ANNALES DE LA FACULTÉ DES SCIENCES DE TOULOUSE

NDIAYE EL HADJI OUMAR

Étude du problème du logarithme discret dans IF_{p^3}

Annales de la faculté des sciences de Toulouse 6^e série, tome 4, n° 2 (1995), p. 269-296

<http://www.numdam.org/item?id=AFST_1995_6_4_2_269_0>

Annales de la Faculté des Sciences de Toulouse Vol. IV, n° 2, 1995

Étude du problème du logarithme discret dans $\mathbb{F}_{p^3}$ (*)

EL HADJI OUMAR NDIAYE(1)

RÉSUMÉ. — L'algorithme présenté ici nous permet de résoudre le problème du logarithme discret dans $\mathbb{F}_{p^3}$ ($p \equiv 1 \pmod 3$), pour un coût de l'ordre de $\exp(24\sqrt{\log p \log\log p})$. L'intérêt suscité par ce problème en cryptographie n'a cessé de croître depuis 1976, date à laquelle Diffie et Hellman ont inventé la cryptographie à clé publique. La sécurité de certains systèmes à clé publique, qui ont vu le jour par la suite, repose sur la difficulté du problème du logarithme discret dans les corps finis ; cette sécurité est d'autant plus assurée que p est "grand". Or les algorithmes relatifs à $\mathbb{F}_{p^m}$ ont un coût sous-exponentiel seulement pour p "petit" et m "grand". D'où l'intérêt de l'étude pour les corps $\mathbb{F}_{p^m}$ où p est grand et m petit (par exemple $m = 2, 3, 4$). Comme l'algorithme de El Gamal (1985) relatif à $\mathbb{F}_{p^2}$, la présente étude répond à cette catégorie et utilise les anneaux d'entiers de corps algébriques.

ABSTRACT. — In this paper, we present a subexponential algorithm of discrete logarithm in $\mathrm{GF}(p^3)$, $p \equiv 1 \pmod 3$, which runs in time $O\left(\exp(24\sqrt{\log p \log\log p})\right)$. The discrete logarithm problem is of great interest since 1976, when Diffie and Hellman introduced the concept of public key cryptosystem. Since then, several cryptosystems that rely on the difficulty of computing logarithms in finite fields $\mathbb{F}_p$, for a large prime p, have been presented. The algorithms for computing discrete logarithm in $\mathbb{F}_{p^m}$ run in subexponential-time only in the case that m grows and p is fixed. So it can be interesting to examine the case of p large and m small (for example $m = 2, 3, 4$). In this purpose, as El Gamal (1985) for $\mathbb{F}_{p^2}$, we present a method which use the rings of algebraic integers.

(*) Reçu le 1 mars 1993

(1) Département de Mathématiques, 123 avenue Albert Thomas, F-87060 Limoges Cedex (France)

1. Introduction

Nous avons à résoudre le problème suivant :

PROBLÈME .— *Soient p un nombre premier ≥ 5, k un polynôme irréductible sur le corps $\mathbb{F}_p$, g un générateur de $\mathbb{F}_{p^3}^* = \left(\mathbb{F}_p[X]/(k)\right)^*$.*

y étant donné dans $\mathbf{F}_{p^3}$, trouver $x \in [0\,,\, p^3-2]$ tel que $g^x = y$ dans $\mathbb{F}_{p^3}$.

Un tel problème est dit problème du logarithme discret. La démarche qui sera suivie pour résoudre ce problème est analogue à celle présentée dans l'algorithme de El Gamal [3] pour $\mathbb{F}_{p^2}$. L'algorithme de El Gamal reprend celui d'Adleman [1] et de Hellman et Reyneri [5]. El Gamal travaille dans l'anneau des entiers quadratiques via un théorème établissant un isomorphisme entre $\mathbf{F}_{p^2}$ et $E(\sqrt{m})/(p)$, où m est un non résidu quadratique modulo p et $E(\sqrt{m})$ l'anneau des entiers quadratiques de $\mathbb{Q}(\sqrt{m})$.

Nous allons de même montrer que, si $p \equiv 1 \pmod 3$ et m non cube dans $\mathbf{F}_p$ alors, on peut expliciter un $\mathbb{F}_p$-isomorphisme entre $\mathbf{F}_{p^3}$ et $E(\sqrt[3]{m})/(p)$, qui nous permettra de travailler dans $E(\sqrt[3]{m})$ lorsque celui-ci est factoriel.

Notations

- p est un nombre premier ≥ 5;
- k est un polynôme irréductible dans $\mathbb{F}_p[X]$, de degré 3;
- $\mathbb{F}_{p^3}$ est le corps $\mathbb{F}_p[X]/(k)$;
- g est un générateur de $\mathbf{F}_{p^3}^*$;
- m est un entier non cube dans $\mathbb{F}_p$;
- $E(\sqrt[3]{m})$ est l'anneau des entiers de $Q(\sqrt[3]{m})$;
- (p) est l'idéal principal $pE(\sqrt[3]{m})$ dans $E(\sqrt[3]{m})$.

2. Structure de l'ensemble $E(\sqrt[3]{m})$

Dans cette partie, on donnera les différentes formes pouvant être prises par les entiers de $\mathbb{Q}(\sqrt[3]{m})$ et de l'ensemble $E(\sqrt[3]{m})/(p)$ des classes de $E(\sqrt[3]{m})$ modulo l'idéal $(p) = pE(\sqrt[3]{m})$ dans $E(\sqrt[3]{m})$, m étant un entier non cube dans $\mathbf{F}_p$. Nous établirons aussi un isomorphisme grâce auquel on pourra passer d'un corps de polynômes $\mathbf{F}_p[X]/(X^3 - m)$ au corps $E(\sqrt[3]{m})/(p)$.

Rappelons qu'une base de $E(\sqrt[3]{m})$ sur $\mathbb{Z}$ est (*cf.* [2] :

- si m sans facteur carré :

  i) si $m \not\equiv \pm 1 \pmod 9$,

$$\{1,\ \sqrt[3]{m},\ \sqrt[3]{m^2}\}$$

  ii) si $m \equiv \pm 1 \pmod 9$,

$$\left\{1,\ \sqrt[3]{m},\ \frac{\sqrt[3]{m^2} \pm \sqrt[3]{m} + 1}{3}\right\}$$

- si $m = hk^2$ avec $(h,k) = 1$, h et k sans facteur carré, $k \leq h$:

  iii) si $m \not\equiv \pm 1 \pmod 9$,

$$\left\{1,\ \sqrt[3]{m},\ \frac{\sqrt[3]{m^2}}{k}\right\}$$

  iv) si $m \equiv \pm 1 \pmod 9$,

$$\left\{1,\ \sqrt[3]{m},\ \frac{\sqrt[3]{m^2} \pm k^2\sqrt[3]{m} + k^2}{3k}\right\}.$$

Ainsi on a le résultat suivant.

LEMME 1. — *Soit m un entier non cube dans $\mathbb{F}_p$. Alors $E(\sqrt[3]{m})/(p) \cong \mathbb{Z}[\sqrt[3]{m}]/(p)$.*

En effet, dans le cas i), on a $E(\sqrt[3]{m}) = \mathbb{Z}[\sqrt[3]{m}]$, et dans les autres cas $\mathbb{Z}[\sqrt[3]{m}] \subset E(\sqrt[3]{m})$. On montre que $(E\sqrt[3]{m})/(p) \cong \mathbb{Z}[\sqrt[3]{m}]/(p)$ en prouvant que : pour tout $\alpha \in E(\sqrt[3]{m})$, il existe $\beta \in \mathbb{Z}[\sqrt[3]{m}]$ tel que $\alpha - \beta \in pE(\sqrt[3]{m})$.

Si nous nous plaçons dans le cas iii) par exemple, et prenons $\alpha \in E(\sqrt[3]{m})$, quelconque, α s'écrit

$$\alpha = a + b\sqrt[3]{m} + \frac{c}{k}\sqrt[3]{m^2}.$$

Si

$$c \equiv i \pmod k \tag{1}$$

et

$$p \equiv j \pmod{k}, \tag{2}$$

on a

$$(j,k) = 1 \quad \text{et} \quad c - ij^{-1}p \equiv 0 \pmod{k}, \tag{3}$$

où j^{-1} est l'inverse de j dans $\mathbb{F}_p$. Alors

$$\beta = a + b\sqrt[3]{m} + (c - ij^{-1}p)\frac{\sqrt[3]{m^2}}{k} \in \mathbb{Z}[\sqrt[3]{m}] \quad \text{et} \quad \alpha - \beta \in pE(\sqrt[3]{m}).$$

D'où le résultat. Avec les cas ii) et iv), on a

$$\alpha = a + b\sqrt[3]{m} + c\frac{\sqrt[3]{m^2} \pm k^2\sqrt[3]{m} + k^2}{3k}$$

avec $k = 1$ dans ii), $k \geq 2$ sinon. En remplaçant k par $3k$ dans (1), (2) et (3), on a le même résultat.

Nous avons ainsi montré que les éléments de $E(\sqrt[3]{m})/(p)$ sont de la forme $a + b\sqrt[3]{m} + c\sqrt[3]{m^2}$ avec $a, b, c \in \mathbb{F}_p$.

Un pas essentiel de la transformation du problème consiste au passage d'un corps de polynômes à p^3 éléments au corps $E(\sqrt[3]{m})/(p)$. Nous avons le théorème immédiat suivant.

THÉORÈME 1. — *Soient p un nombre premier, $m \in \mathbb{N}$ un entier non cube dans $\mathbb{F}_p$, $E(\sqrt[3]{m})$ l'ensemble des entiers de $\mathbb{Q}(\sqrt[3]{m})$. Alors l'application :*

$$\begin{aligned} \chi : \frac{\mathbb{F}_p[X]}{(X^3 - m)} &\to \frac{E(\sqrt[3]{m})}{(p)} \\ a\overline{X}^2 + b\overline{X} + c &\mapsto a\sqrt[3]{m^2} + b\sqrt[3]{m} + c \pmod{p} \end{aligned}$$

est un isomorphisme de $\mathbb{F}_p$-algèbres.

3. Étude de quelques isomorphismes

Soit $\ell := aX^3 + bX^2 + cX + d \in \mathbb{F}_p[X]$ avec $a \neq 0$. Le but de cette partie est d'expliciter un isomorphisme entre $\mathbb{F}_p[X]/(\ell)$ et $\mathbb{F}_p[X]/(X^3 - m)$, $m \in \mathbb{F}_p$ sous certaines hypothèses que l'on précisera.

Dans le paragraphe 3.1 de cette partie, on construira un polynôme unitaire k à partir du polynôme ℓ et on définira un isomorphisme entre $\mathbb{F}_p[X]/(\ell)$ et $\mathbf{F}_p[X]/(k)$. Dans le paragraphe 3.2, on cherchera à trouver un entier $m_1 \in \mathbb{F}_p$ tel que l'on puisse définir un isomorphisme entre $\mathbb{F}_p[X]/(k)$ et $\mathbf{F}_p[X]/(X^3 - m_1)$. Enfin, dans le paragraphe 3.3, on établira un isomorphisme entre $\mathbb{F}_p[X]/(X^3 - m_1)$ et $\mathbb{F}_p[X]/(X^3 - m)$.

D'abord un résultat qui nous aidera à prouver l'existence de quelques isomorphismes.

LEMME 2. — *Soit p un nombre premier, P un polynôme à coefficients dans $\mathbf{F}_p$. Soit*

$$\begin{aligned} t : \mathbf{F}_p[X] &\to \frac{\mathbb{F}_p[X]}{(P)} \\ \sum a_i X^i &\mapsto \sum a_i \big(h(X)\big)^i \pmod P \end{aligned}$$

où h est un polynôme de $\mathbb{F}_p[X]$. Alors :

- *t est un morphisme de $\mathbf{F}_p$-algèbre si :*
$$h(X^i X^J) = h(X^i)h(X^j), \quad \text{pour tous } i \text{ et } j.$$
- *si ℓ est un polynôme de $\mathbf{F}_p[X]$ tel que $P \mid \ell \circ h$, alors il existe une application $\overline{t} : \mathbf{F}_p[X]/(\ell) \to \mathbb{F}_p[X]/(P)$ telle que $\overline{t} \circ s = t$, où s est la surjection canonique de $\mathbb{F}_p[X]$ dans $\mathbb{F}_p[X]/(\ell)$;*
- *$\overline{t}$ est un isomorphisme si :*
$$\text{pour tout polynôme } Q \in \mathbb{F}_p[X], \quad P \mid Q \circ h \Rightarrow \ell \mid Q.$$

Dans la suite, les isomorphismes seront définis à partir d'une fonction h.

3.1 Isomorphisme explicite entre $\mathbb{F}_p[X]/(\ell)$ et $\mathbb{F}_p[X]/(k)$

THÉORÈME 2. — *Soient p un nombre ≥ 5, $\ell := aX^3 + bX^2 + cX + d$ un polynôme de degré 3, à coefficients dans $\mathbf{F}_p$. Soient $t \in \mathbb{F}_p$ le polynôme défini par $k(X) := a^{-1}\ell(X + t)$, où a^{-1} est l'inverse de a dans $\mathbb{F}_p$. Alors l'application*

$$\begin{aligned} \psi : \frac{\mathbf{F}_p[X]}{(\ell)} &\to \frac{\mathbb{F}_p[X]}{(k)} \\ \alpha\overline{X}^2 + \beta\overline{X} + \gamma \pmod \ell &\mapsto \alpha\big(\overline{\overline{X}} + t\big)^2 + \beta\big(\overline{\overline{X}} + t\big) + \gamma \pmod k \end{aligned}$$

est un isomorphisme de $\mathbf{F}_p$-algèbres.

On prouve ce résultat en appliquant le lemme 2 avec $h(X) = X + t$.

COROLLAIRE .— *Avec les mêmes hypothèses en choisissant* $t = -b/3a$, *on a* $k(X) = X^3 + b'X + c'$ *avec*

$$b' = \frac{1}{a}\left\{\frac{-b^2}{3a} + c\right\}, \quad c' = \frac{1}{a}\left\{\frac{2}{27}\frac{b^3}{a^2} - \frac{1}{3}\frac{cb}{a} + d\right\}.$$

C'est un tel polynôme k qui sera utilisé dans l'algorithme qui fait l'objet de cette étude.

3.2 Isomorphisme entre $\mathbf{F}_p[X]/(k)$ et $\mathbf{F}_p[X]/(X^3 - m_1)$

On va définir ici un isomorphisme dans le cas général. Mais, avec les hypothèses d'application de l'algorithme (section 1), cet isomorphisme ne sera utilisé que dans un cas particulier.

THÉORÈME 3.— *Soient* p *un nombre premier* ≥ 5, $k(X) = X^3 + bX + c \in \mathbf{F}_p[X]$. *Alors, il existe* $m_1 \in \mathbf{F}_p$ *tel que*

$$\mathbf{F}_p[X]/(k) \cong \mathbf{F}_p[X]/(X^3 - m_1)$$

si l'une ou l'autre des conditions suivantes est vérifiée :

a) $p \equiv 1 \pmod 3$ *et (k irréductible ou k a trois facteurs irréductibles de degré* 1*).*

b) $p \equiv 2 \pmod 3$ *et k a deux facteurs irréductibles.*

Preuve.— On se situe dans le seul cas qui nous intéresse, c'est-à-dire $p \equiv 1 \pmod 3$ et k irréductible dans $\mathbf{F}_p$.

Soient α, β, γ les racines de k. Alors $\{\alpha, \beta, \gamma\} = \{\alpha, \alpha^p, \alpha^{p^2}\}$ (*cf.* [5]). Dans toute la suite, on notera j une racine cubique de l'unité dans $\mathbf{F}_p$. Posons

$$u := \alpha + \beta j + \gamma j^2$$
$$v := \alpha + \beta j^2 + \gamma j\,.$$

Les racines α, β et γ sont caractérisées par :

$$\begin{cases} \alpha + \beta + \gamma = 0 \\ \alpha\beta + \alpha\gamma + \beta\gamma = b \\ \alpha\beta\gamma = -c\,. \end{cases}$$

Utilisant ces trois relations, on a

$$uv = -3b$$

et

$$\begin{aligned} u^3 + v^3 &= (u+v)^3 - 3uv(u+v) \\ &= (3\alpha)^3 + 9b(3\alpha) \\ &= 27(\alpha^3 + \alpha b) \\ &= -27\,c\,. \end{aligned}$$

Donc u^3 et v^3 sont racines de l'équation

$$X^2 + (27\,c)X - 27\,b^3 = 0\,. \qquad \text{(E)}$$

Le discriminant D de (E) est $D = -27(-4b^3 - 27\,c^2) = -27\,\Delta$, où $\Delta := -4b^3 - 27\,c^2$ est le discriminant de k. Montrons que D est un carré dans $\mathbb{F}_p$.

1) -27 est un carré dans $\mathbf{F}_p$. En effet,

$$\left(\frac{-27}{p}\right) = \left(\frac{-3}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1\,.$$

2) Il reste à montrer que Δ est un carré dans $\mathbf{F}_p$:

$$\begin{aligned} \Delta &= \left[(\alpha-\beta)(\alpha-\gamma)(\beta-\gamma)\right]^2 \\ &= \left[(\alpha-\alpha^p)(\alpha-\alpha^{p^2})(\alpha^p-\alpha^{p^2})\right]^2 = \left[g(\alpha)\right]^2 \end{aligned}$$

avec

$$g(\alpha) = (\alpha-\alpha^p)(\alpha-\alpha^{p^2})(\alpha^p-\alpha^{p^2})\,.$$

On a

$$g(\alpha^p) = \big(g(\alpha)\big)^p = g(\alpha) \quad \text{et} \quad g(\alpha^{p^2}) = \big(g(\alpha)\big)^{p^2} = g(\alpha)\,.$$

Donc

$$\text{trace}\,\big(g(\alpha)\big) = g(\alpha) = \big(g(\alpha)\big)^p = \big(g(\alpha)\big)^{p^2} = 3g(\alpha) \in \mathbb{F}_p\,,$$

car si $g(\alpha)$, $\big(g(\alpha)\big)^p$ et $\big(g(\alpha)\big)^{p^2}$ sont racines de $x^3 + a_2x^2 + a_1x + a_0$, alors

$$g(\alpha) + \big(g(\alpha)\big)^p + \big(g(\alpha)\big)^{p^2} = -a_2 \in \mathbb{F}_p\,.$$

Donc $\Delta = \big(g(\alpha)\big)^2$ est un carré dans $\mathbf{F}_p$.

Par suite, $D = -27\,\Delta$ est un carré dans $\mathbf{F}_p$. Soit alors δ une racine de l'équation $x^2 \equiv D \pmod{p}$. On a

$$\{u^3, v^3\} = \left\{ \frac{-27\,c + \delta}{2}\,,\ \frac{-27\,c - \delta}{2} \right\}.$$

Posons

$$m_1 := \frac{-27\,c + \delta}{2}\,.$$

m_1 n'est pas un cube dans $\mathbb{F}_p$ car, sinon on aurait $m_1 = \omega^3$ avec $\omega \in \mathbb{F}_p$ et $(1/3)\,(\omega - 3b/\omega)$ serait une racine de $k(X)$ dans $\mathbb{F}_p$, en effet :

$$\begin{aligned}
&\left[\frac{1}{3}\left(\omega - \frac{3b}{\omega}\right)\right]^3 + \frac{b}{3}\left(\omega - \frac{3b}{\omega}\right) + c = \\
&\qquad = \frac{1}{27}\left(\omega^3 - 27\,\frac{b^3}{\omega^3} + 27\,c\right) \\
&\qquad = \frac{1}{27}\left(-\frac{27\,c + \delta}{2} - 54\,\frac{b^3}{-27\,c + \delta} + 27\,c\right) \\
&\qquad = \frac{\delta^2 - 27\,(4b^3 + 27\,c^2)}{54\,(-27\,c + \delta)} = 0\,.
\end{aligned}$$

Donc $X^3 - m_1$ est irréductible dans $\mathbf{F}_p$ et $\mathbf{F}_p[X]/(X^3 - m_1)$ et $\mathbf{F}_p[X]/(k)$ sont deux corps isomorphes.

Isomorphisme explicite

Définissons une application

$$\begin{aligned}
\phi : \frac{\mathbf{F}_p[X]}{(k)} &\longrightarrow \frac{\mathbb{F}_p[X]}{(X^3 - m_1)} \\
\alpha\overline{X}^2 + \beta\overline{X} + \gamma &\longmapsto \alpha h\big(\overline{\overline{X}}\big)^2 + \beta h\big(\overline{\overline{X}}\big) + \gamma
\end{aligned}$$

où

$$h\big(\overline{\overline{X}}\big) = \frac{1}{3}\left(\overline{\overline{X}} - \frac{3b}{m_1}\,\overline{\overline{X}}^2\right).$$

On montre, par le lemme 2, que ϕ est un isomorphisme.

3.3 Isomorphisme explicite entre $\mathbb{F}_p[X]/(X^3 - m')$ et $\mathbb{F}_p[X]/(X^3 - m)$

D'abord nous donnons un lemme.

LEMME 3. — *Soit $p \equiv 1 \pmod 3$, un nombre premier. Soit j une racine cubique de l'unité dans $\mathbb{F}_p$, $j \neq 1$. Alors tout élément non nul de $\mathbb{F}_p$ s'écrit sous la forme $j^i r^3$ avec $r \in \mathbb{F}_p^*$ et $i \in \{0, 1, 2\}$.*

En effet, la relation $\mathfrak{R}$ définie par $x \mathfrak{R} y \Leftrightarrow xy^{-1} = r^3$ dans $\mathbb{F}_p^*$ est une relation d'équivalence dont les classes sont r^3, jr^3, j^2r^3. D'où

$$\mathbb{F}_p = \{r^3 \mid r \in \mathbb{F}_p\} \cup \{jr^3 \mid r \in \mathbb{F}_p\} \cup \{j^2r^3 \mid r \in \mathbb{F}_p\}.$$

THÉORÈME 4. — *Soient m et m' deux éléments de $\mathbb{F}_p^*$, m et m' à la fois cubes ou non cubes dans $\mathbb{F}_p$. Alors :*

$$\frac{\mathbb{F}_p[X]}{(X^3 - m')} \cong \frac{\mathbb{F}_p[X]}{(X^3 - m)}.$$

Preuve. — On se situe dans le seul cas où m et m' ne sont pas cubes dans $\mathbb{F}_p$.

Alors $p \equiv 1 \pmod 3$ et les deux polynômes $X^3 - m$ et $X^3 - m'$ sont irréductibles dans $\mathbb{F}_p$, donc

$$\frac{\mathbb{F}_p[X]}{(X^3 - m')} \cong \frac{\mathbb{F}_p[X]}{(X^3 - m)}$$

Par le lemme 3 ci-dessus, on a :

- soit $mm' = r^3$ avec $r \in \mathbb{F}_p$, auquel cas on définit un isomorphisme δ par

$$\delta : \frac{\mathbb{F}_p[X]}{(X^3 - m')} \cong \frac{\mathbb{F}_p[X]}{(X^3 - m)}$$

$$a\overline{X}^2 + b\overline{X} + c \quad \mapsto \quad a\left(\frac{r}{m}\overline{\overline{X}}^2\right)^2 + b\left(\frac{r}{m}\right)\overline{\overline{X}}^2 + c$$

- soit $m'/m = r^3$, auquel cas :

$$\delta : a\overline{X}^2 + b\overline{X} + c \quad \mapsto \quad a\left(r\overline{\overline{X}}\right)^2 + b\left(r\,\overline{\overline{X}}\right) + c.$$

En appliquant le lemme 2, avec $h(\overline{\overline{X}}) = (r/m)\overline{\overline{X}}^2$ ou $r\overline{\overline{X}}$ selon les cas, on montre que δ est bien un isomorphisme.

3.4 Isomorphisme entre $\mathbf{F}_p[X]/(\ell)$ et $E(\sqrt[3]{m})/(p)$

Les résultats des paragraphes précédents nous permettent d'établir le théorème suivant.

THÉORÈME 5.— *Soit p un nombre premier, $p \equiv 1 \pmod 3$. Soient $\ell := aX^3 + bX^2 + cX + d \in \mathbb{F}_p[X]$, un polynôme irréductible dans $\mathbf{F}_p$, de degré 3, $\mathbf{F}_{p^3}$ le corps $\mathbf{F}_p[X]/(\ell)$, et m un entier non cube dans $\mathbb{F}_p^*$. Posons :*

$$b' := \frac{1}{a}\left(-\frac{b^2}{3a} + c\right), \quad c' := \frac{1}{a}\left(\frac{2}{27}\frac{b^3}{a^2} - \frac{1}{3}\frac{cd}{a} + d\right),$$
$$\theta := \sqrt[3]{m} \in \mathbb{C} \quad \text{et} \quad D := -27(-4b'^3 - 27c'^2).$$

Alors D est un carré (mod p) *et, en posant $m_1 := (-27c' + \delta)/2$, avec δ une racine carrée* (mod p) *de D, on peut définir un isomorphisme f entre $\mathbf{F}_p^3$ et $E(\theta)/(p)$ par*

$$\alpha\overline{X}^2 + \beta\overline{X} + \gamma \quad \mapsto \quad \alpha\big(h(\theta)\big)^2 + \beta h(\theta) + \gamma,$$

où $\varepsilon \in \{-1, 1\}$ est tel que $m_1 m^\varepsilon$ soit un cube dans $\mathbf{F}_p$ et

$$h(\theta) = \left(\frac{1}{3}\left(r\theta^{-\varepsilon} - \frac{3b'}{r}\theta^\varepsilon\right) - \frac{b}{3a}\right)$$

avec r une solution de $x^3 \equiv m_1 m^\varepsilon \pmod p$.

En effet, on a vu, au paragraphe 3.1, qu'on peut construire un polynôme $k = X^3 + b'X = c'$ à partir du polynôme ℓ, avec b' et c' définis comme dans le théorème, et que k est irréductible sur $\mathbf{F}_p$ si ℓ l'est. Soit $\Delta = -4b'^3 - 27c'^2$, le discriminant de k. Comme au paragraphe 3.2, on montre que $D = -27\,\Delta$ est un carré (modulo p). En composant les différents isomorphismes établis aux paragraphes 3.1, 3.2 et 3.3, on obtient l'isomorphisme f. Doù le théorème.

Exemple.— Soit le polynôme ℓ défini par $\ell(X) = 2X^3 + X^2 + X + 1 \in \mathbb{F}_7[X]$. Alors ℓ est irréductible sur $\mathbb{F}_7$ et k est le polynôme défini par

$$k(X) = 2^{-1}\ell(X + 1) = X^3 + X + 6.$$

On vérifie que $m = 2$ est non cube dans $\mathbb{F}_7$. Par la démarche indiquée au paragraphe 3.2, on trouve $m_1 = 4$. L'isomorphisme f cherché est défini par :

$$f : \frac{\mathbb{F}_7[X]}{(\ell)} \quad \to \quad \frac{E(\sqrt[3]{2})}{(7)}$$

$$a\overline{X}^2 + b\overline{X} + c \pmod{\ell} \quad \mapsto \quad ah\left(\overline{\overline{X}}\right)^2 + bh\left(\overline{\overline{X}}\right) + c \pmod 7$$

où

$$h : \overline{\overline{X}} \quad \mapsto \quad 1 + 5\sqrt[3]{2} + 3\sqrt[3]{2^2}\,.$$

4. Travail dans $E(\sqrt[3]{m})$

Pour une table de petites valeurs de m telles $E(\sqrt{m})$ soit factoriel, on peut consulter ([7], [8]). On cherche à trouver un entier m non cube dans $\mathbb{F}_p$, pour lequel $E(\sqrt[3]{m})$ est factoriel. On conjecture qu'il existe une infinité d'entiers m tels que $E(\sqrt[3]{m})$ soit factoriel. Disposant d'une liste assez grande de tels entiers (2, 3, 5, 6, 10, 12, ...), on teste successivement, à partir de 2, si un entier de cette liste est non cube modulo p. On s'arrête dès que la condition est satisfaite. Si la condition n'est pas satisfaite après parcours de toute la liste, on se contentera du plus petit entier m non cube modulo p rencontré.

Situons-nous dans le cas où on a trouvé un entier m pour lequel l'anneau $E(\sqrt[3]{m})$ est factoriel. On transpose ensuite l'algorithme d'Adleman dans $E(\sqrt[3]{m})/(p)$. Grâce à l'isomorphisme établi au paragraphe 3, on peut effectuer le transfert du problème de $\mathbb{F}_p^3$ à $E(\sqrt[3]{m})/(p)$. En effet, si $\overline{h}$ et $\overline{w}$ sont les images respectives de g et y par l'isomorphisme f, le problème consistera à trouver $x \in [\,0\,,\, p^3-2\,]$ tel que l'on ait $\overline{h}^x = \overline{w}$ dans $E(\sqrt[3]{m})/(p)$. On notera h et w des représentants respectifs de $\overline{h}$ et $\overline{w}$ dans $\mathbb{Z}[\sqrt[3]{m}\,]$.

On se fixe un entier N ; l'étude de l'estimation du coût de l'algorithme montrera que

$$N = \mathrm{O}\left(\exp\sqrt{\frac{3}{2}\log p \log\log p}\right)$$

minimise ce coût.

L'implémentation de cet algorithme nécessite d'abord la fixation d'un ensemble B dont les éléments sont les irréductibles non associés de norme inférieure à N, et l'unité fondamentale de $E(\sqrt[3]{m})$.

Pour construire B, on procède de la manière suivante :

- on sélectionne les entiers irréductibles α dont la valeur absolue de la norme est première et inférieure à la borne N ; soient α_1, α_2 les deux conjugués de α ; alors $\alpha_1, \alpha_2 \notin \mathbb{Q}(\sqrt[3]{m})$ tandis que $\beta = \alpha_1\alpha_2 \notin E(\sqrt[3]{m})$; si β est irréductible dans $E(\sqrt[3]{m})$ et $\mathcal{N}(\beta) \leq N$, on sélectionne également β ;
- on ajoute à la liste obtenue tous les nombres premiers de $\mathbb{Z}$, irréductibles dans $E(\sqrt[3]{m})$ et dont la norme est $\leq N$;
- on ajoute ensuite à cette liste l'unité fondamentale de $E(\sqrt[3]{m})$;
- on trie la liste ainsi constituée dans l'ordre croissant des normes.
- on élimine tous les associés de chaque élément (autres que l'élément lui-même).

Soit $z = a + b\sqrt[3]{m} + c\sqrt[3]{m^2} \in E(\sqrt[3]{m})$. La norme de z est le nombre $\mathcal{N}(z)$ défini par $\mathcal{N}(z) = a^3 + b^3m + c^3m^2 - 3mabc$ qui est dans $\mathbb{Z}$. Les conjugués complexes de z sont $z_1 = a + bj\sqrt[3]{m} + cj^2\sqrt[3]{m^2}$ et $z_2 = a + bj^2\sqrt[3]{m} + cj\sqrt[3]{m^2}$, où j est une racine cubique de l'unité dans $\mathbb{Q}(\sqrt[3]{m^2})$, et le produit

$$z_1 \cdot z_2 = (a^2 - bcm) + (c^2m - ab)\sqrt[3]{m} + (b^2 - ac)\sqrt[3]{m^2}$$

est un élément de $E(\sqrt[3]{m})$. On a, pour tout $b_i \in B$,

$$\mathcal{N}(b_i) = \begin{cases} 1 & \text{si } i = 1,\ b_1 \text{ est l'unité fondamentale,} \\ p_i & \text{si } b_i \in B_1 \text{ avec } p_i \text{ premier dans } \mathbb{Z}, \\ p_i^2 & \text{si } b_i \in B_2, \\ p_i^3 & \text{si } b_i \in B_3, \end{cases}$$

où

- B_1 est l'ensemble des irréductibles de $E(\sqrt[3]{m})$, de norme première,
- B_2 l'ensemble des produits $\alpha_1\alpha_2$ de conjugués de α, irréductibles dans $E(\sqrt[3]{m})$,
- B_3 l'ensemble des nombres premiers de $\mathbb{Z}$ qui sont irréductibles dans $E(\sqrt[3]{m})$.

On appelle B-lisse un entier dont la décomposition en facteurs irréductibles ne fait intervenir que des éléments de B.

L'ensemble B étant fixé, on cherchera dans la deuxième partie de l'algorithme à trouver les indices de ses éléments relativement à h, c'est-à-dire les entiers x_i tels que $h^{x_i} = b_i \pmod p$. Ce calcul, qui domine le temps d'exécution de l'algorithme, repose essentiellement sur la décomposition de l'élément z, représentant de $\overline{z} = \overline{h}^u$, dans $\mathbb{Z}[\sqrt[3]{m}]$. Si z est B-lisse, on obtient une équation linéaire dont les inconnues sont les $x_i = \mathrm{ind}_h(b_i)$, puisque $h^u = \prod_{i=1}^n b_i^{r_i} \pmod p$ équivaut à $\sum_{i=1}^n r_i x_i = u \pmod{p^3-1}$. Avec "assez" d'équations, on détermine les x_i.

On sait que $\mathcal{N}(\alpha) \in \mathbb{Z}$ si $\alpha \in E(\sqrt[3]{m})$ et que si $\beta \mid \alpha$ dans $E(\sqrt[3]{m})$ alors $\mathcal{N}(\beta) \mid \mathcal{N}(\alpha)$, dans $\mathbb{Z}$. Pour tenter d'obtenir la décomposition de z en facteurs irréductibles de B, on procède par divisions successives de z par les b_i. Mais, avant d'effectuer la division de z par les b_i pour trouver ses facteurs, on peut faire un test permettant de savoir si z a des chances d'être B-lisse ou non. En effet, si N_B est l'ensemble des normes des b_i, on a, soit $\mathcal{N}(z)$ est N_B-lisse, auquel cas on effectue la division par les b_i et on teste si le résultat est dans $E(\sqrt[3]{m})$, soit $\mathcal{N}(z)$ n'est pas N_B-lisse, auquel cas z n'est pas B-lisse. Le test de divisibilité est effectué de b_n à b_1.

L'algorithme suivant permet d'effectuer ces opérations dans $E(\sqrt[3]{m})$.

Algorithme

entrée : z à décomposer en facteurs irréductibles.

sortie : $v = (v_{ij})$ si z est B-lisse, Faux sinon.

Début
  $q := z$;
  Si $\mathcal{N}(q)$ est N_B-lisse alors
    pour i de n à 1 et $(q \neq 1)$ faire
    début
      $j := i$; $v_{ij} := 0$;
      tant que $(q/b_i \in E(\sqrt[3]{m})$ faire
      début
        $q := q/b_i$;
        $v_{ij} := v_{ij} + 1$
      fin;
      si $(q = 1)$ alors Retourner $(v = (v_{ij}))$
    fin;
    si $(q \neq 1)$ alors Retourner (Faux);
  Sinon retourner (Faux)
Fin.

Remarques

1) Puisqu'on conjecture qu'il existe une infinité d'entiers m pour lesquels $E(\sqrt[3]{m})$ est factoriel, on devrait pouvoir en trouver suffisamment qui sont inférieurs à p pour p "grand" et, parmi ceux-ci, un entier m non cube (modulo p) tel que $E(\sqrt[3]{m})$ soit factoriel. Toutefois, nous allons donner une version nous permettant de travailler dans un anneau non-factoriel. Pour qu'un élément B-lisse α se décompose de façon *unique* en produits d'éléments de B, nous modifions la construction de B. Dans le sous-ensemble B_1 de B, considérons la relation d'équivalence R définie par $\alpha R\beta \Leftrightarrow \mathcal{N}(\alpha) = \mathcal{N}(\beta)$. Pour chaque classe $\widehat{\alpha}$ de R, on choisit au plus deux représentants. On supprime B_2 et on garde B_3.

Cette différence réduit sensiblement le nombre de candidats potentiels de l'ensemble B, et par conséquent, les chances de parvenir à une décomposition d'un élément z en facteurs irréductibles de B.

2) Nous avons vu dans la section 2 que $\mathbb{Z}[\sqrt[3]{m}] \subset E(\sqrt[3]{m})$. On serait ainsi tenté de se limiter aux seuls irréductibles de l'anneau $\mathbb{Z}[\sqrt[3]{m}]$, mais, dans ce cas,

- d'une part, on exclurait de B un certain nombre de candidats; par exemple, pour $m = 17 \equiv -1 \pmod 9$:

$$E(\sqrt[3]{m}) = \left\{ \frac{a + b\sqrt[3]{m} + c\sqrt[3]{m^2}}{3} \;\middle|\; a, b, c \in \mathbb{Z} \;\; a \equiv c \equiv -b \pmod 3 \right\} ;$$

on exclurait ainsi de B les éléments

$$\frac{4 + 2\sqrt[3]{17} + \sqrt[3]{17^2}}{3}, \frac{2 + \sqrt[3]{17} + 2\sqrt[3]{17^2}}{3}, \frac{7 + 2\sqrt[3]{17} + \sqrt[3]{17^2}}{3},$$
$$\frac{8 + 7\sqrt[3]{17} + 2\sqrt[3]{17^2}}{3}, \ldots$$

- d'autre part, l'anneau $\mathbb{Z}[\sqrt[3]{m}]$ pourrait être non factoriel, alors que $E(\sqrt[3]{m})$ serait factoriel.

5. Présentation de l'algorithme

On divisera l'algorithme en trois parties :

Première partie. — Détermination de m et B

1) Trouver un entier m non cube dans $\mathbf{F}_p$ "convenable".

2) Fixer l'ensemble $B = \{b_1, b_2, \ldots, b_n\}$ d'entiers cubiques irréductibles selon les critères définis au paragraphe précédent.

Deuxième partie. — Calcul des indices des irréductibles b_i

1) Choisir au hasard des nombres $0 \leq u_i \leq p^3 - 2$, de sorte que $z_i = h^{u_i} \pmod p$ soit B-lisse; on obtient un vecteur v_i dont les composantes sont les puissances des facteurs b_i de z_i. On s'arrête lorsqu'on a trouvé n vecteurs v_i indépendants.

2) Résoudre le système de $AX = b$ modulo $(p^3 - 1)$, où :

   a) A est une matrice carrée d'ordre n, dont les lignes sont les vecteurs v_i, précédemment calculés.

   b) b les vecteurs dont les composantes sont les entiers u_i choisis à l'étape 1.

   Soit $(x_1, x_2, \ldots, x_n)$ la solution du système. Les x_i sont les indices relatifs à h des éléments b_i de B.

Troisième partie. — Résolution de l'équation

1) Choisir au hasard un nombre $0 \leq s \leq p^3 - 2$ tel que wh^s soit B-lisse.

2) $wh^s = \prod_{i=1}^{n} b_i^{\alpha_i}$ et le logarithme cherché est

$$x = \sum_{i=1}^{n} \alpha_i x_i - s \pmod{p^3 - 1}.$$

Remarque. — Les deux premières parties de l'algorithme n'ont pas a être réexécutées tant qu'on travaille dans le même corps $\mathbf{F}_{p^3}$, avec le même générateur g. D'où un gain de temps assez considérable pour calculer le logarithme d'un nouvel y dans $\mathbf{F}_{p^3}$.

6. Exemples de résolution

Les exemples suivants ont été obtenus sur un PC 286, en Turbo Pascal 5.5.

I. Exemple 1

Base : $p = 823$

Polynôme irréductible (modulo 823) : $k = X^3 + X + 7$

Générateur de $\mathbb{F}^*_{823^3}$: $g = X^3 + 2$

$y = X^2$

1.— Isomorphisme trouvé :

$$f : \overline{X} \mapsto 517\sqrt[3]{2} + 13\sqrt[3]{2^2}$$

Générateur $h = f(\overline{X} + 2)$ de $\left(E(\sqrt[3]{2})/(823)\right)^*$:

$$h = 2 + 517\sqrt[3]{2} + 13\sqrt[3]{2^2}$$

Le représentant choisi de $\overline{w} = f(y)$ est $w = 548 + 338\sqrt[3]{2} + 637\sqrt[3]{2^2}$. On fixe le nombre d'éléments irréductibles de B à 16 :

$1 + \sqrt[3]{2} + \sqrt[3]{2^2}$;	$\sqrt[3]{2}$;	$1 + \sqrt[3]{2}$;	$1 + \sqrt[3]{2^2}$;
$1 - \sqrt[3]{2} + \sqrt[3]{2^2}$;	$3 + 2\sqrt[3]{2} + \sqrt[3]{2^2}$;	$5 + 3\sqrt[3]{2} + 3\sqrt[3]{2^2}$;	$1 + \sqrt[3]{2} + 2\sqrt[3]{2^2}$;
$1 + 2\sqrt[3]{2} - \sqrt[3]{2^2}$;	$5 + 4\sqrt[3]{2} + 4\sqrt[3]{2^2}$;	$5 + 3\sqrt[3]{2} + 2\sqrt[3]{2^2}$;	$1 + 3\sqrt[3]{2} + \sqrt[3]{2^2}$;
$3 + 4\sqrt[3]{2} - \sqrt[3]{2^2}$;	$3 + 2\sqrt[3]{2}$;	$5 + 2\sqrt[3]{2} + 2\sqrt[3]{2^2}$;	$3 + 2\sqrt[3]{2^2}$;

2.— Choix des u_i :

$u_1 = 83$,	$u_9 = 37847$,
$u_2 = 12413$,	$u_{10} = 197779$,
$u_3 = 17201$,	$u_{11} = 202347$,
$u_4 = 18689$,	$u_{12} = 231676$,
$u_5 = 19633$,	$u_{13} = 321486$,
$u_6 = 27885$,	$u_{14} = 323574$,
$u_7 = 29781$,	$u_{15} = 343525$,
$u_8 = 34127$,	$u_{16} = 370107$,

$$z_1 = 68 + 76\sqrt[3]{2} + 56\sqrt[3]{2^2}, \qquad z_9 = 669 + 543\sqrt[3]{2} + 423\sqrt[3]{2^2},$$
$$z_2 = 528 + 576\sqrt[3]{2} + 342\sqrt[3]{2^2}, \qquad z_{10} = 248 + 200\sqrt[3]{2} + 168\sqrt[3]{2^2},$$
$$z_3 = 770 + 598\sqrt[3]{2} + 479\sqrt[3]{2^2}, \qquad z_{11} = 2 + 184\sqrt[3]{2} + 278\sqrt[3]{2^2},$$
$$z_4 = 56 + 48\sqrt[3]{2} + 34\sqrt[3]{2^2}, \qquad z_{12} = 822 + 708\sqrt[3]{2} + 534\sqrt[3]{2^2},$$
$$z_5 = 814 + 641\sqrt[3]{2} + 517\sqrt[3]{2^2}, \qquad z_{13} = 746 + 597\sqrt[3]{2} + 485\sqrt[3]{2^2},$$
$$z_6 = 637 + 479\sqrt[3]{2} + 568\sqrt[3]{2^2}, \qquad z_{14} = 101 + 85\sqrt[3]{2} + 65\sqrt[3]{2^2},$$
$$z_7 = 378 + 351\sqrt[3]{2} + 324\sqrt[3]{2^2}, \qquad z_{15} = 8 + 136\sqrt[3]{2} + 32\sqrt[3]{2^2},$$
$$z_8 = 330 + 165\sqrt[3]{2} + 150\sqrt[3]{2^2}, \qquad z_{16} = 807 + 663\sqrt[3]{2} + 519\sqrt[3]{2^2},$$

$$v_1 = (0,6,0,2,1,1,0,0,0,0,0,0,0,0,0,0)$$
$$v_2 = (0,5,1,0,1,2,0,0,2,0,0,0,0,0,0,0)$$
$$v_3 = (0,2,0,2,1,0,1,0,0,0,1,0,0,0,0,0)$$
$$v_4 = (1,5,1,0,0,0,0,0,0,0,0,0,0,0,0,1)$$
$$v_5 = (2,1,0,1,1,0,0,0,0,0,0,0,0,0,0,2)$$
$$v_6 = (1,0,0,0,1,0,0,1,3,0,0,0,0,0,1,0)$$
$$v_7 = (1,1,1,0,4,1,0,0,0,0,0,0,0,1,0,0)$$
$$v_8 = (0,1,1,2,2,0,0,0,1,0,1,0,0,0,0,0)$$
$$v_9 = (2,0,0,1,2,0,0,1,0,0,0,0,0,1,0,0)$$
$$v_{10} = (0,9,1,1,0,0,0,0,0,1,0,0,0,0,0,0)$$
$$v_{11} = (0,3,0,0,1,0,0,0,2,0,0,1,0,0,1,0)$$
$$v_{12} = (0,3,1,0,2,2,0,0,0,0,0,1,0,0,0,0)$$
$$v_{13} = (0,1,0,0,0,0,0,3,0,0,0,0,1,0,0,0)$$
$$v_{14} = (1,0,0,0,1,0,0,1,0,0,0,0,0,1,0,0,0)$$
$$v_{15} = (0,9,0,0,1,0,0,0,1,0,0,0,1,0,0,0)$$
$$v_{16} = (1,0,1,0,1,0,0,1,0,0,0,1,0,0,0,1)$$

Indices des irréductibles b_i (ou solution de $AX = b \pmod{823^3 - 1}$)

$$x_1 = 431111052, \qquad x_5 = 414190184,$$
$$x_2 = 453910408, \qquad x_6 = 93492345,$$
$$x_3 = 143929735, \qquad x_7 = 269195765,$$
$$x_4 = 56752851, \qquad x_8 = 474415253,$$

$$x_9 = 165003180, \qquad x_{13} = 352932383,$$
$$x_{10} = 173855649, \qquad x_{14} = 8034335,$$
$$x_{11} = 525071798, \qquad x_{15} = 415068920,$$
$$x_{12} = 266414489, \qquad x_{16} = 500076458.$$

3. — Pour $s = 6511$, on a

$$wh^s \pmod{823} = 450 + 425\sqrt[3]{2} + 250\sqrt[3]{2^2} = b_2\, b_4^2\, b_6\, b_9^2\, b_{16}$$

Résultat :

$$x = 376101230 \pmod{823^3 - 1}.$$

Temps d'exécution : $8'\,29''\,24$.

II. Exemple 2

Les deux exemples suivants s'effectuent dans le corps $\mathbb{F}_{79^3}$. Pour le premier, on travaille dans l'anneau factoriel $E(\sqrt[3]{2})$, et pour le second, dans l'anneau $E(\sqrt[3]{7})$ non factoriel. On notera que le temps d'exécution du cas non factoriel est largement supérieur à celui obtenu avec le cas factoriel. De plus, dans le deuxième exemple, il a fallu prendre des éléments de normes très élevées par rapport à la borne N, pour trouver un nombre d'irréductibles voisin de celui du premier.

Cas factoriel

Base : $p = 79$

Polynôme irréductible (modulo p) : $k = X^3 + X + 6$

Générateur de $\mathbb{F}_{79^3}^*$: $g = X + 1$

$y = X^2 + X + 5$

1. — Isomorphisme trouvé :

$$f : \overline{X} \mapsto 73\sqrt[3]{2} + 11\sqrt[3]{2^2} \pmod{79}.$$

Générateur $h = f(\overline{X} + 1)$ de $\left(E\sqrt[3]{2}\right)/(79))^*$

$$h = 1 + 73\sqrt[3]{2} + 11\sqrt[3]{2^2}.$$

Le représentant choisi de $\overline{w} = f(y)$ est $w = 53 + 78\sqrt[3]{2} + 47\sqrt[3]{2^2}$. On fixe le nombre d'éléments irréductibles de B à 8 :

$$1 + \sqrt[3]{2} + \sqrt[3]{2^2}; \quad \sqrt[3]{2}; \quad 1 + \sqrt[3]{2};$$
$$1 + \sqrt[3]{2^2}; \quad 3 + 2\sqrt[3]{2} + \sqrt[3]{2^2}; \quad 5 + 3\sqrt[3]{2} + 3\sqrt[3]{2^2}.$$
$$1 + \sqrt[3]{2} + 2\sqrt[3]{2^2}; \quad 3 + \sqrt[3]{2};$$

2.— Choix des u_i :

$$u_1 = 930, \quad u_5 = 23679,$$
$$u_2 = 12069, \quad u_6 = 26310,$$
$$u_3 = 12758, \quad u_7 = 26436,$$
$$u_4 = 15262, \quad u_8 = 33840,$$

$$z_1 = 5 + 6\sqrt[3]{2} + 3\sqrt[3]{2^2}, \quad z_5 = 18 + 10\sqrt[3]{2} + 11\sqrt[3]{2^2},$$
$$z_2 = 12 + 12\sqrt[3]{2} + 12\sqrt[3]{2^2}, \quad z_6 = 36 + 36\sqrt[3]{2} + 26\sqrt[3]{2^2},$$
$$z_3 = 64 + 52\sqrt[3]{2} + 36\sqrt[3]{2^2}, \quad z_7 = 32 + 28\sqrt[3]{2} + 20\sqrt[3]{2^2},$$
$$z_4 = 12 + 11\sqrt[3]{2} + 8\sqrt[3]{2^2}, \quad z_8 = 58 + 48\sqrt[3]{2} + 39\sqrt[3]{2^2},$$

$$v_1 = (0,0,0,3,0,0,0,0), \quad v_5 = (0,2,0,0,1,0,0,1),$$
$$v_2 = (0,6,3,0,0,0,0,0), \quad v_6 = (0,5,0,0,1,0,1,0),$$
$$v_3 = (1,7,1,0,0,0,0,1), \quad v_7 = (1,7,2,0,0,0,0,0),$$
$$v_4 = (0,1,1,0,0,1,0,0), \quad v_8 = (1,2,0,0,0,0,2,0).$$

Indices des irréductibles b_i (ou solution de $AX = b \pmod{79^3 - 1}$) :

$$x_1 = 56316, \quad x_5 = 362026,$$
$$x_2 = 42140, \quad x_6 = 382071,$$
$$x_3 = 84039, \quad x_7 = 439660,$$
$$x_4 = 310, \quad x_8 = 70411.$$

3.— Pour $s = 475$, on a

$$wh^s \pmod{79} = 36 + 28\sqrt[3]{2} + 24\sqrt[3]{2^2} = b_1 b_2^6 b_5.$$

Résultat :

$$x = 177669 \pmod{79^3 - 1}.$$

Temps d'exécution : $8'\,0''\,70$.

Cas non factoriel

Base : $p = 79$

Polynôme irréductible (modulo p) : $k = X^3 = X + 6$

Générateur de $\mathbb{F}^*_{79^3}$: $g = X + 1$

$y = X^2 + 6$

1.— Isomorphisme trouvé :

$$f : \overline{X} \mapsto 3\sqrt[3]{7} + 5\sqrt[3]{7^2} \pmod{79}.$$

Générateur $h = f(\overline{X} + 1)$ de $\left(E(\sqrt[3]{7})/(79)\right)^*$:

$$h = 1 + 3\sqrt[3]{7} + 5\sqrt[3]{7^2}.$$

Le représentant choisi de $\overline{w} = f(y)$ est $w = 56 + 17\sqrt[3]{7} + 9\sqrt[3]{7^2}$. On fixe le nombre d'éléments irréductibles de B à 7 :

$$\begin{array}{llll} 2 - \sqrt[3]{3}\,; & \sqrt[3]{7}\,; & 2\,; & 3\,; \\ 2 + 2\sqrt[3]{7} + \sqrt[3]{7^2}\,; & 4 + \sqrt[3]{7}\,; & 3 + 2\sqrt[3]{7}\,. & \end{array}$$

2.— Choix des u_i :

$$\begin{array}{ll} u_1 = 2107\,, & u_5 = 21861\,, \\ u_2 = 7598\,, & u_6 = 22796\,, \\ u_3 = 10535\,, & u_7 = 56059\,, \\ u_4 = 20065\,, & \end{array}$$

$$\begin{array}{ll} z_1 = 64\sqrt[3]{7}\,, & z_5 = 28 + 14\sqrt[3]{7} + 4\sqrt[3]{7^2}\,, \\ z_2 = 72\sqrt[3]{7} + 48\sqrt[3]{7^2}\,, & z_6 = 21 + 12\sqrt[3]{7^2}\,, \\ z_3 = 48\sqrt[3]{7^2}\,, & z_7 = 21 + 14\sqrt[3]{7^2}\,, \\ z_4 = 28\sqrt[3]{7} + 78\sqrt[3]{7^2}\,, & \end{array}$$

$$v_1 = (0,1,6,0,0,0,0)\,, \qquad v_5 = (0,2,1,0,1,0,0)\,,$$
$$v_2 = (0,1,3,1,0,0,0)\,, \qquad v_6 = (0,2,0,1,0,1,0)\,,$$
$$v_3 = (0,2,4,1,0,0,0)\,, \qquad v_7 = (0,3,0,0,0,0,1)\,.$$
$$v_4 = (1,2,1,0,2,1,0)\,,$$

Indices des irréductibles b_i (ou solution de $AX = b \pmod{79^3 - 1}$) :

$$x_1 = 44148\,, \qquad x_5 = 422191\,,$$
$$x_2 = 229663\,, \qquad x_6 = 24903\,,$$
$$x_3 = 126420\,, \qquad x_7 = 353146\,.$$
$$x_4 = 31605\,,$$

3.— Pour $s = 12627$, on a

$$wh^s \pmod{79} = 18 + 24\,\sqrt[3]{7} + 8\,\sqrt[3]{7^2} = b_3\,b_7^2\,.$$

Résultat :

$$x = 327047 \pmod{79^3 - 1}\,.$$

Temps d'exécution : 1 h 2′ 10″ 70.

7. Estimation du coût de l'algorithme

Rappelons que n est le cardinal de l'ensemble B des irréductibles de "petites normes", fixé au départ. Il est clair que si n est très "petit", la probabilité ε qu'un nombre z, représentant de $\overline{z} \in E(\sqrt[3]{m})/(p)$, soit B-lisse, devient trop faible et, par conséquent, le coût de la recherche d'un élément B-lisse trop élevé. Et si n est très "grand", effectuer le test de divisibilité de z par les irréductibles b_i et rechercher les facteurs de z deviennent trop coûteux.

On voit donc que l'ordre de grandeur de n joue un rôle très important dans notre algorithme. Nous allons alors estimer n en fonction du majorant N des normes des irréductibles B_i, puis N et le coût de l'algorithme en fonction de p.

La valeur de la borne N qui va être fixée sera celle qui minimisera le coût de la recherche des indices de ces irréductibles.

L'optimisation du coût de cette partie de l'algorithme est essentielle, en ce sens que la détermination des indices des élements b_i conduit à celle du logarithme de tout élément y de $\mathbf{F}_{p^3}$. Par ailleurs, comme nous l'avons remarqué après la présentation de l'algorithme, cette partie, qui ne dépend pas de l'élément y dont on cherche le logarithme, peut être réutilisée tant qu'on ne souhaite pas changer p et le générateur choisi g de $\mathbf{F}_{p^3}^*$.

Pour estimer le coût de l'algorithme, nous allons d'abord calculer n en fonction de N. Ensuite nous déterminerons N (en fonction de p) tel que le coût de la partie 2 de l'algorithme soit optimal. Nous donnerons enfin les coûts relatifs aux première et troisième parties.

L'étude du comportement asymptotique du nombre n d'éléments de l'ensemble B des irréductibles nous amène à rappeler les quatre lemmes suivants.

LEMME 4. — *Soit $q \in \mathbb{Z}$ un nombre premier. Alors q se factorise dans $E(\sqrt[3]{m})$ comme suit :*

cas où $q \nmid m$:

1) $(q) = Q_1 Q_2$ *avec* $\mathcal{N}(Q_i) = q^i \Leftrightarrow q \equiv 2 \pmod 3$;

2) $(q) = Q_1 Q_2 Q_3$ *avec* $\mathcal{N}(Q_i = q)$, *les* Q_i *deux à deux distincts* $\Leftrightarrow q \equiv 1 \pmod 3$ *et m est un cube modulo q ;*

3) $(q) = (q)$ *inerte* $\Leftrightarrow q \equiv 1 \pmod 3$ *et m est un non cube modulo q ;*

cas où $q \mid m$:

- *si* $m \equiv \pm 1 \pmod 9$:

$$(3) = 3_1\, 3_2 \quad \text{avec } \mathcal{N}(3_1) = \mathcal{N}(3_2) = 3\,,$$

- *sinon* $(q \neq 3)$

$$(q) = Q^3 \quad \text{avec } \mathcal{N}(Q) = q\,.$$

Se référer à [2] pour une preuve de ce lemme.

LEMME 5. — *Soit $q \in \mathbb{Z}$ un nombre premier, $q \equiv 1 \pmod 3$. Alors le nombre de cubes dans $\mathbf{F}_q$ est $(q-1)/3$.*

D'après le théorème de Dirichlet sur la distribution des nombres premiers dans une progression arithmétique, nous avons [6] le lemme suivant.

LEMME 6. — *Soient $k \geq 1$ et i deux entiers tels que* $\operatorname{pgcd}(i,k) = 1$. *Soit P_i l'ensemble des nombres premiers q tels que $q \equiv i \pmod k$. La densité de l'ensemble P_i est $1/\varphi(k)$, où φ est la fonction d'Euler.*

(En d'autres termes, les différentes classes modulo k de nombres premiers contiennent chacune le même nombre d'éléments).

Nous avons également besoin, pour l'estimation du cardinal de B, du résultat suivant [6].

LEMME 7.— *Soit* $f(X) = a_k X^k + a_{k-1}X^{k-1} + \cdots + a_0$ *un polynôme de degré* k, *à coefficients entiers; irréductible dans* $\mathbb{Q}$. *Soient* K *le corps engendré par les racines de* f, *et* $r = [K : \mathbb{Q}]$. *Alors l'ensemble* $P_f = \{q\ ;\ q \text{ premier}; f \text{ se décompose totalement dans } \mathbb{F}_q\}$ *a une densité* $\nu = 1/r$.

Grâce à ce résultat, on peut estimer la densité de l'ensemble

$$\{q \equiv 1 \pmod 3\ ;\ q \text{ premier}; m \text{ cube dans } \mathbb{F}_q\},$$

m étant l'entier non cube dans $\mathbb{Q}$, choisi au début de l'algorithme. Cet ensemble est exatement P_f avec $f(X) = X^3 - m$.

En effet, on sait que si $q \equiv 1 \pmod 3$ et $f(X)$ a une racine dans $\mathbb{F}_q$, soit X_0, les deux autres racines sont aussi dans $\mathbb{F}_q$ et sont données par $X_1 = jX_0$, $X_2 = j^2X_0$, où j est une racine cubique de l'unité dans $\mathbb{F}_q$. On a ici $r = 3$, et donc P_f a une densité $\nu = 1/3$.

Pour N "assez grand", le lemme 6 nous donne

$$\begin{aligned}\operatorname{card}\{q \le N\ ;\ q \text{ premier}; q \equiv 2 \pmod 3\} \sim \\ \sim \operatorname{card}\{q \le N\ ;\ q \text{ premier}; q \equiv 1 \pmod 3\} \sim \frac{\pi(N)}{2},\end{aligned}$$

où $\pi(N)$ est le nombre de nombres premiers inférieurs ou égaux à N.

On peut dès lors chercher à estimer le nombre n d'éléments de B.

Le lemme 4 nous indique qu'un nombre premier q se décompose en produit d'au plus 3 facteurs irréductibles de $E(\sqrt[3]{m})$. Donc le nombre maximal d'irréductibles de normes $\le N$ est $3\pi(N)$. D'où la majoration $n \le 3\pi(N)$.

Cherchons maintenant à minorer n. Les facteurs obtenus dans la décomposition des nombres premiers $q \in \mathbb{Z}$ sont de trois types :

- Les facteurs de normes premières : on en a $\pi(N)/2$ avec les nombres premiers $q \in \mathbb{Z}$, $q \le N$, $q \equiv 2 \pmod 3$ et $\pi(N)/2$ avec les nombres premiers $q \in \mathbb{Z}$, $q \le N$, $q \equiv 1 \pmod 3$ et m cube (mod q). D'où au total $\pi(N)$ facteurs de normes premières.

- Les facteurs de normes $q^2 \leq N$: on en a $\pi(\sqrt{N})/2$ avec les nombres premiers $q \in \mathbb{Z}$, $q \leq N$, $q \equiv 2 \pmod 3$.
- Les facteurs de normes $q^3 \leq N$: on en a $\pi(\sqrt[3]{N})/3$ avec les nombres premiers $q \in \mathbb{Z}$, $q \leq N$, $q \equiv 1 \pmod 3$ et m non cube (mod q).

On a donc

$$n = \pi(N) + \frac{\pi(\sqrt{N})}{2} + \frac{\pi(\sqrt[3]{N})}{3} > \pi(N)\,.$$

On prendra dans la suite $n = c \cdot \pi(N)$ avec $1 < c \leq 3$.

Avant de donner une estimation de la complexité de la deuxième partie de l'algorithme, nous allons d'abord chercher à estimer les "chances" pour qu'un élément α soit B-lisse, α étant un représentant de $\overline{\alpha} \in E(\sqrt[3]{m})/(p)$.

Notons S l'ensemble des éléments B-lisses de

$$R := \left\{a + b\sqrt[3]{m} + c\sqrt[3]{m^2}\ ;\ 0 \leq a,\, b, c \leq p-1\right\},$$

un ensemble de représentants des éléments de $E(\sqrt[3]{m})/(p)$. On a le résultat suivant.

LEMME 8. — *Le cardinal de S est supérieur C^u_{n+u} où*

$$u = \left[\frac{\log\left((p-1)^3(m+m^2)/27\right)}{\log N}\right].$$

Preuve. — Nous allons nous intéresser ici aux éléments lisses de $E(\sqrt[3]{m})$ de la forme

$$a + b\sqrt[3]{m} + c\sqrt[3]{m^2} \quad \text{avec } 0 \leq a,\, b,\, c \leq p-1 \text{ si } m \not\equiv \pm 1 \pmod 9 \qquad (1)$$

ou de la forme

$$\frac{a + b\sqrt[3]{m} + c\sqrt[3]{m^2}}{3} \quad \text{avec } 0 \leq a,\, b,\, c \leq p-1 \text{ si } m \equiv \pm 1 \pmod 9. \qquad (9)$$

Nous appellerons $E_1(\sqrt[3]{m})$ le sous-ensemble de $E(\sqrt[3]{m})$ des éléments de la forme (1) ou (2), et R_1 l'ensemble des éléments B-lisses de $E_1(\sqrt[3]{m})$.

Notons que le majorant des normes des éléments de $E_1(\sqrt[3]{m})$ est $N_{\max} = (p-1)^3(m+m^2)$ pour (1) et $N_{\max} = (p-1)^3(m+m^2)/27$ pour (2).

Montrons d'abord que, dans les cas (1) et (2) $\mathrm{card}(S) \geq \mathrm{card}(R_1)$. Le résultat est immédiat dans le cas (1), puisque $\mathrm{card}(S) = \mathrm{card}(R_1)$. Dans le deuxième cas, si un élément $\alpha \in E_1(\sqrt[3]{m})$ est lisse, alors 3α, qui appartient à S, l'est aussi, puisque 3 ou ses facteurs doivent être inclus dans B. Donc, dans tous les cas, $\mathrm{card}(S) \geq \mathrm{card}(R_1)$.

Montrons enfin que $\mathrm{card}(R_1) \geq C_{n+u}^{u}$. En multipliant au plus u éléments de $B \setminus \{b_1\}$ entre eux, l'élément β obtenu vérifie

$$\mathcal{N}(\beta) \leq N^u \leq N^{\frac{\log\left((p-1)^3(m+m^2)/27\right)}{\log N}} = \frac{(p-1)^3(m+m^2)}{27}.$$

Toutes ces combinaisons (avec répétition éventuelle) donnent chacune un élément de R_1. Le nombre d'éléments B-lisses, de norme $\leq N_{\max}$, que l'on peut ainsi produire est C_{n+u}^{u} et est inférieur à $\mathrm{card}(R_1)$. D'où le lemme.

Conséquence. — La probabilité ε qu'un nombre de R soit lisse est $\geq C_{n+u}^{u}/p^3$.

À l'aide de ces résultats, on peut alors énoncer le théorème suivant.

THÉORÈME 6. — *Le coût de la deuxième partie de l'algorithme est en* $\mathrm{O}\left(\exp(\sqrt{24 \log p \log\log p})\right)$

Preuve. — Comme nous le verrons, le coût de la deuxième partie de l'algorithme domine ceux de deux autres parties. Nous déterminons d'abord ce coût.

Tester si un élément $\alpha = h^{u_i}$ est B-lisse exige n divisions, auxquelles il faut ajouter un certain nombre de divisions supplémentaires dues à d'éventuels facteurs multiples b_j, soit t ce nombre. On a

$$t \leq \log \frac{(p-1)^3(m+m^2)}{27} = 3\log(p-1) + \log \frac{m+m^2}{27}.$$

Comme dans les algorithmes de Hellman-Reyneri [4] et de El Gamal [3], nous fixerons deux bornes $n_1 = 4n$ et $n_2 = 2n_1/\varepsilon$ majorant respectivement le nombre d'éléments lisses que l'on souhaite obtenir et le nombre de tentatives pour trouver ces éléments.

Négligeant le coût du calcul de h^{u_i}, qui est polynomial en $\log(u_i)$, le coût des opérations de la deuxième partie de l'algorithme est en $\mathrm{O}\left(n_2(n+1)\right) + \mathrm{O}\left(n_1 n^3\right)$, la première expression étant le coût de la recherche des éléments

B-lisses et la deuxième celui de la résolution (par la méthode de Gauss) du système de n équations à n inconnues (indices des b_j). Nous verrons plus tard que $t \ll n$; d'où en remplaçant n_2 par sa valeur, on a

$$\mathrm{O}\big(n_2(n+1)\big) = \mathrm{O}\left(\frac{n^2}{\varepsilon}\right) = \mathrm{O}\left(n^2 p^3 \frac{u!n!}{(n+u)!}\right). \qquad (*)$$

En utilisant la formule de Stirling, on peut majorer $(*)$ par

$$\mathrm{O}\left(n^2 p^3 \frac{u^u}{n^u}\right).$$

Puisque

$$n \sim c\frac{N}{\log N} \quad \text{et} \quad u \sim \frac{3\log p}{\log N},$$

alors on a

$$\begin{aligned}(*) &= \mathrm{O}\left[p^3 \left(c\frac{N}{\log N}\right)^2 \left[\frac{3\log p}{cN}\right]^{\frac{3\log p}{\log N}}\right] \\ &= \mathrm{O}\left[\exp\left(3\log p + 2\log N + \frac{3\log p}{\log N}\left(\log\log p - \log N\right)\right)\right] \\ &= \mathrm{O}\left[\exp\left\{2\log N + 3\frac{\log p}{\log N}\log\log p\right\}\right].\end{aligned}$$

L'expression

$$g_p(N) := 2\log N + 3\frac{\log p}{\log N}\log\log p$$

est minimale pour

$$\log N = \sqrt{\frac{3}{2}\log p \log\log p}.$$

Reportant cette valeur dans l'estimation asymptotique de n, on voit que

$$t \leq 3\log(p-1) + \log\frac{m+m^2}{27} \ll n.$$

N doit être entier, nous prendrons donc

$$N := \left\lfloor \exp\left(\sqrt{\frac{3}{2}\log p \log\log p}\right)\right\rfloor.$$

Pour tout $\delta > 0$, et pour N tendant vers l'infini, on a

$$\frac{1}{1+\delta}\sqrt{\frac{3}{2}\log p \log\log p} < \log N \leq \sqrt{\frac{3}{2}\log p \log\log p}.$$

D'où un coût de l'ordre de

$$O\Big((1+\delta)\exp\big(\sqrt{24\log p \log\log p}\big)\Big)\ . \qquad (**)$$

Le coût relatif à la résolution du système par la méthode de Gauss est en $O(n_1 n^3) = O(n^4)$. On montre, comme précédemment, que cette expression est majorée par $O(N^4)$, elle-même majorée par $(**)$. D'où un coût de l'algorithme de l'ordre de

$$O\Big(\exp\big(\sqrt{24\log p \log\log p}\big)\Big)\ .$$

Nous allons maintenant passer à l'étude des complexités des parties 1 et 3 de l'algorithme.

Complexité de la partie 1

La proportion des non cubes modulo p est $\frac{2}{3}(p-1)$, d'après le lemme 5, et tester si un entier m est cube ou non modulo p revient à calculer $m^{(p-1)/3} \pmod p$, opération nécessitant un coût en $O(\log^3 p)$. Alors, sous l'hypothèse de Riemann généralisée, trouver un non cube modulo p présente une complexité polynomiale en $\log p$.

Pour la détermination de l'ensemble B, on a les estimations suivantes :

- Le nombre d'éléments $a + b\sqrt[3]{m} + c\sqrt[3]{m^2}$ sélectionnés est inférieur ou égal à N/m.
- Trier ces éléments (dans l'ordre croissant des normes) exige un coût maximal en $O(N \log N)$.
- Pour tester la primalité des normes, en général "petites" et inférieures à N, on peut soit utiliser une liste de petits nombres premiers et tester l'appartenance de chaque norme à cette liste, soit effectuer directement ce test par un algorithme approprié (par divisions successives par exemple).

Complexité de la partie 3

Dans cette partie, le coût dominant est celui relatif à la recherche d'un entier s tel que $z' = wh^s$ soit B-lisse. Si on néglige le coût du calcul de h^s et de wh^s, la complexité de cette étape est en $O(n/\varepsilon)$ qui est bien inférieure à $(**)$.

Conclusion. — On s'aperçoit que le coût de la deuxième partie de l'algorithme domine celui des autres parties. D'où une complexité de l'algorithme inférieure ou égal à

$$O\left(\exp\left(\sqrt{24 \log p \log\log p}\right)\right) .$$

Références

[1] ADLEMAN (L.) . — *A subexponential algorithm for the discrete logarithm problem with applications to cryptography*, Proc. 20th IEEE Fond. Comp. Sci. Symp., 1979, pp. 55-60.

[2] COHN (H.) . — *A Classical Invitation to Algebraic Numbers and Class Fields*, Springer Verlag, 1978.

[3] EL GAMAL (T.) . — *A Subexponential-Time of Computing discrete logarithm over $GF(p^2)$*, IEEE Transaction on information theory **IT-31**, n° 4, July 1985, pp. 473-481.

[4] HELLMAN (M.) et REYNERI (J.) . — *Fast computation of discrete logarithms over $GF(p^m)$*, Crypto '82 Conf., Santa Barbara, CA (August 1982).

[5] LIDL (R.) et NIEDERREITER (H.) . — *Introduction to finite fields and their applications*, Cambridge University Press, 1986.

[6] SERRE (J.-P.) . — *A Course in Arithmetic*, Springer-Verlag, New-York, 1973.

[7] VINCENT CIOFFARI (G.) . — *The Euclidean Condition in Pure Cubic and Complex Quartic Fields*. Mathematics of Computation **33**, number 145 (January 1979), pp. 389-398.

[8] BOREVITCH (Z. I.) et CHAFAREVITCH (I. R.) . — *Théorie des nombres*, Gauthier-Villars Paris, 1967.