcal{V}(\{P_1, \dots P_r\})$; en particulier si $S = \{P\}$ alors $\mathcal{V}(S)$ est not $\mathcal{V}(P)$.
Si $S = (P_i)_{i \in I}$ alors $\mathcal{V}(S) = \bigcap_{i \in I} \mathcal{V}(P_i)$.

Définition 1.2.3. *Soient $\mathbb{K}$ un corps algébriquement clos et $F \in \mathbb{K}[X_1, \dots, X_n]$.*
L'ensemble $\mathcal{V}(F) = \{a \in \mathbb{A}^n, F(a) = 0\}$ qui n'est rien d'autre que l'ensemble des zéros communs de F, est appelé hypersurface définie par F. Le degré de $\mathcal{V}(F)$ est le degré de F.
Une courbe algébrique affine plane est une hypersurface du plan affine.

On appelle conique, cubique, quartique, quintique, sextique,. . .,respectivement une courbe de degré $2, 3, 4, 5, 6, \dots$

Remarque 1.2.4.
Tout ensemble algébrique affine peut être défini par l'annulation d'un nombre fini de polynômes.

Proposition 1.2.5.

1. *Le vide et l'espace tout entier sont des ensembles algébriques affines.*
2. *Une intersection quelconque d'ensembles algébriques affines en est un.*
3. *Une réunion finie d'ensembles algébriques affines en est un.*

Cette proposition nous montre l'existence d'une topologie sur $\mathbb{A}^n(\mathbb{K})$ dont les fermés sont des ensembles algébriques affines. Elle est appelée topologie de Zariski.

Définition 1.2.6. *Soit A une partie de $\mathbb{A}^n$.*
On appelle idéal de A dans $\mathbb{A}^n$, l'ensemble noté $\mathcal{I}(A)$ défini par :

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

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

1.2.2 Irréductibilité

Définition 1.2.7. *On dit qu'un espace topologique E est irréductible s'il est non vide et s'il n'est pas la réunion de deux fermés distincts de E.*
En d'autres termes E est irréductible s'il est non vide et si deux ouverts non vides de E se rencontrent, ou encore si tout ouvert non vide de E est dense.

Définition 1.2.8. *Un ensemble algébrique affine est dit irréductible, s'il l'est pour la topologie de Zariski.*
On appelle variété algébrique affine tout ensemble algébrique affine irréductible.

Théorème 1.2.9.
Tout ensemble algébrique affine se décompose de façon unique (à permutation près) en une réunion finie d'ensembles algébriques affines irréductibles $A_1, \ldots, A_r$ non contenus l'un dans l'autre.
Les éléments $A_1, \ldots, A_r$ sont appelés composantes irréductibles de A.

Preuve
Raisonnons par l'absurde :
Supposons que A ne peut pas se décomposer en une réunion finie d'irréductibles non contenus l'un dans l'autre.
Considérons la famille $(A_i)_{1 \leqslant i \leqslant r}$ d'ensembles algébriques non vides ne pouvant pas se décomposer en une réunion finie d'irréductibles non contenus l'un dans l'autre.

Comme $\mathbb{K}[X_1, \ldots, X_n]$ est noethérien, la famille $(\mathcal{I}(A_i))_{1 \leqslant i \leqslant r}$ admet un élément maximal c'est-à- dire, $\exists\, j = 1, \ldots, r, \quad \forall\, i = 1, \ldots, r\,;$
d'où,

$$\mathcal{I}(A_i) \subset \mathcal{I}(A_j).$$

Ainsi,

$$\exists\, j = 1, \ldots, r, \forall\, i = 1, \ldots, r \quad A_j \subset A_i.$$

Donc la famille $(A_i)_{i=1,\ldots,r}$ admet un élément minimal $V = A_j$ qui est forcément réductible.
Ecrivons $V = V_1 \cup V_2$ avec V_1 et V_2 des fermés distincts de V.
Il en résulte alors que V se décompose en une réunion d'irréductibles ce qui est absurde.
A se décompose en une union finie d'irréductibles non contenus l'un dans l'autre.
Unicité de la décomposition :
Supposons que :

$$A = A_1 \cup A_2 \cup \cdots \cup A_r, A_i \text{ irréductibles.}$$
$$A = B_1 \cup B_2 \cup \cdots \cup B_s, B_j \text{ irréductibles.}$$

On peut écrire pour $i = 1, \ldots, r,\ j = 1, \ldots, s$

$$\begin{aligned} A_i &= A \cap A_i \\ &= (B_1 \cup B_2 \cup \cdots \cup B_s) \cap A_i \\ &= (B_1 \cap A_i) \cup (B_2 \cap A_i) \cup \cdots \cup (B_s \cap A_i) \end{aligned}$$

d'où,

$$\exists j = 1, \ldots, s : A_i = B_j \cap A_i$$

par suite

$$A_i \subset B_j (*).$$

De la même manière on a :

$$\begin{aligned} B_j &= B_j \cap A \\ &= B_j \cap (A_1 \cup A_2 \cup \cdots \cup A_r) \\ &= (B_j \cap A_1) \cup (B_j \cap A_2) \cup \cdots \cup (B_j \cap A_r) \end{aligned}$$

donc,

$$\exists \ \ l = 1, \ldots, r \quad B_j = B_j \cap A_l$$

d'où ;

$$B_j \subset A_l(**).$$

Les relations $(*)$ et $(**)$ donnent $A_i \subset B_j \subset A_l$.
D'où $A_i = A_l$ et par suite $A_i = B_j$. □

1.3 Variétés Projectives

Soit $\mathbb{K}$ le corps de base considéré pour définir $\mathbb{A}^n = \mathbb{K}^n$.
Considérons la relation qu'on notera $\Re$ définie sur $\mathbb{K}^{n+1}\backslash\{0\}$ par : pour tous vecteurs non nuls x, y de $\mathbb{K}^{n+1}$, on a : $x\Re y$ s'il existe $\lambda \in \mathbb{K}^* : y = \lambda x$.
On remarque que $\Re$ est une relation de colinéarité qui est une relation d'équivalence. Ainsi, deux vecteurs x et y sont équivalents si et seulement si, ils sont colinéaires.

1.3.1 Ensembles projectifs

Définition 1.3.1. *On appelle espace projectif de dimension n sur $\mathbb{K}$ et l'on note $\mathbb{P}^n$ (ou $\mathbb{P}(\mathbb{K}^{n+1})$), ou encore $\mathbb{P}^n(\mathbb{K})$, l'ensemble des classes d'équivalence par $\Re$:*

$$\mathbb{P}^n = (\mathbb{K}^{n+1}\backslash\{0\})/\Re.$$

En d'autres termes $\mathbb{P}^n$ est l'ensemble des droites vectorielles de $\mathbb{K}^{n+1}$. Si un point $P \in \mathbb{P}^n$ a pour vecteur directeur (représentant) $(x_0, \ldots, x_n) \in \mathbb{K}^{n+1}\backslash\{0\}$, on écrit $P = (x_0 : \ldots : x_n)$; on dit que $(x_0 : \ldots : x_n)$ est un système de coordonnées homogènes de P et ne sont définis qu'à multiplication par un scalaire non nul près.
$\mathbb{P}^1$, $\mathbb{P}^2$ sont appelés respectivement droite projective et plan projectif sur $\mathbb{K}$.
On dit que P est un zéro de $F \in \mathbb{K}[X_0, \ldots, X_n]$ si $F(P) = 0$; pour tout choix de coordonnées homogènes $(x_0 : \ldots : x_n)$ de P, $F(P) = 0$ est noté $F(x_0, \ldots, x_n) = 0$.
On montre que $P = (x_0 : \ldots : x_n)$ est un zéro de F si et seulement si $F(\lambda x_0, \ldots, \lambda x_n) = 0$ pour $\lambda \in \mathbb{K}$.
Si E est un $\mathbb{K}$ espace vectoriel de dimension finie n, on définit de la même manière l'espace projectif associé à E noté $\mathbb{P}E$ ou $\mathbb{P}(E)$ de dimension $n-1$.
En particulier $\emptyset = \mathbb{P}(\{0\})$ est un espace projectif de dimension -1.
Si F est un sous-espace vectoriel non nul de E, l'inclusion $F\backslash\{0\} \subset E\backslash\{0\}$

induit une inclusion $\mathbb{P}F \subset \mathbb{P}E$.
Les sous-espaces de $\mathbb{P}E$ ainsi obtenus sont appelés sous-espaces linéaires de $\mathbb{P}E$, on a

$$\mathbb{P}(F) \cap \mathbb{P}(F') = \mathbb{P}(F \cap F').$$

Pour chaque $i = 0, \ldots, n$, on définit un sous-ensemble $U_i \subset \mathbb{P}^n$ de la manière suivante

$$U_i = \{P = (x_0 : \ldots : x_n) \in \mathbb{P}^n | \, x_i \neq 0\}.$$

Chacun des U_i est isomorphe à $\mathbb{A}^n$ par

$$U_i \simeq \mathbb{A}^n : \, (x_0 : \ldots : x_n) \longmapsto \Big(\frac{x_0}{x_i}, \ldots, \frac{x_n}{x_i}\Big).$$

Les U_i recouvrent $\mathbb{P}^n$.
Le complémentaire de U_i est l'espace linéaire $\mathbb{P}\mathbb{H}_i$ où $\mathbb{H}_i$ est l'hyperplan d'équation $x_i = 0$ dans $\mathbb{K}^{n+1}$.
On peut voir $\mathbb{P}^n$, comme l'espace $\mathbb{A}^n$ auquel on adjoint "les points à l'infini". Ainsi la droite projective $\mathbb{P}^1$ est la droite affine $\mathbb{K}$ auquel on adjoint un seul "point à l'infini".
Mieux le complémentaire dans $\mathbb{P}^n$ de n'importe quel hyperplan projectif s'identifie naturellement à $\mathbb{A}^n$.

Définition 1.3.2. *Un élément F de $\mathbb{K}[X_0, \ldots, X_n]$ est dit homogène de degré d si pour tout $\lambda \in \mathbb{K}^*$, on a $F(\lambda x_0, \ldots, \lambda x_n) = \lambda^d F(x_0, \ldots, x_n)$.*

Une conséquence immédiate est que, si F est homogène, on a pour tout $\lambda \neq 0, F(x_0, \ldots, x_n) = 0$ si et seulement si $F(\lambda x_0, \ldots, \lambda x_n) = 0$.

Définition 1.3.3. *Soit $S \subset \mathbb{K}[X_0, \ldots, X_n]$ constitué de polynômes homogènes.*
L'ensemble $\mathcal{V}(S) = \{P = (x_0 : \ldots : x_n) \in \mathbb{P}^n \mid \forall \; F \in S, \; F(P) = 0\}$ est appelé ensemble algébrique projectif défini par S.

On notera souvent dans le cas d'un ensemble fini $\mathcal{V}(F_1, \ldots, \, F_r)$ au lieu de $\mathcal{V}(\{F_1, \ldots, \, F_r\})$.

Définition 1.3.4. *On appelle hypersurface définie par un polynôme homogène l'ensemble des zéros de F (pour F non constant et $\mathbb{K}$ algébriquement clos). On note $\mathcal{V}(F) = \{P \in \mathbb{P}^n \mid F(P) = 0\}$, le degré de $\mathcal{V}(F)$ est celui de F.*

On appelle conique, cubique, quartique, quintique, sextique, ..., respectivement une courbe de degré $2, 3, 4, 5, 6, \ldots$

Remarque 1.3.5.
Les résultats obtenus dans $\mathbb{A}^n$ se transforment (presque tous) dans le cadre projectif. On peut en citer quelques uns :
• *tout $\mathcal{V}(S)$ peut être défini par l'annulation d'un nombre fini de polynômes.*
• *l'intersection quelconque et l'union finie d'ensembles algébriques projectifs en est un.*
• *les ensembles $\emptyset$, $\mathbb{P}^n$ sont algébriques projectifs.*
Donc, comme en affine, en projectif on peut définir une topologie de Zariski dont les fermés sont des ensembles algébriques.

Définition 1.3.6. *Soit $A \subset \mathbb{P}^n$. On appelle idéal de A sur $\mathbb{P}^n$, l'ensemble : $\mathcal{I}(A) = \{F \in \mathbb{K}[X_0, \ldots, X_n]$, homogène $\mid \forall\ P \in A,\ F(P) = 0\}$; c'est l'ensemble des polynômes nuls sur A.*

Remarque 1.3.7.
La notion d'irréductibilité et ses propriétés en affine se comportent telles qu'elles sont dans le cadre projectif.

Définition 1.3.8. *On appelle variété projective, tout ensemble algébrique projectif irréductible.*

Chapitre 2

Méthode de LENSTRA

Les définitions, les propositions et les théorèmes cités dans ce chapitre font référence aux travaux dans [3], [4] et [5].
Dans cette partie, notre objectif est d'étudier un algorithme (créé par H.W.LENSTRA) de factorisation des entiers qui est basé sur les courbes elliptiques.
On va donc commencer d'abord par définir la notion de courbe elliptique sur un corps et sur un type d'anneau particulier, à savoir $\mathbb{Z}/N\mathbb{Z}$.
Ensuite on va décrire l'algorithme en lui même qui repose sur les propriétés des points d'une courbe elliptique.
Et enfin donner quelques exemples de factorisation.
Dans tout le chapitre, on notera N l'entier à factoriser et p un facteur premier de N.

2.1 Les courbes elliptiques

2.1.1 Définition d'une courbe elliptique et premiers résultats

Définition 2.1.1. *Soit $\mathbb{K}$ un corps.*
Une courbe elliptique est une cubique irréductible, non singulière, définie comme l'ensemble des solutions dans le plan $\mathbb{P}^2(\mathbb{K})$ de l'équation de Weierstrass homogène suivante :

$$\mathbb{E} : Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \quad (1)$$

avec $a_i \in \mathbb{K}$.

Une courbe elliptique doit être non singulière, c'est-à-dire que si on écrit l'équation (1) sous la forme d'une équation $F(X, Y, Z) = 0$, alors les dérivées partielles de F ne doivent pas s'annuler simultanément en un point de la courbe.
Remarquons qu'une telle courbe admet un unique point de coordonnées Z nulle, le point à l'infini $(0 : 1 : 0)$. Il sera noté dans la suite O.
Par la suite nous utiliserons la plupart du temps la représentation affine de l'équation de Weierstrass sur $\mathbb{K}$ une équation du type :

$$\mathbb{E} : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (2)$$

avec $a_i \in \mathbb{K}$.
Pour $Z \neq 0$, un point (X, Y, Z) solution de l'équation (1) correspond à un point $(x, y) = \left(\frac{X}{Z}, \frac{Y}{Z}\right)$ solution de l'équation (2).
L'ensemble des solutions de l'équation (1) correspond à l'union des solutions de l'équation (2) et du point O.

2.1.2 Courbe elliptique sur un corps de caractéristique $p > 3$

Proposition 2.1.2. *Soit* $\mathbb{K}$ *un corps de caractéristique* $p > 3$. *Une courbe* $\mathbb{E}$ *donnée par l'équation* (2) *peut prendre alors la forme simplifiée suivante :*

$$\mathbb{E} : y^2 = x^3 + ax + b \quad (3)$$

dite équation réduite de Weierstrass où $a, b \in \mathbb{K}$ *;*
avec :

$$\Delta \neq 0 \text{ tel que } \Delta = -16(4a^3 + 27b^2) \text{ et } \jmath(\mathbb{E}) = 1728\frac{4a^3}{4a^3 + 27b^2}.$$

Preuve
Puisque $\mathbb{K}$ n'est pas de caractéristique 2, on peut effectuer un changement de variables suivant :

$$(x, y) = \left(x, y + \frac{a_1}{2}x + \frac{a_3}{2}\right),$$

on a :

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
$$y^2 + 2y\Big(\frac{a_1}{2}x + \frac{a_3}{2}\Big) = x^3 + a_2x^2 + a_4x + a_6.$$

En ajoutant le terme

$$\Big(\frac{a_1}{2}x + \frac{a_3}{2}\Big)^2$$

de l'expression à gauche et celle à droite. On obtient

$$\Big(y + \Big(\frac{a_1}{2}x + \frac{a_3}{2}\Big)\Big)^2 = x^3 + \Big(\frac{4a_2 + a_1^2}{4}\Big)x^2 + \Big(\frac{2a_4 + a_1a_3}{2}\Big)x + \Big(\frac{4a_6 + a_3^2}{4}\Big).$$

On pose :

$$b_2 = a_1^2 + 4a_2, b_4 = 2a_4 + a_1a_3, b_6 = a_3^2 + 4a_6.$$

Il vient,

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

Puisque la caractéristique du corps n'est ni 2, ni 3 on peut effectuer le changement de variables suivant :

$$(x, y) = \Big(x - \frac{b_2}{12}, y\Big).$$

On a

$$\begin{aligned}
\mathbb{E} : \ y^2 &= x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4} \\
&= \Big(x - \frac{b_2}{12}\Big)^3 + \frac{b_2}{4}\Big(x - \frac{b_2}{12}\Big)^2 + \frac{b_4}{2}\Big(x - \frac{b_2}{12}\Big) + \frac{b_6}{4} \\
&= x^3 - \Big(\frac{b_2^2 - 24b_4}{48}\Big)x - \frac{-b_2^3 + 36b_2b_4 - 216b_6}{864}.
\end{aligned}$$

L'équation que nous venons d'obtenir devient alors :

$$y^2 = x^3 - \frac{c_4}{48}x - \frac{c_6}{864}.$$

Il suffit de poser $a = -\frac{c_4}{48}$ et $b = -\frac{c_6}{864}$ pour obtenir l'équation souhaitée.
On peut effectuer les mêmes changements de variables pour obtenir les nouvelles équations de Δ et $\jmath(\mathbb{E})$. □
Sur un corps fini, le nombre de points de la courbe est fini. Le théorème de HASSE nous permet d'en connaitre approximativement ce nombre.

Théorème 2.1.3. *(Théorème de HASSE)*
Soit $\mathbb{F}_q = \mathbb{Z}/q\mathbb{Z}$ un corps fini et soit $\mathbb{E}$ une courbe elliptique définie sur $\mathbb{F}_q$. Le nombre de points de la courbe est :

$$\sharp\mathbb{E}(\mathbb{F}_q) = q + 1 - t,$$

où t est tel que :

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

2.2 Structure de groupe sur une courbe elliptique

2.2.1 Résultat géométrique fondamental

Proposition 2.2.1. *L'ensemble des points de l'intersection d'une courbe C et d'une droite L est fini si et seulement si ces deux courbes n'ont pas de composante irréductible en commun.*

Preuve
CN $\Longrightarrow$) Supposons que C et L ont une composante irréductible en commun. Soient C l'ensemble des solutions de

$$F_1(X, Y, Z) = 0$$

et L l'ensemble des solutions

$$F_2(X, Y, Z) = 0.$$

Comme L est une droite, F_2 est un polynôme homogène de degré 1 donc irréductible. Dire que C et L ont une composante commune (irréductible) revient à dire que F_1 s'écrit sous la forme :

$$F_1(X, Y, Z) = F_2(X, Y, Z)G(X, Y, Z)$$

où $G(X, Y, Z)$ non constant. L'ensemble des points L (i.e. les solutions de $F_2(X, Y, Z) = 0$) est inclus dans C, donc il y'a une infinité de points à l'intersection de C et de L. Ce qui est absurde, ainsi C et L n'ont pas de composante irréductible en commun.
CS $\Longleftarrow$) Supposons que C et L n'ont pas de composante commune. Montrons

que l'ensemble des points à l'intersection de C et de L est fini.
La droite L est définie par un polynôme homogène de degré 1 :

$$L : F_2(X, Y, Z) = aX + bY + cZ.$$

Soit $P = (X_P, Y_P, Z_P)$ un point d'intersection de C et L.
Si $Z_P \neq 0$; les coordonnées affines du point P vérifient alors,

$$f_2(x_P, y_P) = ax_P + by_P + c = 0.$$

On peut supposer que $b \neq 0$. Dans ce cas :

$$y_P = -\frac{ax_P + c}{b}$$

va vérifier

$$f_1\Big(x_P, -\frac{ax_P + c}{b}\Big) = 0.$$

C'est un polynôme en x_P non nul du fait que C et L n'ont pas de composante commune. Il admet donc un nombre fini de racines.
Si $Z_P = 0$; les coordonnées homogènes de P vérifiant alors le systme d'équation suivant :

$$\begin{cases} aX_P + bY_P = 0 \\ F_1(X_P, Y_P, 0) = 0. \end{cases}$$

En supposant par symétrie que $b \neq 0$, nous voyons que les coordonnées homogènes de P doivent vérifier $F_1(X_P, -\frac{a}{b}X_P, 0)$.
Cette équation est un polynôme en X_P non nul puisque C et L n'ont pas de composante commune, il admet donc un nombre fini de racines.
Ainsi ; si C et L n'ont pas de composante commune, elles se coupent en un nombre fini de points. □
Et on a le résultat suivant.

Corollaire 2.2.2.
Soient C une cubique irréductible et L une droite. C et L se coupent en un nombre fini de points.

Proposition 2.2.3.
Soient une cubique non singulière C et une droite L définies sur un corps $\mathbb{K}$. Si la cubique C a au moins deux points d'intersection (comptés avec leur multiplicité) avec la droite L, alors le nombre de points d'intersection (comptés avec leur multiplicité) entre C et L est exactement 3.

Preuve
En effet comme C est irréductible, nous savons grâce à la proposition 2.2.1 que le nombre de points d'intersection de C et de L est fini. Soit la droite

$$L : aX + bY + cZ = 0$$

où par symétrie, nous supposons $c \neq 0$. Les points $P(X, Y, Z)$ sont racines du polynôme i.e. $F(P) = F(X, Y, Z) = 0$

$$F\Big(X, Y, -\frac{aX + bY}{c}\Big)$$

où F est le polynôme de degré 3 qui définit C.
Posons

$$q(X, Y) = F\Big(X, Y, -\frac{aX + bY}{c}\Big)$$

et soient $P_1 = (a_1, b_1, c_1)$ et $P_2 = (a_2, b_2, c_2)$ deux points de l'intersection de C et L (avec éventuellement $P_1 = P_2$). Comme $q(P_1) = q(P_2) = 0$, on peut écrire :

$$q(X, Y) = \vartheta(X, Y)(b_1X - a_1Y)(b_2X - a_2Y)$$

où ϑ est un polynôme de degré 1.
Il n'a donc qu'une racine que nous noterons (a_3, b_3).
Le point

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

est alors le troisième point à l'intersection de C et L. D'où le résultat. □
Cette proposition permet de définir la loi de composition de la sécante tangente ci-dessous :

i) Si $P, Q \in C(\mathbb{K})$ et $P \neq Q$, nous pouvons définir $L = (PQ)$ la droite sécante passant par P et Q. Grâce la proposition précédente nous savons que cette droite coupe la courbe C en un troisième point unique qui appartient donc à $C \cap L$. Nous noterons ce troisième point $P * Q$.

ii) Si $P \in C(\mathbb{K})$, nous pouvons définir $L = (PP)$, la droite tangente C au point P.
Grâce à la proposition précédente nous savons qu'il existe un troisième point unique (en comptant les multiplicités) qui appartient à $C \cap L$. Nous noterons ce troisième point $P * P$.

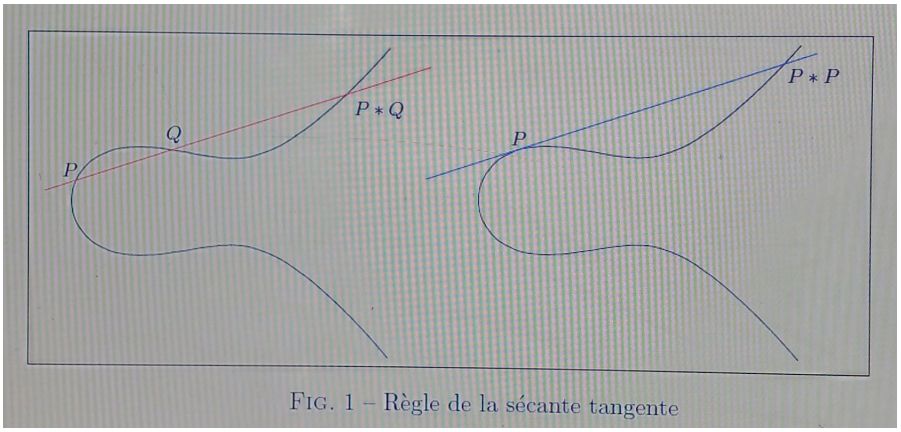

FIG. 1 – Règle de la sécante tangente

Nous pouvons constater que sur la figure 1, une droite verticale coupant la courbe C ne semble pas couper en un troisième point. Ceci est lié à la difficulté de représenter $\mathbb{P}^2$ sur un plan. Ce troisième point existe bien sûr, et appartient à $\mathbb{P}^1$. Pour une courbe elliptique il correspond au point O.

Proposition 2.2.4.
Soient $\mathbb{K}$ un corps et C une cubique irréductible non singulière. Pour tous points P_1, P_2, Q_1 et Q_2 de $C(\mathbb{K})$, nous avons :

$$(P_1 * P_2) * (Q_1 * Q_2) = (P_1 * Q_1) * (P_2 * Q_2).$$

Pour la démonstration de ce résultat voir [7].

2.2.2 Loi du groupe sur une courbe elliptique

Théorème 2.2.5.
Soit un corps $\mathbb{K}$.
Soit $\mathbb{E}$ une courbe elliptique définie sur $\mathbb{K}$. Soient P et Q deux points de cette courbe.
Alors l'opération $P + Q = O * (P * Q)$ définit une structure de groupe commutatif ayant O comme élément neutre.

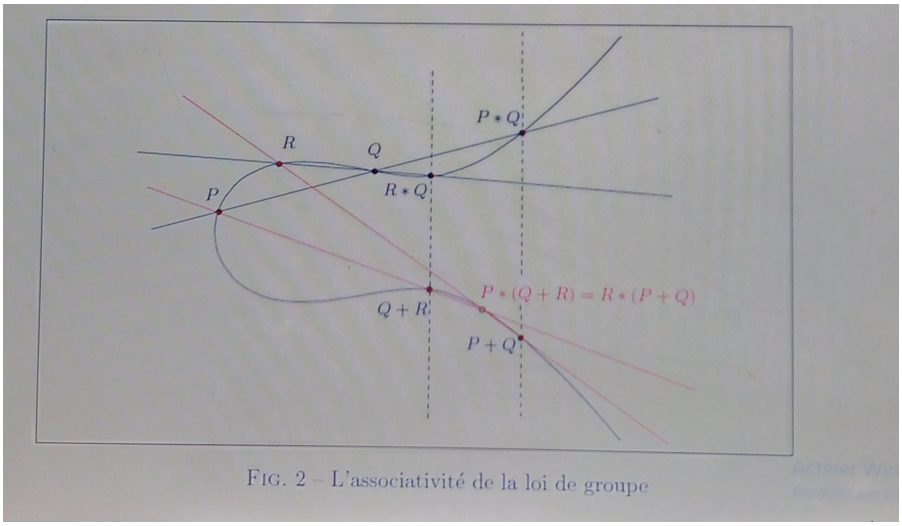

FIG. 2 – L'associativité de la loi de groupe

Preuve

1) La loi + est bien interne puisque $P+Q$ est l'intersection d'une droite et d'une cubique i.e. un point de la courbe.

2) La loi + est associative (voir FIGURE 2). En effet, si P, Q et R sont trois points de la courbe on a :

$$\begin{aligned} P*(Q+R) &= P*(O*(Q*R)) \\ &= ((P*Q)*Q)*((O*((Q*R)) \text{ car P} = ((\text{P}*\text{Q})*\text{Q}) \\ &= ((P*Q)*O)*(Q*(Q*R)) \text{ voir 2.2.4} \\ &= (O*(P*Q)*R) \ \textit{voir} \text{ FIGURE 2} \\ &= (P+Q)*R \end{aligned}$$

d'où l'associativité.
En appliquant O sur les deux membres de l'égalité. Nous trouvons

$$P+(Q+R) = (P+Q)+R.$$

3) L'élément O est le neutre pour la loi + (voir FIGURE 3).
En effet :

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

et

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

4) Tout point P possède un inverse pour la loi $+$. Vérifions que le point

$$-P = (O * O) * P$$

est bien l'inverse de P :

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

De la même manière on montre $(-P) + P = O$.

5) En fin la loi $+$ est commutative. Si P et Q sont deux points de la droite $P + Q = O * (Q * P) = Q + P$.

□

Les propriétés de la loi de groupe sur une courbe elliptique sont représentées sur la FIGURE 4.

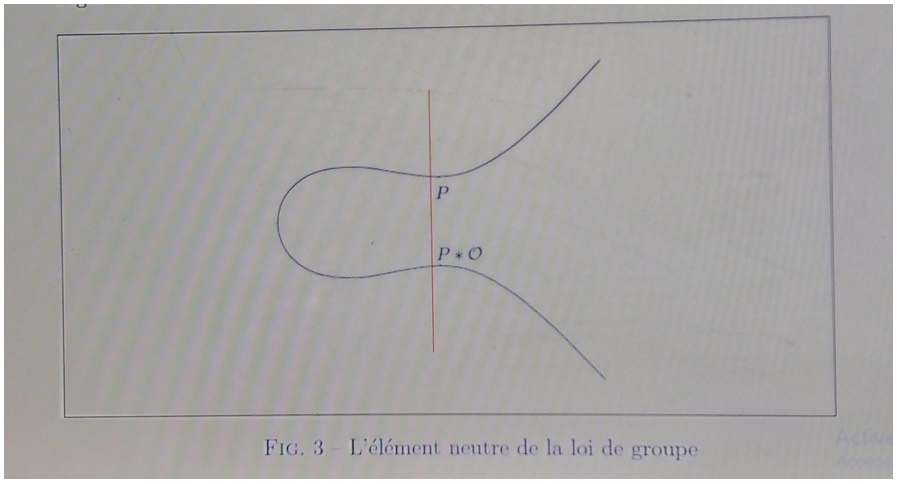

FIG. 3 – L'élément neutre de la loi de groupe

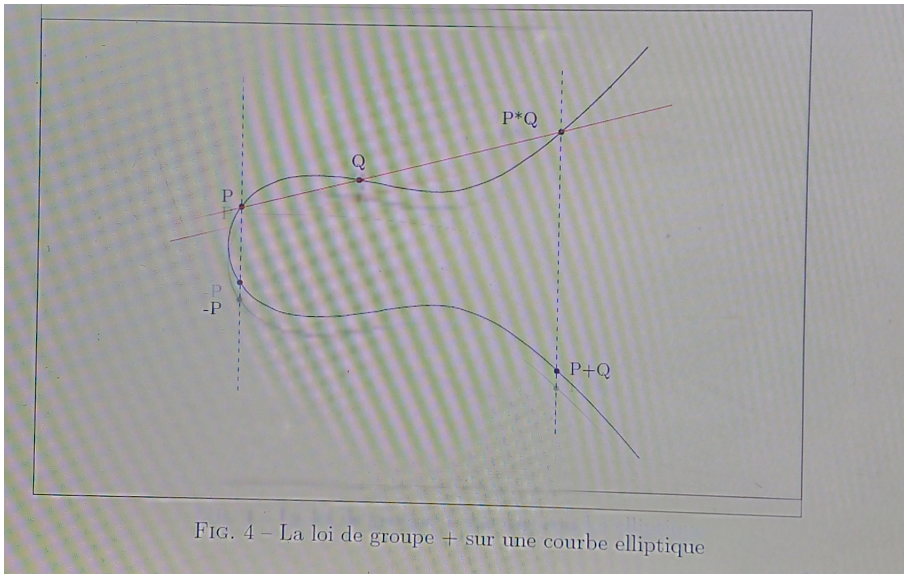

FIG. 4 – La loi de groupe + sur une courbe elliptique

2.3 Formules explicites

Nous allons considérer des courbes elliptiques définies sur des corps $\mathbb{K}$ de caractéristique $(p > 3)$. L'équation de Weierstrass définissant une courbe elliptique $(\mathbb{E})$ sur $\mathbb{K}$, prend la forme suivante :

$$\mathbb{E} : y^2 = x^3 + ax + b.$$

Dans ce paragraphe, $P = (x_P, y_P)$ et $Q = (x_Q, y_Q)$ seront deux points de notre courbe différents de O.

Remarque 2.3.1. *Un point P d'une courbe elliptique est dit d'ordre m si $mP = P + P + \cdots + P = O$ et $m'P \neq O$ pour tout entier m' vérifiant $1 \leqslant m' < m$.*
S'il existe un tel m alors le point P est d'ordre fini. Sinon P est d'ordre infini.

Remarque 2.3.2. *L'inverse du point P est son symétrique par rapport à l'axe des abscisses :*

$$\begin{cases} x_{-P} = x_P \\ y_{-P} = -y_P \end{cases} \tag{2.3.1}$$

2.3.1 Calcul de l'addition de P et Q

Considérons que $P \neq Q$, sinon additionner P et Q revient à doubler le point P.
Si $x_P \neq x_Q$:
La droite L passant par P et Q a pour équation :

$$L : y = \lambda x + \gamma \text{ avec } \lambda = \frac{y_Q - y_P}{x_Q - y_P} \text{ et } \gamma = y_P - \lambda x_P.$$

Les coordonnées des points d'intersection de la droite L et la courbe $(\mathbb{E})$ sont solutions du système :

$$\begin{cases} y^2 = x^3 + ax + b \\ y = \lambda x + \gamma \end{cases} \tag{2.3.2}$$

d'où ;

$$(\lambda x + \gamma)^2 = x^3 + ax + b$$

et donc :

$$x^3 - \lambda^2 x^2 + (a - 2\lambda\gamma)x + (\gamma^2 - b) = 0 \text{ (4)}.$$

Les coordonnées des points P, Q et $P*Q$ sont trois solutions de notre système, l'équation (4) peut donc être écrite de la manière suivante :

$$(x - x_P)(x - x_Q)(x - x_{P*Q}) = 0.$$

Ce qui donne après développement :

$$x^3 - (x_P + x_Q + x_{P*Q})x^2 + (x_P x_Q + x_Q x_{P*Q})x - x_P x_Q x_{P*Q} = 0 \text{ (5)}.$$

En égalisant les coefficients de (4) et de (5). On obtient :

$$\begin{cases} x_{P*Q} = \lambda^2 - x_P - x_Q \\ y_{P*Q} = \lambda x_{P*Q} + \gamma. \end{cases} \tag{2.3.3}$$

En remplaant γ par sa valeur, on obtient :

$$\begin{cases} x_{P*Q} = \lambda^2 - x_P - x_Q \\ y_{P*Q} = \lambda(x_{P*Q} - x_P) + y_P. \end{cases} \tag{2.3.4}$$

Le point $P + Q$ est le symétrique par rapport à l'axe des abscisses du point $P * Q$, donc :

$$\begin{cases} x_{P+Q} = \lambda^2 - x_P - x_Q \\ y_{P+Q} = \lambda(x_P - x_{P+Q}) - y_P. \end{cases} \tag{2.3.5}$$

Si $x_P = x_Q$:
Or on a supposé que $P \neq Q$. Comme $x_P = x_Q$ on a forcément $y_P \neq y_Q$. Le point Q est donc l'inverse du point P, ainsi $P + Q = O$.

2.3.2 Calcul du doublement de P

Si $y_p \neq 0$:
La droite tangente $\mathbb{E}$ passant par le point P a pour équation $L : y = \lambda x + \gamma$ où λ est la pente de la tangente la courbe $\mathbb{E}$ en P et $\gamma = y_P - \lambda x_P$. Notons :

$$\mathbb{E} : f(x, y) = y^2 - x^3 - ax - b = 0 \text{ (6)}.$$

Le coefficient λ est alors donné par :

$$\lambda = -\frac{\frac{\partial f}{\partial x} \mid P}{\frac{\partial f}{\partial y} \mid P} = \frac{3x_P^2 + a}{2y_P}.$$

On remarque ensuite le même calcul qu'au paragraphe précédent (il suffit de remplacer Q par P et $P * Q$ par $2P$). On obtient :

$$\begin{cases} x_{2P} = \lambda^2 - 2x_P \\ y_{2P} = \lambda(x_P - x_{2P}) - y_P \end{cases} \tag{2.3.6}$$

avec

$$\lambda = \frac{3x_P^2 + a}{2y_P}.$$

Si $y_P = 0$:
La tangente en P à la courbe $\mathbb{E}$ est verticale et ne coupe $\mathbb{E}$ qu'au point P.
Le point P est alors un point d'ordre 2 et on a $2P = O$.

2.4 La méthode de factorisation : Elliptic Curves Method (ECM)

On peut utiliser les courbes elliptiques pour factoriser certains entiers. La méthode (ECM) dont nous allons donner le principe est due à LENSTRA ; c'est un algorithme probabiliste rapide pour la décomposition en produit de facteurs premiers qui utilise des courbes elliptiques.
Cet algorithme comprend quatre étapes.

L'idée est la suivante : supposons que nous voulions factoriser un entier N. On note p un diviseur premier de N (que l'on ne connait pas).
On choisit aléatoirement une courbe elliptique sur $\mathbb{Z}/N\mathbb{Z}$. On fait les calculs sur les courbes elliptiques (addition de points ...) comme si N est premier, en espérant une erreur de calcul au moment de calculer certains inverses.

✓ **Etape 1 : Choix d'une courbe elliptique**

$\mathbb{E} : y^2 = x^3 + ax + b$ et une borne $B \in \mathbb{N}$.

On tire au hasard trois entiers a, x, y compris entre 0 et $N-1$. Puis on calcule le pgcd de ces différents cas :

posons $d = \text{pgcd}(\Delta, N)$, avec $\Delta = 4a^3 + 27b^2$.

- Si $d = N$, on recommence au choix des trois variables.
- Si $d \neq 1$ et $d \neq N$ on a un diviseur non trivial, c'est encore mieux car
$$\text{pgcd}(4a^3 + 27b^2, N)$$
donne un diviseur strict de N.
- Si $d = 1$, trivial.

Remarquons que puisque $4a^3 + 27b^2$ est premier avec N, il est premier avec p et est inversible dans $\mathbb{Z}/p\mathbb{Z}$. L'équation $b = y^2 - x^3 - ax$ dfinit une courbe elliptique sur $\mathbb{E}(\mathbb{Z}/p\mathbb{Z})$, que nous noterons $\mathbb{E}(a, b, p)$ (signalons que, puisqu'on ne connait pas p, on ne connait pas cette courbe elliptique).

✓ **Etape 2 : Choix d'un point sur la courbe elliptique**

On trouve deux entiers x et y tels que
$y^2 = x^3 + ax + b$. En particulier, $P = (x, y)$ est un point de la courbe elliptique $\mathbb{E}(a, b, N)$.

✓ **Etape 3 : Choix d'un entier auxiliaire**

On choisit k un entier qui est produit de petits facteurs premiers à des exposants déjà élevés. Par exemple, $k = 2^{10}3^85^67^4$.

✓ **Etape 4 : Calcul sur les courbes elliptiques**

Dans cette partie, nous allons regarder les courbes elliptiques sur l'anneau $\mathbb{Z}/N\mathbb{Z}$ de manière naïve, (i.e. en réduisant les coefficients des courbes elliptiques et les points sur ces courbes modulo N).

L'idée est de regarder une courbe elliptique sur l'anneau $\mathbb{Z}/N\mathbb{Z}$ où N est le nombre à factoriser, mais de manière naïve ; c'est-à-dire que pour additionner deux points de la courbe nous calculons la pente de la courbe passant par ces points et la réduisons modulo N.

On calcule les coordonnées du point kP, en utilisant les formules classiques, les calculs s'effectuant modulo N. Ces calculs font intervenir des divisions, et n'est pas toujours possible modulo N : il faut que le dénominateur D soit premier avec N. Mais ce qu'on espère, c'est ce qui n'est pas le cas.
En effet, si D n'est pas premier avec $N, \text{pgcd(D, N)}$ donne un diviseur premier de N.
Si les calculs n'aboutisent pas, on recommence à l'étape 1 en changeant de courbe elliptique.
Pourquoi ça marche ?
Si une courbe elliptique $\mathbb{E}(a, b, p)$ (p diviseur de N) comporte m points, tel que m est produit de facteurs premiers, alors $m \mid k$.
k est donc un multiple du cardinal du groupe de la courbe elliptique et d'après le théorème de Lagrange $kP = O$ (point à l'infini). Dans ce cas, dans le calcul de kP, une erreur va se produire et on va trouver un diviseur de N.
Pour le choix de la borne lissité, on peut tenir du raisonnement suivant : si p est un facteur de N alors $p \leq \sqrt{N}$ d'apès le théorème de HASSE, on peut prendre $B \geq (N^{\frac{1}{4}} + 1)^2$.

Factorisation par la méthode de LENSTRA

Exemple 2.4.1.
Factorisons $N = 3397$ par la méthode des courbes elliptiques (ECM)
Choisissons la courbe elliptique définie par $\mathbb{E} : y^2 = x^3 + 4x + 25$ et le point $P = (3, -8)$
Vérifions que $P \in \mathbb{E}$.
En effet $3^3 + 4 \times 3 + 25 = 64 = 8^2 = y^2$ d'où $y = 8$ ou $y = -8$.
Soit $y = -8$, d'où $P \in \mathbb{E}$.
On commence par calculer $2P$ selon les formules habituelles. On calcule la pente de la tangente en P qui vaut ;

$$\lambda = \frac{3x_P^2 + a}{2y_P} = \frac{31}{-16} \equiv C \ [3397].$$

Trouvons l'entier C.
Nous avons

$$\frac{31}{-16} \equiv C \ [3397]$$
$$-16C \equiv 31 \ [3397].$$

Pour éliminer le -16 *qui est devant le* C*, il faut chercher un* y *tel que* $-16y \equiv 1\ [3397]$. *Pour cela on peut résoudre l'équation* $-16y + 3397x = 1$. *En utilisant l'algorithme* d'EUCLIDE :

$$\begin{aligned} 3397 &= (-212)(-16) + 5 \\ -16 &= -4(5) + 4 \\ 5 &= 1(4) + 1 \Longrightarrow 1 = 5 - 1(4). \end{aligned}$$

On tire

$$\begin{aligned} 1 &\equiv -3(3397 + 212(-16)) - (-16) \\ &\equiv -16(-637) \\ &\equiv -16(2760), \\ -16(2760) &\equiv 1\ [3397]; \end{aligned}$$

donc -16 est inversible modulo N d'inverse 2760

$$\begin{aligned} \text{on a} - 16C &\equiv 31\ [3397] \\ 2760(-16)C &\equiv 2760 \times 31\ [3397] \\ C &\equiv 85560\ [3397] \\ C &= 635\ [3397] \end{aligned}$$

Par suite, la pente de la tangente en P est $\frac{31}{-16} \equiv 635\ [3397]$. On tire le point $2P$ de coordonnées (x_{2P}, y_{2P})

$$\begin{aligned} x_{2P} &\equiv \lambda^2 - 2x_P \\ &\equiv 635^2 - 2 \times 3\ [3397] \\ &\equiv 403219\ [3397] \\ &\equiv 2373\ [3397] \\ y_{2P} &\equiv -y_P + \lambda(x_P - x_{2P})\ [3397] \\ &\equiv -(-8) + 635(3 - 2373)\ [3397] \\ &\equiv -443(3397) - 71\ [3397] \\ &\equiv (3397 - 71)\ [3397] \\ &\equiv 3326\ [3397]. \end{aligned}$$

D'où

$$2P = (2373, 3326).$$

On calcul ensuite

$$3P = 2P + P.$$

La pente de la droite $(P, 2P)$ serait

$$\lambda = \frac{y_{2P} - y_P}{x_{2P} - x_P} = \frac{3326 - (-8)}{2373 - 3} = \frac{3334}{2370}.$$

Mais 2370 n'est pas inversible modulo N. En effet le

$$\text{pgcd}(2370, 3397) = 79 \neq 1.$$

Le calcul de λ échoue et révèle, ce faisant, un facteur de $N = 3397$, à savoir 79.
Finalement le nombre 79 est un facteur de 3397.

Chapitre 3

Autres méthodes de factorisation

Dans ce chapitre, on donne quelques méthodes de factorisation des entiers. Les méthodes de factorisation citées dans ce chapitre font référence aux travaux dans [6].
Soit $N \geqslant 2$. Trouver les nombres premiers $p_1, p_2, \ldots, p_s$ et les entiers $e_1, e_2, \ldots, e_s$ tels que $N = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$.
Par réduction, on se ramène aux trois problèmes suivants :
• Est ce que N est un nombre premier ?
• Sinon, est ce que N est une puissance d'un nombre premier ?
• Sinon, trouver d avec $2 \leqslant d < N$ et d un diviseur de N.
Le cas le plus défavorable est que si $N = pq$ avec p et q des premiers de même taille.

3.1 Méthode $p - 1$ de POLLARD

Cette méthode repose sur le petit théorème de FERMAT que nous allons énoncer ci-dessous.
Elle a été présentée par J.M. POLLARD en 1974. Soit N un entier composé. La méthode de factorisation $p - 1$ de POLLARD permet de déterminer les diviseurs premiers de N.

Théorème 3.1.1.

Soit p un nombre premier. Tout entier a satisfait :

$$a^p \equiv a[p]$$

de plus si a n'est pas divisible par p alors

$$a^{p-1} \equiv 1[p].$$

Preuve
Considérons d'abord le cas où p ne divise pas a, alors $a \in (\mathbb{Z}/p\mathbb{Z})^*$.
Par conséquent, nous avons

$$\begin{aligned} a^p &\equiv a[p] \\ &= a + kp \end{aligned}$$

donc on a :

$$\begin{aligned} a^p - a &= kp \\ (a^{p-1} - 1) &= kp \ (car\ p\ ne\ divise\ pas\ a) \\ a^{p-1} &= 1 + kp \\ &\equiv 1[p]. \end{aligned}$$

Si p divise a alors $a \equiv 0[p]$, donc c'est trivial. □

Définition 3.1.2. *Un entier N est $B-$lisse si tous les facteurs premiers de N sont inférieurs ou égaux B.*
Un entier N est $B-$super lisse si toutes les puissances premières divisant N sont inférieures ou égales à B.

La méthode de factorisation $p-1$ de POLLARD permet de factoriser un nombre N dont un facteur premier p est tel que $p-1$ est $B-$ super lisse. Cela signifie que $p-1$ est un facteur de $B!$ (avec $B! = B \times (B-1) \times \cdots \times 1$).
Choisissons un entier b tel que $1 < b < N$.
On peut supposer que b est premier avec N, donc on a :

$$\begin{aligned} b^{B!}[N] &= b^{k_1(p-1)}[N] \\ &= (b^{k_1}[N])^{p-1}[N] \\ &= (b^{k_1}[N])^{p-1} + k_2 N \end{aligned}$$

avec $k_1, k_2 \in \mathbb{Z}$ et $b \in \mathbb{Z}/N\mathbb{Z}$.
Et donc, d'après le petit théorème de Fermat :

$$\begin{aligned} b^{B!}[N] &= b^{k_1(p-1)}[N] \\ &= (b^{k_1}[N])^{p-1}[N] \\ b^{B!} &= (b^{k_1}[N])^{p-1} \\ donc & \\ b^{B!} &\equiv 1[p] \end{aligned}$$

posons $M = B!$.
Et comme b est premier avec N. L'entier p est donc un facteur de :

$$b^M[N] - 1.$$

Les nombres N et $b^M[N] - 1$ ont donc un facteur commun que l'on peut faire apparaitre grâce à un calcul de pgcd.
Pratiquement on calculera

$$\mathrm{pgcd}(\mathrm{b}^{\mathrm{t!}}[\mathrm{N}] - 1, \mathrm{N})$$

pour t allant 1 à B et s'arrêtant dés que le pgcd est différent de 1, on obtient un facteur non trivial de N qui est un multiple de p, ce qui permet souvent d'obtenir p.
Algorithme $p-1$ de POLLARD :

1. on choisit un entier naturel B, dans la plupart des cas, choisir $B = N^{\frac{1}{4}}$ est suffisant,
2. on choisit un entier b tel que $1 < b < N$ (par exemple $b = 2$ ou $b = 3$),
3. on calcule le $\mathrm{pgcd}(\mathrm{b}, \mathrm{N}) = \mathrm{d}$,
   si l'on a $d \neq 1$, on obtient un diviseur non trivial de N et l'algorithme est terminé,
4. si l'on a $d = 1$, on calcule $b^M[N]$, puis l'entier :

$$d = \mathrm{pgcd}((b^M[N] - 1, N),$$

- si l'on a $1 < d < N$, alors d est un diviseur non trivial de N.
- si $d = 1$, on reprend la première étape avec un plus grand entier B.

- si $d = N$, on recommence à la première étape avec un plus petit B ou à la deuxième étape avec un autre entier b.

Factorisation par la méthode de $p-1$ de POLLARD

Exemple 3.1.3.
Factoriser l'entier $N = 1403$.
Application de la méthode $p-1$ *de* POLLARD.
On choisit $B = 2$ et évaluer
2^M [1403] pour $B = 2, 3, 4, \ldots$, et on calcule

$$\mathrm{pgcd}(2^{\mathrm{M}} - 1, 1403)$$

$*B = 2$,
$2^{2!} = 4$

$$\mathrm{pgcd}(2^{2!} - 1, 1403) = 1$$

donc est un facteur trivial, passer à la prochaine étape.
$*B = 3$,
$2^{3!} = 64$

$$\mathrm{pgcd}(2^{3!} - 1, 1403) = 1$$

donc est un facteur trivial, passer à la prochaine étape.
$*B = 4$,
$2^{4!} = (2^{3!})^4 \equiv (64)^4 \equiv 142$ [1403]

$$\mathrm{pgcd}(2^{4!} - 1, 1403) = 1$$

donc est un facteur trivial, passer à la prochaine étape.
$*B = 5$,
$2^{5!} \equiv ((64)^4)^5 \equiv 794$ [1403]

$$\mathrm{pgcd}(2^{5!} - 1, 1403) = 61 \neq 1$$

et nous trouvons

$$1403 = 61 \times 23$$

donc l'algorithme s'arrête là ;
61 est donc un diviseur non trivial.

3.2 Méthode rho de POLLARD

C'est une méthode présentée par POLLARD en 1975. Soit N un entier composé. Son efficacité pour factoriser N dépend de la taille du plus petit diviseur premier de N.

Principe

Il repose sur l'idée suivante. On choisit un polynôme $f(X)$ à coefficients dans $\mathbb{Z}$ et un entier $X_0 < N$, par exemple $X_0 = 1$ ou 2, ou un autre entier choisi de façon aléatoire. On considère la suite $(X_i)_{i\in\mathbb{N}}$ par les égalités :

$$X_{i+1} = f(X_i)\ [N] \text{ pour } i = 0, 1, 2, \ldots$$

Autrement dit, X_{i+1} est le reste de la division euclidienne de $f(X_i)$ par N. Les entiers X_i sont compris entre 0 et $N - 1$.

On calcule le terme de cette suite dans l'espoir de trouver deux entiers distincts, disons X_i et X_j, qui sont congrus modulo un diviseur de N autre que 1.

On peut alors expliciter ce diviseur en calculant le $\mathrm{pgcd}(|\mathrm{X_i} - \mathrm{X_j}|, \mathrm{N})$.

Factorisation par la méthode rho de POLLARD

Exemple 3.2.1.

Illustrons cette idée avec un petit entier N, par exemple $N = 319$ (pour lequel cette méthode est évidemment inutile). Prenons $f(X) = X^2 + 1$ (ce n'est pas un hasard) et $X_0 = 1$.

On vérifie que l'on a :

$$X_1 = 2,\ X_2 = 5,\ X_3 = 26,\ X_5 = 246.$$

On obtient l'égalité $\mathrm{pgcd}(\mathrm{X_5} - \mathrm{X_3}, \mathrm{N}) = 11$*, d'où* $N = 11 \times 29$.

Dans l'application de cette méthode, il importe de choisir $f(X)$ de sorte que ses valeurs sur les entiers soient suffisamment aléatoires. Par exemple, un polynôme de degré 1 ne convient pas. Des expérimentations numériques poussées laissent penser que certains polynômes de degré 2, comme $X^2 + 1$, sont généralement bien adaptés.

3.3 Méthode de FERMAT

Soit N un entier. Elle très efficace pour factoriser N et surtout si N s'écrit comme un produit de deux entiers proches l'un de l'autre. Elle repose sur

le fait trouver une factorisation de N est équivalent à écrire N comme une différence de deux carrés.
Plus précisément :

Lemme 3.3.1.
L'ensemble des couples $(a, b) \in \mathbb{N}^2$ tels que $N = ab$ avec $a \geq b$, et celui des couples $(r, s) \in \mathbb{N}^2$ tels que $N = r^2 - s^2$ sont en bijection.

Preuve
Soient A l'ensemble des couples $(a, b) \in \mathbb{N}^2$ tels que $N = ab$, avec $a \geq b$ et B l'ensemble des couples $(r, s) \in \mathbb{N}^2$ tels que $N = r^2 - s^2$.
Les applications $f : A \longrightarrow B$ et $g : B \longrightarrow A$ définies par :
$f((a, b)) = \left(\frac{a+b}{2}, \frac{a-b}{2}\right)$ et $g((r, s)) = (r + s, r - s)$.
Sont réciproques l'une de l'autre.
En effet, il suffit de remarquer que pour tout $(a, b) \in \mathbb{N}^2$ on a l'égalité :

$$ab = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2$$

et que si $N = r^2 - s^2$ où $(r, s) \in \mathbb{N}^2$, alors $N = (r - s)(r + s)$, $r + s \geq r - s$.
Dans le cas où N est le produit de deux entiers proches l'un de l'autre, il est facile d'écrire N comme une différence de deux carrés, et donc de factoriser N. C'est l'idée de FERMAT.
Plus généralement, soit $\llcorner N^{\frac{1}{2}} \lrcorner$ la partie entière $N^{\frac{1}{2}}$.
Supposons que l'on ait $N = ab$ où a et b sont proches l'un de l'autre, avec $a \geq b$.
Posons $r = \frac{a+b}{2}$ et $s = \frac{a-b}{2}$.
On a $N = r^2 - s^2$. L'entier s est petit et r donc plus grand que $N^{\frac{1}{2}}$ tout en lui étant plus proche. Par suite, il existe un petit entier naturel u tel que $((\llcorner N^{\frac{1}{2}} \lrcorner + x)^2 - N), x = 1, 2, 3, \ldots$ soit un carré.
Afin de déterminer un tel entier x, on examine successivement les entiers $\llcorner N^{\frac{1}{2}} \lrcorner + 1$, $\llcorner N^{\frac{1}{2}} \lrcorner + 2$, $\ldots$ et on teste pour chacun d'eux si son carré moins N est un carré. Si l'on y parvient, on obtient N comme une différence de deux carrés, ce qui fournit une factorisation de N. □

Factorisation par la méthode de FERMAT

Exemple 3.3.2.
factoriser l'entier $N = 7081$

$$\llcorner N^{\frac{1}{2}} \lrcorner = 84$$

$$(84+1)^2 - 7081 = 7225 - 7081 = 144 = 12^2$$

$$(84+1)^2 - 7081 = 12^2$$

d'où l'égalité,
$N = (r-12)(r+12)$ *avec* $r = \llcorner N^{\frac{1}{2}} \lrcorner + 1$

$$N = (85-12)(85+12) = (73)(97).$$

Finalement $N = 73 \times 97$ *, on obtient ainsi* $N = pq$*.*

Factorisation par la méthode de FERMAT

Exemple 3.3.3.
factoriser l'entier $N = 2027651281$

$$\llcorner N^{\frac{1}{2}} \lrcorner = 45029$$

il faut aller jusqu'à $u = 12$ *:*

$$(45029+12)^2 - 20276512812 = 1040400 = (1020)^2$$

ce qui donne la factorisation de N
$N = (r-1020)(r+1020)$ *avec* $r = \llcorner N^{\frac{1}{2}} \lrcorner + 12$

$$N = (45041-1020)(45041+1020) = (44021)(46061).$$

Finalement $N = 44021 \times 46061$*, on obtient ainsi* $N = pq$*.*

3.4 Quelques applications

La cryptographie est de proposer des méthodes pour coder facilement de l'information de telle sorte que le décodage soit difficile. Si l'on ne possède pas la signature d'authentification adéquate comme dans la méthode de RSA qui est un système de codage à clé publique de taille infrieure et utilise la notion de factorisation aussi bien qu'avec les courbes elliptiques.
La méthode de cryptographie a été inventé en 1977 par Ron RIVEST, Adi SHAMIR et Len ADLEMAN :
PRINCIPE DE FONCTIONNEMENT :
Si Bernard souhaite recevoir des messages en utilisant le RSA, il procéde de la façon suivante :
• Création des clés : Bernard créé quatre nombres p, q, e, et d.

1. p et q des grands nombres premiers distints,
2. on calcule $N = pq$,
3. on pose : $z = (p-1)(q-1)$ et on choisit un entier e au hasard, premier avec z tel que $1 < e < z$,
4. on calcule $d \times e \equiv 1[z]$ pour enfin déterminer l'unique inverse e et d, on peut trouver d à partir de e, p et q en utilisant l'algorithme d'EUCLIDE.
5. Distribution des clés :
   $\star K_{pub} = (e, n)$ constitue la clé publique de Bernard,
   $\star K_{pri} = (d, n)$ constitue sa clé privée.
   • Envoi du message codé :
   Alice veut envoyer un message codé à son ami Bernard. Elle le représente sous forme d'un ou plusieurs entiers.
   M (message clair) compris entre 0 et $N - 1$.
   Alice calcule $C = M^e[N]$, tel que C (message crypté).
   • Réception de message codé :
   Bernard reçoit C et il le calcule grâce à sa clé privée,
   $M = C^d[N]$, tel que M (message décrypté).

Exemple 3.4.1.
On se donne deux entiers p et q,
$p = 11$ *et* $q = 5$.
Donc on calcule N,

$$N = 11 \times 5 = 55$$

On calcule $z = (p-1)(q-1) = 10 \times 4 = 40$.
On choisit e un entier premier avec z tel que $1 < e < z$ *alors* $1 < e < 40$.
Donc on peut prendre $e = 7$, *on calcul d à partir de* $(d \times e) \equiv 1\,[z]$.
On trouve $d = 23$.
On a maintenant nos clés :
$*$ *La clé publique est* $(e, N) = (7, 40)$ *(clé de cryptage),*
$*$ *La clé privée est* $(d, N) = (23, 40)$ *(clé décryptage)*

Exemple 3.4.2.
On se donne deux nombres $p = 29,\ q = 37$,
On calcule $N = pq = 29 \times 37 = 1073$.
On calcule z, tel que $1 < e < z$,
$z = 1008$ *et soit* $e = 71$

On choisit tel que $71 \times d \equiv\ 1\ [1008]$,
On trouve $d = 1079$,
On a maintenant nos clés.
∗ *La clé publique est* $(e, N) = (71, 1073)$ *(clé de cryptage),*
∗ *La clé privée est* $(d, N) = (1079, 1073)$ *(clé décryptage).*
On va crypter le message le message "HELLO" tel que $M = 7269767679$. *Ensuite, il faut découper le message en blocs qui comportent moins de chiffres que* N,
N *comporte quatre chiffres, on va découper notre message en blocs de trois chiffres* 726 976 767 900 *(on complète avec des zéros). Ensuite on crypte chacun de ces blocs :*

$$726^{71}\ [1073] = 436$$
$$976^{71}\ [1073] = 822$$
$$767^{71}\ [1073] = 825$$
$$900^{71}\ [1073] = 552.$$

Le message crypté est 436 822 825 552.
On peut le décrypter avec d :

$$436^{1079}\ [1073] = 726$$
$$822^{1079}\ [1073] = 976$$
$$825^{1079}\ [1073] = 767$$
$$522^{1079}\ [1073] = 900.$$

C'est- à- dire la suite de chiffre est 726 976 767 900,
On retrouve notre message en clair 7269767679 : "HELLO".

Conclusion

Dans ce mémoire, après avoir rappelé les notions de bases, et quelques propriétés, nous avons donné la définition d'une courbe elliptique et nous avons décrit la méthode de factorisation d'entiers basée sur les courbes elliptiques ; puis nous avons donné d'autres exemples de factorisation. D'autres améliorations sont envisageables, nous n'avons pas pu les décrire toutes. Il est par exemple possible d'utiliser d'autres formes que celle proposée par LENSTRA. Ainsi, partant de ces méthodes de factorisation nous avons présenté quelques applications.

Bibliographie

[1] Les livres de Franois LIRET (Arithmétique) et de Jean-Pierre LAMOITIER (Arithmétique modulaire)

[2] Oumar SALL : Cours master II, géométrie algébrique 2021.

[3] Thomas BAIGNÈRES : Factorisation de Grands Nombres à l'aide des courbes Elliptiques ; (ECOLE POLYTECHNIQUE FEDERALE DE LAUSANNE) Mars 2003.

[4] Benchaa SOUAD : INTRODUCTION AUX COURBES ELLIPTIQUES.

[5] Samuel MIMRAM : TIPE-Courbes elliptiques et factorisation (version dtaillée) 2001-2002.

[6] Alain KRAUSS : cours de cryptotographie ; (Université Pierre et Marie Curie) MM067 2009-2010.

[7] Ian BLAKE, Gadiel SEROUSSI, and Nigel SMART. Elliptic Curves in Cryptography Cambrige University Press, 1999.

[8] Jr.H.W.LENSTRA.Factoring integers with elliptic curves. Technical report, November 1987.

[9] Marc JOYE. Introduction élémentaire la thorie des courbes elliptiques, 1995
http : // WWWW.dice.ucl.ac.be / crypto /
une approche mathématiques des courbes elliptiques. Peu de choses en ce qui concerne la méthode ECM.