Attaque du problème du logarithme discret dans les corps finis

Idir Lankri et Iyari Rojas

Table des matières

Introduction

L'algorithme de *calcul d'index* est utilisé pour résoudre le problème du logarithme discret dans $\mathbb{F}_q^*$, il a été mis en évidence par Kraitchik dans ses articles *Théorie des nombres* (1922) et *Recherche sur la théorie des nombres* (1924). C'est un algorithme sous-exponentiel dans une implémentation optimale. Dans la pratique il est utilisé avec q premier ou égal à 2^n car il est plus facile à implémenter dans ces cas-là. On commencera par introduire la théorie mathématique nécessaire à la compréhension de cet algorithme puis nous le présenterons, enfin nous expliquerons notre implémentation.

1 Corps finis

1.1 Résultats préliminaires

Les théorèmes et propositions énoncés dans cette partie ne seront pas démontrés.

1.1.1 Anneaux, idéaux premiers et maximaux

Soit A un anneau. On note A^* le groupe multiplicatif des éléments inversibles de A.

Définition. Soit A un anneau commutatif. Soient $a \in A\backslash\{0\}$ et $b \in A$. On dit que a divise b dans A s'il existe $c \in A$ tel que $b = ac$.

Définition. Soit A un anneau commutatif. Soit $a \in A$. a est irréductible dans A si :

1. $a \notin A^*$
2. si $b \in A$ divise a dans A, alors $b \in A^*$ ou il existe $c \in A^*$ tel que $b = ca$

Définition. Soit A un anneau. A est dit intègre s'il est commutatif, non réduit à $\{0\}$ et pour tous $x, y \in A\backslash\{0\}$, $xy \neq 0$.

Remarque.

1. Tout sous-anneau d'un anneau intègre est intègre.
2. Un corps commutatif est intègre.

Définition.

1. Soit A un anneau commutatif. Soit I un idéal de A. I est dit principal s'il existe $a \in A$ tel que $I = \{ab | b \in A\}$. I est alors noté (a).
2. Un anneau est dit principal s'il est intègre et si ses idéaux sont principaux.

Remarque. Soit A un anneau commutatif. Soient $a, b \in A$. $(a) \subseteq (b)$ si et seulement si b divise a (dans A).

Définition. Soit A un anneau commutatif. Soit I un idéal de A.

1. I est dit premier dans A si :
   (a) $I \neq A$
   (b) pour tous $x, y \in A$, si $xy \in I$, alors $x \in I$ ou $y \in I$.
2. I est dit maximal dans A si :
   (a) $I \neq A$
   (b) si J est un idéal de A contenant I, alors $J = I$ ou $J = A$

Proposition 1. *Soit A un anneau commutatif. Soit I un idéal de A.*

1. *I est premier dans A si et seulement si A/I est intègre.*
2. *I est maximal dans A si et seulement si A/I est un corps.*

Proposition 2.

1. *Les idéaux premiers de $\mathbb{Z}$ sont les $n\mathbb{Z}$ avec $n = 0$ ou n premier.*
2. *Les idéaux maximaux de $\mathbb{Z}$ sont les $p\mathbb{Z}$ avec p premier.*

Corollaire 1. *Soit $n \in \mathbb{N}$. $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.*

1.1.2 Anneaux de polynômes

Théorème 1. *Soit k un corps commutatif. Soit $P \in k[X]$, $P \neq 0$. P se décompose de manière unique (à l'ordre près) sous la forme :*

$$P = a \prod_{i=1}^{n} P_i^{\alpha_i}$$

où $n \geq 1$, $a \in k^*$, $\alpha_1, \ldots, \alpha_n \in \mathbb{N}$ et $P_1, \ldots, P_n \in k[X]$ sont irréductibles et unitaires.

Proposition 3. *Soit A un anneau commutatif. Soient $P(X) \in A[X]$ et $a \in A$. a est racine simple de $P(X)$ si et seulement si $P(a) = 0$ et $P'(a) \neq 0$.*

Théorème 2. *Soit k un corps commutatif. Soit $P \in k[X]$ un polynôme de degré $n \in \mathbb{N}$. P a au plus n racines dans k.*

Proposition 4. *Soit A un anneau commutatif. $A[X]$ est intègre si et seulement si A est intègre.*

Théorème 3. *Soit k un corps commutatif.*

1. *$k[X]$ est un anneau principal.*
2. *Les idéaux premiers de $k[X]$ sont $\{0\}$ et les (P) où $P \in k[X]$ est irréductible.*
3. *Les idéaux maximaux de $k[X]$ sont les (P) où $P \in k[X]$ est irréductible.*

Corollaire 2. *Soit k un corps commutatif. Soit $P \in k[X]$. $k[X]/(P)$ est un corps (commutatif) si et seulement si P est irréductible dans $k[X]$.*

Remarque. Soit k un corps commutatif. Soit $P \in k[X]$ tel que $\deg P \geq 1$. On note $\rho : k[X] \to k[X]/(P)$ la surjection canonique.

1. (a) Clairement, k s'injecte dans $k[X]$. Par conséquent, on dira maintenant que $k[X]$ «contient» k.
   (b) k est isomorphe à $\rho(k)$. On peut donc identifier k à $\rho(k)$ et ainsi, on dira désormais que $k[X]/(P)$ «contient» k et que pour tout $x \in k$, $\rho(x) = x$.
2. Soit $Q \in k[X]$. Il y a un élément «privilégié» dans $\rho(Q)$ à savoir le reste $R \in k[X]$ de la division euclidienne de Q par P. En effet, R est l'unique polynôme tel que :

$$\deg R < \deg P \text{ et } \rho(Q) = \rho(R)$$

1.1.3 Corps des fractions d'un anneau intègre

Théorème 4. *Soit A un anneau intègre. Il existe un corps commutatif K et un morphisme d'anneaux injectif $i : A \to K$ tels que, pour tout morphisme d'anneaux injectif $f : A \to L$ (L corps commutatif), il existe un morphisme d'anneaux injectif $g : K \to L$ tel que $f = g \circ i$.*

Remarque. Dans la démonstration du théorème précédent, K est construit de la manière suivante : soit $B = \{(a, b) | a \in A, b \in A \backslash \{0\}\}$ et soit $\mathcal{R}$ la relation d'équivalence sur B définie par :

$$\forall (a, b) \in B \ \forall (c, d) \in B \ (a, b) \mathcal{R} (c, d) \Leftrightarrow ad - bc = 0$$

on pose alors $K = B/\mathcal{R}$. K ainsi construit est appelé le corps des fractions de A (par exemple, $\mathbb{Q}$ est le corps des fractions de $\mathbb{Z}$). Avec cette construction de K et en notant $\frac{a}{b}$ la classe de $(a, b) \in B$ par $\mathcal{R}$, on définit i par :

$$\forall a \in A \ i(a) = \frac{a}{1}$$

Corollaire 3. *Soit $i : \mathbb{Z} \to \mathbb{Q}$ l'injection canonique. Pour tout morphisme d'anneaux injectif $f : \mathbb{Z} \to L$ (L corps commutatif), il existe un morphisme d'anneaux injectif $g : \mathbb{Q} \to L$ tel que $f = g \circ i$.*

1.1.4 Groupes abéliens de type fini

Définition. Soit $(G, +)$ un groupe abélien. Soit $(v_i)_{i \in I}$ un système d'éléments de G. $(v_i)_{i \in I}$ est dit générateur de G si :

$$\forall g \in G \ \exists J \subseteq I \text{ (J fini) } \exists (n_j)_{j \in J} \in \mathbb{Z}^J \ g = \sum_{j \in J} n_j v_j$$

Définition. Soit G un groupe abélien. G est dit de type fini s'il admet un système générateur fini.

Théorème 5. *Tout groupe abélien de type fini est isomorphe à $\mathbb{Z}^r \times \mathbb{Z}/a_1\mathbb{Z} \times \ldots \times \mathbb{Z}/a_n\mathbb{Z}$ où $r \in \mathbb{N}$, $n \in \mathbb{N}$ et $a_1, \ldots, a_n \geq 2$ sont tels que $a_1 | \ldots | a_n$; r, n et les a_i sont uniques.*

1.2 Cyclicité du groupe multiplicatif d'un corps fini

Théorème 6. *Soit K un corps commutatif. Soit G un sous-groupe fini de $(K^*, \times)$. Alors G est cyclique.*

Démonstration. $(G, \times)$ est commutatif car K l'est. Comme G est fini, $(G, \times)$ est donc un groupe abélien de type fini (car il admet un système générateur fini, en l'occurrence tous ses éléments). Par le théorème 5, on a donc :

$$(G, \times) \simeq \mathbb{Z}^r \times \mathbb{Z}/a_1\mathbb{Z} \times \ldots \times \mathbb{Z}/a_n\mathbb{Z}$$

où $r \in \mathbb{N}$, $n \in \mathbb{N}$ et $a_1, \ldots, a_n \geq 2$ sont tels que $a_1 | \ldots | a_n$ (r, n et les a_i sont uniques). On a $r = 0$ car sinon, G serait infini, ce qui n'est pas le cas. Donc :

$$(G, \times) \simeq \mathbb{Z}/a_1\mathbb{Z} \times \ldots \times \mathbb{Z}/a_n\mathbb{Z} = (H, +)$$

Supposons que G n'est pas cyclique. Alors $n \geq 2$. Comme a_1 divise a_2, il existe $k \in \mathbb{N}\backslash\{0\}$ tel que $a_2 = a_1 k$. Soit $E = \{(y, kz, 0_H, \ldots, 0_H) \in H | y, z \in \mathbb{Z}/a_1\mathbb{Z}\}$. Les éléments de E sont solutions de l'équation $a_1 x = 0_H$. Or, $|E| = a_1^2$, donc l'équation $a_1 x = 0_H$ a au moins a_1^2 solutions dans $(H, +)$. Ainsi, puisque $(G, \times)$ et $(H, +)$ sont isomorphes, on en déduit que l'équation $x^{a_1} = 1_G$ admet au moins a_1^2 solutions dans $(G, \times)$. Le polynôme $X^{a_1} - 1 \in K[X]$ a donc au moins $a_1^2 > a_1$ (car $a_1 > 1$) racines dans K (car $G \subseteq K$), ce qui est impossible d'après le théorème 2. G est donc cyclique. □

Corollaire 4. *Soit K un corps commutatif fini. Alors $(K^*, \times)$ est cyclique*

1.3 Existence et unicité des corps finis à p^n éléments

1.3.1 Caractéristique d'un corps

Proposition 5. *Soit K un corps commutatif. Soit $\phi : \mathbb{Z} \to K, n \mapsto n.1_K$. ϕ est un morphisme d'anneaux injectif ou de noyau $p\mathbb{Z}$ avec p premier. Dans le premier cas, K est dit de caractéristique nulle et contient un corps isomorphe à $\mathbb{Q}$. Dans le second cas, K est dit de caractéristique p et contient un corps isomorphe à $\mathbb{Z}/p\mathbb{Z}$.*

Démonstration. Si ϕ n'est pas injectif, alors :

$$\exists n \in \mathbb{N}\backslash\{0\} \ \ker \phi = n\mathbb{Z}$$

Ainsi, $\mathbb{Z}/n\mathbb{Z} \simeq \phi(\mathbb{Z})$. Or, $\phi(\mathbb{Z})$ est un sous-anneau de K qui est un corps commutatif, donc $\phi(\mathbb{Z})$ est intègre. $n\mathbb{Z}$ est donc un idéal premier et puisque $n \neq 0$, n est premier. Donc $\mathbb{Z}/n\mathbb{Z}$ est un corps et ainsi, K contient un corps (en l'occurrence $\phi(\mathbb{Z})$) isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Soit $i : \mathbb{Z} \to \mathbb{Q}$ l'injection canonique. Si ϕ est injectif, par le corollaire 3, il existe un morphisme d'anneaux injectif $\psi : \mathbb{Q} \to K$ tel que $\phi = \psi \circ i$. Donc $\psi(\mathbb{Q}) \subseteq K$ est isomorphe à $\mathbb{Q}$. □

Remarque. On conserve les notations du théorème précédent. Etant donné que $\ker \phi = p\mathbb{Z}$, on a $\phi(p) = 0_K$ et donc, pour tout $x \in K$, $px = \phi(p)x = 0_K$.

Théorème 7. *Soit K un corps commutatif de caractéristique un nombre premier p. L'application $F : K \to K, x \mapsto x^p$ est un morphisme d'anneaux injectif.*

Démonstration. Soit $k \in \{1, \dots, p-1\}$. On a :

$$k\binom{p}{k} = p\binom{p-1}{k-1}$$

Donc p divise $k\binom{p}{k}$. Comme p et k sont premiers entre eux, en fait, p divise $\binom{p}{k}$. Ainsi, puisque K est commutatif et de caractéristique p, on en déduit :

$$\forall x \in K\ \forall y \in k\ F(x+y) = (x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} = x^p + y^p = F(x) + F(y)$$

F est donc un morphisme de groupes. Et comme K est commutatif, on a d'autre part :

$$\forall x \in K\ \forall y \in k\ F(xy) = (xy)^p = x^p y^p = F(x)F(y) \text{ et } F(1) = 1^p = 1$$

Ainsi, F est un morphisme d'anneaux. K étant un corps commutatif, il est en particulier intègre, d'où :

$$\ker F = \{x \in K | x^p = 0\} = \{0\}$$

F est donc injectif. □

Corollaire 5. *On reprend les mêmes hypothèses et notations que le théorème précédent. Soit $n \in \mathbb{N}\backslash\{0\}$. $\phi_n : K \to K, x \mapsto x^{p^n}$ est un morphisme d'anneaux injectif, en effet, $\phi_n = F^n$.*

1.3.2 Cardinal d'un corps fini

Définition. Un corps K est une extension d'un corps k si $k \subseteq K$.

Proposition 6. *Soit L une extension d'un corps K. Alors L est un K-espace vectoriel en munissant le groupe $(L, +)$ de la loi externe $K \times L \to L, (x, y) \mapsto xy$. Si on suppose de plus que K et L sont finis, L est alors de dimension finie (sur K) car il admet un système générateur fini, à savoir tous ses éléments. Dans ce cas, il existe donc $n \in \mathbb{N}\backslash\{0\}$ tel que L est isomorphe à K^n et $|L| = |K|^n$.*

Proposition 7. *Soit K un corps commutatif fini. Il existe $n \in \mathbb{N}\backslash\{0\}$ et $p \in \mathbb{N}$ premier tels que $|K| = p^n$.*

Démonstration. K n'est pas de caractéristique nulle, sinon K contiendrait un corps isomorphe à $\mathbb{Q}$ et serait donc infini, absurde. Ainsi, K est de caractéristique un nombre premier p et contient un corps k isomorphe à $\mathbb{Z}/p\mathbb{Z}$ et donc $|k| = |\mathbb{Z}/p\mathbb{Z}| = p$. Par la proposition 6, K est donc un espace vectoriel de dimension finie sur k et il existe $n \in \mathbb{N}\backslash\{0\}$ tel que K est isomorphe à k^n. D'où, $|K| = |k|^n = p^n$. □

Remarque. Soit K un corps commutatif fini d'ordre p^n (p premier et $n \in \mathbb{N}\backslash\{0\}$).

1. K contient un corps isomorphe à $\mathbb{Z}/p\mathbb{Z}$ mais on dira dorénavant que K «contient» $\mathbb{Z}/p\mathbb{Z}$.
2. p est en fait la caractéristique de K et n la dimension de K vu comme espace vectoriel sur $\mathbb{Z}/p\mathbb{Z}$.

1.3.3 Théorème d'existence et d'unicité des corps finis

Proposition 8. *Soit k un corps commutatif. Soit $P \in k[X]$, P irréductible. $k[X]/(P)$ est un corps (commutatif) dans lequel P a une racine.*

Démonstration. On pose $K = k[X]/(P)$ et $P = a_0 + \ldots + a_n X^n$ avec $n \in \mathbb{N}\backslash\{0\}$ et $a_0, \ldots, a_n \in k$ ($a_n \neq 0$). P étant irréductible, K est un corps commutatif. Soit $\rho : k[X] \to K$ la surjection canonique. On pose $\alpha = \rho(X)$. Comme $\ker \rho = (P)$, on a $\rho(P) = 0$. Or, puisque ρ est un morphisme d'anneaux, on a :

$$\rho(P) = \prod_{i=0}^{n} \rho(a_i)\rho(X)^i = \prod_{i=0}^{n} a_i \alpha^i$$

D'où, $P(\alpha) = 0$ et P a une racine dans K. □

Définition. Soit k un corps commutatif. Soit $P \in k[X]$ avec $n = \deg P \geq 1$. P est scindé dans k si :

$$\exists a \in k^* \ \exists x_1, \ldots, x_n \in k \ P = a \prod_{i=1}^{n} (X - x_i)$$

Définition. Soit k un corps commutatif. Soit $P \in k[X]$. Un corps de décompostion de P sur k est une extension K de k telle que :

1. P est scindé dans K
2. pour tout corps L tel que $k \subseteq L \subseteq K$, si P est scindé dans L, alors $L = K$

Théorème 8. *Soit k un corps commutatif. Soit $P \in k[X]$ tel que $\deg P \geq 1$. Il existe un corps de décomposition (commutatif) de P sur k, unique à isomorphisme près.*

Démonstration. On montre l'existence et l'unicité par récurrence sur le degré de P.

Si $\deg P = 1$, on a :

$$\exists a \in k^* \ \exists b \in k \ P = aX + b = a(X + a^{-1}b)$$

P est donc scindé dans k et k est un corps de décomposition (commutatif) de P sur k (et par conséquent, on a automatiquement l'unicité). Ce résultat se généralise à tout polynôme de $k[X]$ scindé dans k.

On suppose qu'il existe un corps de décomposition (commutatif), unique à isomorphisme près, pour tout polynôme de degré égal à $n \geq 1$. Soit $P \in k[X]$ tel que $\deg P = n + 1$.

Montrons qu'il existe un corps de décomposition de P sur k. Par le théorème 1,

$$P = a\prod_{i=1}^{q} P_i^{\beta_i}$$

où $q \geq 1$, $a \in k^*$, $\beta_1, \ldots, \beta_q \in \mathbb{N}$ et $P_1, \ldots, P_q \in k[X]$ sont irréductibles et unitaires. Soit $K_1 = k[X]/(P_1)$. Alors il existe $\alpha_1 \in K_1$ tel que $P(\alpha_1) = 0$. D'où :

$$\exists Q \in K_1[X]\ P = (X - \alpha_1)Q \text{ avec } \deg Q = n$$

D'après l'hypothèse de récurrence, il existe donc un corps de décomposition (commutatif) K de Q sur K_1 et donc :

$$\exists b \in K^*\ \exists \gamma_1, \ldots, \gamma_n \in K\ Q = b\prod_{i=1}^{n}(X - \gamma_i)$$

Ainsi,

$$P = b(X - \alpha_1)\prod_{i=1}^{n}(X - \gamma_i) \text{ avec } \alpha_1 \in K_1 \subseteq K$$

Donc P est scindé dans K. On pose :

$$\mathcal{L} = \{k \subseteq L \subseteq K \text{ (L corps)} | P \text{ est scindé dans } L\}$$

Alors, $\bigcap_{L\in\mathcal{L}} L$ est un corps de décomposition commutatif de P sur k. Ce qui conclut la preuve de l'existence.

Montrons maintenant l'unicité. On peut supposer que P n'est pas scindé dans k (voir l'initialisation de la récurrence). Soient K et K' deux corps de décomposition de P sur k. P n'étant pas scindé dans k, il existe $Q \in k[X]$ ($\deg Q \geq 2$) irréductible (dans $k[X]$) et divisant P. Q admet une racine $x \in K$ (respectivement $x' \in K'$) car sinon P ne serait pas scindé dans K (respectivement K'), ce qui est absurde puisque K (respectivement K') est un corps de décomposition de P sur k.

Un polynôme de $k[X]$ peut être vu comme un polynôme de $K[X]$ (respectivement $K'[X]$) car $k \subseteq K$ (respectivement $k \subseteq K'$). On peut donc considérer les morphismes d'anneaux $\phi : k[X] \to K, R \mapsto R(x)$ et $\phi' : k[X] \to K', R \mapsto R(x')$. Comme $k[X]$ est principal, il existe $S \in k[X]$ tel que $\ker\phi = (S)$. On a aussi $(Q) \subseteq (S)$ car x est une racine de Q. Or, Q est irréductible dans $k[X]$, d'où $(Q) = (S) = \ker\phi$. Pareillement, $\ker\phi' = (Q)$. D'où, $\phi(k[X]) \simeq k[X]/(Q) \simeq \phi'(k[X])$. On peut ainsi dire que $x = \phi(X)$ et $x' = \phi'(X)$ sont égaux à isomorphisme près. On a d'une part :

$$\exists P_1 \in K[X]\ P = (X - x)P_1 \text{ avec } \deg P_1 = n$$

et d'autre part :

$$\exists P_2 \in K'[X]\ P = (X - x')P_2 \text{ avec } \deg P_2 = n$$

Par l'hypothèse de récurrence, il existe un unique corps de décomposition M (respectivement M') de P_1 (respectivement P_2) sur K (respectivement K'). Or, $K \subseteq K \subseteq M$ (respectivement $K' \subseteq K' \subseteq M'$) et P_1 (respectivement P_2) est scindé dans K (respectivement K'), donc $K = M$ (respectivement $K' = M'$). De plus, comme P_1 et P_2 sont égaux à isomorphisme près (car x et x' le sont), on a finalement que $K \simeq K'$. □

Théorème 9. *Soient p un nombre premier et $n \in \mathbb{N}\backslash\{0\}$. Il existe un corps (commutatif) à p^n éléments et deux tels corps sont isomorphes.*

Démonstration. On pose $k = \mathbb{Z}/p\mathbb{Z}$ et $q = p^n$. Soit $P(X) = X^q - X \in k[X]$. Soit K le corps de décomposition de $P(X)$ sur k. On a :

$$P'(X) = qX^{q-1} - 1 = -1 \text{ car } q \equiv 0 \bmod p$$

Donc $P'(X)$ n'a pas de racine et donc $P(X)$ n'a pas de racine multiple. Ainsi :

$$P(X) = \prod_{i=1}^{q} (X - \alpha_i) \text{ où } \alpha_1, \ldots, \alpha_q \in K \text{ sont distinctes}$$

Soient maintenant $L = \{\alpha_1, \ldots, \alpha_q\} \subseteq K$ et $\phi : K \to K, x \mapsto x^q$. Par le corollaire 5, ϕ est un morphisme d'anneaux, en particulier un morphisme de groupes additifs. Donc $\phi - \mathrm{id}_K$ est un morphisme de groupes. Comme $L = \ker(\phi - \mathrm{id}_K)$, $(L, +)$ est un sous-groupe de $(K, +)$.

Soit $\psi : (K^*, \times) \to (K^*, \times), x \mapsto x^{q-1}$. ψ est un morphisme de groupes, en effet, comme K est commutatif, on a :

$$\forall x \in K^* \ \forall y \in K^* \ \psi(xy) = (xy)^{q-1} = x^{q-1}y^{q-1} = \psi(x)\psi(y)$$

$L\backslash\{0\}$ est formé des racines de $X^{q-1} - 1$, ainsi, $L\backslash\{0\} = \ker\psi$. Donc $(L\backslash\{0\}, \times)$ est un sous-groupe de $(K^*, \times)$. Ainsi, $(L, +)$ et $(L\backslash\{0\}, \times)$ sont des groupes et donc L est un corps. Or, $|L| = q$, cela montre donc l'existence d'un corps à $q = p^n$ éléments.

En fait, $L = K$. En effet, $k \subseteq L \subseteq K$ et $P(X)$ est scindé dans L, ainsi, puisque K est le corps de décomposition de $P(X)$ sur k, $L = K$. L'unicité de L vient donc de celle de K. □

Notation. Soient p un nombre premier et $n \in \mathbb{N}\backslash\{0\}$. On note $\mathbb{F}_{p^n}$ l'unique (à isomorphisme près) corps à p^n éléments. En particulier, $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

1.4 Représentation de $\mathbb{F}_{p^n}$

Théorème 10. *Soit k un corps commutatif. Soit $P \in k[X]$, P irréductible de degré $n \geq 1$. La surjection canonique est notée $\rho : k[X] \to k[X]/(P)$. On pose $K = k[X]/(P)$ et $x = \rho(X)$. K est un k-espace vectoriel de dimension n et $\{1, \ldots, x^{n-1}\}$ en est une base.*

Démonstration. On pose $\mathcal{B} = \{1, \dots, x^{n-1}\}$. Comme $k \subseteq K$, K est un k-espace vectoriel. Montrons que $\mathcal{B}$ est une partie génératrice de K. Soit $u \in K$. Par surjectivité de ρ, on a :

$$\exists U \in k[X]\ u = \rho(U)$$

Divisons U par P :

$$\exists! Q \in k[X]\ \exists! R \in k[X]\ U = PQ + R \text{ avec } \deg R < n$$

On pose $R = a_0 + \ldots + a_{n-1}X^{n-1}$ où $a_0, \dots, a_{n-1} \in k$. Puisque ρ est un morphisme d'anneaux et $u = \rho(U) = \rho(R)$, on a :

$$u = \sum_{i=0}^{n-1} \rho(a_i)\rho(X)^i = \sum_{i=0}^{n-1} a_i x^i$$

Donc $\mathcal{B}$ engendre K. Montrons maintenant que $\mathcal{B}$ est libre. Soient $\lambda_0, \dots, \lambda_{n-1} \in k$ tels que :

$$\sum_{i=0}^{n-1} \lambda_i x^i = 0$$

On a :

$$\rho(\sum_{i=0}^{n-1} \lambda_i X^i) = \sum_{i=0}^{n-1} \rho(\lambda_i)\rho(X)^i = \sum_{i=0}^{n-1} \lambda_i x^i = 0$$

Donc $S = \lambda_0 + \ldots + \lambda_{n-1}X^{n-1} \in \ker \rho = (P)$. On en déduit que P divise S. Or, $\deg P > \deg S$ d'où nécessairement $S = 0$ et donc pour tout $i \in \{0, \dots, n-1\}$, $\lambda_i = 0$. Ainsi, $\mathcal{B}$ est une base de K qui est donc de dimension n sur k. □

Proposition 9. *Soient p un nombre premier et $n \in \mathbb{N}\backslash\{0\}$. Il existe $P \in \mathbb{F}_p[X]$ tel que P est irréductible de degré n tel que $\mathbb{F}_{p^n} \simeq \mathbb{F}_p[X]/(P)$.*

Démonstration. On pose $q = p^n$. Par le corollaire 4, $(\mathbb{F}_q^*, \times)$ est un groupe cyclique à $q-1$ éléments. Soit $\alpha \in \mathbb{F}_q^*$ un générateur de $\mathbb{F}_q^*$. Soit $f : \mathbb{F}_p[X] \to \mathbb{F}_q, Q \mapsto Q(\alpha)$. f est bien définie car α est un générateur de $\mathbb{F}_q^*$. f est clairement un morphisme d'anneaux. Puisque $\mathbb{F}_p[X]$ est principal,

$$\exists P \in \mathbb{F}_p[X]\ \ker f = (P)$$

Soit $x \in \mathbb{F}_q^*$. Comme α est un générateur de $\mathbb{F}_q^*$, on a :

$$\exists m \in \{0, \dots, q-2\}\ x = \alpha^m$$

Donc $x = f(X^m)$. De plus, $0 = f(0)$ car f est un morphisme de groupes additifs. Donc :

$$\forall x \in \mathbb{F}_q\ \exists R \in \mathbb{F}_p[X]\ x = f(R)$$

Ainsi, f est surjectif et donc $\mathbb{F}_p[X]/(P) \simeq \mathbb{F}_q$. $\mathbb{F}_q$ étant un corps, $\mathbb{F}_p[X]/(P)$ est aussi un corps et donc P est irréductible. De plus, par le théorème précédent, $\mathbb{F}_p[X]/(P)$ est un $\mathbb{F}_p$-espace vectoriel de dimension le degré de P et d'autre part, $\mathbb{F}_q$ ($\supseteq \mathbb{F}_p$) est un $\mathbb{F}_p$-espace vectoriel de dimension n. D'où, $\deg P = n$. □

2 Algorithme de *calcul d'index*

2.1 Position du problème

Définition (logarithme discret)**.** Soit $(G, \times)$ un groupe cyclique d'ordre $N \in \mathbb{N}$. Soit g un générateur de G. On considère l'isomorphisme de groupes $\phi : \mathbb{Z}/N\mathbb{Z} \to G, \overline{n} \mapsto g^n$ (en effet, ϕ est clairement un morphisme de groupes surjectif entre deux groupes de même ordre). Le logarithme discret de G en base g (noté $\log_g$) est l'isomorphisme ϕ^{-1}. Pour $x \in G$, le logarithme discret de x en base g (noté $\log_g(x)$) est l'unique entier $m \in \{0, \ldots, N-1\}$ tel que $x = \phi(\overline{m}) = g^m$.

Autant le calcul de $\phi(\overline{m}) = g^m$ $(0 \leq m \leq N-1)$ est «facile» [1], autant celui de $\phi^{-1}(x) = log_g(x)$ $(x \in G)$ est difficile. En effet, on ne connaît pas d'algorithme polynomial pour déterminer $log_g(x)$. C'est pourquoi on parle du *problème du logarithme discret*. La robustesse de certains protocoles cryptographiques (par exemple, le protocole de Diffie-Hellman) repose sur la difficulté de ce problème.

Pour p un nombre premier et $n \geq 1$, on a vu précédemment que $\mathbb{F}_{p^n}$ était un corps fini commutatif à p^n éléments. De plus, par la proposition 9, on a :

$$\exists P \in \mathbb{F}_p[X] \ \mathbb{F}_{p^n} \simeq \mathbb{F}_p[X]/(P) \text{ où } P \text{ est irréductible de degré } n$$

D'après le théorème 10, $\mathbb{F}_{p^n}$ est formé des classes (modulo (P)) des polynômes de degré strictement inférieur à n, à isomorphisme près. Dans la suite, on identifiera, pour simplifier, les éléments de $\mathbb{F}_{p^n}$ aux polynômes à coefficients dans $\mathbb{F}_p$ et de degré strictement inférieur à n et les calculs dans $\mathbb{F}_{p^n}$ se feront modulo P.

Enfin, par le corollaire 4, $(\mathbb{F}_{p^n}^*, \times)$ est un groupe cyclique d'ordre $p^n - 1$. Parler de logarithme discret dans $\mathbb{F}_{p^n}^*$ a donc un sens. Nous allons maintenant étudier l'algorithme de *calcul d'index* qui permet de «résoudre» le problème du logarithme discret dans $\mathbb{F}_{p^n}$.

2.2 Fonctionnement de l'algorithme

Soient p un nombre premier et $n \in \mathbb{N}\backslash\{0\}$. On pose $q = p^n$. On considère le corps

$$\mathbb{F}_q \simeq \mathbb{F}_p[X]/(P) \text{ avec } P \text{ irréductible de degré } n$$

Soient G un générateur supposé unitaire de $(\mathbb{F}_q^*, \times)$ et $H \in \mathbb{F}_q^*$. On cherche le logarithme discret de H en base G. Pour cela, l'algorihtme de *calcul d'index* procède en trois étapes que nous allons maintenant détailler. On suppose néanmoins qu'un pré-calcul nous a donné les logarithmes discrets des constantes (voir la partie suivante), c'est-à-dire que l'on connaît $\log_G(k)$ pour tout $k \in \mathbb{F}_p^*$.

1. Par «facile», on entend que le calcul de g^m peut se faire en au plus $2\log_2(m)$ multiplications.

Étape 1 On fixe une borne b qui paramètre un sous-ensemble fini de $\mathbb{F}_q^*$ appelé *base de facteurs* et noté $\mathcal{B}$. $\mathcal{B}$ est définie ainsi :

$$\mathcal{B} = \{B \in \mathbb{F}_q^* | B \text{ irréductible unitaire, } B \neq G \text{ et } \deg B \leq b\}$$

On essaie alors de factoriser des puissances du générateur suivant la base de facteurs. On aboutit ainsi à des relations de la forme :

$$G^\alpha \equiv \prod_i B_i^{\alpha_i} \bmod P \text{ où les } B_i \in \mathcal{B}$$

Étape 2 En passant au logarithme discret dans les relations obtenues précédemment, on récupère des équations de congruences du type :

$$\alpha \equiv \sum_i \alpha_i \log_G(B_i) \bmod (q-1)$$

De cette manière, on dispose d'un système d'équations dont les inconnues sont les logarithmes discrets des éléments de $\mathcal{B}$. Lorsque l'on a suffisamment d'équations (au moins $|\mathcal{B}|$), on peut résoudre le système modulo $q-1$ et on connaît ainsi $\log_G(B)$ pour tout $B \in \mathcal{B}$.

Étape 3 On cherche un entier β tel que $G^\beta H$ soit décomposable dans la base de facteurs :

$$G^\beta H \equiv \lambda \prod_i B_i^{\beta_i} \bmod P \text{ avec } \lambda \in \mathbb{F}_p^*$$

On en déduit :

$$\log_G(H) \equiv \log_G(\lambda) - \beta + \sum_i \beta_i \log_G(B_i) \bmod (q-1)$$

Les $\log_G(B_i)$ et $\log_G(\lambda)$ étant connus, on a ainsi trouvé le logarithme de H en base G, ce qui était notre but.

Remarque.

1. Un des principaux avantages de cet algorithme est que les étapes 1 et 2 ne dépendent pas de l'élément dont on cherche le logarithme discret. Ainsi, les résultats obtenus à l'issue de l'étape 2 sont réutilisables pour un autre élément.
2. Dans le cas où $n = 1$, la base de facteurs est formée des nombres premiers inférieurs à un certain entier.

Exemple. On pose $P = X^5 + X^3 + 1$. On a $\mathbb{F}_{32} \simeq \mathbb{F}_2[X]/(P)$. X est un générateur de $\mathbb{F}_{32}^*$. On cherche le logarithme discret de $H = X^4 + X^3 + X + 1$ en base X. On prend $b = 2$. On a alors :

$$\mathcal{B} = \{X + 1, X^2 + X + 1\}$$

On a :

$$\begin{cases} X^5 & \equiv & (X+1)(X^2+X+1) \bmod P \\ X^{11} & \equiv & (X+1)^3 \bmod P \end{cases}$$

On en déduit le système :

$$\begin{cases} \log_X(X^2+X+1) + \log_X(X+1) & \equiv & 5 \bmod 31 \\ 3\log_X(X+1) & \equiv & 11 \bmod 31 \end{cases}$$

En résolvant ce système modulo 31, on obtient :

$$\log_X(X+1) = 14 \text{ et } \log_X(X^2+X+1) = 22$$

Or, on a :

$$H \equiv (X+1)^2(X^2+X+1) \bmod P$$

D'où :

$$\log_X(H) \equiv 2\log_X(X+1) + \log_X(X^2+X+1) = 2 \times 14 + 22 = 50 \bmod 31$$

On a donc finalement $\log_X(H) = 19$.

2.3 Remarques diverses

On conserve les notations de la partie précédente.

2.3.1 Pré-calcul des logarithmes discrets des constantes

On va voir maintenant comment le calcul des logarithmes discrets (dans $\mathbb{F}_q^*$) des constantes se ramène à un calcul de logarithme discret dans $\mathbb{F}_p^*$.

Pour $S \in \mathbb{F}_q^*$, on note $|S|$ l'ordre de S. Comme G est un générateur de $\mathbb{F}_q^*$, on a :

$$|G| = q - 1 = p^n - 1 = (p-1)s \text{ avec } s = \sum_{k=0}^{n-1} p^k$$

On a $|G^s| = p - 1$, donc G^s est un générateur de $\mathbb{F}_p^*$. Ainsi, on est ramené à un calcul de logarithme discret dans $\mathbb{F}_p^*$ qui peut se faire par l'algorithme *rho-Pollard*[2]. En effet, on a alors :

$$\forall \lambda \in \mathbb{F}_p^* \ \log_G(\lambda) = (p-1)\log_{G^s}(\lambda)$$

Si p est petit, le calcul de logarithme discret dans $\mathbb{F}_p^*$ peut même se faire directement «à la main». Ainsi, dans les corps finis de petite caractéristique, le calcul des logarithmes des constantes est insignifiant et même inexistant en caractéristique 2.

2. On peut aussi le faire par l'algorithme de *calcul d'index* mais cet algorithme nous intéresse surtout quand $n \geq 2$.

2.3.2 Base de facteurs

Le choix de la borne b paramétrant la base de facteurs $\mathcal{B}$ est primordial. En effet, si b est «petit», la résolution du système linéaire (étape 2 de l'algorithme) est plus simple car le système a moins d'inconnues mais en contrepartie, un polynôme a moins de chances de se décomposer suivant $\mathcal{B}$ (étape 1 de l'algorithme). Inversement, si b est «grand», l'étape 1 est facilitée alors que l'étape 2 est rendue plus délicate. Il faut donc trouver un juste milieu pour ne pas compromettre l'une des deux premières étapes.

Déterminer la base de facteurs, c'est en fait trouver les polynômes de $\mathbb{F}_p[X]$ irréductibles unitaires de degré strictement inférieur à b. Pour cela, on peut procéder de manière analogue au *crible d'Ératosthène* qui permet de trouver les nombres premiers inférieurs à un certain entier. On énumère d'abord tous les polynômes unitaires de degré compris entre 1 et b. On élimine ensuite tous les polynômes divisibles par X. Parmi les polynômes encore présents, on élimine ceux qui sont divisibles par $X+1$. On passe ensuite au polynôme suivant encore présent et on répète l'opération, et ainsi de suite. De cette manière, lorsqu'on arrive au dernier polynôme, tous les polynômes qui n'ont pas été éliminés sont irréductibles dans $\mathbb{F}_p[X]$.

2.3.3 Algèbre linéaire

Si $q-1$ n'est pas premier, alors $\mathbb{Z}/(q-1)\mathbb{Z}$ n'est pas un corps et tout élément non nul n'est pas nécessairement inversible modulo $q-1$. De ce fait, on peut se retrouver face un problème lors de la résolution du système linéaire obtenu lors de l'étape 2 de l'algorithme. En effet, supposons $q-1$ non premier. Si on utilise la méthode du *pivot de Gauss* pour résoudre le système, on peut avoir, après triangularisation du système, une équation (d'inconnue x) de la forme :

$$ax \equiv c \bmod (q-1)$$

où $a, c \in \mathbb{Z}/(q-1)\mathbb{Z}$ et $\text{pgcd}(a, q-1) \neq 1$. Dans ce cas, a n'a pas d'inverse modulo $q-1$ puisque a et $q-1$ ne sont pas premiers entre eux. On ne peut donc pas en déduire directement la valeur de x. On pose $\delta = \text{pgcd}(a, q-1)$. On a :

$$\exists k \in \mathbb{Z}\ ax + (q-1)k = c$$

D'où :

$$\frac{a}{\delta}x + \frac{q-1}{\delta}k = \frac{c}{\delta}$$

$\frac{a}{\delta}$ et $\frac{q-1}{\delta}$ sont bien des entiers car $\delta = \text{pgcd}(a, q-1)$. $\frac{c}{\delta}$ est un entier bien défini parce que x est le logarithme discret d'un élément de la base de facteurs, par conséquent, x existe et est unique, et donc les deux membres de la dernière égalité sont définis et égaux. On a ainsi :

$$\frac{a}{\delta}x \equiv \frac{c}{\delta} \bmod \frac{q-1}{\delta}$$

Comme $\delta = \text{pgcd}(a, q-1)$, $\frac{a}{\delta}$ et $\frac{q-1}{\delta}$ sont premiers entre eux. On peut donc inverser $\frac{a}{\delta}$ modulo $\frac{q-1}{\delta}$ afin de trouver x.

2.4 Implémentation

Cet algorithme étant utilisé avec des grands nombres pour être utilisé en tant que cryptosystème, on a choisi d'utiliser la bibliotheque GMP qui nous permet de gérer les grands nombres et de plus par exemple d'inverser un nombre modulo p ou de faire la division euclidienne de nombres par des fonctions de la bibliothèque.

Notre programme se divise en deux parties : la partie sur les polynômes où sont générés les polynômes irréductibles de degré inférieur à une certaine borne et où est décomposé un élément dans la base et la partie algèbre linéaire où sont résolus les systèmes d'équations avec le pivot de Gauss. Ensuite dans le $main()$ on choisit une borne et on prend comme base les polynômes irréductibles de degré inférieur à cette borne. Pour faire le système, qui sera une matrice, par lequel on calculera le log des éléments de la base on choisit des puissances premières du générateur et on en choisit assez pour avoir assez de lignes dans la matrice du système pour qu'une partie de ces lignes forment une base. On choisit des puissances premières pour qu'il n'y ait pas de lignes colinéaires. La partie algèbre linéaire nous renvoie le log des éléments de la base. Puis on choisit aléatoirement s jusqu'à ce que $\alpha^s h$ soit décomposable dans la base et on en déduit x.

2.4.1 Partie polynômes

Dans la partie polynômes, les types définis sont le type polynôme qui consiste en un entier représentant le degré et un tableau de coefficients et le type liste de polynômes. Sont définies dans cette partie les fonctions addition et multiplication de polynômes, la division euclidienne de polynômes. La division euclidienne calcule le reste et le quotient de la division de deux polynômes, on calcule le quotient en rajoutant à chaque fois le monôme qu'il faut pour que, multiplié par le diviseur, il annule le monôme de plus grand degré du reste courant , le reste initial étant le dividende.

Les polynômes unitaires de degré inférieur à une certaine borne sont d'abord générés pour ensuite en extraire les éléments irréductibles qui formeront la base de facteurs. Dans la fonction $factoriser()$ est décomposé, dans la base de facteurs irréductibles générés, α^k ou $P\alpha^k$ par divisions euclidiennes successives puis est renvoyé la ligne représentant la relation entre les log des éléments de la base.

2.4.2 Partie algèbre linéaire

Dans la partie algèbre linéaire, il a été nécessaire de créer deux types : le type ligne et le type matrice, la grande taille de ces objets nous a contraint à nous servir de listes, les listes ne nécessitant pas d'avoir de grands segments de

mémoires disponibles. On a donc programmé les fonctions qui renvoient la p-ième ligne d'une matrice et le p-ième élément d'une ligne. Pour simplifier le code du pivot de Gauss, on a aussi défini les fonctions multiplication par un scalaire, addition de deux lignes et une fonction qui fait une permutation circulaire des lignes à partir de la k-ième ligne.

La fonction pivot de Gauss triangularise dans un premier temps le système par les opérations élémentaires puis calcule la solution de proche en proche. Pour trianguláriser le système on commence par mettre des zéros sur la première colonne, sauf sur la première ligne de cette colonne, en multipliant par le bon coefficient chaque ligne puis en additionnant la première ligne avec chaque ligne, et on fait de même avec les autres colonnes pour mettre des zéros sur les lignes de la colonne en dessous de la diagonale. Comme les lignes sont faites à partir du passage au log des puissances premières du générateur il se peut que lorsque la triangulation se fait un zéro apparaisse sur la diagonale d'une ligne, ce que l'on ne veut pas car on ne pourra pas en déduire la solution, donc dans ce cas on fait une permutation circulaire sur les lignes supérieures à cette ligne. Et on recommence à faire les opérations sur les lignes pour mettre un zéro sur la colonne correspondante jusqu'à qu'il n'y ait plus de zéro sur la diagonale. C'est pour cela que l'on prend plus de lignes que d'éléments de la base.

2.5 Complexité

Fonction	Complexité
$div\_eucl\_pol()$	$O((n-m)m)$
$pow\_deg\_fixe()$	$O(p^n)$
$polynomes()$	$O(borne * p^{borne})$
$cribler()$	$O((borne-n)^2 * n * p^{borne})$
$generer\_base()$	$O(borne^4 * p^{borne})$
$factoriser()$	$O((k-borne) * borne^2 + borne^5)$
$piv\_gauss()$	$O(nb\_lignes * m^4)$
$generer\_syst()$	$O(nb\_rel * borne^5)$

Conclusion

Notre implémentation n'est pas optimale principalement car nous avons choisis de résoudre le système linéaire par le pivot de Gauss alors que nous aurions pu utiliser des techniques plus modernes comme en utilisant la factorisation de Cholesky ou la décomposition LU. Par voie de conséquence, notre implémentation n'est pas sous-exponentielle mais exponentielle. Nous aurions pu aussi gérer le cas où on se place dans $\mathbb{F}_{p^n}$ avec $p > 2$ et $n > 1$ dans ce cas il aurait fallu utiliser d'autres algorithmes pour calculer le logarithme des constantes.

Références

[1] Leonard M. Adleman et Jonathan Demarrais : A subexponential algorithm for discrete logarithms over all finite fields. *Mathematics of computation*, 61(203):1–15, 1993.

[2] Antoine Joux et Reynald Lercier : Algorithmes pour résoudre le problème du logarithme discret dans les corps finis. *Nouvelles Méthodes Mathématiques en Cryptographie*, pages 23–53, 2007.

[3] A. M. Odlyzko : Discrete logarithms in finite fields and their cryptographic significance. *Advances in Cryptology : Proceedings of EUROCRYPT 84*, pages 224–314, 1985.

[4] Douglas Stinson : *Cryptographie, théorie et pratique*. Vuibert, 2003.

[5] Henk C. A. van Tilborg, éditeur. *Encyclopedia of cryptography and security*. Springer, 2005.