De la cryptographie sur les corps quadratiques réels

Simon Pierre Desrosiers
École d'informatique
Université McGill, Montréal
Septembre 2002

A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfilment of the requirements of the degree of Master

Remerciements

Je tiens à remercier Claude Crépeau, mon superviseur, pour sa patience et son soutien, Paul Dumais pour son temps et son aide, Henri Darmon pour son temps et ses conseils et Sean Hallgren pour ses contributions.

Résumé

Nous présentons dans ce mémoire un protocole d'échange de clefs utilisant les propriétés des corps quadratiques réels ainsi qu'une introduction mathématique suffisamment étoffée pour permettre la compréhension du dit protocole. Nous présentons finalement deux protocoles quantiques permettant de résoudre le problème du régulateur sur les corps quadratiques réels et le problème du logarithme discret aussi appelé problème de l'idéal principal.

Abstract

We describe here a key-exchange protocol over real quadratic fields. This is accompanied by all the pertinent algebraic background needed for the understanding of the protocol. We also present two quantum algorithms that solve the regulator problem over real quadratic fields and the discrete logarithm problem also known as the principal ideal problem.

Introduction

La cryptographie est d'abord et avant tout la science du secret, de la confidentialité. Depuis ses balbutiements en antiquité le cœur de cette discipline réside dans le chiffrement de données. C'est-à-dire qu'étant donné un texte, ou une suite de nombre, appelé M, nous voulons transformer mathématiquement le message M en un nouveau message M' tel que nul autre que le détenteur de la clef adéquate ne puisse déchiffrer le message M', c'est à dire le retransformer en M. Bien sur, la cryptographie s'est développée beaucoup depuis et de nouvelles sous-disciplines s'y sont ajoutées telles que la signature électronique, l'authentification électronique, les preuves à divulgations nulles, les calculs multi-partis etc. Mais le chiffrement demeure toujours et encore la discipline fondamentale de la cryptographie moderne. Qui dit chiffrement dit clef. Deux systèmes de chiffrement sont utilisés : les systèmes à clefs secrètes, ou système à clefs symétriques et les systèmes à clefs publiques, ou à clefs asymétriques. Le premier système est certainement le plus intuitif et est le plus ancien. Le second, n'a été proposé que fort récemment, mais s'est avéré un des plus grand succès de la cryptographie moderne. Décrivons ces deux systèmes brièvement. Les systèmes à clefs secrètes requièrent des deux partis qu'ils se rencontrent, d'une manière ou d'une autre, et qu'ils s'échangent une clef commune qui leur servira à chiffrer et à déchiffrer. Les systèmes à clefs publiques sont beaucoup moins contraignants puisqu'un seul des deux partis génerera le système de clefs de son propre chef. Deux clefs seront générées, une publique, appelée C et une privée appelée D. La clef publique C sera alors publiée, c'est-à-dire mise à la disposition de tous, alors que la clef privée sera gardée secrète et ne sera connue que du parti qui a généré le système de clefs. Dès lors la clef C pourra être utilisée par quiconque pour chiffrer un message M et transmettre M' au parti possédant la clef D qui l'utilisera afin de déchiffrer M' en un message M. Le plus connu et le plus utilisé des systèmes à clefs publiques est sans conteste le système RSA. Un bon représentant des systèmes à clefs secrètes est certainement le système DES en passe d'être remplacé par le système AES.

Les systèmes à clefs publiques ont un avantage majeur sur les systèmes à clefs privées : ils n'exigent pas que les deux partis se rencontrent préalablement afin d'échanger une clef. Il serait effectivement bien laborieux d'aller échanger une clef en personne à chaque fois que l'on désire faire un achat sur internet. La cryptographie a cependant développés quantité d'algorithmes et de protocoles qui ont pour but de contourner cet obstacle : les protocoles d'échange de clefs. Ces protocoles permettent à deux partis d'interagir et d'obtenir à la fin de leur interaction une clef commune qui s'avère complètement, on l'espère, inconnue de tout parti ennemi qui aurait pu espionner la conversation. Le plus connu de ces protocoles est certainement le protocole d'échange de clef de DIFFIE et HELLMAN qui utilise les propriétés des corps de nombres naturels. Nous présentons dans le chapitre 4 de ce mémoire un protocole d'échange de clefs proposé en 1989, le protocole de BUCHMANN et WILLIAMS. Ce protocole est fort peu connu pour deux raisons principalement : le protocole de DIFFIE et HELLMAN est ubiquiste et d'utilisation et de compréhension fort simple ; or le protocole de BUCHMANN et WILLIAMS s'avère fort complexe au niveau théorique ce qui peut rebuter beaucoup d'informaticiens à tenter son implantation. C'est pourquoi nous faisons dans les chapitres 1,2 et 3 une introduction que nous jugeons suffisamment complète pour donner au lecteur une bonne compréhension des structures algébriques utilisées par l'algorithme de BUCHMANN et WILLIAMS. Nous ne donnons alors au chapitre 4 qu'une description de la construction théorique du protocole sans aucune preuve. Nous croyons que la compréhension des bases mathématiques sur lesquelles s'appuie le protocole est plus pertinente que les preuves laborieuses prouvant que le protocole est de complexité raisonnable.

Mais il n'y a pas que la cryptographie qui ait fait des progrès ces dernières années. L'informatique a elle aussi fait une avancé spectaculaire. L'utilisation des règles de la physique quantique a permis la construction d'un nouveau modèle de calculateur qui, bien qu'il ne permette pas la résolution de nouveaux problèmes, permet de résoudre avec une efficacité spectaculaire certains problèmes. Le modèle le plus utilisé, celui du circuit quantique, a permis l'élaboration par SHOR d'un algorithme permettant la factorisation en temps polynomial ; un problème qui n'avait pas reçu de solution en plus de 3000 ans. C'est cet algorithme qui a attiré le regard des informaticiens sur cette nouvelle discipline. L'informatique quantique n'avait pas, auparavant, prouvé qu'elle puisse être vraiment utile à des fins calculatoires. La physique quantique avait bien été utilisée auparavant pour créer un protocole permettant l'échange de clefs tel que la physique classique ne le permettait pas, mais rien de significatif au niveau du calcul n'existait malgré l'existence de modèle de calcul quantique. Mais avec l'algorithme de SHOR, l'informatique entrait dans une nouvelle ère, du moins au niveau théorique. Nous présentons dans l'annexe une introduction à l'informatique quantique qui devrait s'avérer suffisante à la compréhension de l'algorithme de factorisation de SHOR. La lecture de l'annexe est fortement recommandée avant l'attaque du chapitre 5 où nous présentons un résultat extrêmement récent. Deux algorithmes quantiques proposés par Sean HALLGREN permettant de casser l'algorithme d'échange de clefs présenté au chapitre 4. Ces 5 chapitres plus l'annexe constituent une première réunion de tout ce matériel en un seul travail. Et c'est là une partie de notre objectif, c'est-à-dire réunir tout le matériel algébrique de base avec les preuves pertinentes permettant de comprendre l'algorithme de BUCHMANN et WILLIAMS, de présenter l'algorithme lui-même et finalement de présenter les derniers résultats disponibles du monde quantique s'attaquant à ce protocole. De plus nous faisons ici une analyse qui n'avait jamais été faite qui nous permet d'affirmer pour la première fois que l'un des deux algorithmes d'HALLGREN est correct. Cependant notre analyse jette un doute plus que profond sur le second algorithme d'HALLGREN. Les preuves incluses dans ce mémoire y sont soit parce qu'elles ont été jugées nécessaires à une bonne compréhension de la matière, soit parce qu'elles sont absentes de la littérature scientifique ou finalement soit parce qu'elles étaient incomplètes ou erronées dans la littérature scientifique pertinente.

Chapitre 1

Corps quadratiques

Un corps quadratique $\mathcal{K} = \mathbb{Q}(\sqrt{D})$ est défini par l'adjonction de la racine $\sqrt{D}$ au corps $\mathbb{Q}$. Soit, tous les nombres $\frac{a+b\sqrt{D}}{c}$ où a, b et $c \in \mathbb{Z}$.

Si $D > 0$, nous dirons que $\mathcal{K}$ est un corps quadratique réel.

Et si $D < 0$ nous dirons que $\mathcal{K}$ est un corps quadratique complexe.

À tout nombre quadratique $\lambda = \frac{a+b\sqrt{D}}{c}$ le conjugué de λ est défini comme étant $\bar{\lambda} = \frac{a-b\sqrt{D}}{c}$. La norme d'un nombre quadratique, $N(\lambda)$ est ainsi définie :

$$N(\lambda) = \lambda\bar{\lambda} = \frac{a^2 - b^2 D}{c^2}.$$

Quelques propriétés des conjugués et des normes peuvent être aisément dérivées :

$$\begin{array}{lrcl}
\textit{1.} & (\overline{\lambda_1 \lambda_2}) & = & \bar{\lambda}_1 \bar{\lambda}_2 \\
\textit{2.} & N(\bar{\lambda}) & = & N(\lambda) \\
\textit{3.} & N(a/c) & = & (a^2/c^2) \quad \text{où } a \text{ et } c \in \mathbb{Z} \\
\textit{4.} & N(\lambda_1 \lambda_2) & = & N(\lambda_1) N(\lambda_2)
\end{array}$$

1.1 Modules

Dans le cas qui nous concerne, un **module** $\mathfrak{M}$ sera défini comme un groupe additif d'objets pris sur $\mathcal{K}$. Donc si $\alpha \in \mathfrak{M}$ alors $n\alpha \in \mathfrak{M}$ pour tout $n \in \mathbb{Z}$. Donc trivialement $0 \in \mathfrak{M}$.

Soit u une combinaison linéaire d'un ensemble fini de vecteurs V_i

$$u = x_1V_1 + x_2V_2 + \cdots + x_nV_n \tag{1.1}$$

où les $x_i \in \mathbb{Z}$. Tous les u possiblement ainsi définis forment un module $\mathfrak{M}$ et les vecteurs $V_1, V_2, \ldots, V_n$ forment la base du module $\mathfrak{M} = [V_1, V_2, \ldots, V_n] = [\mathbf{V}]$. La base sera appelée minimale si tous les u n'ont qu'une seule représentation possible.

Un module $\mathfrak{N}$ ne consistant que d'éléments venant d'un autre module $\mathfrak{M}$ est appelé **sous-module** de $\mathfrak{M}$.

Lemme 1.1.0.1 *Tout sous-module $\mathfrak{N}$ d'un module $\mathfrak{M} = [\mathrm{V}]$, tous deux unidimensionnels, a pour base $[n\mathrm{V}]$ pour un n judicieusement choisi .*

Démonstration :

Supposons qu'$\mathfrak{N}$ n'est pas égal à 0. Le sous-module contient donc des multiples entiers de V. Soit le plus petit $|n| > 0$ pour lequel $n\mathrm{V} \in \mathfrak{N}$. Pour tout m tel que $m\mathrm{V} \in \mathfrak{N}$, $n|m$. Sinon, par algorithme d'Euclide, $m = nq + r$, où $0 < r < |n|$. Ce qui impliquerait que le vecteur $r\mathrm{V} = m\mathrm{V} - qn\mathrm{V} \in \mathfrak{N}$ puisque $n\mathrm{V}$ et $m\mathrm{V}$ appartiennent à $\mathfrak{N}$. Mais ceci contredirait l'hypothèse de minimalité de n. *CQFD.*

1.2 Entiers quadratiques

Nous appellerons **entiers quadratiques** sur $\mathcal{K}$ tous les nombres $\alpha \in \mathcal{K}$ qui sont solution d'un polynôme

$$x^2 + Bx + C \tag{1.2}$$

où B et $C \in \mathbb{Z}$. Nous appellerons désormais **entiers rationnels** l'ensemble $\mathbb{Z}$ afin d'éviter toute confusion. Par **entiers** nous entendrons désormais tous les entiers quadratiques,— ce qui comprend l'ensemble $\mathbb{Z}$.

Cette condition impose donc une contrainte sur les a, b et c possibles dans $\alpha = \frac{a+b\sqrt{D}}{c}$, si l'on veut qu'$\alpha$ soit un entier quadratique.

Supposons premièrement que D n'ait pas de diviseur quadratique,— $D \neq r^2D_0$, pour $r > 1$ et r et $D_0 \in \mathbb{Z}$. On peut aisément voir que pour tout $D = r^2D_0$ et $a, b, c \in \mathbb{Z}$, il existe $a', b', c' \in \mathbb{Z}$ tels que

$$\frac{a + b\sqrt{D_0}}{c} = \frac{a' + b'\sqrt{D}}{c'}.$$

Donc D et D_0 engendrent le même corps $\mathcal{K}$. Pour tout $\alpha = (a + b\sqrt{D})/c \in \mathcal{K}$, α est solution à (1.2) si et seulement si $-B = \alpha + \bar{\alpha}$ et $C = \alpha\bar{\alpha} = N(\alpha)$. Donc α est un entier quadratique si et seulement si $-B = \alpha + \bar{\alpha} = 2a/c \in \mathbb{Z}$ et $C = \alpha\bar{\alpha} = (a^2 - b^2 D_0)/c^2 \in \mathbb{Z}$, pour a, b, c relativement premiers et appartenant à $\mathbb{Z}$.

Certaines conclusions s'imposent aisément. Ainsi $\mathrm{pgcd}(a, c) = 1$. Sinon, supposons que $\mathrm{pgcd}(a, c) = p$. Alors afin que C puisse être un entier rationnel, il faut que p^2, qui divise c^2, divise $a^2 - b^2 D_0$. Donc $a^2 - b^2 D_0 \equiv 0 \pmod{p^2}$, ou $a^2 \equiv b^2 D_0 \pmod{p^2}$. D'où l'on peut conclure que $p^2 | b^2 D_0$. Mais étant donné que D_0 n'a pas de diviseur quadratique, $p^2 | b^2$. Ce qui implique que $p|a, p|b$ et $p|c$, ce qui contredit l'hypothèse de départ, à savoir qu'a, b et c sont relativement premiers.

Étant donné l'intégralité de B, si $c \neq 1$, alors nécessairement $c = 2$. Ce qui implique ceci en retour

$$a^2 - b^2 D_0 = c^2 C \equiv 0 \pmod{4}. \tag{1.3}$$

Considérons les diverses possibilités de parité pour a et b lorsque $c = 2$. On peut aisément voir que l'équation (1.3) n'est vrai que si a et b sont impairs. Supposons qu'a et b soient pairs, alors a, b et c ne sont pas relativement premiers. Finalement si a et b n'ont pas la même parité, la seule solution est d'avoir a pair et b impair ; ce qui implique que $4|D_0$ ce qui est impossible étant donné le choix de D_0. Donc, en résumé, $a^2 \equiv b^2 \equiv 1 \pmod{4}$ et $D_0 \equiv 1 \pmod{4}$. De là, il peut être aisément conclu que si $D_0 \not\equiv 1 \pmod{4}$ alors $c = 1$.

À l'inverse, si $D_0 \equiv 1 \pmod{4}$ et a et b sont tous deux impairs, alors c peut être égale à 2 afin que B et C appartiennent à $\mathbb{Z}$ et qu'α soit un entier. De plus, si $D_0 \equiv 1 \pmod{4}$, α est un entier même si $c = 2$ et a et b sont pairs ; la fraction ne sera cependant pas réduite. Cependant si a et b sont de parité différente, c ne peut être égal à 2.

Un entier quadratique peut donc être exprimé de manière générale par

$$\alpha = \begin{cases} \frac{a+b\sqrt{D_0}}{2} & \text{où } a \equiv b \pmod{2} \text{ si } D_0 \equiv 1 \pmod{4}, \\ \\ a + b\sqrt{D_0} & \forall a, b \text{ si } D_0 \not\equiv 1 \pmod{4} \end{cases} \tag{1.4}$$

Il faut noter ici que rien n'interdit à b d'être égal à 0. Dans ce cas c n'est égal à 2 que si $D_0 \equiv 1 \pmod{4}$, et étant donné qu'$a \equiv b \pmod{2}$, a est forcé d'être pair. Ce qui implique que seulement les entiers rationnels sont des entiers quadratiques,— aucun rationnel ($\mathbb{Q}$) n'appartenant pas à $\mathbb{Z}$ n'est un entier quadratique.

Il existe une manière plus intéressante d'écrire le résultat (1.4) qui nous permettra d'exprimer tous les entiers comme un module $\mathfrak{D}$ sur $\mathcal{K}$. Il nous suffit d'observer qu'

$(a+b\sqrt{D_0})/2 = (a-b)/2 + b(1+\sqrt{D_0})/2$. Dès lors si nous définissons $a' = (a-b)/2$ et $b' = b$, toujours sous la conditions $a \equiv b \pmod 2$, alors

$$(a+b\sqrt{D_0})/2 = a' + b'(1+\sqrt{D_0})/2, \tag{1.5}$$

où a' et b' sont des entiers rationnels quelconques. Alors on peut définir

$$\omega_0 = \begin{cases} \frac{1+\sqrt{D_0}}{2} & \text{si } D_0 \equiv 1 \pmod 4, \\ \sqrt{D_0} & \text{si } D_0 \not\equiv 1 \pmod 4. \end{cases} \tag{1.6}$$

Ainsi, dans les deux cas, les entiers quadratiques forment un module dans $\mathbb{Q}(\sqrt{D})$ qu'on peut écrire

$$\mathfrak{D} = [1, \omega_0]. \tag{1.7}$$

Le corps $\mathcal{K} = \mathbb{Q}(\sqrt{r^2 D_0})$ étant indépendant de r, les entiers quadratiques $\mathfrak{D}$ sur $\mathcal{K}$ le sont aussi.

Un résultat important émerge de la définition même des entiers quadratiques :

Lemme 1.2.0.2 *La norme de tout entier quadratique α est un entier rationnel. De plus elle est égale à 0 si et seulement si $\alpha = 0$.*

1.3 Anneaux d'intégrité

Bien que $\mathcal{K}$ soit un corps, $\mathfrak{D}$ n'en est pas un. Évidement $\mathfrak{D}$ est un anneau puisque pour tout $\alpha, \beta \in \mathfrak{D}$, $\alpha + \beta \in \mathfrak{D}$ et $\alpha\beta \in \mathfrak{D}$. De plus l'anneau $\mathfrak{D}$ possède la propriété supplémentaire de n'avoir pas de diviseur du zéro. C'est-à-dire qu'il n'existe pas d'α et β tels que $\alpha\beta = 0$. Un tel anneau est appelé **anneau d'intégrité**.

La stabilité de l'addition sur $\mathfrak{D}$ est évidente. La stabilité de la multiplication sur $\mathfrak{D}$ peut être aisément démontrée. Ainsi $(a+b\omega_0)(a'+b'\omega_0) = aa' + (ab'+a'b)\omega_0 + bb'\omega_0^2$. Si $D_0 \not\equiv 1 \pmod 4$, alors $\omega_0 = \sqrt{D_0}$ et on obtient $(aa' + bb'D_0) + (ab' + a'b)\omega_0$, qui est clairement un membre du module $\mathfrak{D} = [1, \omega_0]$. Et si $D_0 \equiv 1 \pmod 4$, alors $\omega_0^2 = (1 + 2\sqrt{D_0} + D_0)/4 = (2 + 2\sqrt{D_0} + D_0 - 1)/4 = \omega_0 + (D_0 - 1)/4$. On obtient finalement $(aa' + bb'(D_0-1)/4) + (ab' + a'b + bb')\omega_0$ qui appartient aussi clairement au module $\mathfrak{D} = [1, \omega_0]$.

Ces propriétés nous permettent de considérer des congruences sur $\mathfrak{O}$: $\xi_1 \equiv \xi_2 \pmod{\eta}$ si $(\xi_1 - \xi_2)/\eta \in \mathfrak{O}$, où $\eta \in \mathfrak{O}$,— ce qui est un abus de notation(puisqu'il n'existe pas nécessairement d'inverse multiplicatif sur $\mathfrak{O}$), il serait plus juste d'écrire qu'il existe un $t \in \mathfrak{O}$ tel que $t\eta = (\xi_1 - \xi_2)$.

Théorème 1.3.1 *Si $\mathfrak{O}$ contient un sous anneau $\mathfrak{O}^*$ qui n'est pas composé uniquement de rationnels, alors $\mathfrak{O}^*$ est caractérisé par un unique nombre naturel n tel que $\mathfrak{O}^*$ est le sous-ensemble d'entiers de $\mathfrak{O}$ qui sont congrus à un entier rationnel quelconque modulo n.*

Démonstration :

Clairement ceci signifie que $\mathfrak{O}^*$ est l'ensemble de tous les nombres $\alpha \in \mathfrak{O}$ tels que $\alpha \equiv r \pmod{n}$ pour $r \in \mathbb{Z}$,— il faut cependant utiliser la valeur positive de n pour obtenir l'unicité mentionnée dans le théorème. Évidemment tous les entiers de $\mathfrak{O}$ qui sont congrues à un nombre naturel quelconque forment un anneau puisque les entiers forment eux-mêmes un anneau.

À l'inverse considérons le terme $x + y\omega_0 \in \mathfrak{O}^*$. Étant donné que $\mathfrak{O}^* \supsetneq \mathbb{Z}$ il existe un terme $x + y\omega_0$ où $y \neq 0$. Puisque $\mathfrak{O}^*$ contient $\mathbb{Z}$, $x \in \mathfrak{O}^*$, donc $y\omega_0 \in \mathfrak{O}^*$. Soit le plus petit tel $|y|$ et appelons-le n. Par le lemme 1.1.0.1 nous savons que tous les termes $y\omega_0$ (dans $x + y\omega_0$) sont des multiples de $n\omega_0$. L'expression générale d'un entier appartenant à $\mathfrak{O}^*$ est donc $\xi = x + yn\omega_0$ pour x et y quelconque. Ou $\xi \equiv x \pmod{n}$ pour tous les $\xi \in \mathfrak{O}^*$ et inversement tous les $\xi \in \mathfrak{O}^*$ sont de la forme $x + yn\omega_0$. *CQFD*

L'anneau d'intégrité $\mathfrak{O}^*$ correspondant à n sera noté par $\mathfrak{O}_n$. Donc $\mathfrak{O}_1 = \mathfrak{O}$.

Souvent, les modules $\mathfrak{O}_n$ sont appelés «ordres» et écris $\mathcal{O}_n$. Un ordre $\mathcal{O}$ est souvent défini comme un sous-anneau de $\mathbb{Q}(\sqrt{D_0})$ tel que $\mathbb{Z} \in \mathcal{O}$. L'ordre $\mathcal{O}_1 = \mathfrak{O}_1$ est alors appelé ordre maximal,— le plus grand ordre sur $\mathbb{Q}(\sqrt{D_0})$. Nous n'utiliserons pas ici cette nomenclature.

1.4 Modules et treillis

Un concept mathématique important doit être brièvement introduit. Nous ne pourrons qu'en effleurer toutes les subtilités et devrons même nous faire violence et demeurer un peu flou dans les preuves de certains théorèmes car ceci nous éloignerait trop de notre sujet principal. Cependant le lecteur doit développer une intuition du sujet afin de pouvoir comprendre l'une des preuves pivots de ce mémoire.

La définition d'un module donnée dans la section 1.1 est un peu simpliste. Évidement l'ensemble tel que défini par l'équation (1.1) est un module, mais un module n'a pas nécessairement de base finie. L'ensemble $\mathbb{Q}$ forme un module selon la définition donnée, mais n'a pas de base. Il nous faut donc introduire quelques concepts.

Nous dirons qu'un ensemble fini de vecteurs $\mathbf{V} = [V_1, V_2, \ldots, V_n]$ est **linéairement dépendant** s'il existe des entiers rationnels $a_1, a_2, \ldots, a_n$, dont certains ne sont pas égaux à 0, tels que

$$a_1V_1 + a_2V_2 + \cdots + a_nV_n = 0. \tag{1.8}$$

Autrement, ils seront dit **linéairement indépendants**. La **dimension** d'un module $\mathfrak{M}$ sera définie comme étant le nombre maximum de vecteurs linéairement indépendants de $\mathfrak{M}$.

Une **norme** est une fonction définie sur un ensemble de vecteurs $\mathbf{V}$ et dénotée $\|v\|$, pour un vecteur $v \in \mathbf{V}$. Une norme doit respecter les trois propriétés suivantes.

- Pour que le vecteur $v \in \mathbf{V}$ soit nul il faut et il suffit que $\|v\| = 0$, (axiome de séparation).
- Pour tout vecteur $v \in \mathbf{V}$ et scalaire α, on a $\|\alpha v\| = |\alpha|\|v\|$, (axiome de linéarité).
- Pour tout couple de vecteurs $u, v \in \mathbf{V}$, on a $\|u + v\| \leq \|u\| + \|v\|$, (inégalité triangulaire).

Un module est dit discret lorsqu'il existe une norme telle que pour tout $v \neq 0 \in \mathbf{V}$

$$\|v\| \geq k \in \mathbb{R} \tag{1.9}$$

pour un k constant et positif. Plusieurs normes peuvent répondre à cette définition. Mais l'existence d'une seule norme est suffisante. Cette définition est parfois énoncée ainsi : il existe une norme et un k constant tels que pour tous $u, v \in \mathbf{V}$, $\|v - u\| \geq k$.

Finalement, un **treillis** est défini comme étant un module discret possédant une base finie.

Dans le cas qui nous concerne, nous pouvons constater que les entiers quadratiques forment un treillis. Premièrement $\mathfrak{D}$ possède une base finie de dimension 2, soit $[1, \omega_0]$.

Si la norme

$$\|\xi\| = \sqrt{\frac{|\xi|^2 + |\bar{\xi}|^2}{2}} \tag{1.10}$$

est choisie il peut aisément être prouvé que $\mathfrak{D}$ est discret. Primo, $\|\xi\| = 0$ si et seulement si $|\xi|^2 + |\bar{\xi}|^2 = 0$. Ce qui n'est possible que si $\xi = 0$.

Secundo, si a est un scalaire,

$$\|a\xi\| = \sqrt{(|a\xi|^2 + |a\bar{\xi}|^2)/2} = \sqrt{a^2(|\xi|^2 + |\bar{\xi}|^2)/2} = a\sqrt{(|\xi|^2 + |\bar{\xi}|^2)/2} = a\|\xi\|.$$

Tertio si ξ et η sont des entiers quadratiques, alors nous désirons prouver : $\|\xi+\eta\| \leq \|\xi\| + \|\eta\|$. Par définition nous avons (et nous cherchons à obtenir) :

$$\sqrt{(|\xi+\eta|^2 + |\bar{\xi}+\bar{\eta}|^2)/2} \leq \sqrt{(|\xi|^2 + |\bar{\xi}|^2)/2} + \sqrt{(|\eta|^2 + |\bar{\eta}|^2)/2}.$$

En multipliant par 4 et en prenant le carré des 2 côtés de l'équation nous obtenons :

$$|\xi+\eta|^2 + |\bar{\xi}+\bar{\eta}|^2 \leq |\xi|^2 + |\eta|^2 + |\bar{\xi}|^2 + |\bar{\eta}|^2 + \mathbf{C} \tag{1.11}$$

où $\mathbf{C} = 2\sqrt{(((|\xi|^2 + |\bar{\xi}|^2)(|\eta|^2 + |\bar{\eta}|^2))} \geq 0$.

En utilisant l'identité «$a^2 + b^2 = (a+b)^2 - 2ab$», nous pouvons écrire $|\xi|^2 + |\eta|^2 = (|\xi|+|\eta|)^2 - 2|\xi||\eta|$ et $|\bar{\xi}|^2 + |\bar{\eta}|^2 = (|\bar{\xi}|+|\bar{\eta}|)^2 - 2|\bar{\xi}||\bar{\eta}|$. Ce qui nous permet de réécrire l'équation (1.11) ainsi :

$$|\xi+\eta|^2 + |\bar{\xi}+\bar{\eta}|^2 + 0 \leq (|\xi| + |\eta|)^2 + (|\bar{\xi}| + |\bar{\eta}|)^2 + \mathbf{C}'. \tag{1.12}$$

Étant donné que la valeur absolue respecte l'inégalité triangulaire, nous savons que $|\xi+\eta|^2 \leq (|\xi| + |\eta|)^2$ et $|\bar{\xi}+\bar{\eta}|^2 \leq (|\bar{\xi}| + |\bar{\eta}|)^2$. Donc si $\mathbf{C}' \geq 0$, il pourra être conclu que dans l'équation (1.11), la partie gauche est inférieure ou égale terme à terme à la partie droite. Et donc, étant donné que toutes les équations sont équivalentes entre elles, nous devrons conclure que l'inégalité triangulaire est respectée par la norme choisie.

Il ne nous reste plus qu'à démontrer que $\mathbf{C}'$ est supérieur ou égal à 0.

$$\mathbf{C}' = 2\sqrt{(|\xi||\eta|)^2 + (|\xi||\bar{\eta}|)^2 + (|\bar{\xi}||\eta|)^2 + (|\bar{\xi}||\bar{\eta}|)^2} - 2(|\xi||\eta| + |\bar{\xi}||\bar{\eta}|).$$

$\mathbf{C}' \geq 0$ si et seulement si

$$(|\xi||\eta|)^2 + (|\xi||\bar{\eta}|)^2 + (|\bar{\xi}||\eta|)^2 + (|\bar{\xi}||\bar{\eta}|)^2 \geq (|\xi||\eta|)^2 + (|\bar{\xi}||\bar{\eta}|)^2 + 2(|\xi||\eta||\bar{\xi}||\bar{\eta}|).$$

Ou $(|\xi||\bar{\eta}|)^2 + (|\bar{\xi}||\eta|)^2 \geq 2(|\xi||\eta||\bar{\xi}||\bar{\eta}|)$. Finalement

$$(|\xi||\bar{\eta}|)^2 - 2(|\xi||\eta||\bar{\xi}||\bar{\eta}|) + (|\bar{\xi}||\eta|)^2 = ((|\xi||\bar{\eta}|) - (|\bar{\xi}||\eta|))^2 \geq 0.$$

Ce qui est trivialement vrai. Ce qui implique que $\mathbf{C}'$ est supérieur ou égal à 0 et que l'inégalité (1.12) ainsi que l'inégalité (1.11) sont vraies . *CQFD.*

Finalement nous pouvons vérifier que $\mathfrak{D}$ est discret en remarquant que $(|\xi|-|\bar{\xi}|)^2 \geq 0$. Si l'expression est développée, nous obtiendrons

$$|\xi|^2 + |\bar{\xi}|^2 \geq 2|\xi\bar{\xi}| = 2|N(\xi)|.$$

Par le lemme 1.2.0.2, nous savons que $|N(\eta)| \geq 1$ à moins qu'ξ ne soit 0. Donc $\|\xi\| \geq 1$. *CQFD*

Notons au passage que $\|\xi\| = \|\bar{\xi}\|$ ainsi que $\|a\| = |a|$ si $a \in \mathbb{Z}$. Le treillis des entiers quadratiques, associé à la norme (1.10), peut être représenté dans le plan euclidien par des points définis par les paires $(\eta, \bar{\eta})$, où $\eta \in \mathfrak{D}$. La norme (1.10) devient alors simplement la distance, divisée par $\sqrt{2}$, entre un point du treillis et l'origine du plan.

Un sous-module $\mathfrak{M}$ d'un treillis $\mathfrak{L}$ est lui aussi évidement un treillis puisque toutes les propriétés de $\mathfrak{L}$ sont stables sur $\mathfrak{M}$. $\mathfrak{M}$ sera appelé **sous-treillis**. Donc tout module quadratique est un sous-treillis de $\mathfrak{D}$ de dimension 2 ou moins.

Théorème 1.4.1 *Tout treillis possède une base minimale.*

Théorème 1.4.2 *Tout module qui possède une base forme un treillis.*

Théorème 1.4.3 *Tout module quadratique $\mathfrak{M}$ possède une base $\mathfrak{M} = [a, b + c\omega_0]$ où $a > b \geq 0$ et $c > 0$. De plus a est le plus petit entier rationnel positif appartenant à $\mathfrak{M}$ et $b + c\omega_0$ est l'entier sur $\mathfrak{M}$ où ω_0 possède le plus petit coefficient.*

Théorème 1.4.4 *Deux modules quadratiques, $\mathfrak{M}_1 = [\alpha, \beta]$ et $\mathfrak{M}_2 = [\gamma, \delta]$, sont équivalents (égaux) si et seulement s'ils peuvent être mis en relation à l'aide d'une matrice de dimension 2×2 composée d'éléments appartenant à $\mathbb{Z}$ et ayant pour déterminant ± 1 :*

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \gamma \\ \delta \end{pmatrix}. \tag{1.13}$$

Le dernier théorème entend par équivalence de module qu'ils génèrent exactement les mêmes points dans le plan.

1.5 Discriminent d'un module

Soit le module $\mathfrak{M} \in \mathfrak{D}$ ayant la base $\mathfrak{M} = [\xi_1, \xi_2]$, où ξ_1 et ξ_2 appartiennent à $\mathfrak{D}$. Nous définirons la différente du module, d, ainsi :

$$d = d(\mathfrak{M}) = \begin{vmatrix} \xi_1 & \xi_2 \\ \bar{\xi}_1 & \bar{\xi}_2 \end{vmatrix} = \xi_1\bar{\xi}_2 - \bar{\xi}_1\xi_2. \tag{1.14}$$

Nous pouvons aisément remarquer que la différente n'est égal à 0 que si et seulement si ξ_1 et ξ_2 sont linéairement dépendants. Ou si et seulement si le module $\mathfrak{M}$ est unidimensionnel.

Le module $\mathfrak{D}_n = [1, n\omega_0]$ a pour différente

$$d = d(\mathfrak{D}_n) = n(\omega_0 - \bar{\omega}_0) = \begin{cases} n\sqrt{D_0} & \text{si } D_0 \equiv 1 \pmod 4 \\ 2n\sqrt{D_0} & \text{si } D_0 \not\equiv 1 \pmod 4 \end{cases} \tag{1.15}$$

Le discriminent Δ, que nous définirons par $\Delta = d^2$, est cependant une quantité beaucoup plus importante. Le discriminent est toujours un entier rationnel positif,— pour $D_0 > 0$. Donc pour le module $\mathfrak{D}_n$:

$$\Delta = \Delta(\mathfrak{D}_n) = \begin{cases} n^2 D_0 & \text{si } D_0 \equiv 1 \pmod 4 \\ 4n^2 D_0 & \text{si } D_0 \not\equiv 1 \pmod 4 \end{cases} \tag{1.16}$$

De manière générale, si $\mathfrak{M}$ est un sous-module de $\mathfrak{D}_n$ alors

$$\Delta(\mathfrak{M}) = j^2 \Delta(\mathfrak{D}_n) \tag{1.17}$$

où j est appelé l'index de $\mathfrak{M}$ sur $\mathfrak{D}_n$. L'entier j, représente aussi le nombre de classes d'équivalences des éléments de $\mathfrak{D}_n$ modulo $\mathfrak{M}$. Nous dirons que deux éléments α_1 et α_2 appartenant à $\mathfrak{D}_n$ sont congrus modulo $\mathfrak{M}$,— $\alpha_1 \equiv \alpha_2 \pmod{\mathfrak{M}}$,— si $(\alpha_1 - \alpha_2) \in \mathfrak{M}$.

1.6 Unités et divisibilité sur un anneau d'intégrité

Nous dirons qu'un élément $\alpha_1 \in \mathfrak{D}$ divise un élément $\alpha \in \mathfrak{D}$ s'il existe un élément $\alpha_2 \in \mathfrak{D}$ tel que

$$\alpha = \alpha_1\alpha_2. \tag{1.18}$$

Un élément $\rho \in \mathfrak{D}$ qui divise 1 est appelé **unité**. Les unités sont donc par définition les éléments inversibles de l'anneau d'intégrité $\mathfrak{D}$.

Théorème 1.6.1 *L'ensemble des unités sur $\mathfrak{D}_n$ est formé de tous les éléments qui ont leur norme égale à* ± 1.

Démonstration :

Par définition, pour une unité ρ, il existe un η tel que $\rho\eta = 1$. Étant donné la propriété multiplicative des normes, nous pouvons écrire $N(\rho)N(\eta) = N(1) = 1$. Par le lemme 1.2.0.2 nous savons que la norme d'un entier quadratique appartient à $\mathbb{Z}$. Les deux seules solutions possibles pour la norme d'une unité sont donc ± 1.

À l'inverse, si la norme d'un élément ρ est égale à ± 1 il est alors trivial que ρ divise 1. *CQFD*

Corollaire 1.6.1.1 *Les unités sur $\mathfrak{D}$ forment un groupe multiplicatif infini.*

Théorème 1.6.2 *L'ensemble* $\mathfrak{U} = \{\log|\rho|\}$, *où ρ est une unité sur $\mathfrak{D}_n$, constitue un treillis unidimensionnel.*

Corollaire 1.6.2.1 *Il existe une unité $\epsilon \in \mathfrak{D}_n$, appelée* **unité fondamentale**, *tel que pour toute unité $\rho \in \mathfrak{D}_n$, $\rho = \pm\epsilon^k$ pour un k appartenant à $\mathbb{Z}$.*

Afin que l'unité fondamentale soit unique, nous la choisirons positive. Un résultat immédiat du théorème 1.6.2 émerge : l'unité fondamentale est l'unité pour laquelle $\log|\rho|$, où $\rho > 0$, est minimal. Nous appellerons **régulateur**, et le dénoterons par $\mathfrak{R}$, le logarithme de l'unité fondamentale. $\mathfrak{R}$ génère $\mathfrak{U}$.

1.7 Idéaux

Un **idéal** $\mathfrak{a}$ sur $\mathfrak{D}_n$ est un sous-anneau de $\mathfrak{D}_n$ (donc un sous-module) avec la propriété supplémentaire que pour tout élément $\eta \in \mathfrak{D}_n$, $\alpha\eta \in \mathfrak{a}$ pour tout $\alpha \in \mathfrak{a}$.

Un idéal $\mathfrak{a}$ est dit **principal** s'il existe un élément $\alpha \in \mathfrak{a}$ tel que $\mathfrak{a} = \{\alpha\eta\}$ pour $\eta \in \mathfrak{D}_n$. Nous écrirons alors $\mathfrak{a} = (\alpha)$ ou $\mathfrak{a} = \alpha\mathfrak{D}_n$.

Théorème 1.7.1 *Si $(\alpha) = (\beta)$ alors $\alpha = \beta = 0$ ou α/β est une unité .*

Démonstration :

Étant donné l'égalité, nous savons que $\beta \in (\alpha)$. Donc $\beta = \eta\alpha$ pour un $\eta \in \mathfrak{D}_n$. Similairement $\alpha = \xi\beta$ pour un $\xi \in \mathfrak{D}_n$. On peut donc, à moins qu'$\alpha = \beta = 0$, conclure que $\beta = \eta\xi\beta$ ou $\eta\xi = 1$. *CQFD.*

Nous noterons parfois, lorsque nécessaire, par $L(\mathfrak{a})$ le plus petit entier rationnel de l'idéal $\mathfrak{a}$.

Théorème 1.7.2 *Tout idéal* $\mathfrak{a} \in \mathfrak{D}_n$ *en tant que module possède une base* $[a, b + c\omega_n]$ *où* $L(\mathfrak{a}) = a > b \geq 0$ *et* $a \geq c > 0$*. De plus* $c|a$ *et* $c|b$*. La base possédant ces propriétés est unique.*

Démonstration :

Étant donné qu'$\mathfrak{a}$ est un module, le théorème 1.4.3 s'applique certainement ici. Il ne nous reste plus qu'à prouver que $0 < c \leq a$, que $c|a$ et $c|b$, ainsi que l'unicité de la base.

Le théorème 1.4.3 nous dit qu'a est le plus petit entier rationnel positif de l'idéal $\mathfrak{a}$, il est donc certainement unique. Supposons alors qu'une seconde base $[a, b' + c'\omega_n]$ existe ayant ces propriétés. Puisqu'$\mathfrak{a}$ est un module et que ces bases sont minimales, on peut écrire $ax + (b + c\omega_n)y = b' + c'\omega_n$. En égalisant les parties rationnelles et quadratiques nous obtenons $ax + by = b'$ et $cy = c'$.

Mais puisque b et b' sont compris entre 0 et a alors nécessairement $x = 0$ et $y = 1$. Supposons le contraire ; alors quel que soit x et y, $|y| > 1$. Ceci impliquerait alors que $|c'| > |c|$. Ce qui nous mènerait immédiatement à une contradiction puisqu'il serait impossible d'écrire $b + c\omega_n$ dans la nouvelle base $[a, b' + c'\omega_n]$. Donc, nécessairement, $y = 1$; ce qui impose à x d'être égal à 0. Et donc $c' = c$ et l'unicité de c est confirmée.

Étant donné qu'$a \in \mathfrak{a}$ et qu'$\omega_n \in \mathfrak{D}_n$, $a\omega_n \in \mathfrak{a}$. Il existe donc ici aussi une unique représentation $a\omega_n = ax + (b + c\omega_n)y$. Ceci impose cependant qu'$a = cy$ et donc que $c|a$. Donc $c < a$ et peut toujours être choisi positif en multipliant par -1 si nécessaire.

$N(b + c\omega_n)$ étant un entier rationnel et a étant le plus petit rationnel, il faut nécessairement qu'a divise $N(b + c\omega_n)$; sinon nous pourrions, par l'algorithme d'Euclide, construire un entier rationnel plus petit qu'a et appartenant à $\mathfrak{a}$. Ceci implique, par la définition de $N(b + c\omega_n)$, que le d, le pgcd(a, c), divise b. Nous savons qu'$ar + cs = d$ pour r et s judicieusement choisis. Nous savons aussi qu'$a\omega_n \in \mathfrak{a}$. Donc $a\omega_n r + (b + c\omega_n)s = bs + d\omega_n$. Nous pouvons aussi écrire $bs + \omega_n = ax + (b + c\omega_n)y$ où x et $y \in \mathbb{Z}$. Ce qui impose l'égalité $cy = d$. Mais $d \leq c$ et $|cy| \geq |c|$, donc $sc = d$, $s = 1$ et $c = d$. Donc $c|b$ par les commentaires précédents. *CQFD.*

Théorème 1.7.3 *Un module* $[a, b+c\omega_n]$ *tel que* $c|a, c|b$ *et* $ac|N(b+c\omega_n)$ *est un idéal sur* $\mathfrak{O}_n$.

Démonstration :

Nous pouvons supposer sans perte de généralité que $c = 1$ (voir la démonstration du théorème précédent). Donc, soit le module $\mathfrak{M} = [a, b + \omega_n]$ où $a|N(b + \omega_n)$. Par définition $\mathfrak{M}$ est un idéal si et seulement si pour tout $\alpha \in \mathfrak{O}_n$ et pour tout $\beta \in \mathfrak{M}$, $\alpha\beta \in \mathfrak{M}$. Développons le cas général et essayons de l'exprimer comme un élément de $\mathfrak{M}$.

Soient $\alpha = x + y\omega_n \in \mathfrak{O}_n$ et $\beta = ra + s(b + \omega_n) \in \mathfrak{M}$ où x, y, r et $s \in \mathbb{Z}$. Nous voulons montrer que $(x + y\omega_n)(ra + s(b + \omega_n)) \in \mathfrak{M}$. En développant l'expression, nous obtenons $xra + xsb + xs\omega_n + y\omega_n ra + y\omega_n sb + ys\omega_n^2$.

Supposons maintenant qu'$\omega_n = (1 + \sqrt{D})/2$. Dans ce cas,

$$\omega_n^2 = (1 + 2\sqrt{D} + D)/4 = (1 + \sqrt{D} + 1 + \sqrt{D} + (D - 1))/4 = \omega_n + (D - 1)/4.$$

Nous pouvons donc réunir les termes ainsi :

$$\alpha\beta = xra + xsb + ys(D - 1)/4 + \omega_n(\underbrace{ys + xs + yra + ysb}_{m}) \tag{1.19}$$

où m est de toute évidence un entier rationnel.

Nous désirons, alors, exprimer l'équation (1.19) ainsi :

$$\alpha\beta = al + m(b + \omega_n) \tag{1.20}$$

où l et $m \in \mathbb{Z}$ et m est défini à l'équation (1.19). Remarquons d'abord que

$$N(b + \omega_n) = (b + 1/2 + \sqrt{D}/2)(b + 1/2 - \sqrt{D}/2) = b^2 + b - (D - 1)/4.$$

Alors $al + mb = xra + xsb + ys(D - 1)/4$. En remplaçant m, nous obtenons $al = xra + xsb + ys(D - 1)/4 - ysb - xsb - yrab - ysb^2$.

Regroupons les termes et simplifions :

$$al = xra - yrab + ys((D - 1)/4 - b - b^2). \tag{1.21}$$

Nous nous apercevons qu'a divise les deux premiers termes trivialement et qu'a divise le dernier groupe, puisque l'expression $(D - 1)/4 - b - b^2$ n'est rien d'autre que la norme de $(b + \omega_n)$, qu'a divise par hypothèse. Ce qui implique qu'$l \in \mathbb{Z}$.

Nous avons donc démontré que pour $D \equiv 1 \pmod 4$, $\mathfrak{M}$ est un idéal. La preuve pour $D \not\equiv 1 \pmod 4$ est similaire, l'arithmétique étant simplifiée par le fait qu'ω_n est alors égal à $\sqrt{D}$. Nous ne ferons donc pas cette partie de la démonstration. *CQFD.*

Nous dirons qu'un idéal $\mathfrak{a} = [a, b + c\omega_n]$ est **primitif** s'il possède une base où $c = 1$. Nous appellerons l'index du module $\mathfrak{a}$ la **norme de l'idéal** $\mathfrak{a}$ et l'écrirons $N(\mathfrak{a})$. $N(\mathfrak{a}) = cL(\mathfrak{a})$ et $N(\mathfrak{a}) = L(\mathfrak{a})$ pour un idéal primitif.

Nous définirons la sommes de deux idéaux comme étant l'ensemble

$$\mathfrak{c} = \mathfrak{a} + \mathfrak{b} = \{\alpha + \beta\} \quad \text{où } \alpha \in \mathfrak{a}, \quad \beta \in \mathfrak{b}. \tag{1.22}$$

On peut aisément voir que $\mathfrak{c}$ est un idéal. De plus l'addition d'idéaux est commutative, — $\mathfrak{a}+\mathfrak{b} = \mathfrak{b}+\mathfrak{a}$,— et associative,— $\mathfrak{a}+(\mathfrak{b}+\mathfrak{c}) = (\mathfrak{a}+\mathfrak{b})+\mathfrak{c}$. De plus l'inclusion $\mathfrak{a} \subseteq \mathfrak{a} + \mathfrak{b}$ peut-être trivialement vérifiée.

Nous utiliserons la notation $\mathfrak{a} + \mathfrak{b} = (\mathfrak{a}, \mathfrak{b})$. Dans le cas particulier des idéaux principaux, nous utiliserons, si $\mathfrak{a} = (\alpha)$ et $\mathfrak{b} = (\beta)$;

$$\mathfrak{a} + \mathfrak{b} = \begin{cases} (\alpha) + \mathfrak{b} = (\alpha, \mathfrak{b}) \\ (\alpha) + (\beta) = (\alpha, \beta) \end{cases}$$

Finalement l'idéal $(\alpha_1, \alpha_2, \ldots, \alpha_t) = \alpha_1\mathfrak{D}_n + \alpha_2\mathfrak{D}_n + \cdots + \alpha_t\mathfrak{D}_n$.

L'idéal $\mathfrak{a} = (\alpha, \beta)$ peut être vu comme un module ayant pour base $[\alpha, \beta]$ où les coefficients sont pris sur $\mathfrak{D}_n$. Donc, naturellement, si le module $\mathfrak{M} = [\alpha, \beta]$ est un idéal, alors (α, β) constitue le même idéal.

Nous définirons la multiplication d'idéaux $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$ comme étant l'ensemble de toutes les combinaisons linéaires finies possibles de multiples d'éléments pris sur $\mathfrak{a}$ avec des éléments de $\mathfrak{b}$ où les coefficients sont pris sur l'anneau d'intégrité où sont définis $\mathfrak{a}$ et $\mathfrak{b}$. En notation mathématique si $\alpha_i \in \mathfrak{a} \subseteq \mathfrak{D}_n$, $\beta_j \in \mathfrak{b} \subseteq \mathfrak{D}_n$ et $\eta_{i,j} \in \mathfrak{D}_n$ alors

$$\mathfrak{c} = \left\{ \sum_{i=1}^{q} \sum_{j=1}^{r} \eta_{i,j}\alpha_i\beta_j \right\} \tag{1.23}$$

Cette définition émerge de la théorie des ensembles et est totalement indépendante de la base des idéaux considérés. Dans le cas qui nous concerne nous pouvons utiliser une autre définition pour des idéaux quadratiques. Si $\mathfrak{a} = (\alpha_1, \alpha_2)$ et $\mathfrak{b} = (\beta_1, \beta_2)$ alors

$$\mathfrak{c} = \mathfrak{a}\mathfrak{b} = (\alpha_1\beta_1, \alpha_1\beta_2, \alpha_2\beta_1, \alpha_2\beta_2) \tag{1.24}$$

La réduction de système de générateurs à une base de 2 éléments n'est pas une tâche triviale. Nous donnerons plus loin, à la section 3.2, un algorithme permettant de multiplier 2 idéaux réduits (un concept définit plus loin) et de récupérer une base canonique.

Évidement, l'équation (1.24) nous permet de voir, que pour deux idéaux principaux, $\mathfrak{a} = (\alpha)$ et $\mathfrak{b} = (\beta)$ leur multiplication $\mathfrak{c} = \mathfrak{a}\mathfrak{b} = (\alpha\beta)$ est un idéal principal. Nous pouvons, de plus, aisément prouver que la multiplication d'idéaux est commutative, associative et distributive sur l'addition d'idéaux,— $\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) = \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c}$.

Lemme 1.7.3.1 *Si l'idéal primitif $\mathfrak{a}$ a pour base $[a, b + \omega_n]$, alors toutes les bases $[a, \pm(na + b + \omega_n)]$, où $n \in \mathbb{Z}$, génèrent aussi l'idéal $\mathfrak{a}$.*

Nous dirons qu'un idéal $\mathfrak{a} = [a, b + \omega_n] \subseteq \mathfrak{O}_n$ est **réduit** si et seulement si il est primitif et qu'il n'existe pas d'$\alpha \in \mathfrak{a}$ tel que les deux affirmations suivantes soient vrais simultanément : $|\alpha| < L(\mathfrak{a})$ et $|\bar{\alpha}| < L(\mathfrak{a})$.

Théorème 1.7.4 *$\mathfrak{a} \subseteq \mathfrak{O}_n$ est un idéal réduit si et seulement si il existe un $\beta \in \mathfrak{a}$ tel que $\mathfrak{a} = [a, \beta]$ et que β respecte les deux conditions suivantes : $\beta > a$ et $-a < \bar{\beta} < 0$.*

Démonstration :

Supposons qu'$\mathfrak{a} = [a, \gamma]$ soit un idéal réduit où $a = L(\mathfrak{a})$. Il existe certainement une infinité de paires (x, y), où x et $y \in \mathbb{Z}$, telles que $|xa + y\bar{\gamma}| < a$. Ceci est évident puisque pour l'unité fondamentale ϵ, ϵ^{-1} est inférieur à 1. Il existe donc un $n_0 > 0$ tel que pour une paire quelconque (r, s), $|\epsilon^{-n}||ra + s\bar{\gamma}| < a$ et ce pour tout $n > n_0$.

Choisissons l'une de ces paires $v = ra + s\gamma$ et considérons tous les éléments qui répondent simultanément aux conditions $|xa + y\gamma| < v$ et $|xa + y\bar{\gamma}| < a$. Nous pouvons facilement visualiser ceci en utilisant la représentation des treillis quadratiques décrite à la page 18. Les 2 conditions réunies demandent qu'un point du treillis soit à l'intérieur d'une boîte ayant une surface de $4a|v|$ unités carrés et centrée à l'origine du plan. Mais par les propriétés d'un treillis, seulement un nombre fini de point du treillis peuvent exister dans une boîte finie.

Soit $\beta > 0$, un tel point, tel que β soit minimal parmi tous ces points. Puisque $|\bar{\beta}| < a$ et qu'$\mathfrak{a}$ est réduit, alors nécessairement $\beta > a$. On peut donc écrire $0 < \beta - a < \beta$, ce qui implique que $|\overline{\beta - a}| = |\bar{\beta} - a| > |a| > |\bar{\beta}|$, sinon, nous aurions un élément plus petit que β qui répondrais aux mêmes conditions que β, ce qui contredirait la minimalité de β. Cette dernière équation implique que $\bar{\beta}$ et a n'ont pas le même signe et donc que $\bar{\beta} < 0$.

Il ne reste plus qu'à prouver ici que $[a, \beta]$ forme une base équivalente à $[a, \gamma]$. Soient p et $q \in \mathbb{Z}$ tels que $\beta = pa + q\gamma$. Si $|q| > 1$, alors soit s tel que $p \equiv s \pmod{|q|}$, où $|s| \leq |q|/2$. Alors $(\beta - sa)/q = \gamma + xa$ pour x un entier rationnel. Si $|\mu| = |(\beta - sa)/q| \in \mathfrak{a}$, nous pouvons donc écrire la chaîne d'inégalités suivante : $|\bar{\mu}| = |(\bar{\beta} - sa)/q| \leq |\bar{\beta}/q| + |sa/q| \leq a/2 + a/2 = a$. Donc $|\bar{\mu}| < a$. Par définition $\mu > 0$ et en écrivant la chaîne d'inégalités $\mu \leq |\beta/q| + |sa/q| \leq \beta/2 + a/2 < \beta$, nous arrivons à la conclusion que μ possède les mêmes caractéristiques que β tout en étant plus petit que β, contredisant du même coup l'hypothèse de minimalité de β. En conclusion $|q| \leq 1$ et donc étant donné que q ne peut pas être égal à 0, $q = \pm 1$, et par le lemme 1.7.3.1, $[a, \gamma] = [a, \beta]$.

À l'inverse, supposons qu'$\mathfrak{a} = [a, \beta]$, où $a = L(\mathfrak{a})$ et $\beta > a$ et $-a < \bar{\beta} < 0$. Si $\mathfrak{a}$ n'est pas un idéal réduit, alors il doit exister un $\rho \neq 0 \in \mathfrak{a}$, tel que $|\rho| < a$ et $|\bar{\rho}| < a$. Soient x et y tels que $\rho = xa + y\beta$. Nous pouvons donc réécrire : $|xa + y\beta| < a$ et $|xa + y\bar{\beta}| < a$. Nous constatons immédiatement, par la première inégalité, que si $x = 0$ alors $y = 0$ ainsi que si $y = 0$ alors $x = 0$; donc $xy \neq 0$. Si $xy > 0$, alors il peut être vérifiée que la première inégalité ne peut être satisfaite. Si $xy < 0$, alors cette fois-ci c'est la seconde inégalité qui ne peut être satisfaite. Nous concluons donc que ρ ne peut exister et qu'$\mathfrak{a}$ est un idéal réduit. *CQFD.*

Corollaire 1.7.4.1 *Si $\mathfrak{a}$ est un idéal réduit sur $\mathfrak{D}_n$ alors $L(\mathfrak{a}) < \sqrt{\Delta_n}$.*

Démonstration :

Du corollaire précédent nous savons qu'$\mathfrak{a} = [a, \beta]$, où $\beta > a$ et $-a < \bar{\beta} < 0$. Donc $a < \beta - \bar{\beta} = \omega_n - \bar{\omega}_n = \sqrt{\Delta_n}$. *CQFD*

Nous déduisons du théorème précédent qu'il n'existe qu'un nombre fini d'idéaux réduit sur $\mathfrak{D}_n$, puisqu'il n'existe qu'un nombre fini de a possibles et que les b possibles dans la base $[a, b + \omega_n]$ sont compris entre 0 et a.

Théorème 1.7.5 *Si $\mathfrak{a} = [a, \gamma] \subseteq \mathfrak{D}_n$ est un idéal primitif et que $L(\mathfrak{a}) < \sqrt{\Delta_n}/2$, alors $\mathfrak{a}$ est un idéal réduit sur $\mathfrak{D}_n$.*

Démonstration :

Définissons β comme étant égal à $\gamma + \lfloor -\bar{\gamma}/a \rfloor\, a$. Alors, par le lemme 1.7.3.1 $\mathfrak{a} = [a, \beta]$. De plus en réécrivant $\bar{\beta} = (\bar{\gamma}/a + \lfloor -\bar{\gamma}/a \rfloor)a$, nous nous apercevons aisément que $-a < \bar{\beta} < 0$. Sachant que $\beta - \bar{\beta} = \omega_n - \bar{\omega_n}$, il peut être écrit, $\beta > \omega_n - \bar{\omega}_n - a$. De plus les conditions du théorèmes imposent qu'$\omega_n - \bar{\omega}_n = \sqrt{\Delta_n} > 2a$. Donc $\beta > a$.

Nous pouvons donc, en appliquant le théorème 1.7.4, conclure qu'$\mathfrak{a}$ est un idéal réduit. *CQFD*

Pour terminer cette section, nous donnerons quelques résultats en vrac. Nous n'en donnerons pas les démonstrations qui peuvent toutes trouvées dans [9]. Ces résultats sont utiles afin de développer une intuition plus grandes des idéaux et servirons plus tard à accélérer certaines preuves.

Nous dirons que l'idéal $\mathfrak{c}$ divise l'idéal $\mathfrak{a}$ s'il existe un idéal $\mathfrak{b}$ tel que $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$.

Théorème 1.7.6 *L'idéal $\mathfrak{a}$ divise l'idéal $\mathfrak{b}$ si et seulement si $\mathfrak{b} \subseteq \mathfrak{a}$.*

Théorème 1.7.7 *Si $\mathfrak{b} = (\beta)$ est un idéal qui divise l'idéal $\mathfrak{a}$, alors pour tout $\alpha \in \mathfrak{a}$ $\beta|\alpha$.*

L'idéal conjugué $\bar{\mathfrak{a}}$ de $\mathfrak{a}$ est défini comme étant $\bar{\mathfrak{a}} = \{\bar{\alpha}\}$ pour tous les $\alpha \in \mathfrak{a}$. Alors $\bar{\mathfrak{a}}$ est un idéal.

Lemme 1.7.7.1 *Si $\mathfrak{a} = [L(a), \gamma]$ est un idéal, alors $\mathfrak{a}\bar{\mathfrak{a}} = (N(\mathfrak{a})) = (N(L(a)))$.*

Théorème 1.7.8 *Si $\mathfrak{a}$ et $\mathfrak{b}$ sont des idéaux, alors $N(\mathfrak{a})N(\mathfrak{b}) = N(\mathfrak{a}\mathfrak{b})$.*

Théorème 1.7.9 *Si $\mathfrak{a} = (\alpha)$ est un idéal principal, alors $N(\mathfrak{a}) = |N(\alpha)|$.*

Particulièrement, si $\alpha \in \mathbb{Z}$ alors $N(\mathfrak{a}) = \alpha^2$.

1.7.1 Classe d'idéaux

Nous dirons que deux idéaux, $\mathfrak{a}$ et $\mathfrak{b}$, appartenant à $\mathfrak{O}_n$ sont **équivalents** s'il existe des entiers α et β tous deux appartenant à $\mathfrak{O}_n$ tels que

$$\mathfrak{a}(\alpha) = \mathfrak{b}(\beta). \tag{1.25}$$

Nous écrirons alors : $\mathfrak{a} \sim \mathfrak{b}$.

Cette relation est évidement transitive, réflexive et symétrique. Chaque idéal $\mathfrak{a}$ appartient à une classe d'équivalence que nous noterons $\mathbf{A} = \mathring{\mathfrak{a}}$, où $\mathring{\mathfrak{a}}$ est la classe d'équivalence de $\mathfrak{a}$. Nous définirons ensuite le produits de classes d'équivalences comme étant le produit de membres représentatifs. Ou, si $\mathbf{C} = \mathbf{AB}$, alors $\mathbf{C} = \mathring{\mathfrak{c}}$ où $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$. Il est évident que l'unité sur ce groupe est l'ensemble de tous les idéaux principaux.

Lemme 1.7.9.1 *Si* $\mathfrak{a}$ *et* $\mathfrak{b}$ *sont deux idéaux équivalents appartenant à* $\mathfrak{D}_n$*, alors il existe un* $\gamma \in \mathfrak{a}$ *tel que*

$$(\gamma)\mathfrak{b} = (L(\mathfrak{b}))\mathfrak{a}$$

où $0 < \gamma < L(a)$.

Chapitre 2

Fractions continues

2.1 Fractions continues finies

Une **fraction continue** est une expression de la forme

$$\phi = a_0 + \cfrac{1}{a_1 \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots + \cfrac{1}{a_t}}}}$$

où $a_o, a_1, \ldots, a_t \in \mathbb{Z}$.

Nous utiliserons la notation

$$\phi = [a_0, a_1, a_2, \ldots, a_t]$$

où $a_0, a_1, \ldots, a_t$ sont appelés **quotients incomplets** de la fraction continue.

Trivialement

- $[a_0] = \frac{a_0}{1}$,
- $[a_0, a_1] = \frac{a_0 a_1 + 1}{a_0}$ et
- $[a_0, a_1, a_2] = \frac{a_2 a_1 a_0 + a_2 + a_0}{a_2 a_1 + 1}$.

De plus

$$[a_0, a_1] = a_0 + \frac{1}{a_1},$$

$$[a_0, a_1, a_2, \ldots, a_{t-1}, a_t] = [a_0, a_1, a_2, \ldots, a_{t-2}, a_{t-1} + \frac{1}{a_t}] \text{ et}$$

$$[a_0, a_1, a_2, \ldots, a_{t-1}, a_t] = a_0 + \frac{1}{[a_1, a_2, \ldots, a_{t-1}, a_t]} = [a_0, [a_1, a_2, \ldots, a_{t-1}, a_t]].$$

Plus généralement

$$[a_0, a_1, a_2, \ldots, a_{t-1}, a_t] = [a_0, a_1, \ldots, a_{m-1}, [a_m, a_{m+1}, \ldots, a_t]]. \tag{2.1}$$

2.2 Réduites

Nous appellerons le nombre rationnel

$$[a_0, a_1, \ldots, a_n] \qquad (0 \leq n \leq t)$$

la **réduite** d'ordre n de $[a_0, a_1, \ldots, a_t]$

Théorème 2.2.1 *Si A_n et B_n sont ainsi définis :*

$$\begin{array}{lll} A_0 = a_0, & A_1 = a_1 a_0 + 1, & A_n = a_n A_{n-1} + A_{n-2} \quad (2 \leq n \leq t), \\ B_0 = 1, & B_1 = a_1, & B_n = a_n B_{n-1} + B_{n-2} \quad (2 \leq n \leq t), \end{array}$$

alors

$$[a_0, a_1, \ldots, a_n] = \frac{A_n}{B_n}.$$

Théorème 2.2.2 *A_n et B_n ont les propriétés suivantes*

1. $A_n B_{n-1} - A_{n-1} B_n = (-1)^{n-1}$;
2. $A_n B_{n-2} - A_{n-2} B_n = (-1)^n a_n$;
3. $B_n \geq B_{n-1} \quad \forall n \geq 1$, *avec inégalité pour* $n > 1$;
4. $B_n \geq n$, *avec inégalité pour* $n > 3$;
5. $B_n \geq \Phi^{n-1}$ *où* $\Phi = \frac{1+\sqrt{5}}{2}$.

2.3 Assignation de valeurs

Si $\phi = [a_0, a_1, \ldots, a_{t-1}, a_t]$, alors on peut exiger qu'$a_i > 0, \forall i > 1$. Nous appellerons ϕ_i la quantité $[a_i, a_{i+1}, \ldots, a_{t-1}, a_t]$.
Donc trivialement $\phi_0 = [a_0, a_1, \ldots, a_{t-1}, a_t] = \phi$ et $\phi_i > 1$. Si $x_n = \frac{A_n}{B_n}$, alors $\phi = x_n$.

Théorème 2.3.1

$$\phi_{i+1} = \frac{1}{(\phi_i - \lfloor \phi_i \rfloor)}$$

et

$$a_i = \lfloor \phi_i \rfloor.$$

2.4 Caractéristiques diverses des fractions continues

2.4.1 Différence entre les réduites et le nombre à approximer

Théorème 2.4.1 *Si $n \geq 0$, alors*

$$\left| x - \frac{A_n}{B_n} \right| \leq \frac{1}{B_n B_{n+1}} \leq \frac{1}{B_n^2} \leq \frac{1}{\Phi^{2(n-1)}}.$$

Théorème 2.4.2 *Si*

$$\left| \frac{p}{q} - x \right| \leq \frac{1}{2q^2}, \tag{2.2}$$

alors, p/q est une réduite de x.

2.4.2 Fractions continues périodiques

Si $\phi \in \mathbb{Q}$ alors $\phi = [a_0, a_1, a_2, \ldots, a_t]$ et t est fini. Une fraction continue infinie représente toujours un nombre irrationnel. Si ϕ est de la forme $\frac{a+b\sqrt{D}}{c}$ où $a, b, c \in \mathbb{Z}$ et $D \geq 0$ alors la fraction continue le représentant est périodique. C'est à dire qu'$a_l = a_{l+k}$ pour tout $l \geq L$ et un k fixe appelé période de la fraction continue. La suite $a_L, a_{L+1}, \ldots, a_{L+k-1}$ forme la période de la fraction continue. La fraction peut être écrite ainsi

$$\phi_i = \begin{cases} [a_i, a_{i+1}, \ldots, \dot{a}_L, \dot{a}_{L+1}, \ldots, \dot{a}_{L+k-1}] & \text{pour } i < L, \\ [\dot{a}_i, \dot{a}_{i+1}, \ldots, \dot{a}_{i+k-1}] & \text{pour } i \geq L. \end{cases}$$

Si ϕ est représenté par une fraction continue périodique alors $\phi = \frac{a+b\sqrt{D}}{c}$ où $a, b, c \in \mathbb{Z}$ et $D \geq 0$.

2.4.3 Autres Caractéristiques

Par l'équation (2.1) et la définition des réduites nous pouvons écrire

$$\phi = \phi_0 = \frac{\phi_m A_{m-1} + A_{m-2}}{\phi_m B_{m-1} + B_{m-2}}, \tag{2.3}$$

et donc

$$\phi_m = \frac{A_{m-2} - \phi B_{m-2}}{\phi B_{m-1} - A_{m-1}}. \tag{2.4}$$

Si nous utilisions l'équation (2.4) pour définir ϕ_{m+1} et que nous remplacions ϕ_{m+1} par $(P_{m+1} + \sqrt{D})/Q_{m+1}$ et ϕ_0 par $(P_0 + \sqrt{D})/Q_0$, et qu'après avoir développé le tout, nous réunissions les termes irrationnels en une égalité, nous obtiendrions :

$$G_m = P_{m+1}B_m + Q_{m+1}B_{m-1} = A_m Q_0 - B_m P_0. \tag{2.5}$$

Cette expressions nous sera utile pour simplifier certain calculs.

2.5 Fraction continue d'un entier quadratique

Soit l'entier quadratique $\phi = \frac{P+\sqrt{D}}{Q}$, où P et $Q \in \mathbb{Z}$. Dans le développement en fraction continue de ϕ, ϕ_i est évidement un entier quadratique, puisque chaque a_i est entier. De plus ϕ_i est de la forme $\frac{P_i+\sqrt{D}}{Q_i}$,où P_i et $Q_i \in \mathbb{Z}$ et peuvent être ainsi calculés :

Théorème 2.5.1 *Si $\phi = \frac{P+\sqrt{D}}{Q}$, $P, Q \in \mathbb{Z}$, est un entier quadratique où $Q|(D- P^2)$ alors $\phi_0 = \phi, P_0 = P$ et $Q_0 = Q$ et $\phi_i = \frac{P_i+\sqrt{D}}{Q_i}$ où*

- $P_{i+1} = q_i Q_i - P_i$,
- $Q_{i+1} = \frac{(D-P_{i+1}^2)}{Q_i}$ *et*
- $q_i = \left\lfloor \frac{(P_i+\sqrt{D})}{Q_i} \right\rfloor$.

Alors

- $P_i, Q_i \in \mathbb{Z}$,

– $Q_i|(D-P_i^2)$.

Démonstration :

Procédons par récurrence. Le cas de base, $i=0$, s'avère être vrai trivialement puisqu'il s'agit des conditions mêmes du théorème.

Supposons que pour tous les $0 \leq i \leq j$, $P_i, Q_i(\neq 0) \in \mathbb{Z}$, que $Q_i|(D-P_i^2)$ et que $\phi_i = (P_i+\sqrt{D})/Q_i$. Alors
$$P_{i+1} = q_iQ_i - P_i \in \mathbb{Z}.$$
De plus

$$\begin{aligned} Q_{i+1} &= (D-P_{i+1}^2)/Q_i \\ &= (D-(q_iQ_i-P_i)^2)/Q_i \\ &= (D-P_i^2)/Q_i + 2q_iP_i - q_i^2Q_i \in \mathbb{Z}. \end{aligned}$$

Étant donné que D n'est pas un carré parfait, $D-P_{i+1}^2 \neq 0$, et donc
$$Q_{i+1} = (D-P_{i+1}^2)/Q_i \neq 0.$$
Finalement

$$\begin{aligned} \phi_{i+1} &= \frac{1}{(\phi_i - \lfloor \phi_i \rfloor)} = \frac{1}{\frac{P_i+\sqrt{D}}{Q_i} - q_i} = \frac{Q_i}{P_i - q_iQ_i + \sqrt{D}} \\ &= \frac{Q_i}{-P_{i+1}+\sqrt{D}} = \frac{Q_i(P_{i+1}+\sqrt{D})}{D-P_{i+1}^2} = \frac{P_{i+1}+\sqrt{D}}{Q_{i+1}} = \phi_{i+1}. \end{aligned}$$

CQFD.

Si $Q \not| (D-P^2)$ alors nous pouvons remplacer Q par $|Q|Q$, P par $|Q|P$ et D par Q^2D.

Le résultat suivant peut être utilisé afin que tous les calculs soient effectués sur $\mathbb{Q}$.

Théorème 2.5.2
$$q_i = \begin{cases} \left\lfloor \frac{P_i + \lfloor \sqrt{D} \rfloor}{Q_i} \right\rfloor & si\ Q_i > 0, \\ \left\lfloor \frac{P_i + 1 + \lfloor \sqrt{D} \rfloor}{Q_i} \right\rfloor & si\ Q_i < 0. \end{cases}$$

Donc $\left\lfloor \sqrt{D} \right\rfloor$ n'a à être calculé qu'une seule fois.

Soit $\psi_m = \frac{\sqrt{D}-P_m}{Q_{m-1}}$. Alors$\frac{(\sqrt{D}-P_m)(\sqrt{D}+P_m)}{Q_{m-1}(\sqrt{D}+P_m)} = \frac{D-P_m^2}{Q_{m-1}(\sqrt{D}+P_m)} = \frac{Q_m}{\sqrt{D}+P_m} = 1/\phi_m$. Évidement $0 < \psi_m < 1$.

Soit la fonction θ_m ainsi définie :

$$\theta_1 = 1, \quad \theta_k = \prod_{i=1}^{k-1} \psi_i \quad (k > 1). \tag{2.6}$$

Alors trivialement, $\theta_2 = \psi_1, \theta_3 = \psi_1\psi_2 \ldots$ et

$$\theta_m < \theta_{m-1} \quad \text{ou} \quad \theta_{m-1}^{-1} > \theta_m^{-1}. \tag{2.7}$$

Théorème 2.5.3

$$N(\theta_k) = \frac{(-1)^{k-1}Q_{k-1}}{Q_0} \qquad et \tag{2.8}$$

$$\theta_k = (-1)^{k-1}(A_{k-2} - \phi B_{k-2}). \tag{2.9}$$

Démonstration :

Par le théorème 2.5.1 nous savons que $Q_{i+1} = \frac{(D-P_{i+1}^2)}{Q_i}$. Utilisé conjointement avec (2.6), l'équation (2.8) peut être prouvée par récurrence.

CAS DE BASE : $k = 2$.

$\theta_2 = \psi_1 = \frac{\sqrt{D}-P_1}{Q_0}$.

$N(\theta_2) = \frac{\sqrt{D}-P_1}{Q_0}\frac{-\sqrt{D}-P_1}{Q_0} = -\frac{D-P_1^2}{Q_0^2} = -\frac{Q_1}{Q_0} = (-1)^{2-1}\frac{Q_1}{Q_0}$.

RÉCURRENCE :

Supposons maintenant que (2.8) soit vrai pour tous les $j \geq 2$ et inférieurs à k.

Alors, étant donné la propriété multiplicative des normes, $N(\theta_k) = N(\theta_{k-1})N(\psi_{k-1})$.

$N(\theta_{k-1}) = \frac{(-1)^{k-2}Q_{k-2}}{Q_0}$ par hypothèse et $N(\psi_{k-1}) = -\frac{D-P_{k-1}^2}{Q_{k-2}^2} = -\frac{Q_{k-1}}{Q_{k-2}}$.

Donc $N(\theta_k) = \frac{(-1)^{k-2}Q_{k-2}}{Q_0}(-\frac{Q_{k-1}}{Q_{k-2}}) = \frac{(-1)^{k-1}Q_{k-1}}{Q_0}$.

La seconde partie du théorème 2.5.3 se prouve aussi par récurrence en utilisant l'équation (2.4). *CQFD.*

En remplaçant ϕ_0 par $(P_0 + \sqrt{D})/Q_0$ dans l'équation (2.9) et en utilisant l'équation 2.5, nous obtenons :

$$\begin{aligned} \theta_k =& (-1)^{k-1}\frac{(A_{k-2}Q_0 - P_0B_{k-2} - \sqrt{D}B_{k-2})}{Q_0} \\ =& (-1)^{k-1}\frac{G_{m-2} - \sqrt{D}B_{k-2}}{Q_0}. \end{aligned} \tag{2.10}$$

Étant donné que G_m peut être exprimé à l'aide de termes n'appartenant qu'au dénominateur de réduites de différents ordres, nous avons ainsi éliminé, dans l'expression pour θ_k, tous les termes A_i des réduites, ce qui simplifiera les calculs. Nous pouvons donner encore une autre expression pour θ_k. En remarquant que $\theta_{k+2} = \psi_{k+1}\psi_k\theta_k$, ainsi que l'identité $\psi_{k+1}\psi_k = -q_k\psi_k + 1$, alors nous pouvons écrire les récurrences suivantes :

$$\theta_{k+2} = -q_k\theta_{k+1} + \theta_k, \quad \theta_{k+2}^{-1} = q_k\theta_{k+1}^{-1} + \theta_k^{-1}. \tag{2.11}$$

Pour les quelques théorèmes suivants, nous nous intéresserons au signe de $\bar{\phi}_m$.

Théorème 2.5.4 *Pour tout $m \geq 1$, $\bar{\phi}_m < 0$ si et seulement si $P_m < \sqrt{D}$ et $Q_m > 0$.*

Démonstration :

Trivialement, lorsque $P_m < \sqrt{D}$ et $Q_m > 0$ alors $\bar{\phi}_m = (P_m - \sqrt{D})/Q_m < 0$.

Par contre si $\bar{\phi}_m < 0$. Étant donné que $\phi_m > 1$, nous savons que $2\sqrt{D}/Q_m = \phi_m - \bar{\phi}_m > 0$. Ceci impose donc à Q_m d'être positif et à P_m d'être inférieur à $\sqrt{D}$. *CQFD.*

Nous noterons au passage qu'étant donné que $\phi_m > 1$, nous pouvons écrire $P_m > Q_m - \sqrt{D} > -\sqrt{D}$. Donc, lorsque $\bar{\phi}_m < 0$, on a $|P_m| < \sqrt{D}$ et $0 < Q_m < P_m + \sqrt{D} < 2\sqrt{D}$.

Théorème 2.5.5 *Pour tout* $m \geq 2$, *si* $\left|\phi_o - \bar{\phi}_0\right| > 1/B_{m-1}B_{m-2}$, *alors* $\bar{\phi}_m < 0$.

Démonstration :

Par l'équation (2.3), nous savons que :

$$\begin{aligned}
\phi_0 &= \frac{\phi_m A_{m-1} + A_{m-2}}{\phi_m B_{m-1} + B_{m-2}} \\
&= \frac{\phi_m A_{m-1} B_{m-1} + A_{m-2} B_{m-1}}{B_{m-1}(\phi_m B_{m-1} + B_{m-2})} \\
&= \frac{\phi_m A_{m-1} B_{m-1} + A_{m-2} B_{m-1} + A_{m-1} B_{m-2} - A_{m-1} B_{m-2}}{B_{m-1}(\phi_m B_{m-1} + B_{m-2})} \\
&= \frac{\phi_m A_{m-1} B_{m-1} + A_{m-1} B_{m-2}}{B_{m-1}(\phi_m B_{m-1} + B_{m-2})} - \frac{A_{m-1} B_{m-2} - A_{m-2} B_{m-1}}{B_{m-1}(\phi_m B_{m-1} + B_{m-2})} \\
&= \frac{A_{m-1}}{B_{m-1}} + \frac{(1)^{m-1}}{B_{m-1}(\phi_m B_{m-1} + B_{m-2})}.
\end{aligned}$$

Pour obtenir la dernière égalité, il faut utiliser la première propriété du théorème 2.2.2. Nous pouvons donc écrire :

$$(-1)^m(\phi_0 - \bar{\phi}_0) = \frac{1}{B_{m-1}(\bar{\phi}_m B_{m-1} + B_{m-2})} - \frac{1}{B_{m-1}(\phi_m B_{m-1} + B_{m-2})}.$$

Donc si $\bar{\phi}_m > 0$, alors

$$\begin{aligned}
\left|\phi_0 - \bar{\phi}_0\right| &< \max\left\{\frac{1}{B_{m-1}(\bar{\phi}_m B_{m-1} + B_{m-2})}, \frac{1}{B_{m-1}(\phi_m B_{m-1} + B_{m-2})}\right\} \\
&< \frac{1}{B_{m-1}B_{m-2}}.
\end{aligned}$$

CQFD.

Corollaire 2.5.5.1 *Si, pour tout* $m > 2$, $B_{m-2}^2 > \left|Q_0/2\sqrt{D}\right|$, *alors* $\bar{\phi}_m < 0$.

Démonstration :

Nous savons que $|\phi_0 - \bar{\phi}_0| = 2\sqrt{D}/|Q_0| > B_{m-2}^{-2} > 1/B_{m-2}B_{m-1}$. *CQFD.*

Corollaire 2.5.5.2 *Si* $m > \max[1, 3 + \log(|Q_0|/2\sqrt{D})/(2\log\Phi)]$, *alors* $\bar{\phi}_m < 0$.

Démonstration :

Si $m > 3 + \log(|Q_0|/2\sqrt{D})/(2\log\tau)$, alors ceci implique que $\tau^{2(m-3)} > |Q_0|/2\sqrt{D}$. Par la dernière expression du théorème 2.2.2 nous pouvons conclure que $B_{m-2}^2 > \tau^{2(m-3)} > \left|Q_0/2\sqrt{D}\right|$ et $m \geq 2$. Nous pouvons donc appliquer le corollaire 2.5.5.2 et obtenir le résultat escompté. *CQFD.*

Chapitre 3

Entiers quadratiques et idéaux quadratiques

3.1 Lien entre les deux concepts

Dans ce chapitre, nous ferons le lien entre la section sur les idéaux (section (1.7)) et le chapitre précédent sur les fractions continues. Nous y décrirons comment un idéal peut être représenté par un nombre quadratique, et vice versa. En utilisant les propriétés des fractions continues et celles des idéaux, nous montrerons toute une série de nouvelles propriétés des idéaux et des nombres quadratiques.

Définissons la valeur σ comme étant égale à 1 si $D_0 \not\equiv 1 \pmod 4$ et à 2 autrement. Alors l'ω_0 de l'équation (1.6) peut se réécrire ainsi :

$$\omega_0 = \frac{\sigma - 1 + \sqrt{D_0}}{\sigma}.$$

Ainsi nous pourrons traiter toutes les congruences possibles de D_0 d'un seul coup.

Soit l'idéal $\mathfrak{a} = [a, b + \omega_n]$, nous pouvons associer à cet idéal un nombre quadratique $(P + \sqrt{D})/Q$ tel que $Q = a\sigma$ et $P = b\sigma + \sigma - 1$. Alors $\mathfrak{a}$ peut être ainsi réécrit :

$$\mathfrak{a} = \left[\frac{Q}{\sigma}, \frac{P + \sqrt{D}}{\sigma}\right] \tag{3.1}$$

où P et Q sont des entiers rationnels, $\sigma | Q$ et $\sigma Q | (D - P^2)$. La dernière propriété est facile à comprendre si nous nous souvenons qu'$a | N(b + \omega_n) = -(D - P^2)/\sigma^2$. Donc, à tout idéal primitif nous pouvons associer une paire d'entiers rationnels (P, Q). Trivialement, l'idéal (1) est associé à $(\sigma - 1, \sigma)$.

À l'inverse, soient P et $Q \in \mathbb{Z}$ tels que $\sigma | Q$ et $\sigma Q | (D - P^2)$ alors le module $[Q/\sigma, (P + \sqrt{D})/\sigma]$ constitue un idéal ayant pour base $[a, b + \omega_n]$, où $a = Q/\sigma$ et $b = (P + 1 - \sigma)/\sigma$.

Qu'arrive-t'il si nous développons $(P + \sqrt{D})/Q$ en fraction continue ? Les paires (P_i, Q_i) représentent-elles des idéaux primitifs légaux ? C'est ce qu'affirme le théorème suivant qui est d'une importance centrale dans la théorie des idéaux quadratiques ainsi que dans la théorie des formes binaires quadratiques.

Théorème 3.1.1 *Soit $\mathfrak{a}_1 = \mathfrak{a} = [a, b + \omega_n]$ et soient $P_0 = P$ et $Q_0 = Q$, pour P et Q tels que définis plus haut. Si $\phi_{m-1} = \frac{P_{m-1} + \sqrt{D}}{Q_{m-1}}$ est obtenu par le développement en fraction continue de $\phi_0 = \frac{P_0 + \sqrt{D}}{Q_0}$, alors $\mathfrak{a}_m = [Q_{m-1}/\sigma, (P_{m-1} + \sqrt{D})/\sigma]$ est un idéal et*

$$(Q_0 \theta_m)\mathfrak{a}_m = (Q_{m-1})\mathfrak{a} \tag{3.2}$$

où θ_m est défini par l'équation (2.6)

Démonstration :

À l'aide d'une preuve similaire à celle du théorème 2.5.1 il peut aisément être démontré que le module $\mathfrak{a}_m$ est un idéal.

À l'aide de l'équation (2.9) du théorème 2.5.3 nous pouvons écrire

$$\begin{pmatrix} \theta_m \\ \theta_{m+1} \end{pmatrix} = X_m \begin{pmatrix} 1 \\ \phi_0 \end{pmatrix},$$

où

$$X_m = (-1)^m \begin{pmatrix} -A_{m-2} & B_{m-2} \\ A_{m-1} & -B_{m-1} \end{pmatrix}$$

et, par la première propriété du théorème 2.2.2 $|X| = \pm 1$. Nous pouvons donc écrire l'égalité de module suivante :

$$(\theta_m)[1, \psi_m] = [\theta_m, \theta_{m+1}] = [1, \phi_0]. \tag{3.3}$$

Remarquons que $(Q_0/\sigma)[1, \phi_0] = \mathfrak{a}_1$. De plus, puisque nous savons que $\psi_m = 1/\phi_m = (\sqrt{D} - P_m)/Q_{m-1}$ et donc $(Q_{m-1}/\sigma)[1, 1/\phi_m] = [Q_{m-1}/\sigma, (\sqrt{D} - P_m)/\sigma]$.

Par définition $P_m = \left\lfloor (P_{m-1} + \sqrt{D}) Q_{m-1} \right\rfloor Q_{m-1} - P_{m-1}$. Nous pouvons donc écrire $(Q_{m-1}/\sigma)[1, 1/\phi_m] = [Q_{m-1}/\sigma, (P_{m-1} - rQ_{m-1} + \sqrt{D})/\sigma]$ où $r \in \mathbb{Z}$. Alors, par le lemme 1.7.3.1, $(Q_{m-1}/\sigma)[1, 1/\phi_m] = \mathfrak{a}_m$.

Nous pouvons maintenant réécrire l'équation (3.3) ainsi

$$(Q_0\theta_m)\mathfrak{a}_m = (Q_{m-1})\mathfrak{a}_m$$

CQFD.

L'équation (3.2) du théorème 3.1.1 peut être ainsi reformulée :

$$(L(\mathfrak{a}_1)\theta_m)\mathfrak{a}_m = (L(\mathfrak{a}_m))\mathfrak{a}_1 \tag{3.4}$$

Corollaire 3.1.1.1 *Si $\mathfrak{a}_i$ est un idéal réduit obtenu par développement en fraction continue d'un idéal $\mathfrak{a}_j$ réduit, où $i \geq j$ alors*

$$\mathfrak{a}_i = \bar{\psi}_{i-1}\mathfrak{a}_{i-1} \tag{3.5}$$

et

$$\mathfrak{a}_i = \left(\frac{\bar{\theta}_i}{\bar{\theta}_j}\right)\mathfrak{a}_j. \tag{3.6}$$

Théorème 3.1.2 *Si $\bar{\phi}_m < 0$, alors $\mathfrak{a}_{m+1}$ est un idéal réduit.*

Démonstration :

Soit $\gamma = |P_m + \sqrt{D}|/\sigma$. Étant donné que $\phi_m > 1$, nous savons donc que $\gamma > |Q_m/\sigma| = L(\mathfrak{a}_{m+1})$. Par définition, nous pouvons écrire que $N(\gamma) = \phi_m\bar{\phi}_m L(\mathfrak{a}_{m+1})^2 < 0$ et en conclure que $\bar{\gamma} < 0$. Soit

$$\beta = \lfloor -\bar{\gamma}/L(\mathfrak{a}_{m+1}) \rfloor L(\mathfrak{a}_{m+1}) + \gamma.$$

Par le lemme 1.7.3.1 nous pouvons écrire

$$\mathfrak{a}_{m+1} = [L(\mathfrak{a}_{m+1}), \gamma] = [L(\mathfrak{a}_{m+1}), \beta]$$

où $\beta > L(\mathfrak{a}_{m+1})$ et, en utilisant le même truc que dans la preuve du théorème 1.7.5, nous déduisons que $-L(\mathfrak{a}_{m+1}) < \bar{\beta} < 0$. Nous pouvons donc conclure, par le théorème 1.7.4, que l'idéal $\mathfrak{a}_{m+1}$ est un idéal réduit. *CQFD.*

Du théorème précédent et du corollaire 2.5.5.2 nous pouvons aisément conclure le corollaire suivant :

Corollaire 3.1.2.1 *Soit* $\mathfrak{a} = \mathfrak{a}_1 = [Q_0/\sigma, (P_0 + \sqrt{D})/\sigma]$ *un idéal primitif sur* $\mathfrak{D}_n$, *alors pour tout* $m \geq m_0$ *tel que*

$$m_0 > \max[2, 4 + \log(|Q_0|/2\sqrt{D})/(2\log\Phi)],$$

$\mathfrak{a}_m$ *est un idéal réduit.*

Le théorème suivant est important d'un point de vue calculatoire et est donc mentionné ici sans démonstration.

Théorème 3.1.3 *Pour le plus petit* $m \geq 1$, *dans le développement en fraction continue de* $\phi_0 = (P_0 + \sqrt{D})/Q_0$, *tel que* $0 < Q_{m-1} < \sqrt{D}$, $\mathfrak{a}_m$ *est un idéal réduit et*

$$\theta_m^{-1} < \frac{2Q_0}{Q_{m-1}}.$$

Nous avons démontré jusqu'ici que le développement en fraction continue appliqué à un idéal primitif $\mathfrak{a}_1$ quelconque générera éventuellement un idéal réduit $\mathfrak{a}_m$ équivalent à $\mathfrak{a}_1$.

Théorème 3.1.4 *Si* $\mathfrak{a} = \mathfrak{a}_1$ *est un idéal réduit, alors* $-1 < \bar{\phi}_1 < 0$.

Démonstration :

Étant donné qu'$\mathfrak{a}_1$ est réduit, nous savons que $L(\mathfrak{a}_1) = Q_0/\sigma < \sqrt{\Delta} = 2\sqrt{D}/\sigma$,— corollaire 1.7.4.1. Soit $\gamma = L(\mathfrak{a}_1)\psi_1 = (\sqrt{D} - P_1)/\sigma \in \mathfrak{a}_1$. γ pouvant aussi être écrit ainsi, $\gamma = Q_0/(\sigma\phi_1)$, nous déduisons que $0 < \gamma < Q_0/\sigma$, puisque $\phi_i > 1$. Étant donné qu'$\mathfrak{a}_1$ est réduit, cela implique que $|\bar{\gamma}| > Q_0/\sigma$. Sachant que $0 < \sqrt{D} - P_1 < 2\sqrt{D}$ donc $P_1 + \sqrt{D} > 0$ et donc $\bar{\gamma} = (-P_1 - \sqrt{D})/\sigma < -Q_0/\sigma < 0$. Ce qui nous permet de conclure que $\bar{\gamma}/(Q_0/\sigma) = \bar{\psi}_1 < -1$. Sachant que $\bar{\phi}_1 = 1/\bar{\psi}_1$ nous pouvons obtenir le résultat escompté. *CQFD.*

Nous savons, par les commentaires qui suivent le théorème 2.5.4, que $|P_i| < \sqrt{D}$, lorsque $\bar{\phi}_i < 0$. Nous pouvons conclure, par le même raisonnement, que $0 < P_i < \sqrt{D}$ lorsque $-1 < \bar{\phi}_i < 0$.

Les théorèmes 3.1.2, 3.1.4 et le corollaire 3.1.2.1, pris ensemble, nous montrent que le développement en fraction continue d'un idéal quadratique générera éventuellement un idéal quadratique réduit et que tous les idéaux successifs seront, eux aussi, réduits. Le théorème suivant nous apprend, lui, que tous les idéaux réduits d'une classe d'équivalence seront éventuellement engendrés par cette méthode.

Théorème 3.1.5 *Si $\mathfrak{a} = \mathfrak{a}_1$ et $\mathfrak{b}$ sont deux idéaux réduits et équivalents sur $\mathfrak{O}_n$ et que $(\gamma)\mathfrak{b} = (L(\mathfrak{b}))\mathfrak{a}$ où $\gamma \in \mathfrak{a}$ et $0 < \gamma < L(\mathfrak{a})$, alors il existe un $m \geq 1$ tel que $\mathfrak{b} = \mathfrak{a}_m$ et $\theta_m = \gamma/L(\mathfrak{a})$.*

Nous pouvons conclure de cette section que les idéaux principaux réduits forment un cycle, que nous appellerons $\mathcal{R}$, dans lequel nous pouvons nous déplacer en utilisant le développement en fraction continue. De plus chaque idéal $\mathfrak{a}_i$, appartenant à $\mathcal{R}$, a deux voisins bien définis. L'un,— celui de droite $(\mathfrak{a}_{i+1})$,— se calcule en utilisant le développement en fraction continue tel que décrit jusqu'ici, et l'autre,— celui de gauche $(\mathfrak{a}_{i-1})$,— se calcule avec un algorithme similaire mais qui va dans l'autre direction du cycle. Le lemme suivant nous sera utile pour dériver cet algorithme.

Lemme 3.1.5.1 *Si $\mathfrak{a}_1 = \mathfrak{a}$ est un idéal primitif réduit, alors*

$$q_i = \left\lfloor (P_{i+1} + \sqrt{D})/Q_i \right\rfloor .$$

Démonstration :

Étant donné les conditions du théorème, nous savons que $-1 < \bar{\phi}_i < 0$ pour tous les $i \geq 1$. Par définition $\phi_{i+1} = 1/(\phi_i - q_i)$. Nous pouvons donc isoler ϕ_i et conclure que

$$0 < (-1/\bar{\phi}_{i+1}) - q_i < 1.$$

Ceci impose donc à q_i d'être la partie entière de $\bar{\phi}_{i+1}$, puisque $q_i \in \mathbb{N}$. Donc

$$\phi_i = \lfloor (-1/\bar{\phi}_{i+1}) \rfloor = \lfloor -\bar{\psi}_{i+1} \rfloor = \left\lfloor (P_{i+1} + \sqrt{D})/Q_i \right\rfloor .$$

CQFD.

À l'aide de ce lemme, nous pouvons nous apercevoir que le théorème 2.5.1 est parfaitement inversible, dès que nous tombons sur un idéal $\mathfrak{a}_i$ réduit lors du développement en fraction continue. Nous pouvons dès lors calculer, à partir de $\mathfrak{a}_i$, aussi aisément $\mathfrak{a}_{i-1}$ qu'$\mathfrak{a}_{i+1}$, ainsi que toutes les valeurs qui s'y rattachent.

3.2 Composition et multiplication d'idéaux

Nous avons décidé, au chapitre 1, de retarder à plus tard la description d'un algorithme de multiplication d'idéaux. Nous ne donnerons ici qu'un algorithme qui génère la base canonique de la partie primitive résultant de la multiplication de deux idéaux principaux et réduits.

Soit l'idéal $\mathfrak{c} = \mathfrak{a}\mathfrak{b}$ où $\mathfrak{a}$ et $\mathfrak{b}$ sont principaux et réduits. Alors l'idéal $\mathfrak{c}$ est un idéal principal. Il n'est cependant pas nécessairement primitif. Si $\mathfrak{c} = [a_3, b_3 + c_3\omega_n]$, nous savons par le théorème 1.7.2 que $c_3|b_3$ et que $c_3|a_3$. Nous pouvons donc sortir de l'idéal $\mathfrak{c}$ l'idéal principal (c_3). Donc $\mathfrak{a}\mathfrak{b} = [a_4, b_4 + \omega_n](c_3)$. Malheureusement le module $\mathfrak{c}' = [a_4, b_4 + \omega_n]$, où $a_4c_3 = a_3$ et $b_4c_3 = b_3$, n'est peut-être pas un idéal, mais un simple module. S'il s'avérerait être un idéal, il serait un idéal principal. Il nous faut démontrer que le module $\mathfrak{c}'$ est aussi un idéal et nous n'aurons plus qu'à calculer la base canonique $[a_4, b_4 + \omega_n]$.

Nous savons par le théorème 1.7.8 que $N(\mathfrak{a})N(\mathfrak{b}) = N(\mathfrak{c}) = N(\mathfrak{c}')N((c_3))$. Étant donné que $a_3|N(b_3 + c_3\omega_n)$ et que $c_3|b_3$, nous pouvons écrire qu'$a_3|N((b_3/c_3 + \omega_n)c_3)$, ce qui implique qu'$a_3|(c_3^2N(b_4 + \omega_n))$. Maintenant, a_3 est soit égal à c_3 ou $a_3 \not| c_3$,— puisque $a_3|c_3$ et $c_3|a_3 \iff a_3 = c_3$,— ce qui implique, si $a_3 \neq c_3$ qu'$a_3|N(b_4 + \omega_n)$ et donc, par le théorème 1.7.3 et sachant qu'$a_4|a_3$, $a_4|N(b_4 + \omega_n)$ et $\mathfrak{c}'$ constitue un idéal principal. Si $a_3 = c_3$ alors l'idéal $\mathfrak{c}' = [1, b_4 + \omega_n] = [1, \omega_n] = \mathfrak{i}$ et donc, là aussi, $\mathfrak{c}'$ constitue un idéal principal.

Nous savons, par le théorème 1.7.8 et la définition de la norme pour les idéaux primitifs, que $N(\mathfrak{c}) = a_1a_2$ où $a_1 = L(\mathfrak{a})$ et $a_2 = L(\mathfrak{b})$. De plus par le théorème 1.7.9, nous pouvons écrire que $a_1a_2 = N(\mathfrak{c}')c_3^2$. Donc $N(\mathfrak{c}') = L(\mathfrak{c}') = a_4 = a_1a_2/c_3^2$. Il ne nous reste plus qu'à calculer c_3 et b_4

Réécrivons le tout sous la forme décrite au début de ce chapitre. C'est-à-dire : $\mathfrak{a} = [Q_1/\sigma, (P_1 + \sqrt{D})/\sigma]$, $\mathfrak{b} = [Q_2/\sigma, (P_2 + \sqrt{D})/\sigma]$ et $\mathfrak{c}' = [Q_4/\sigma, (P_4 + \sqrt{D})/\sigma]$. L'idéal $\mathfrak{c}$ sera dénoté, lui, par $[a_3/\sigma, (b_3 + c_3\sqrt{D})/\sigma]$ puisqu'il n'est pas nécessairement primitif. Alors,

$$\begin{aligned}
\mathfrak{c} &= [Q_1/\sigma, (P_1 + \sqrt{D})/\sigma][Q_2/\sigma, (P_2 + \sqrt{D})/\sigma] \\
&= \begin{matrix}[Q_1Q_2/\sigma^2, (Q_1P_2 + Q_1\sqrt{D})/\sigma^2, \\ (Q_2P_1 + Q_2\sqrt{D})\sigma^2, (P_1P_2 + D + (P_1 + P_2)\sqrt{D})/\sigma^2]\end{matrix} \\
&= [a_3/\sigma, (b_3 + c_3\sqrt{D})/\sigma] = (c_3)[Q_4/\sigma, (P_4 + \sqrt{D})/\sigma]
\end{aligned} \tag{3.7}$$

Nous pouvons donc écrire que $N(\mathfrak{c}') = Q_4/\sigma = \frac{Q_1Q_2}{\sigma^2c_3^2}$

Étant donné l'équivalence des bases, nous pouvons écrire la combinaison linéaire suivante

$$c_3 = \mu Q_1/\sigma + \eta Q_2/\sigma + \lambda(P_1 + P_2)/\sigma \tag{3.8}$$

où μ, η et $\lambda \in \mathbb{Z}$. Par le théorème 1.4.3, nous devons trouver le coefficient c_3 minimal. Les coefficients μ, η et λ peuvent donc être calculés à l'aide de l'algorithme d'Euclide ; nous nous apercevons immédiatement que $c_3 = \text{pgcd}(Q_1/\sigma, Q_2/\sigma, (P_1 + P_2)/\sigma)$.

Connaissant c_3, nous sommes désormais en mesure de calculer P_4. Naturellement, la même combinaisons linéaire qui a servi à calculer c_3 nous servira à calculer b_3. Donc

$$b_3 = \mu Q_1 P_2/\sigma + \eta Q_2 P_1/\sigma + \lambda(P_1 P_2 + D)/\sigma \tag{3.9}$$

pour les mêmes μ, η et λ qu'à l'équation (3.8). Cependant P_4 n'est pas b_3, mais par définition

$$P_4 \equiv \frac{1}{c_3}(\mu Q_1 P_2/\sigma + \eta Q_2 P_1/\sigma + \lambda(P_1 P_2 + D)/\sigma) \pmod{Q_4} \tag{3.10}$$

Voilà donc une méthode de base pour calculer $\mathfrak{c}'$. Récapitulons le tout :

Théorème 3.2.1 *Soient* $\mathfrak{a}_i = [Q_{i-1}/\sigma, (P_{i-1} + \sqrt{D})/\sigma]$ *et* $\mathfrak{a}_j = [Q_{j-1}/\sigma, (P_{j-1} + \sqrt{D})/\sigma]$ *deux idéaux réduits, alors,* $\mathfrak{a}_i\mathfrak{a}_j = (U)\mathfrak{c}$ *où l'idéal* $\mathfrak{c} = [Q_k/\sigma, (P_k + \sqrt{D})/\sigma]$ *est primitif et peut être calculé ainsi :*

1. *À l'aide de l'algorithme d'Euclide, calculez* x_1, y_1 *et* Y *tels que :*

$$x_1 Q_{i-1}/\sigma + y_1 Q_{j-1}/\sigma = Y = \text{pgcd}(Q_{i-1}/\sigma, Q_{j-1}/\sigma) \tag{3.11}$$

   où x_1, y_1 *et* $Y \in \mathbb{Z}$.

2. *À l'aide de l'algorithme d'Euclide, calculez* x_2, y_2 *et* U *tels que :*

$$x_2(P_{i-1} + P_{j-1})/\sigma + y_2 Y = U = \text{pgcd}((P_{i-1} + P_{j-1})/\sigma, Y) \tag{3.12}$$

   où x_2, y_2 *et* $U \in \mathbb{Z}$

3. *Posez* $Q_k := \frac{Q_{i-1}Q_{j-1}}{\sigma U^2}$

4. *Posez*

$$\begin{aligned} P_k \equiv \frac{1}{U}(y_2 x_1 Q_{i-1} P_{j-1}/\sigma &+ y_2 y_1 Q_{j-1} P_{i-1}/\sigma \\ &+ x_2(P_{i-1}P_{j-1} + D)/\sigma) \pmod{Q_k}. \end{aligned} \tag{3.13}$$

Nous nous apercevons facilement qu'$x_1 y_2 = \mu$, qu'$y_1 y_2 = \eta$ et qu'$x_2 = \lambda$.

Nous pouvons donc réduire l'idéal $\mathfrak{c}$ obtenu à l'aide du développement en fraction continue. Résumons le tout :

Théorème 3.2.2 *Si l'idéal*

$$\mathfrak{c} = \frac{1}{U}\mathfrak{a}_i\mathfrak{a}_j = \left[Q/\sigma, (P+\sqrt{D})/\sigma\right]$$

a été obtenu à l'aide du théorème 3.2.1, alors l'idéal $\mathfrak{a}'_k \sim \mathfrak{a}_1 = \mathfrak{c}$ *est réduit et est obtenu ainsi :*

1. *Soient* $Q'_0 = Q$, $P'_0 = P$, $B_{-2} = 1$ *et* $B_{-1} = 0$.
2. *Calculez* q'_{i-1}, Q'_i, P'_i *tels que prescrit au chapitre 2 ainsi que* $B_{i-1} = q'_{i-1}B_{i-2} + B_{i-3}$ *jusqu'à ce que* $\sigma < Q'_i < \sqrt{D}$.
3. *Calculez* q'_i, Q'_{i+1}, P'_{i+1} *et* B_i.
4. *Définissez*

$$k := i+2,\ \mathfrak{a}'_k := \left[Q'_{k-1}/\sigma, (P'_{k-1}+\sqrt{D})/\sigma\right] \text{ et}$$

$$\theta'_k := (-1)^{k-1}\frac{G_{k-2} - B_{k-2}\sqrt{D}}{Q'_0}.$$

De plus, $0 < P'_{k-1} < \sqrt{D}$, $\sigma < Q'_{k-1} < 2\sqrt{D}$ *et* $i \in \Theta(\log(|Q_0|/2\sqrt{D})/(2\log\Phi))$.

L'étape 3 est nécessaire pour s'assurer que $-1 < \bar{\phi}_{k-1} < 0$, ce qui implique que $0 < P'_{k-1} < \sqrt{D}$.

Lemme 3.2.2.1 *Pour* B_{k-2} *tel que défini au dernier théorème,*

$$B_{k-2} < (q'_{k-2}+1)(Q'_0\sqrt{D}).$$

3.3 La fonction de distance

Nous commencerons cette section par montrer que l'idéal principal $(1) = \mathfrak{i} = \mathfrak{O}_n$ est un idéal réduit. Par définition $\mathfrak{i}$ est réduit si et seulement si aucun $\alpha \in \mathfrak{i}$ n'existe tel que $-1 < \alpha < 1$ et $-1 < \bar{\alpha} < 1$. Supposons au contraire qu'il existe un $\alpha = b + c\omega_n \neq 0 \in \mathfrak{i}$ tel que $-1 < b + c\bar{\omega}_n < 1$ et $-1 < b + c\omega_n < 1$. Supposons, sans perte de généralité, que $(b + c\omega_n) > 0$. Alors, ceci implique

$$-1 < -(b+c\omega_n) < N(b+c\omega_n) < (b+c\omega_n) < 1. \tag{3.14}$$

Mais par le lemme 1.2.0.2, nous savons que la norme de tout entier quadratique est un entier rationnel et qu'elle n'est égale à 0 que si l'entier quadratique est égal à 0. L'équation (3.14) exprime donc une impossibilité et nous en concluons qu'$\mathfrak{i}$ est un idéal réduit.

Par le corollaire 3.1.1.1, tout idéal principal réduit peut donc être exprimé ainsi :

$$\mathfrak{a}_i = (\alpha) = \bar{\theta}_i \mathfrak{i} = \bar{\theta}_i(1) = (\bar{\theta}_i). \tag{3.15}$$

Nous appellerons $\mu_i = |\bar{\theta}_i|$ le générateur de $\mathfrak{a}_i$, ceci simplement pour distinguer la fonction θ et les générateurs d'idéaux principaux.

À chaque idéal principal et réduit, nous pouvons associer un nombre réel que nous appellerons **distance de l'idéal**. Cette distance, que nous noterons δ, sera défini ainsi :

$$\delta_i = \log(\mu_i). \tag{3.16}$$

Cette fonction est, de toute évidence, monotone croissante puisque $-1 < \bar{\phi}_i < 0$, ou $\bar{\psi}_i < -1$, pour les idéaux réduits.

Il peut aussi être aisément démontrées, sachant que $0 < P_i < \sqrt{D}$ ainsi que $\sigma < Q_i < 2\sqrt{D}$, les propriétés suivantes de $\bar{\psi}_i$.

Corollaire 3.3.0.1 *Si $\mathfrak{a}_1 = \mathfrak{i}$, alors $\forall i \geq 1$:*

1. $q_i < |\bar{\psi}_i| < q_i + 1$,
2. $\bar{\psi}_i \bar{\psi}_{i+1} > 2$ *et*
3. $1 + 1/\sqrt{\Delta} < |\bar{\psi}_i| < \sqrt{\Delta}$.

De ce corollaire, nous déduisons que la distance n'augmente que de $\mathcal{O}(\log(D))$ à chaque itération du développement en fraction continue.

Théorème 3.3.1 *Soit $\mathfrak{c} = (1/U)\mathfrak{a}_i\mathfrak{a}_j$, où $\mathfrak{a}_i$ et $\mathfrak{a}_j$ sont deux idéaux principaux et réduits, et soit $\mathfrak{a}'_k$ l'idéal réduit calculé à partir du théorème 3.2.2 où $\mathfrak{a}'_1 = \mathfrak{c}$. Alors $\mathfrak{a}'_k = \mathfrak{a}_m = (\bar{\theta}_m)\mathfrak{i}$, pour $m \geq 1$, et $\delta_m = \delta_i + \delta_j + \varepsilon$, où $|\varepsilon| = (\log(D) + \mathcal{O}(1))$.*

Démonstration :

Souvenons nous premièrement que $G_{k-2} = P'_{k-1}B_{k-2} + Q'_{k-1}B_{k-3}$. Nous savons, par le théorème 3.2.1, que $Q'_0 = Q_{i-1}Q_{j-1}/(\sigma U^2)$, donc

$$\frac{|\bar{\theta}'_k|}{U} = \frac{G_{k-2} + B_{k-2}\sqrt{D}}{Q_{i-1}Q_{j-1}}\sigma U.$$

L'étape 3 du théorème 3.2.2 nous assure que $k \geq 2$, ainsi, nous avons $B_{k-2} > 1$, et donc

$$\frac{|\bar{\theta}'_k|}{U} = \frac{G_{k-2} + B_{k-2}\sqrt{D}}{4D} \geq \frac{1}{4D}$$

puisque $0 < P'_{k-1} < \sqrt{D}$.

De plus étant donné que $\sigma < Q'_{k-1} < 2\sqrt{D}$, alors $G_{k-2} < 3\sqrt{D}B_{k-2}$. Donc, en utilisant le lemme 3.2.2.1,

$$\frac{|\bar{\theta}'_k|}{U} \leq |\bar{\theta}'_k| < \frac{3B_{k-2}\sqrt{D} + B_{k-2}\sqrt{D}}{Q'_0} = \frac{4B_{k-2}\sqrt{D}}{Q'_0} < 4(q'_{k-2} + 1) = \mathcal{O}(D).$$

Posons maintenant qu'$\varepsilon = \log(|\bar{\theta}'_k|/U)$, alors par la dernière équation, $|\varepsilon| = \log(D) + \mathcal{O}(1)$. Si $\mathfrak{a}_i = \mu_i$ et $\mathfrak{a}_j = \mu_j$ et si $\mathfrak{a}_m = \mu_m$, alors $\mathfrak{a}_m = (\bar{\theta}'_k/U)\mathfrak{a}_i\mathfrak{a}_j$. Donc $\mu_m = (|\bar{\theta}'_k|/U)\mu_i\mu_j$.
D'où nous concluons que $\delta_m = \log(\mu_m) = \log((|\bar{\theta}'_k|/U)\mu_i\mu_j) = \varepsilon + \delta_i + \delta_j$. *CQFD*

Nous pouvons aussi définir la distance entre un idéal et un nombre réel positif. Soit $\mathfrak{a}_i$ un idéal réduit et principal et x un nombre réel positif, alors la distance entre l'idéal $\mathfrak{a}_i$ et $x \in \mathbb{R}^+$ sera ainsi définie :

$$\partial(\mathfrak{a}_i, x) = \delta_i - x. \tag{3.17}$$

Étant donné que δ est monotone croissante, nous pouvons conclure qu'il existe un unique $i \in \mathbb{Z}$ tel que $\delta_i \leq x < \delta_{i+1}$. Si $\mathfrak{a}_i = \mu_i$ où $\delta_i = \log(\mu_i)$, alors nous appellerons $\mathfrak{a}_i$ le **voisin gauche** de x, que nous noterons $\mathfrak{a}_-(x)$, et $\mathfrak{a}_{i+1}$ le **voisin droit** de x, que nous noterons $\mathfrak{a}_+(x)$.

Évidement, pour un $x \in \mathbb{R}$, nous pouvons calculer l'unique i tel que $\delta_i \leq x < \delta_{i+1}$. Nous n'avons qu'à calculer le développement en fraction continue de $\mathfrak{i}$, ainsi que la distance à chaque itération, jusqu'à ce que nous ayons obtenu le bon idéal. Cependant, si x est polynomial en $\sqrt{\Delta}$, nous aurons besoin d'itérer un nombre exponentiel de fois, puisque, par le corollaire 3.3.0.1, $|\bar{\psi}_i| < \sqrt{\Delta}$. La distance n'augmente donc à chaque itération que d'une quantité logarithmique en $\sqrt{\Delta}$,— $\delta_{i+1} = \delta_i + \mathcal{O}(\log(\sqrt{\Delta}))$.

Supposons, tout d'abord, que nous ayons x, y, i et j tels que $\delta_i \leq x < \delta_{i+1}$ et $\delta_j \leq y < \delta_{j+1}$. En appliquant le théorème 3.2.1 à $\mathfrak{a}_i$ et à $\mathfrak{a}_j$ et ensuite le théorème 3.2.2, nous obtiendrons $\mathfrak{a}_k$, où $k \approx i + j$. De plus $\partial(\mathfrak{a}_k, x + y) = \delta_k - x - y = \partial(\mathfrak{a}_i, x) + \partial(\mathfrak{a}_j, y) + \varepsilon$. Il est cependant évident qu'$\mathfrak{a}_k$ n'est pas nécessairement l'unique idéal tel que $\delta_k \leq x + y < \delta_{k+1}$. Nous pouvons cependant calculer l'unique $\mathfrak{a}_{k'}$ remplissant cette condition en itérant un certain nombre de fois avec l'algorithme de développement en fraction continue. Combien de fois cela sera-t-il nécessaire ? Le théorème 3.3.0.1 nous dit que $\bar{\psi}_i \bar{\psi}_{i+1} > 2$. Ceci implique que $\prod_{i=n_0}^{i<n_0+2r} \bar{\psi}_i > 2^r$. Nous pouvons donc ajouter $\pm\mathcal{O}(\log(\sqrt{\Delta}))$ à la distance avec $\mathcal{O}(\log(\sqrt{\Delta}))$ itérations. Ce qui nous permet de calculer l'idéal $\mathfrak{a}_{k'}$ recherché en temps polynomial du nombre de bits nécessaire pour exprimer D.

Théorème 3.3.2 *Soient $s \in \mathbb{Z}$, $x \in \mathbb{R}$ et $\mathfrak{a}_i$ tel que $\delta_i \leq x < \delta_{i+1}$. Alors $\mathfrak{a}_m$, tel que $\delta_m \leq sx < \delta_{m+1}$, peut être calculé en temps polynomial comme suit :*

1. *Soit la décomposition binaire de s : $s = \sum_{j=0}^{r} b_j 2^{r-j}$ où $b_j \in \{0, 1\}$ et $b_0 = 1$,*
2. *Soient $z_0 := x$ et $\mathfrak{a}_-(z_0) = \mathfrak{a}_i$,*
3. *$\forall j$ de 1 à r*
   - (a) *Calculez $\mathfrak{a}_-(2z_{j-1})$ et définissez $\mathfrak{a}_-(z_j) := \mathfrak{a}_-(2z_{j-1})$,*
   - (b) *Si $b_j = 1$, calculez $\mathfrak{a}_-(x + z_j)$ et définissez $\mathfrak{a}_-(z_j) := \mathfrak{a}_-(x + z_j)$,*
4. *Définissez $\mathfrak{a}_-(sx) := \mathfrak{a}_-(z_r)$.*

Cet algorithme utilise l'exponentiation normale afin de calculer la multiplication à partir de l'addition, communément appelé **multiplication à la russe** (voir [19]). Nous pouvons donc calculer en temps polynomial, pour tout $x = \mathcal{O}(\sqrt{\Delta}) \in \mathbb{R}^+$ l'unique idéal $\mathfrak{a}_m$ tel que $\delta_m \leq x < \delta_{m+1}$.

Chapitre 4

Un algorithme d'échange de clefs

Nous avons développé jusqu'ici un outillage mathématique complexe, mais n'en n'avons mentionné aucune utilisation possible. Bien que tout ce matériel ait été développé dans le cadre de la théorie des nombres, une application cryptographique en a été proposée en 1989 par BUCHMANN et WILLIAMS [5]. Ils proposèrent d'utiliser les idéaux quadratiques réduits afin de construire un protocole d'échange de clefs. Ce protocole est en fait une adaptation du célèbre protocole proposé par DIFFIE et HELLMAN en 1976,voir [10]. Nous commencerons par décrire le protocole de DIFFIE et HELLMAN, pour ensuite expliquer le protocole de BUCHMANN et WILLIAMS, en nous basant sur [25].

4.1 DIFFIE et HELLMAN

Soit p un nombre premier. L'algèbre de base nous apprend que $\mathbb{Z}_p$ forme un corps et que le groupe multiplicatif $\mathbb{Z}_p^*$ constitue un groupe cyclique. C'est à dire qu'il existe un générateur $\alpha \in \mathbb{Z}_p^*$ tel que pour tout $\beta \in \mathbb{Z}_p^*$ il existe un i, où $0 \leq i \leq p-2$, tel que $\beta = \alpha^i$. Le groupe $\mathbb{Z}_p^*$ comporte $p-1$ éléments et est isomorphe au groupe $\mathbb{Z}/(p-1)\mathbb{Z}$. Ceci implique que l'arithmétique du groupe peut être effectuée uniquement sur les exposants, où les exposants sont pris $\pmod{(p-1)}$. Donc si $\beta = \alpha^i$ et $\gamma = \alpha^j$ alors $\beta\gamma = \alpha^i\alpha^j = \alpha^{i+j} = \alpha^{(i+j) \pmod{(p-1)}}$.

Le protocole de DIFFIE et HELLMAN est simple. Deux partis, Bob et Alice, veulent s'échanger une clef qui leur servira plus tard, par exemple, à communiquer à l'aide d'un chiffre. Si Bob et Alice n'ont pas la possibilité de se rencontrer en un lieu sûr où leur conversation ne peut être surveillée par un tiers parti malveillant, ils doivent alors posséder un protocole leur permettant de s'échanger une clef au vu et su de tous, et cela sans compromettre la sûreté de leur clef. Dans le protocole de Diffie et Hellman, Bob et Alice doivent d'abord s'entendre sur un nombre premier p et un générateur α du groupe $\mathbb{Z}_p^*$, tous deux publiques. Ensuite vient le protocole lui-même, voir figure 4.1. Bob choisi un exposant x au hasard, où $2 \leq x \leq p-2$, et calcule $\beta = \alpha^x \in \mathbb{Z}_p^*$. Alice choisi, elle aussi, un exposant y au hasard, où $2 \leq y \leq p-2$, et calcule $\gamma = \alpha^y \in \mathbb{Z}_p^*$. Bob transmet β à Alice et Alice transmet γ à Bob. Finalement Bob calcule $K_b = \gamma^x \in \mathbb{Z}_p^*$ et Alice calcule $K_a = \beta^y \in \mathbb{Z}_p^*$. Évidement $K_b = K_a = \alpha^{xy}$. Alice et Bob ont donc calculé le même élément K. Cet élément K peut maintenant leur servir de clef.

Les informations publiques accessibles à un tiers parti espion sont :

$$p, \alpha, \beta, \gamma. \tag{4.1}$$

Évidement, si notre espion était capable de récupérer l'exposant x à partir de β, le protocole ne serait pas sûr, puisqu'il n'aurait plus qu'à calculer γ^x pour retrouver K. Ce problème est appelé **logarithme discret** et est réputé être calculatoirement difficile. Rien, cependant, n'oblige un tiers parti à calculer le logarithme discret. Nous pourrions imaginer une boîte qui, lorsque donné γ et α en entrée, retournerait $\gamma^{\log_\alpha(\beta)}$. Ce problème est connue sous le nom de **problème de Diffie et Hellman**. Évidement, le problème de Diffie et Hellman n'est pas plus difficile que le logarithme discret, mais l'inverse n'est toujours pas démontré. C'est- à-dire que le problème de Diffie et Hellman pourrait éventuellement s'avérer aisé, sans que le logarithme discret ne le soit.

La notion de difficulté de ces deux problèmes est plus empirique que théorique. Dans les faits, il n'existe présentement aucune preuve rigoureuse pouvant démontrer la difficulté de l'un ou l'autre. Les informaticiens considèrent ces problèmes comme étant difficiles puisqu'aucune solution polynomiale n'est connue.

Fig. 4.1 – Le protocole Diffie et Hellman

Bob calcule $\beta = \alpha^x$	$\xrightarrow{\beta}$	
	$\xleftarrow{\gamma}$	Alice calcule $\gamma = \alpha^y$
Bob calcule $K = \gamma^x$		Alice calcule $K = \beta^y$

4.2 Buchmann et Williams

4.2.1 Une ébauche

Dans cette section nous décrirons un protocole d'échange de clefs qui a été proposé par Buchmann et Williams en 1989 [5]. Ce protocole n'a été bien décrit qu'en 1994 [25] et nous nous baserons sur cet article tout au long de cette section.

Nous commencerons par donner une version simplifiée du protocole. Nous développerons par la suite certains détails afin de donner une version complète du protocole plus loin dans ce chapitre.

Nous utiliserons la notions de distance entre un idéal quadratique et un nombre réel. Bob et Alice doivent tout d'abord s'entendre sur un anneau d'entiers quadratiques $\mathfrak{D}_n$ ayant un grand discriminant $\sqrt{\Delta}$. Notez que D_0 n'a pas à être connu. L'anneau $\mathfrak{D}_n$ est choisi par le simple choix de D qui a peu de chance de ne pas avoir un diviseur quadratique si D a été choisi de manière uniforme.

Bob choisit ensuite un nombre réel positif $b \in \mathcal{O}(\sqrt{\Delta})$, et calcule l'idéal $\mathfrak{b} = \mathfrak{a}_{-}(b)$, ainsi que $\partial(\mathfrak{b}, b)$. Il transmet finalement à Alice le doublet $(\mathfrak{b}, \partial(\mathfrak{b}, b))$. Alice choisit, elle, un nombre réel positif $a \in \mathcal{O}(\sqrt{\Delta})$, et calcule l'idéal $\mathfrak{a} = \mathfrak{a}_{-}(a)$, ainsi que $\partial(\mathfrak{a}, a)$. Elle transmet ensuite à Bob le doublet $(\mathfrak{a}, \partial(\mathfrak{a}, a))$. Bob calcule ensuite l'idéal $\mathfrak{c} = \mathfrak{a}_{-}(ba)$ à partir de b, $\mathfrak{a}$ et $\partial(\mathfrak{a}, a)$. Alice calcule de son côté l'idéal $\mathfrak{c} = \mathfrak{b}_{-}(ab)$ à partir de a, $\mathfrak{b}$ et $\partial(\mathfrak{b}, b)$.

Nous pouvons deviner immédiatement que la fonction $\partial(\mathfrak{a}, a)$ ne révèle strictement rien sur la distance de l'idéal $\mathfrak{a}$, puisque pour tout idéal $\mathfrak{a}_i$ il existe un nombre $x \in \mathbb{R}^{+}$ tel que $\partial(\mathfrak{a}_i, x) = \partial(\mathfrak{a}, a)$. De plus, rien ne semble révélé sur la distance des idéaux $\mathfrak{a}$ et $\mathfrak{b}$ à moins que la version du logarithme discret sur la classe des idéaux soit une tâche aisée à calculer. Nous reviendrons plus loin sur la sûreté de ce protocole. Cet algorithme a cependant deux problèmes. Primo, nous ne savons toujours pas comment Bob pourrait calculer $\mathfrak{c}$ à partir de b, $\mathfrak{a}$ et $\partial(\mathfrak{a}, a)$. Et secundo, cet algorithme utilise des nombres réels dont la précision n'est pas limitée. Il nous faut donc remédier à ces deux problèmes.

4.2.2 Une révision algorithmique

Premier détail, nous ne souhaitons pas calculer des logarithmes à chaque itération. Nous utiliserons donc l'exponentiel de la notion de distance. Si $\mathfrak{a}_j = (\mu_j)$ est un idéal réduit ayant pour distance δ_j, nous définirons sa **distance exponentielle** comme étant e^{δ_j}. La distance exponentielle d'un idéal à un nombre réel x sera dénotée par $\lambda(\mathfrak{a}_j, x)$ et sera définie ainsi :

$$\lambda(\mathfrak{a}_j, x) = e^{\partial(\mathfrak{a}_j, x)} = \mu_j e^{-x}. \tag{4.2}$$

Mais comme nous l'avons mentionné, nous ne pouvons pas, en pratique, utiliser des nombres réels quelconques pour effectuer nos calculs. Nous devrons donc utiliser une approximation rationnelle à toute distance. Nous approximerons donc une distance $\lambda(\mathfrak{a}_j, x) \in \mathbb{R}$ par $\hat{\lambda}(\mathfrak{a}_j, x) \in \mathbb{Q}$ où le dénominateur est fixe. Nous définirons la fonction $\hat{\lambda}$ ainsi :

$$\hat{\lambda}(\mathfrak{a}_j, x) = \frac{\mathrm{M}(\mathfrak{a}_j, x)}{2^p}, \qquad \text{où } \mathrm{M}(\mathfrak{a}_j, x) \in \mathbb{Z}^+. \tag{4.3}$$

La précision de $\hat{\lambda}(\mathfrak{a}_j, x)$ est donc limitée à p bits. Nous définirons l'erreur relative de la fonction $\hat{\lambda}$ par :

$$\rho(\mathfrak{a}_j, x) = \frac{\hat{\lambda}(\mathfrak{a}_j, x)}{\lambda(\mathfrak{a}_j, x)}. \tag{4.4}$$

Étant donné l'erreur introduite dans les calculs, nous ne serons plus capable de calculer $\mathfrak{a}_-(x)$ pour $x \in \mathbb{R}^+$, mais seulement un idéal réduit $\hat{\mathfrak{a}}(x) \in \{\mathfrak{a}_-(x), \mathfrak{a}_+(x)\}$. Pour alléger la notation, nous utiliserons les simplifications suivantes :

$$\lambda(x) = \lambda(\hat{\mathfrak{a}}(x), x),$$

$$\hat{\lambda}(x) = \hat{\lambda}(\hat{\mathfrak{a}}(x), x) = \frac{\mathrm{M}(x)}{2^p} \text{ et}$$

$$\rho(x) = \frac{\hat{\lambda}(x)}{\lambda(x)}.$$

Nous pouvons réécrire la première et la dernière propriété du corollaire 3.3.0.1 ainsi :

Corollaire 4.2.0.1 *Soient $x \in \mathbb{R}^+$ et $j \in \mathbb{Z}$ tels que $\mathfrak{a}_j = \mathfrak{a}_-(x)$ et $\mathfrak{a}_{j+1} = \mathfrak{a}_+(x)$, alors*

1. $1/(q_{j-1} + 1) < \lambda(\mathfrak{a}_-(x), x) \leq 1 < \lambda(\mathfrak{a}_+(x), x) < q_{j-1} + 1,$
2. $\lambda(\mathfrak{a}_-(x), x) > 1/\sqrt{\Delta}$ *et* $\lambda(\mathfrak{a}_+(x), x) < \sqrt{\Delta}.$

Finalement, quelques constantes ainsi que quelques propriétés les concernant doivent être définies avant de présenter les algorithmes dont nous aurons besoin.

Soit $B \geq 2 \in \mathbb{N}$ tel que $B = \Theta(D^n)$ pour un $n \in \mathbb{N}$. B sera utilisé comme borne supérieure dans le choix des distances a et b par Alice et Bob. Posons les constantes suivantes :

$$\begin{aligned} d^* = \left\lceil 2^p\sqrt{D} \right\rceil, \qquad \chi = 1 + \tfrac{1}{2^{p-1}}, \quad g = 1 + \tfrac{1}{47\left\lfloor\sqrt{D}\right\rfloor}, \\ \gamma = \lceil g^{-1}2^p \rceil, \quad K = \left(\tfrac{\chi^2}{1-\gamma^{-1}}\right)^2, \qquad A = g^{1/16B^2} \end{aligned} \tag{4.5}$$

où p est choisi selon le critère suivant :

$$2^p \geq 3072 \left\lfloor \sqrt{D} \right\rfloor B^2.$$

Évidement γ, g, χ, K et A sont plus grand que 1. De plus, le critère utilisé pour choisir p nous garantie, pour la distance exponentielle, une précision polynomiale en $\log D$. Finalement γ sera utilisé comme borne inférieure pour la fonction M partout dans nos algorithmes.

Le théorème suivant nous indique comment calculer à partir de $\hat{\mathfrak{a}}(x)$ et $\hat{\mathfrak{a}}(y)$, l'idéal $\hat{\mathfrak{a}}(x+y)$ où x et y appartiennent à $\mathbb{R}^+$. Nous n'avons jamais formulé rigoureusement un algorithme accomplissant cette tâche, mais n'avons qu'argumenté, bien qu'avec peu de rigueur, en faveur de l'existence d'un tel algorithme.

Théorème 4.2.1 *Soient $\hat{\mathfrak{a}}(x)$ et $\hat{\mathfrak{a}}(y)$ appartenant à $\mathcal{R}$, ainsi que $\mathrm{M}(x)$ et $\mathrm{M}(y)$ où $x, y \in \mathbb{R}^+$ tels que*

- $\mathrm{M}(x)$, $\mathrm{M}(y) \geq \gamma$,
- $\hat{\mathfrak{a}}(x) \in \{\mathfrak{a}_-(x), \mathfrak{a}_+(x)\}$ *et* $\hat{\mathfrak{a}}(y) \in \{\mathfrak{a}_-(y), \mathfrak{a}_+(y)\}$,
- $g^{-1} \leq \rho(x)\rho(y) \leq g$,

alors, l'idéal $\hat{\mathfrak{a}}(x+y) \in \mathcal{R}$ tel que $\hat{\mathfrak{a}}(x+y) \in \{\mathfrak{a}_-(x+y), \mathfrak{a}_+(x+y)\}$ et $\mathrm{M}(x+y) \geq \gamma$ peut être ainsi calculé :

1. *Calculez à l'aide du théorème 3.2.1 l'entier U et l'idéal primitif $\mathfrak{c}$ tels que $\mathfrak{c} = (1/U)\hat{\mathfrak{a}}(x)\hat{\mathfrak{a}}(y)$.*
2. *Calculez, à l'aide du théorème 3.2.2 l'idéal réduit $\mathfrak{a}_k$ ainsi que θ_k tels que $\mathfrak{a}_k = \bar{\theta}_k\mathfrak{c}$.*

3. Posez

$$T := \left\lceil 2^{2p} \frac{G_{k-2} 2^p + B_{k-2} d^*}{Q} \right\rceil, \quad \hat{\theta} := \frac{T}{2^{3p}}, \quad L := g \frac{\hat{\theta}}{U} \hat{\lambda}(x) \hat{\lambda}(y). \tag{4.6}$$

4. **Cas 1 :** $(1 \leq L \leq g^3)$ *Posez*

$$\hat{\mathfrak{a}}(x+y) := \mathfrak{a}_k, \quad \mathrm{M}(x+y) := \left\lceil \frac{\hat{\theta}}{U} 2^p \hat{\lambda}(x) \hat{\lambda}(y) \right\rceil = \left\lceil \frac{L 2^p}{g} \right\rceil.$$

Cas 2 : $(L < 1)$ *Calculez* $\mathfrak{a}_{k+1}$ *et posez*

$$T_k := 2^p, \quad T_{k+1} := \left\lceil \frac{P_k 2^p + d^*}{Q_{k-1}} \right\rceil.$$

Calculez $\mathfrak{a}_{k+j}$*, pour* $j \geq 2$*, ainsi que*

$$T_{k+j} := q_{k+j-2} T_{k+j-1} + T_{k+j-2} \tag{4.7}$$

jusqu'à ce que $k + j = n$ *tel que* $T_n \geq 2^p / L > T_{n-1}$*. Posez*

$$\hat{\mathfrak{a}}(x+y) := \mathfrak{a}_n, \quad \mathrm{M}(x+y) := \left\lceil \frac{T_n \hat{\theta}}{U} \hat{\lambda}(x) \hat{\lambda}(y) \right\rceil = \left\lceil \frac{T_n L}{g} \right\rceil.$$

Cas 3 : $(l > g^3)$ *Posez*

$$T_k := 2^p - 1, \quad T_{k-1} := \left\lceil \frac{(P_{k-1} 2^p + d^*) 2^{p-1}}{Q_{k-2}(2^{p-1}+1)} \right\rceil = \left\lceil \frac{P_{k-1} 2^p + d^*}{\chi Q_{k-2}} \right\rceil.$$

Calculez $\mathfrak{a}_{k-j}$*, pour* $j \geq 1$*, ainsi que*

$$T_{k-j-1} := q_{k-j-1} T_{k-j} + T_{k-j+1}$$

jusqu'à ce que $k - j - 1 = n$ *tel que* $T_{n-1} > L 2^p \geq T_n$*. Posez*

$$\hat{\mathfrak{a}}(x+y) := \mathfrak{a}_n, \quad \mathrm{M}(x+y) := \left\lceil \frac{\hat{\theta} 2^{2p}}{U T_n} \hat{\lambda}(x) \hat{\lambda}(y) \right\rceil = \left\lceil \frac{L 2^{2p}}{g T_n} \right\rceil.$$

Pour une preuve que cet algorithme fait bien ce qu'il prétend faire, consultez [5]. Cet algorithme, bien qu'il semble compliqué, ne fait que ce dont nous avions discuté à la fin du chapitre précédent, mais dans le contexte où $\mathfrak{a}_{-}(x)$ n'est pas connue exactement, et où x n'est accessible qu'à travers l'approximation de sa distance avec l'idéal $\hat{\mathfrak{a}}(x)$. Les trois premières étapes du théorèmes ne sont vraiment que l'initialisation. Au **cas 1**, le critère $1 \leq L \leq g^3$ nous permet de décider que l'idéal $\mathfrak{a}_k$ calculé lors de l'initialisation est le bon idéal,— $\mathfrak{a}_k \in \{\mathfrak{a}_-(x+y), \mathfrak{a}_+(x+y)\}$. Au **cas 2**, nous devons avancer dans le cycle $\mathcal{R}$ en calculant des idéaux $\mathfrak{a}_{k+j}$ dont la distance augmente jusqu'à ce qu'elle réponde à un critère d'arrêt nous permettant de conclure que le dernier idéal $\mathfrak{a}_{k+j}$ calculé est le bon,— $\mathfrak{a}_{k+j} \in \{\mathfrak{a}_-(x+y), \mathfrak{a}_+(x+y)\}$. Et au **cas 3**, nous ne faisons que reculer dans le cycle $\mathcal{R}$.

Quelques remarques supplémentaires s'imposent sur les différentes valeurs utilisées dans ce théorème. Les valeurs $\hat{\theta}$ et L sont des approximations à $|\bar{\theta}_k|$ et $\lambda(\mathfrak{a}_k, x+y)$ respectivement. En utilisant l'équation (2.11) du chapitre 2, nous nous apercevons que T est une approximation à $\bar{\theta}_n/\bar{\theta}_k$, où n et k sont tels qu'utilisés dans le théorème 4.2.1. Le lecteur peut donc s'apercevoir qu'$\mathrm{M}(x+y)$ est bel et bien une approximation à $2^p\lambda(\mathfrak{a}_n, x+y)$.

Nous pouvons donc revoir le théorème 3.3.2, dans ce nouveau contexte.

Théorème 4.2.2 *Soient $s \in \mathbb{Z}$, $x \in \mathbb{R}$ et $\hat{\mathfrak{a}}(x)$. Alors $\hat{\mathfrak{a}}(sx)$, peut être calculé en temps polynomial comme suit :*

1. *Soit la décomposition binaire de s : $s = \sum_{i=0}^{r} b_i 2^{r-i}$ où $b_i \in \{0,1\}$ et $b_0 = 1$,*
2. *Soient $z_0 := x$ et $\hat{\mathfrak{a}}(z_0) := \hat{\mathfrak{a}}(x)$,*
3. *$\forall i$ de 1 à r*
   - (a) *Calculez $\hat{\mathfrak{a}}(2z_{i-1})$ ainsi que $\mathrm{M}(2z_{i-1})$ et définissez $\hat{\mathfrak{a}}(z_i) := \hat{\mathfrak{a}}(2z_{i-1})$ ainsi que $\mathrm{M}(z_i) := \mathrm{M}(2z_{i-1})$.*
   - (b) *Si $b_i = 1$, calculez $\hat{\mathfrak{a}}(z_i + x)$ ainsi que $\mathrm{M}(z_i + x)$ et définissez $\hat{\mathfrak{a}}(z_i) := \hat{\mathfrak{a}}(z_i + x)$ ainsi que $\mathrm{M}(z_i) := \mathrm{M}(z_i + x)$.*
4. *Définissez $\hat{\mathfrak{a}}(sx) := \hat{\mathfrak{a}}(z_r)$ et $\mathrm{M}(sx) := \mathrm{M}(z_r)$.*

Quelques observations s'imposent. Il est évident, en supposant que $g^{-1} \leq \rho(z_{i-1})^2 \leq g$ après l'étape 3a ainsi que $g^{-1} \leq \rho(2z_i)\rho(x) \leq g$ après l'étape 3b, qu'il peut être conclu que $M(z_i) \geq \gamma$, ainsi que $\hat{\mathfrak{a}}(z_i) \in \{\mathfrak{a}_-(z_i), \mathfrak{a}_+(z_i)\}$ et ce pour tout les i, tel que nous l'indique le théorème 4.2.1. Les deux prochains théorèmes nous indiquent que cela est possible. Ils nous fournissent aussi une construction qui respecte les conditions des théorèmes 4.2.1 et 4.2.2.

Théorème 4.2.3 *Soient a et b, deux entiers rationnels bornés par B et c un nombre réel. De plus soit $\hat{\mathfrak{a}}(c) = \mathfrak{a}_i$ tel que $\mathfrak{a}_{i-1}$ et $\mathfrak{a}_i \in \mathcal{R}$, ainsi que $M(c) \geq \gamma$ et $A^{-1} \leq$*

$\rho(c) \leq A$, alors $M(abc) \geq \gamma$, $\hat{\mathfrak{a}}(abc) \in \{\mathfrak{a}_-(abc), \mathfrak{a}_+(abc)\}$ et $g^{-1} \leq \rho(abc) \leq g$ où $\hat{\mathfrak{a}}(abc)$ a été obtenu en appliquant le théorème 4.2.2 à l'idéal $\hat{\mathfrak{a}}(c)$ et à b suivit d'une application du théorème 4.2.2 à l'idéal $\hat{\mathfrak{a}}(bc)$ et à l'entier rationnel a.

Théorème 4.2.4 *Soit*

$$\mathfrak{a} = (\mu) = \left[\frac{Q}{\sigma}, \frac{P+\sqrt{D}}{\sigma}\right] \in \mathcal{R},$$

où $\mathfrak{a}$ est obtenue en réduisant quelques fois l'idéal $\mathfrak{i} = (1)$,— au moins 2 fois. Alors en posant $c = \log(|\mu|)$, $\hat{\mathfrak{a}}(c) = \mathfrak{a}$ et $M(c) = 2^p$, $\hat{\mathfrak{a}}(c)$ et $M(c)$ respectent les conditions du théorème 4.2.3.

Nous avons donc maintenant tous les outils nécessaires à l'implantation du protocole d'échange de clefs présenté à la section 4.2.1 de ce chapitre. Tout à un petit détail près. Nous sommes maintenant capable de calculer un idéal $\hat{\mathfrak{a}}(abc) \in \{\mathfrak{a}_-(abc), \mathfrak{a}_+(abc)\}$. Mais rien n'indique qu'Alice et Bob calculerons le même idéal. Alice pourrait très bien calculer $\mathfrak{a}_-(abc)$ et Bob $\mathfrak{a}_+(abc)$. Il nous faut donc développer une procédure nous permettant de réconcilier les résultats des deux partenaires.

4.2.3 Réconciliation

Le premier résultat de cette section s'applique à l'idéal obtenue par le théorème 4.2.2.

Lemme 4.2.4.1 *Soient l'idéal $\mathfrak{a}_i \in \mathcal{R}$ ainsi que $\mathrm{M}(\mathfrak{a}_i, x)$, où $x \in \mathbb{R}$, alors $\mathrm{M}(\mathfrak{a}_{i-1}, x)$ et $\mathrm{M}(\mathfrak{a}_{i+1}, x)$, peuvent être calculés ainsi :*

1. *Calculez $\mathfrak{a}_{i-1}$ ainsi que $\mathfrak{a}_{i+1}$.*
2. *Posez*

$$s := \begin{cases} 0 & \text{si } P_{i-1} < \left\lfloor\sqrt{D}\right\rfloor \\ \left\lceil \log_2(2\lfloor\sqrt{D}\rfloor + 1)\right\rceil & \text{si } P_{i-1} = \left\lfloor\sqrt{D}\right\rfloor. \end{cases}$$

Posez $t := s + p$, $\tilde{d} := \left\lceil 2^t\sqrt{D}\right\rceil$ et

$$\hat{\psi}_i := \frac{2^p P_i + d^*}{2^p Q_{i-1}}, \quad \frac{1}{\hat{\psi}_{i-1}} := \frac{\tilde{d} - 2^t P_{i-1}}{2^t Q_{i-1}}.$$

3. Alors

$$\mathrm{M}(\mathfrak{a}_{i-1}, x) := \left\lceil \frac{1}{\hat{\psi}_{i-1}} \mathrm{M}(\mathfrak{a}_i, x) \right\rceil, \quad \mathrm{M}(\mathfrak{a}_{i+1}, x) := \left\lceil \hat{\psi}_i \mathrm{M}(\mathfrak{a}_i, x) \right\rceil.$$

Dans ce lemme, $\hat{\psi}_i$ et $\hat{\psi}_{i-1}$ sont des approximations à $|\bar{\psi}_i|$ et $|\bar{\psi}_{i-1}|$ respectivement. Notre objectif est maintenant de fournir une méthode à Alice et Bob leur permettant de calculer le même idéal. La représentation de cet idéal pourra dès lors leur servir de clef.

Soit $\mathfrak{r}(x)$ l'idéal qui minimise $\partial(\mathfrak{a}, x)$ pour tous les $\mathfrak{a} \in \mathcal{R}$. Évidement, $\mathfrak{r}(x) \in \{\mathfrak{a}_-(x), \mathfrak{a}_+(x)\}$. Le théorème suivant fournit la solution à notre problème.

Théorème 4.2.5 *Soient a, b, c, $\hat{\mathfrak{a}}(c)$ et $\mathrm{M}(c)$ tels que décrits au théorème 4.2.3. Si $\lambda(\mathfrak{r}(abc), abc) \geq g^2$ ou $\lambda(\mathfrak{r}(abc), abc) \leq g^{-2}$, alors $\hat{\mathfrak{a}}(abc) = \mathfrak{a}_+(abc)$. Si $g^{-2} < \lambda(\mathfrak{r}(abc), abc) < g^2$, alors $\mathfrak{r}(abc)$ est l'idéal $\mathfrak{j}$ d'entre $\hat{\mathfrak{a}}(abc)$ et ses deux voisins tel que*

$$\frac{2^p}{g^3} < \mathrm{M}(\mathfrak{j}, abc) < \frac{(1+2^p)g^3}{1+2^{-p}g^3}. \tag{4.8}$$

Naturellement $\mathfrak{j}$ est soit $\hat{\mathfrak{a}}(abc)$ où l'un des deux voisins calculés à l'aide du lemme 4.2.4.1. La procédure pour se réconcilier est la suivante. Les deux partenaires appliquent chacun de leur côté la condition explicité par l'équation (4.8). Si les deux partenaires arrivent à calculer l'idéal $\mathfrak{j}$, ils ont donc calculé le même idéal : $\mathfrak{r}(abc)$. S'ils n'y arrivent pas,— aucun des trois idéaux ne réalise la condition (4.8) ,— alors ils ont tous deux calculé l'idéal $\mathfrak{a}_+(abc)$. Si non, le théorème utilise une conditions indépendante des idéaux $\hat{\mathfrak{a}}(abc)$ et $\hat{\mathfrak{a}}(bac)$ calculés par Alice et Bob, et donc si l'un deux n'arrive pas à calculer l'idéal $\mathfrak{j}$ tel que la condition de l'équation (4.8) soit vrai, alors soit $\lambda(\mathfrak{r}(abc), abc) \geq g^2$ ou $\lambda(\mathfrak{r}(abc), abc) \leq g^{-2}$. Et donc, ils ont tous les deux calculé $\mathfrak{a}_+(abc)$. Dans tous les cas, ils peuvent s'entendre sur un unique idéal.

Le protocole est récapitulé à la page 60. Quelques commentaires à propos du protocole sont nécessaires. Primo, ce protocole exige un tour de communication de plus que le protocole original de Diffie et Hellman. Ce second tour ne consiste cependant qu'en un seul bit. Secundo, la structure utilisé pour le protocole n'est pas celle d'un group, mais celle d'un **quasi-groupe**. Étant donné que la distance des idéaux n'est pas une propriété purement additive, la multiplication d'idéaux réduits n'est pas associative. Et tertio, obligation est faite de travailler avec des approximations de nombres réels.

La structure de quasi-groupe est une caractéristique intéressante de ce protocole, en ce sens que c'est une caractéristique rarement utilisée et qu'elle ne semble pas

Fig. 4.2 – Le protocole Buchmann et Williams

Bob		Alice
	D, c, $\hat{\mathfrak{a}}(c)$ et $\mathrm{M}(c)$ $\longleftrightarrow$	
Bob choisit $b \leq B$ et calcule $\hat{\mathfrak{a}}(bc)$ et $\mathrm{M}(bc)$	$\hat{\mathfrak{a}}(bc)$ et $\mathrm{M}(bc)$ $\longrightarrow$	
	$\hat{\mathfrak{a}}(ac)$ et $\mathrm{M}(ac)$ $\longleftarrow$	Alice choisit $a \leq B$ et calcule $\hat{\mathfrak{a}}(ac)$ et $\mathrm{M}(ac)$
Bob calcule $\hat{\mathfrak{a}}(bac)$ et $\mathrm{M}(bac)$ Ainsi que l'unique $\mathfrak{j}$ tel que l'équation (4.8) soit vrai Si $\mathfrak{j}$ existe $\Gamma_{Bob} = 1$ sinon $\Gamma_{Bob} = 0$	Γ_{Bob} $\longrightarrow$	
	Γ_{Alice} $\longleftarrow$	Alice calcule $\hat{\mathfrak{a}}(abc)$ et $\mathrm{M}(abc)$ Ainsi que l'unique $\mathfrak{k}$ tel que l'équation (4.8) soit vrai Si $\mathfrak{k}$ existe $\Gamma_{Alice} = 1$ sinon $\Gamma_{Alice} = 0$
Si $\Gamma_{Bob} = \Gamma_{Alice} = 1$ Alors $K_{Bob} = \mathfrak{j}$ Sinon $K_{Bob} = \hat{\mathfrak{a}}(bac)$		Si $\Gamma_{Bob} = \Gamma_{Alice} = 1$ Alors $K_{Alice} = \mathfrak{k}$ Sinon $K_{Alice} = \hat{\mathfrak{a}}(abc)$

ouvrir une porte d'attaque contre l'algorithme. Les deux autres caractéristiques sont cependant des vices qui mériteraient d'être éliminés. Un protocole a été proposé en 1997 par Scheidler, Stein et Williams, voir [26], où la fonction de distance a maintenant pour image l'ensemble $\mathbb{Z}$, ce qui permet, dans un premier temps, d'éliminer le recours aux approximations de nombres réels, et, dans un second temps, d'éliminer le second tour de communication. Ce protocole utilise les corps réels quadratiques de congruence de fonctions. Ce corps est défini à l'aide du corps fini $\mathbb{F}_q$ et d'un polynôme $\mathrm{D} \in \mathbb{F}_q[x]$ sans diviseur quadratique et de degré pair. Le corps utilisé est alors simplement $\mathrm{K} = \mathbb{F}_q + \mathbb{F}_q\sqrt{\mathrm{D}}$. Le protocole est fort similaire à celui décrit dans ce chapitre, mais la distance y est définie comme le degré d'un polynôme représentatif d'un idéal qui est, lui, toujours un sous-anneau sur K. Tous les calculs y sont fait sur des polynômes.

4.2.4 Sûreté

Tout comme pour le protocole de Diffie et Hellman, peu est connue de la sécurité de ce protocole. Les informations publiques accessibles à un tiers parti espion sont :

$$D, c, B, \hat{\mathfrak{a}}(c), \mathrm{M}(c), \hat{\mathfrak{a}}(bc), \mathrm{M}(bc), \hat{\mathfrak{a}}(ac), \mathrm{M}(ac), \Gamma_{Bob}, \Gamma_{Alice}. \tag{4.9}$$

La seule manière connue de s'attaquer au protocole est de calculer le logarithme discret sur le quasi-groupe. Celui-ci est définie comme le calcul de la distance δ_i associé à un idéal $\mathfrak{a}_i$. Évidement, pour que ce problème soit difficile, il est nécessaire que le nombre d'idéaux contenu dans le cycle $\mathcal{R}$ soit exponentiel en $\log(D)$. Sinon, pour un idéal quelconque, la distance peut être calculée à l'aide de $\frac{|\mathcal{R}|}{2}$ itérations, en moyenne, de l'algorithme de développement en fractions continues. Si $|\mathcal{R}|$ est grand, cette technique naïve est hors de question.

Notons par ℓ la taille de $\mathcal{R}$: $\ell = |\mathcal{R}|$. Alors étant donné que $\mathcal{R}$ est un cycle, par le corollaire 3.1.1.1, nous savons que pour un $i > j$, $\mathfrak{a}_i = \left(\bar{\theta}_i/\bar{\theta}_j\right)\mathfrak{a}_j$. Et donc, si $\mathfrak{a}_i = \mathfrak{a}_j$, alors nécessairement $\left(\bar{\theta}_i/\bar{\theta}_j\right) = \mathfrak{i} = (\epsilon^n)$, où ϵ est l'unité fondamentale. Il peut être démontré, consultez [7], que si $i = j + \ell + 1$ alors $\left(\bar{\theta}_i/\bar{\theta}_j\right) = (\epsilon)$. Ce résultat indique d'ailleurs une manière de base pour calculer ϵ. Le régulateur, $\Re$, du domaine d'intégrité est définie comme le logarithme de l'unité fondamentale : $\Re = \log\epsilon$. La distance d'un idéal est donc toujours inférieur au régulateur : $\forall i\ 0 \leq \delta_i \leq \Re$. Cette discussion est nécessaire pour arriver à la conclusion que si $x \in \mathbb{R}$ est suffisamment grand,— plus grand que le régulateur,— alors l'unique i, tel que $\delta_i \leq x < \delta_{i+1}$, sera supérieur à ℓ. Cette conclusion n'affecte en rien les algorithmes développés jusqu'ici. Mais nous devons en tenir compte à partir de maintenant.

En supposant qu'un adversaire puisse calculer le logarithme discret sur le quasi-groupe, il peut alors récupérer ac, par exemple, ainsi :

$$\hat{\lambda}(\hat{\mathfrak{a}}(ac), ac) = \frac{\mathrm{M}(ac)}{2^p} \approx e^{\partial(\hat{\mathfrak{a}}(ac),ac)}$$

ce qui implique, en isolant ac, que :

$$ac \approx \delta_i - \log(\mathrm{M}(ac)/2^p) + k\Re, \tag{4.10}$$

où δ_i est la distance de l'idéal $\hat{\mathfrak{a}}(c)$ calculé par l'adversaire et $k \in \mathbb{N}$. De manière générale $\Re$ est beaucoup plus grand qu'ac, et donc k devrait être petit, ce qui permettrait à l'adversaire de trouver ac rapidement.

Par un résultat de Buchmann et Williams, [6], si le logarithme discret sur le quasi-groupe peut être solutionné efficacement, cela implique une solution efficace pour le calcul du régulateur. Par un résultat de Schoof, [27], une solution efficace permettant de calculer le régulateur permet de factoriser D efficacement. Le logarithme discret ne peut donc pas avoir de solution efficace en général si la factorisation s'avère difficile. À l'instar du protocole de Diffie et Hellman, l'inverse n'a toujours pas pu être démontré. Il se pourrait donc que ce protocole sur le quasi-groupe soit attaquable sans que le logarithme discret ou la factorisation ne soit solutionnable efficacement. De plus, la factorisation pourrait s'avérer être aisée à solutionner sans que le problème de Buchmann et Wiliams ne le soit.

Chapitre 5

Une attaque quantique

Nous présentons dans ce chapitre un algorithme fort récent dû à Sean HALLGREN [15]. Cet algorithme est une adaptation du célèbre algorithme de SHOR permettant de factoriser. Le lecteur est donc fortement encouragé à lire l'annexe A avant de s'attaquer à ce chapitre.

La transformation de Fourier qui est au cœur de l'algorithme de SHOR est utilisée pour calculer la période de fonctions agissant sur les entiers rationnels modulo un autre entier p. Cependant, les problèmes que nous aimerions résoudre sur les entiers quadratiques,— le calcul du régulateur ou le logarithme discret sur le quasi-groupe par exemple,— sont tous exprimés à l'aide d'entiers rationnels et de nombres réels. Nous devons donc trouver une manière de discrétiser la notion de distance avant de pouvoir construire un algorithme quantique solutionnant le logarithme discret sur le quasi-groupe.

5.1 Calcul du régulateur

Nous savons que la fonction $f : \mathbb{R} \longrightarrow \mathcal{R} \times \mathbb{R}$ définie par $f(x) = (\mathfrak{a}_{-}(x), -\partial(\mathfrak{a}_{-}(x), x))$ est cyclique et a pour période $\Re$, le régulateur.

Nous dirons qu'une fonction $g : \mathbb{Z} \longrightarrow \mathbb{X}$, où $\mathbb{X}$ est un ensemble quelconque, est **périodique** et qu'elle a un pas de S, pour $S \in \mathbb{R}$, si pour une fraction $\frac{1}{h(\lfloor S \rceil)}$ des entiers $k \leq S$, où h est un polynôme : $f(k) = f(k+\lfloor jS \rfloor)$ ou $f(k) = f(k+\lceil jS \rceil)$ $\forall j \in \mathbb{N}$. Nous écrirons alors $f(k) = f(k + [iS])$ où $[jS]$ signifie soit $\lfloor jS \rfloor$ ou $\lceil jS \rceil$ selon le cas,— ou encore $[jS] = jS + \gamma_j$ où $-1 \leq \gamma_j \leq 1$.

Nous pouvons définir une fonction $\hat{f}$ qui sera périodique selon la définition précédente. Considérons la fonction $\hat{f} : \mathbb{Z} \longrightarrow \mathcal{R} \times \mathbb{Z}$ définie par $\hat{f}(k) = (\mathfrak{a}_{-}(k/N), \hbar_{k/N})$ où $\hbar_{k/N} = \lfloor -N\partial(\mathfrak{a}_{-}(k/N), k/N)\rfloor$ et N est un entier rationnel positif. Cette fonction peut certainement être calculée en temps polynomial. Le second membre du doublet, que nous appellerons compte, $\hbar_{k/N}$, ne fait que compter le nombre d'entiers qui sont projetés sur le même idéal. Par exemple, considérons l'entier k tel que $\hat{f}(k) = (\mathfrak{a}_i, \hbar_{k/N})$ où $\mathfrak{a}_i = \mathfrak{a}_{-}(k/N)$ et $\hat{f}(k-1) = (\mathfrak{a}_{i-1}, \hbar_{(k-1)/N})$. Donc k est le premier entier projeté sur $\mathfrak{a}_i$. Alors $\hbar_{k/N} = \lfloor N\partial(\mathfrak{a}_i, k/N)\rfloor$. Mais $\partial(\mathfrak{a}_i, k/N) < 1/N$ sinon $\hat{f}(k-1)$ eût été projeté sur $\mathfrak{a}_i$. Donc $\hbar_{k/N} = 0$. Supposons maintenant que $\hat{f}(k+1)$ soit aussi projetée sur l'idéal $\mathfrak{a}_i$. Nous avons alors $\hbar_{(k+1)/N} = \lfloor N\partial(\mathfrak{a}_i, (k+1)/N)\rfloor = \lfloor N(\partial(\mathfrak{a}_i, k/N) + 1/N)\rfloor = 1$. Et ainsi de suite pour tous les $k+j$ jusqu'à ce que la fonction $\hat{f}$ projette $k+j$ sur un nouvel idéal $\mathfrak{a}_{i+1}$. Le second membre de l'image permet à la fonction $\hat{f}$ d'être surjective sur l'intervalle $\{0, \ldots, \lfloor S\rfloor\}$.

Lemme 5.1.0.1 *Si $N > n(\log(1 + 1/\sqrt{\Delta}))$, où $n \in \mathbb{N}$, alors le pas, S, de la fonction $\hat{f}$ est égal à $N\Re$.*

Nous avons donc une fonction périodique définie sur l'ensemble des entiers rationnels qui a pour période un multiple du régulateur. Le prochain théorème nous permet de calculer le régulateur $\Re$.

Nous aurons besoin du lemme suivant dont la démonstration apparaît ici pour la première fois.

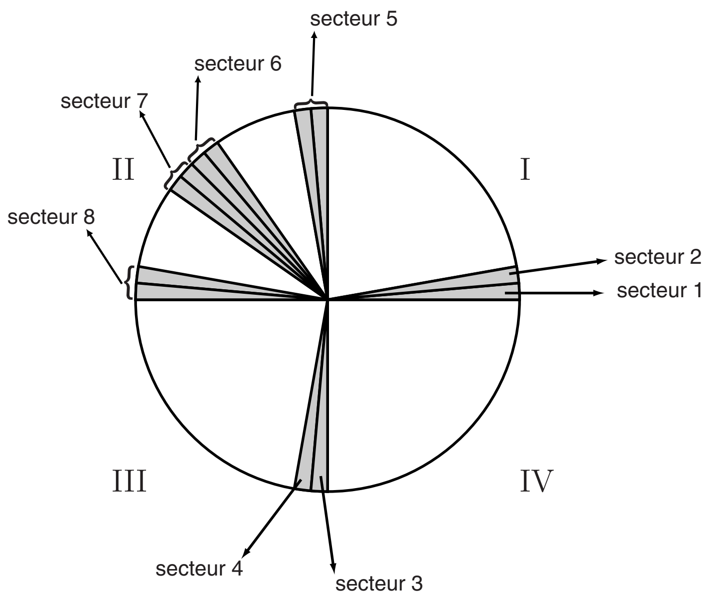
Lemme 5.1.0.2 *Soient une constante z et une fonction $f'(j)$ tels que $-3/4 \leq z \leq 3/4$ et $-1/n \leq f'(j) \leq 1/n$, où $n \geq 64$. Alors il existe une constante c telle que*

$$\left|\sum_{j=0}^{N-1} e^{2\pi i(zj/N + f'(j))}\right|^2 \geq \mathsf{c}N^2.$$

Démonstration :

Définissons d'abord la variable $n' = 360/n$. Cette somme est celle de vecteurs de longueur égale à 1 et disposés à tous les $360°/N \pm \epsilon°$ où ϵ est inférieur à n'. Nous appellerons ϵ un ajustement, et la valeur avant ajustement la valeur fondamentale. Nous souhaitons démontrer que le vecteur résultant de cette somme pointe vaguement dans la direction de 135° et que sa longueur croit polynomialement en N. Les vecteurs de la somme vont de $-n'°$ à $(270 + n')°$. Procédons en créant une nouvelle somme où la «mauvaise influence» des vecteur des cadrans I, III et IV aura été éliminée en «sacrifiant» un certain nombre de vecteurs du cadran II.

FIG. 5.1 – Schéma des compensations



Commençons par corriger les aberrations des vecteurs du cadran IV. Les secteurs mentionnés le sont en référence à la figure 5.1. Il ne se trouve dans ce cadran que des vecteurs dont la valeur fondamentale est comprise entre 0° et n'°, le secteur 1, où $(270 - n')^{\circ}$ et 270°, le secteur 3. Nous devons compenser ces vecteurs à l'aide de vecteurs du cadran II. Considérons les vecteurs dont la valeur fondamentale est comprise entre 0° et n'°. Ces vecteurs, s'ils débordent dans le cadran IV, ont une «mauvaise influence» dans la direction des x. Nous devrons donc utiliser les vecteurs du cadrans II dont la valeur fondamentale est comprise entre $(180 - 2n')^{\circ}$ et 180°, les vecteurs du secteur 8. Nous sommes obligés d'utiliser un plus grand nombre de vecteurs puisque nous ne sommes pas certains que pour chaque vecteur du cadran I, un seul vecteur du cadran II soit suffisant pour le «compenser». Cependant deux de ses vecteurs seront toujours plus que suffisant, quelque soit leur valeur. Le même raisonnement s'applique aux vecteurs dont la valeur fondamentale est comprise entre $(270 - n')^{\circ}$ et 270° ; ils seront compensés par le sacrifice des vecteurs dont la valeur fondamentale est comprise entre 90° et $(90 + 2n')^{\circ}$, les vecteurs dont la valeur fondamentale est dans le secteur 5.

Il nous reste encore deux secteurs dont nous devons corriger la mauvaise influence. Supposons que tous les vecteurs du cadran I se voient ajustés de la pire manière possible, c'est-à-dire qu'ils subissent tous une correction de $(-n'^{\circ})$, et que tous ceux du cadrans II reçoivent un ajustement de $(+n'^{\circ})$. Dans ce cas, l'influence globale de tous les vecteurs des cadrans I et III est un vecteur gisant dans le cadrant IV. Utilisons les vecteurs dont la valeur fondamentale est située entre $135°$ et $(135+2n')°$, le secteur 7, afin de contrecarrer l'influence des vecteurs du cadran I dont la valeur fondamentale est située entre n'° et $2n'^{\circ}$, le secteur 2. Les vecteurs restants, dans le cadran I, sont tous compris dans le pire des cas entre n'° et $(90-n')°$. Les vecteurs du cadran II dont la valeur fondamentale est comprise entre $(135-2n')°$ et $135°$, le secteur 6, servent eux à contrecarrer l'influence des vecteurs du cadran III dont la valeur fondamentale est située entre $(270-2n')°$ et $(270-n')°$, le secteur 4.

Dans la sommes finale, il nous reste donc les vecteurs dont la valeur fondamentale se situe dans l'un des 4 blocs suivants : entre $2n'^{\circ}$ et $90°$; entre $(90+2n')°$ et $(135-2n')°$; entre $(135+2n')°$ et $(180-2n')°$ et finalement entre $180°$ et $(270-2n')°$. Tous ces vecteurs ont une valeur fondamentale qui ne gît pas dans l'un des 8 secteurs de la figure 5.1. Dans le pire des cas les vecteurs des cadrans I et III s'annulent complètement et ne participent pas à la somme finale et dans tous les autres cas ils s'additionnent et donnent un vecteur gisant dans le cadran II qui n'en fera que grossir la somme. Considérons donc les $(N/3)(8\cdot 1/16) = N/6$ vecteurs disponibles du cadran II.

Nous pouvons donc écrire la somme sur les vecteur restants du cadran II ainsi :

$$\left|\sum_{j=0}^{\frac{N}{6}-1} e^{2\pi i(zj/N+f'(j))}\right|^2 .$$

Il y a naturellement un abus de notation ici qui n'est fait que pour simplifier la notation. Cette somme sera assurément inférieur si tous les vecteurs sont regroupés en deux paquets orthogonaux, soit $90°$ et $180\ °$. Tous les vecteurs dont la valeur fondamentale est inférieure à $135°$ subissent une rotation pour les amener à $90°$ et tous ceux qui sont supérieur à $135°$ sont amenés vers $180°$. La somme se simplifie donc à

$$\begin{aligned}\left|\sum_{j=0}^{\frac{N}{6}-1} e^{2\pi i(zj/N+f'(j))}\right|^2 &\geq \left|\frac{N}{12}(-1)+\frac{N}{12}i\right|^2 \\ &=\frac{N^2}{12^2}\left|-1+i\right|^2 = \frac{2N^2}{12^2} \geq \mathsf{c}N^2.\end{aligned} \tag{5.1}$$

CQFD

Nous utiliserons la notations suivante pour décrire l'entier le plus proche d'un nombre $k \in \mathbb{R}$: $\lfloor k \rceil = k + \gamma$ où $-1/2 \leq \gamma < 1/2$.

Théorème 5.1.1 *Soient D un entier rationnel positif sans diviseur quadratique et $\mathfrak{D}$ l'anneau d'intégrité qu'il engendre. Alors le régulateur $\Re$ peut être calculé ainsi :*

1. *Choisissez un entier $q \geq 3S^3$.*

2. *Calculez l'état*
$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle \, |0\rangle^{\otimes h(D)} . \tag{5.2}$$

3. *Calculez l'état*
$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle \left| \hat{f}(a) \right\rangle . \tag{5.3}$$

4. *Mesurez le second registre pour obtenir l'état*
$$\frac{1}{\sqrt{p}} \sum_{j=0}^{p-1} |x_0 + [jS]\rangle \left| \hat{f}(x_0) \right\rangle . \tag{5.4}$$

5. *Appliquez la transformation de Fourier au premier registre avant de le mesurer. Si le résultat est supérieur à q/n répétez la procédure à partir de l'étape 2.*

6. *Répétez jusqu'à l'obtention de deux résultats, c et d inférieurs q/n.*

7. *Calculez successivement les réduites d'ordre m, p_m/q_m de c/d et pour chaque p_m vérifiez si $\mathfrak{a}_-(\lfloor p_m q/(cN) \rceil)$ est un voisin proche de l'idéal $\mathfrak{i}$.*

8. *Le régulateur est proche de la plus petite valeur calculée de $\lfloor p_m q/(cN) \rceil$ s'avérant être proche de $\mathfrak{i}$.*

Démonstration :

L'étape 1 spécifie de choisir un entier q supérieur à $3(N\Re)^3$. Bien que nous ne connaissons pas $\Re$, nous savons qu'il est de l'ordre $\mathcal{O}(\Delta^{1/2+o(1)})$, voir [14] et [27]. Le nombre q peut donc être choisi sans que $\Re$ ne soit connu, puisque nous connaissons une borne supérieure. La taille, $h(D)$, de l'ancille étant déterminée par un polynôme en $\mathcal{O}(\log D)$, le nombre de qubits nécessaire à nos calculs sera donc polynomial dans la taille de notre problème : c'est à dire $\log(D)$.

Nous montrerons ici que cet algorithme calcule avec une bonne probabilité deux nombres c et d de la forme $c = \lfloor kq/S \rceil$ et $d = \lfloor lq/S \rceil$, où $k, l \in \mathbb{N}$.

Après l'étape 4, nous avons en notre possession l'état

$$\frac{1}{\sqrt{p}} \sum_{j=0}^{p-1} |x_0 + [jS]\rangle \left| \hat{f}(x_0) \right\rangle \tag{5.5}$$

où $p = p' + 1$ et $q = \lfloor p'S \rfloor + r$ pour $p', r \in \mathbb{N}$ et $0 \leq r < S$. Après la transformation de Fourier, nous aurons l'état

$$\frac{1}{\sqrt{pq}} \sum_{j=0}^{p-1} \sum_{l=0}^{q-1} e^{2\pi i (x_0 + [jS])l/q} |l\rangle \left| \hat{f}(x_0) \right\rangle. \tag{5.6}$$

Calculons maintenant la probabilité d'obtenir, lors de la mesure du premier registre, un l de la forme $l = k'q/S + \varepsilon$, où $0 \leq k' \leq S$ et $-1/2 \leq \varepsilon \leq 1/2$:

$$\mathcal{P}(l) = \frac{1}{qp} \left| \sum_{j=0}^{p-1} e^{2\pi i [jS]/q} \right|^2. \tag{5.7}$$

Posons que $[jS] = jS + \varsigma_j$ où $-1 < \varsigma_j < 1$. Nous pouvons donc écrire

$$\frac{l[jS]}{q} = (\frac{k'}{S} + \frac{\varepsilon}{q})(jS + \varsigma_j) = \underbrace{\frac{k'jS}{S}}_{\in \mathbb{N}} + \frac{k'\varsigma_j}{S} + \frac{\varepsilon jS}{q} + \frac{\varepsilon \varsigma_j}{q}. \tag{5.8}$$

Étant donné qu'$l \leq q/n$, nous savons que

$$\left| \frac{k'\varsigma_j}{S} + \frac{\varepsilon \varsigma_j}{q} \right| \leq \frac{1}{n}. \tag{5.9}$$

De plus

$$\left| \frac{\varepsilon Sp}{q} \right| \leq \frac{Sp}{2q} = \frac{1}{2} \frac{Sp}{\lfloor Sp \rfloor + r} \leq \frac{1}{2} \frac{Sp}{Sp - 1} \leq \frac{3}{4}. \tag{5.10}$$

pour tous les $S \geq 2$. Posons

$$f'(j) = \left| \frac{k'\varsigma_j}{S} + \frac{\varepsilon \varsigma_j}{q} \right|$$

et $z = \varepsilon Sp/q$, alors

$$\mathcal{P}(l) = \frac{1}{pq} \sum_{j=0}^{p-1} e^{2\pi i (zj/p + f'(j))} \tag{5.11}$$

où $|z| < 3/4$ et $|f'(j)| < 1/n$. Le lemme 5.1.0.2 s'applique et nous en concluons que

$$\mathcal{P}(l) \geq \frac{\mathsf{c}p^2}{pq} = \frac{\mathsf{c}p}{q} > \frac{\mathsf{c}}{S}. \tag{5.12}$$

Donc, la probabilité d'obtenir un l spécifique de la forme $l = k'q/S+\varepsilon$ est supérieur à 1 sur un polynôme en S. Il ne nous reste plus qu'à compter le nombre de l ayant cette forme. Étant donnée que $0 < l = k'q/S + \varepsilon < q/n$, où $0 \leq k' \leq S$, et que $q/S > 1$, nous savons que chaque $k' \in \{0, \ldots, S\}$ engendre un l différent. Étant donné la limite imposé à l nous en déduisons que k varie de 0 à S/n. Ce qui implique qu'il y a environ S/n valeurs de l ayant la forme $l = k'q/S + \varepsilon$. De plus $q = \lfloor p'S \rfloor + r$, où $0 \leq r < S$, nous savons donc que $q/S \leq (p' + 1) = p$. La probabilité d'obtenir un l quelconque de la forme $l = k'q/S + \varepsilon$ est

$$\mathcal{P}(l \text{ soit de la forme } k'q/S + \varepsilon) \geq \frac{\mathsf{c}pS}{qn} \geq \frac{\mathsf{c}p}{np} = \frac{\mathsf{c}}{n}. \tag{5.13}$$

La probabilité d'obtenir un l de la forme désirée est donc supérieur à une constante.

Nous désirons maintenant démontrer que k/l est une réduite de c/d, où $c = \lfloor kq/S \rceil$ et $d = \lfloor lq/S \rceil$. Supposons, sans perte de généralité, que $0 < k \leq l \leq S$, alors

$$\left|\frac{c}{d} - \frac{k}{l}\right| = \left|\frac{kq + \varepsilon_k S}{lq + \varepsilon_l S} - \frac{k}{l}\right| = \left|\frac{S(\varepsilon_k l - \varepsilon_l k)}{l^2 q + \varepsilon_l S l}\right| \leq$$
$$\left|\frac{S(l+k)}{2l^2 q - 2Sl/2}\right| \leq \left|\frac{S}{lq - S/2}\right|.$$

Montrons que

$$\frac{S}{(lq - S/2)} \leq \frac{1}{(2l^2)}. \tag{5.14}$$

Sachant que $q \geq 3S^3$, nous pouvons écrire la chaîne d'inégalités suivantes :

$$4Sl^2 \leq 2lq - S \Longrightarrow 4Sl^2 \leq 6lS^3 \Longrightarrow 4S^2 \leq 6S^3.$$

La dernière inégalité étant toujours vrai, nous en concluons que l'équation 5.14 est, elle aussi, vrai. Ce qui implique, par le théorème 2.4.2, que k/l est une réduite de c/d.

De plus, sachant que $c = \lfloor kq/S \rceil = kq/S + \varepsilon$, nous avons $S = kq/c + \varepsilon S/c$ ou $S = kq/c + \varepsilon_S$ où

$$\varepsilon_S = \frac{\varepsilon S^2}{kq + \varepsilon S} \leq \frac{\varepsilon S^2}{kq - S^2} \leq \frac{\varepsilon S^2}{kq - q} \leq \frac{\varepsilon S^2}{(k-1)q} \leq \frac{\varepsilon}{(k-1)} < \varepsilon.$$

Donc
$$|S - \lfloor kq/c \rceil| \leq 1. \tag{5.15}$$
kq/c est donc très proche de S la période de $\hat{f}$. Connaissant kq/c, nous pouvons donc en temps polynomial vérifier que l'idéal $\mathfrak{i}$ se trouve proche de $kq/(cN)$, puisque $S = N\Re$, où $N \in \mathcal{O}(\log(\Delta))$. Nous pouvons donc trouver le régulateur en temps polynomial. *CQFD*

5.2 Le logarithme discret sur le quasi-groupe

Nous nous servirons de l'algorithme calculant le régulateur afin de calculer le logarithme discret.

Théorème 5.2.1 *Soit $\mathfrak{a}_i$ un idéal $\in \mathfrak{D}$, alors la distance δ_i de l'idéal peut être calculée ainsi*

1. *Calculez le régulateur $\Re$.*
2. *Choisissez un entier rationnel $M > 2\Re$ ainsi qu'un entier rationnel $N > n\sqrt{D}$ tel que $|M\lfloor \Re N \rceil - M\Re N| \leq 1/4$.*
3. *Créez l'état*
$$\frac{1}{\sqrt{M\lfloor N\Re \rceil}\sqrt{\lfloor N\Re \rceil}} \sum_{a=0}^{(M\lfloor N\Re \rceil - 1)} \sum_{b=0}^{(\lfloor N\Re \rceil - 1)} |a\rangle\, |b\rangle \left| \hat{f}(Na\delta_i + b) \right\rangle. \tag{5.16}$$
4. *Mesurez le troisième registre pour obtenir l'état*
$$\frac{1}{\sqrt{M\lfloor N\Re \rceil}} \sum_{a=0}^{M\lfloor N\Re \rceil - 1} |a\rangle \left| \left\lceil \frac{a\delta_i}{\Re} \right\rceil \Re N - a\delta_i N + \gamma_a \right\rangle \left| \hat{f}(k) \right\rangle. \tag{5.17}$$
5. *Appliquez la transformation de Fourier à l'état précédent puis mesurez les deux premiers registres pour obtenir une paire (c, d).*
6. *Recommencez les étapes 3,4 et 5 jusqu'à l'obtention de deux paires (c_1, d_1) et (c_2, d_2), telles que $d_i < \Re N/n$ et $\mathrm{pgcd}(d_1, d_2) = 1$.*
7. *Calculez r et s tels que $rd_1 + sd_2 = 1$ ainsi que $C = (rc_1 + sc_2)/(NM)$. Calculez l'entier rationnel t tel que $C - t\Re < \Re$, puis utilisez cette information pour calculer δ_i exactement.*

Démonstration :

L'entier N peut être calculé à l'aide du développement en fraction continue. Cette procédure est décrite dans [15]. De plus $\lfloor \Re N \rceil = \Re N + \lambda$ et $\lambda \leq 1/4M$.

Le lecteur devrait désormais être familiarisé avec ce type de procédure quantique. Par conséquent, l'état décrit à l'étape 3 ne constituera pas une surprise.

Après la mesure du troisième registre, a et b étant corrélés, nous pouvons donc conclure que si nous avons obtenu l'état $\hat{f}(k)$ alors $a\delta_i N + b = k + t\Re N + \gamma_a$ où $-1 \leq \gamma_a \leq 1$ et $t \in \mathbb{Z}$. La Transformation de Fourier étant indépendante du sous-groupe de départ, nous pouvons supposer que $k = 0$. Le coefficient b étant inférieur à $(\lfloor N\Re \rceil)$, nous devons donc utiliser $\lceil a\delta_i/\Re \rceil$ pour t. Avec cette valeur, $b = \lceil \frac{a\delta_i}{\Re} \rceil \Re N - a\delta_i N + \gamma_a$ variera de 0 à $(\lfloor N\Re \rceil)$.

Nous sommes intéressés à montrer qu'après la transformation de Fourier et la mesure des 2 premiers registres, nous obtiendrons, avec une bonne probabilité, une paire (c, d) telle que

$$c = d\delta_i NM - \lfloor d\delta_i/\Re \rfloor \Re NM + \gamma_d, \tag{5.18}$$

où $-1/2 \leq \gamma_d \leq 1/2$. Après la transformation de Fourier nous aurons l'état

$$\frac{1}{M\lfloor N\Re \rceil \sqrt{\lfloor N\Re \rceil}} \sum_{a,c=0}^{(M\lfloor N\Re \rceil -1)} \sum_{b,d=0}^{(\lfloor N\Re \rceil -1)} e^{2\pi i(ac+bdM)/(M\lfloor \Re N \rceil)} \left|c\right\rangle \left|d\right\rangle \left|\hat{f}(k)\right\rangle. \tag{5.19}$$

Nous devons calculer la probabilité d'obtenir une paire (c, d) respectant la condition (5.18) :

$$\mathcal{P}(c,d) = \frac{1}{\lfloor N\Re \rceil (M\lfloor N\Re \rceil)^2} \left| \sum_{a=0}^{M\lfloor N\Re \rceil -1} e^{2\pi i(ac+bdM)/(M\lfloor \Re N \rceil)} \right|^2. \tag{5.20}$$

Nous pouvons développer $(ac + bdM)$ et obtenir

$$ac + bdM = (d\left\lceil \frac{a\delta_i}{\Re} \right\rceil - \left\lfloor \frac{d\delta_i}{\Re} \right\rfloor)\Re NM + a\gamma_d + dM\gamma_a. \tag{5.21}$$

Nous nous intéressons à la partie fractionnaire de l'équation précédente lorsqu'elle est divisée par $M\lfloor \Re N \rceil = M(\Re N + \lambda)$. Calculons ε, le reste, dans $ac + bdM = tM(\Re N + \lambda) + \varepsilon$. Nous pouvons écrire

$$(d\left\lceil \frac{a\delta_i}{\Re} \right\rceil - \left\lfloor \frac{d\delta_i}{\Re} \right\rfloor)\Re NM + a\gamma_d + dM\gamma_a = tM\Re N + tM\lambda + \varepsilon.$$

Posons $t = (d\lceil \frac{a\delta_i}{\Re} \rceil - \lfloor \frac{d\delta_i}{\Re} \rfloor) \in \mathbb{Z}$. Avec cette valeur de t, ε doit nécessairement être égal à

$$-\lambda M(d\left\lceil \frac{a\delta_i}{\Re} \right\rceil - \left\lfloor \frac{d\delta_i}{\Re} \right\rfloor) + a\gamma_d + dM\gamma_a.$$

Nous pouvons remplacer $\lceil \frac{a\delta_i}{\Re} \rceil$ par $a\delta_i/\Re + \varsigma_a$ et $\lfloor \frac{d\delta_i}{\Re} \rfloor$ par $d\delta_i/\Re - \varsigma_d$ où $0 \leq \varsigma_a, \varsigma_d \leq 1$. Donc

$$\varepsilon = -\lambda M \left(d\frac{a\delta_i}{\Re} + d\varsigma_a - a\frac{d\delta_i}{\Re} + a\varsigma_d \right) + a\gamma_d + dM\gamma_a.$$

En simplifiant nous obtenons

$$\varepsilon = a(\gamma_d - \lambda M \varsigma_d) + dM(\gamma_a - \lambda \varsigma_a). \tag{5.22}$$

Posons $z = |\gamma_d + \lambda M \varsigma_d|$, alors par notre choix de M, $z \leq 3/4$. Posons $f'(a) = dM(\gamma_a - \lambda\varsigma_a)/(M\lfloor \Re N \rceil)$, alors, d étant inférieur à $\Re N/n$, nous avons $|f'(a)| \leq 1/n$. Nous pouvons réécrire la probabilité d'obtenir une paire (c, d) respectant la condition (5.18) ainsi

$$\mathcal{P}(c,d) = \frac{1}{(\lfloor N\Re \rceil)(M(\lfloor N\Re \rceil))^2} \left| \sum_{a=0}^{M(\lfloor N\Re \rceil)-1} e^{2\pi i (f'(a) + za/(M\lfloor \Re N \rceil))} \right|^2. \tag{5.23}$$

Nous pouvons donc appliquer le lemme 5.1.0.2 et obtenir

$$\mathcal{P}(c,d) \geq \frac{c(M(\lfloor N\Re \rceil))^2}{(\lfloor N\Re \rceil)(M(\lfloor N\Re \rceil))^2} \geq \frac{\mathsf{c}}{\Re N}. \tag{5.24}$$

Le nombre de paires (c, d) ayant cette forme est purement conditionné par le nombre de valeurs pouvant être prises par d. Il y a exactement $\lfloor N\Re \rceil$ valeurs possibles pour d. La probabilité d'obtenir une paire quelconque de cette forme est donc à $\frac{\mathsf{c}}{\Re N}(\lfloor N\Re \rceil - 1) \geq \mathsf{c}$, où c est choisi de telle manière à assurer la validité des inégalités. La probabilité d'obtenir une paire ayant les propriétés désirées est donc supérieure à une constante.

Supposons que nous ayons deux paires (c_1, d_1) et (c_2, d_2) ainsi que r et s tels que $rd_1 + sd_2 = 1$. Par définition $C = \delta_i - (a\lfloor d_1\delta_i/\Re \rfloor + b\lfloor d_2\delta_i/\Re \rfloor)\Re + (a\gamma_{d_1} + b\gamma_{d2})/(NM)$. Sachant que $|a|$ et $|b|$ sont inférieures au $\max(d_1, d_2)$, par les propriétés du pgcd, nous pouvons écrire, étant donné le choix de M, $|(a\gamma_{d_1} + b\gamma_{d2})/(NM)| \leq |2RN/NM| \leq 1$. Ceci implique que $C - \delta_i$ est à une distance constante d'un multiple de $\Re$. Le régulateur étant connu, nous pouvons donc retrouver en temps polynomial la distance δ_i. *CQFD*

5.3 Une analyse plus poussée

Le lecteur attentif aura cependant compris que la situation n'est pas aussi simple que les deux derniers algorithmes le laissent entendre. Spécifiquement, les deux démonstrations supposent que la distance entre un idéal et un nombre réel calculée par l'algorithme est parfaitement connue,— elle n'est pas l'approximation d'un nombre réel quelconque. Ceci n'est cependant pas réaliste puisque nous travaillons avec des logarithmes de nombres quadratiques ; donc des nombres réels sur lesquels notre précision est limitée par un soucis pratique. Malheureusement monsieur HALLGREN ne tient pas compte de cette réalité et n'analyse pas plus en détail ses algorithmes. Nous nous devons ici de corriger cette omission. Nous présentons ici une analyse plus poussée en deux segments.

Supposons que nous ayons $\hat{p}$ bits de précision. À chaque arrondissement notre erreur croit donc de $2^{-\hat{p}}$. Le nombre d'arrondissements étant borné par un polynôme en $\log(D)$, pour un $c \in \mathbb{N}$, notre erreur, ϑ, à la fin du calcul est bornée par $\mathcal{O}(\log(D)^c 2^{-\hat{p}})$.

Dans les deux algorithmes, nous connaissons $\partial(\hat{\mathfrak{a}}(x), x)$ parfaitement $\pm\vartheta$, notre erreur. Et donc, lorsque $\partial(\hat{\mathfrak{a}}(x), x) \leq \vartheta$, nous n'avons aucun moyen de savoir si l'idéal $\hat{\mathfrak{a}}(x)$ calculé est à gauche ou à droite de x. Tout ce que nous pouvons affirmer, c'est que l'idéal calculé est l'idéal le plus proche de x, puisque nous connaissons, par le corollaire 3.3.0.1, la distance minimum entre deux idéaux. La précision de nos calculs peut donc être choisie de telle manière à ce que la distance minimum entre deux idéaux soit toujours supérieur d'au moins 2 fois à l'imprécision maximum accumulable dans nos calculs. En conclusion, sans nous trop attarder, nous savons que nous avons calculé soit l'idéal à gauche ou soit l'idéal le plus proche. Lorsque nous avons calculé l'idéal le plus proche, le calcul de notre fonction n'est plus nécessairement ce qu'il devrait être. Les probabilités de nos deux algorithmes quantiques peuvent donc être faussées si ce phénomène se produit trop souvent. Combien de calculs erronés de la fonction $\hat{f}$ pouvons nous souffrir avant que ces algorithmes ne faillissent ?

Considérons premièrement l'algorithme calculant le régulateur $\mathfrak{R}$. Il y a deux endroits délicats dans la démonstration qui doivent être reconsidérés. Premièrement l'équation (5.7), qui devient l'équation (5.11). Et ensuite le calcul du nombre de l de la forme $l = k'q/S + \varepsilon$. Dans le calcul du nombre de l ayant la forme désirée, ce nombre ne dépend pas du calcul de $\hat{f}$ mais uniquement de la transformation de Fourier. Nous devons donc voir ce qui se passe à l'équation (5.11). Cette somme est prise sur tous les éléments y tels que $\hat{f}(y) = \hat{f}(x_0)$. C'est ici que peut intervenir un calcul erroné de $\hat{f}$. Pour un x_0 fixé, combien de fois, $\hat{f}(x_0 + [jS])$ peut-elle être mal calculée et ne pas participer à la superposition (5.5). La réponse est fort simple, n'importe quelle fraction constante inférieur à $1/12$ des calculs de $\hat{f}(x_0 + [jS])$ est acceptable. Supposons que nous ayons une fraction d'erreurs inférieure ou égale à $1/12$. À l'équation (5.11) nous devrons donc prendre la somme pour tous les j de 0 à $p - 1$, où $p/12$ des possibilités auraient pour amplitude 0,— ce qui implique une renormalisation différente de l'état (5.5). L'identité du lemme 5.1.0.2 s'applique cependant toujours, puisque même si toutes les erreurs étaient survenues sur des vecteurs du second cadran, il reste une portion constante de taille exponentielle assurant la validité de la démonstration et donc de l'identité. Une fraction de $1/12$ correspond à $1/4$ des valeurs du cadran II. Même si elles se produisaient toutes en un seul bloc, la démonstration de l'identité fonctionnerait toujours. La constante c sera plus petite que l'original, mais la probabilité finale d'obtenir un l de la forme voulue, sera toujours supérieure à une constante.

Étant donné que $p \geq 3S^2$, dans le théorème 5.1.1, le nombre d'erreurs acceptable est exponentiellement grand. De plus, pour chaque x_0, nous pouvons accepter la même fraction d'erreurs. Le nombre de calculs erronés de $\hat{f}$ varie donc approximativement entre $3S^2/12$ et $3S^3/12$. Ce qui est énorme ! Bien que nous ne puissions rien dire de plus sur la distribution des distances sur l'axe des réels, il serait surprenant qu'un si grand nombre d'entre elles soit proche d'un treillis de nombres rationnels.

Le même raisonnement s'applique sans aucune variation à l'algorithme calculant le logarithme discret. Peut-on faire mieux ? Pour l'algorithme calculant le régulateur, nous pouvons en effet faire mieux. Nous pouvons affirmer qu'avec l'ajout de trois petites conditions, la démonstration de l'algorithme demeure pertinente et l'algorithme fonctionne selon les probabilités prévues. Pour arriver à cette conclusion, nous devons approfondir quelque peu l'analyse précédente. Après la mesure du second registre nous avons en notre possession l'état (5.4). Le second registre est dans l'état $|\hat{f}(x_0)\rangle = |\mathfrak{a}_i, w\rangle$, où $\mathfrak{a}_i$ est l'idéal obtenu lors de la mesure et w est le «compte» de x_0, soit le combientième entier qui a été appliqué sur l'idéal $\mathfrak{a}_i$ par la fonction $\hat{f}$.

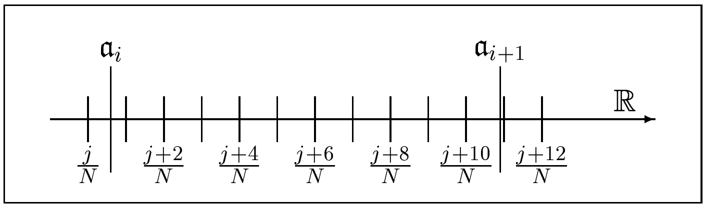
Premièrement, nous requerrons que l'erreur maximale, ϑ_m possible soit inférieure à $1/(2N)$, ou

$$2\vartheta_m < \frac{1}{N}. \tag{5.25}$$

Ceci nous assurera qu'à l'équation (5.4), les entiers corrélés avec $|\hat{f}(x_0)\rangle$ sont soit les bons, ou un de leurs voisins immédiats. Le lecteur peut se référer à la figure 5.2 afin de mieux visualiser la situation, celle-ci ne constitue qu'un exemple simplifié, mais elle éclaire bien la situation. Les deux traits verticaux étiquetés $\mathfrak{a}_i$ et $\mathfrak{a}_{i+1}$ représentent les distances associées aux idéaux $\mathfrak{a}_i$ et $\mathfrak{a}_{i+1}$. Tous les autres traits représentent les nombres réels utilisés par la fonction $\hat{f}$.

En nous basant sur l'exemple de la figure 5.2, lors du calcul de $\hat{f}$ pour l'entier $j+1$, si $\partial(\mathfrak{a}_i, (j+1)/N) \leq \vartheta$ où ϑ est l'erreur accumulé lors du calcul de $\hat{f}$, alors il est fort possible que $j+1$ soit associé à l'idéal $\mathfrak{a}_{i-1}$. Si $j+1$ est associé avec $\mathfrak{a}_i$, nous ne sommes pas embêté. Cependant si $j+1$ est associé avec l'idéal $\mathfrak{a}_{i-1}$, nous nous apercevons immédiatement que l'entier $(j+2)$ sera, lui, associé avec l'idéal $\mathfrak{a}_i$. Le compte de l'entier $(j+2)$ sera soit 0, soit 1. Nous ne pouvons en être certain, cependant nous savons que pour tous les entiers qui suivent et qui seront associés au même idéal,

FIG. 5.2 – Exemple simplifié



la fonction $\hat{f}$ sera toujours calculée de la même façon, c'est-à-dire que pour toutes ces valeurs, la même séquence de multiplications et de réductions des mêmes idéaux sera utilisée; $\partial(\mathfrak{a}_i,(j+k)/N)$ aura donc toujours le même biais. Par biais nous entendons que si $\hat{f}(k) = (\mathfrak{a}_-(k/N),1)$ et que l'erreur sur $\partial(\mathfrak{a}_-(k/N),k/N)$ est ϑ_k alors $\hat{f}(k+j) = (\mathfrak{a}_-(k/N),j+1)$, $\partial(\mathfrak{a}_-(k/N),(k+j)/N) = \partial(\mathfrak{a}_-(k/N),k/N)+j/N$ et l'erreur sur $\partial(\mathfrak{a}_-(k/N),(k+j)/N)$ est ϑ_k, pour $j < d-2$.

La leçon de tout ceci est la suivante,— ceci constitue le second ajout : une fois la mesure du second registre faite, nous pouvons calculer le nombre maximum d'entiers qui peuvent être associés avec l'idéal $\mathfrak{a}_i$ obtenu, appelons ce nombre d. Si le compte, w, obtenu est situé entre 1 et $d-2$, nous passons à l'étape 5 de l'algorithme, sinon nous retournons à l'étape 1. Le nombre d peut être calculé puisque nous connaissons l'idéal $\mathfrak{a}_i$. Nous pouvons donc calculer la distance entre $\mathfrak{a}_i$ et $\mathfrak{a}_{i+1}$, et de là calculer d,— le compte, lui, va de 0 à $d-1$. Donc, si w est compris entre 1 et $d-2$ inclusivement, nous savons que pour tous les $[jS]$ de l'équation (5.4), un entier a été associé avec l'idéal $\mathfrak{a}_i$ obtenu. Il y a donc bel et bien p valeurs dans la somme (5.4).

Ces valeurs qui sont intriquées à $\hat{f}(x_0)$ servent ensuite d'entrée à la transformation de Fourier. La démonstration de l'algorithme est la même sauf aux équations (5.8) et (5.9). Premièrement, lorsque nous développons $[jS]$ en $jS+\varsigma_j$, les conditions sur la valeur ς_j sont modifiées en $-2 < \varsigma_j < 2$, puisque s'il y a une erreur sur l'entier associé à $\mathfrak{a}_i$ pour le cycle j l'entier intriqué est un voisin de celui qui devrait l'être. Ceci implique que l'équation (5.9) devient

$$\left|\frac{k'\varsigma_j}{S} + \frac{\varepsilon\varsigma_j}{q}\right| \leq \frac{2}{n}. \tag{5.26}$$

Ce qui nous amène à conclure que si nous n'acceptons, aux étapes 5 et 6, que des résultats inférieurs à $q/(2n)$, alors l'équation (5.9) redevient valide et nous pouvons toujours appliquer le lemme 5.1.0.2.

Ces trois ajustements ($2\vartheta_m < \frac{1}{N}$, $1 \leq w \leq d-2$ et $l \leq q/(2n)$) nous assurent de la véracité de la démonstration de l'algorithme. Seule la constante c sera modifiée par ces trois ajustements ; elle sera 2 fois plus petite,— en choisissant pour cet algorithme un N supérieur à $2n(\log(1 + 1/\sqrt{\Delta}))$, nous pouvons conserver la même valeur pour la constante. Nous pouvons donc calculer le régulateur.

La situation n'est cependant pas équivalente lors du calcul du logarithme discret. À l'équation (5.17) nous obtenons encore une fois un état $|\hat{f}(x_0)\rangle = |\mathfrak{a}_i, w\rangle$. Cette équation est une somme prise pour tous les a de 0 à $M \lfloor N\Re \rceil - 1$. Idéalement, nous voudrions montrer que pour tous les a , il y existe un b tel que l'amplitude de $|a\rangle |b\rangle$ n'est pas zéro. Idéalement cela est vrai. Mais malheureusement la propriété de non-associativité du quasi-groupe nous rattrape.

En effet, soient a et b tels que $\hat{f}(Na\delta_i + b) = (\mathfrak{a}_{-}(a\delta_i + b/N), 1)$. Alors nous aimerions supposer que $\hat{f}(Na\delta_i + b + 1) = (\mathfrak{a}_{-}(a\delta_i + (b + 1)/N), 2)$ et ainsi de suite jusque à $\hat{f}(Na\delta_i + b + j)$ où $j < d - 2$. Malheureusement, ceci n'est pas toujours vérifiée. Pour réaliser cela nous devons expliciter la manière par laquelle $\hat{f}(Na\delta_i + b)$ est calculée. Nous devons tout d'abord calculer $\mathfrak{a}_{-}(a\delta_i)$ à l'aide de l'exponentiation d'un idéal de base quelconque, ensuite nous devons calculer $\mathfrak{a}_{-}(b/N)$, puis nous devons multiplier ensemble les deux idéaux calculés et enfin réduire afin d'obtenir l'idéal $\mathfrak{a}_{-}(a\delta_i + b/N)$. Donc a étant fixé, le résultat de la multiplication dépend de $\mathfrak{a}_{-}(b/N)$. Si par hasard $\mathfrak{a}_{-}(b/N) \neq \mathfrak{a}_{-}((b + j)/N)$ pour $j < d - 2$, alors l'idéal $\mathfrak{a}_{-}(a\delta_i + b/N)$ calculé ne sera pas nécessairement égal à $\mathfrak{a}_{-}(a\delta_i + (b + j)/N)$, mais surtout $\partial(\mathfrak{a}_{-}(a\delta_i + (b + j)/N), a\delta_i + (n + j)/N)$, fort probablement, ne sera pas égal à $\partial(\mathfrak{a}_{-}(a\delta_i + b/N), a\delta_i + b/N) + j/N$ et $\vartheta_{a,b} \neq \vartheta_{a,(b+j)}$. Dans ce cas nous aurons possiblement sauté une valeur de w, et donc l'amplitude associé à $|a\rangle |b\rangle |\mathfrak{a}_i, w\rangle$ sera 0.

Donc pour chaque a, soit la valeur b associé est la bonne, soit elle est une voisine immédiate de la bonne ou l'amplitude de cette valeur a est zéro. Dans le premier cas, tout va bien. Dans le second cas, nous pouvons adapter la démonstration de l'algorithme, tout comme nous l'avons fait dans le cas du régulateur, afin d'extraire malgré tout la période et dans le dernier cas nous devons nous en remettre à la discussion faite au tout début de cette section. Pour combien de valeur de a l'amplitude sera-t-elle zéro ? Il semble raisonnable d'affirmer que pour une forte proportion des a , il y ait un compte, ou plusieurs, tel que l'amplitude de $|a\rangle |b\rangle \left|\hat{f}(x_0)\right\rangle$ est égale à 0. Malheureusement, nous sommes dans l'impossibilité d'en dire plus pour l'instant. De plus la valeur de N ou de M ne semble pas affecter cette constatation ; seule la probabilité de tomber sur un compte imposant une amplitude égale à 0 varie en fonction de N. Il est donc tout à fait légitime de se demander si cet algorithme fonctionne. Est-il possible de dériver une formulation de la probabilité de succès, fonction de D, M et N, nous permettant de décider s'il vaut la peine d'utiliser cet algorithme ? C'est dans cette direction évidente que les prochains effort dans ce domaine devront être appliqués. Nos travaux dans cette dernière section donnent une solution quantique définitive au problème du régulateur, mais le logarithme discret semble lui pour l'instant sans solution efficace vérifiable. Nous pouvons nous consoler en nous disant que le logarithme discret constitue peut-être une hypothèse calculatoire classique qui résistera à la puissance des calculateurs quantiques.

Conclusion

Nous avons présenté dans les 4 premiers chapitres de ce mémoire, un algorithme d'échange de clefs ainsi que tout le matériel algébrique et la théorie des nombres pertinents permettant au lecteur d'être confortable avec les objets mathématiques utilisés. De plus nous avons fourni une première preuve de l'existence d'un algorithme quantique permettant de calculer le régulateur $\Re$ ainsi qu'une analyse d'un l'algorithme proposé pour calculer le logarithme discret sur le quasi-groupe. Cet algorithme d'échange de clefs ne constituait guère qu'une curiosité théorique tant que les protocoles, dont la sûreté était basée sur le logarithme discret ou sur la factorisation, étaient considérés comme sûr. Malgré que l'algorithme du chapitre 4 soit au moins aussi sûr, sinon plus, que ceux basés sur la factorisation, étant donné sa complexité mathématique et sa complexité d'implantation, son utilisation ne pouvait être que limitée. Avec l'avènement de l'informatique quantique et de l'algorithme de Shor, ces hypothèses calculatoires se sont vues mises à mal,— consultez [34] pour un survol étoffé des implications de l'algorithme de Shor. En effet, si l'informatique quantique peut un jour prendre son envol de manière pratique, même laborieusement, la sécurité de nos protocoles traditionnels ne serait plus. L'algorithme de Buchmann et Williams offrait alors l'espoir de nous fournir une nouvelle hypothèse calculatoire classique qui eut résistée à l'émergence des calculateurs quantiques. Ce ne sont là peut-être qu'espoirs éphémères, puisque les nouveaux algorithmes présentés par Sean Hallgren semblent réduire la possibilité de fonctions à sens unique classique qui le demeurait dans le monde quantique. Bien sûr, une certaine dose de travail doit toujours être abattue afin de prouver hors de tout doute l'efficacité de l'algorithmes calculant le logarithme discret sur le quasi-groupe. Mais nous sommes de l'opinion que les efforts futurs doivent être mis à bon escient afin de découvrir des fonctions à sens uniques quantiques, quitte à ce qu'elles ne soient pas efficacement calculables classiquement. Certaines telles fonction ont déjà été proposée, voir [31] ; il faudrait de surcroît vérifier si le protocoles [26] basé sur les corps quadratiques de congruence de fonctions résiste aux deux algorithmes de Hallgren, ce qui semble douteux à première vu étant donné que la distance dans ce protocole est un entier rationnel. Certains travaux, qui supposent l'existence de permutations à sens unique quantique, ont déjà été accomplis, voir [12]. Quoi qu'il en soit, toute la cryptographie qui se base sur une clef de taille fixe est incertaine. Soit, ce que la physique quantique enlève d'une main elle le redonne de l'autre en nous fournissant un algorithme nous permettant d'échanger une clef en toute sécurité. En effet un protocole quantique d'échange, ou d'amplification, de clefs a été proposé qui offre une sécurité qu'aucun protocole classique ne peut offrir, voir [1]. Mais cette clef doit être utilisée dans un protocole semblable au masque aléatoire de VERNAM si nous ne voulons pas que le protocole de chiffrement soit cassé. Étant donné que l'intimité du commun des mortels serait, elle, jetée aux orties par l'avènement d'ordinateurs quantiques, même s'ils étaient d'emploi fort difficile, puisque les agences de renseignements, et certains organismes très puissants, seraient certainement en mesure de les mettre en œuvre à des fins qui ne seraient pas toujours avouables, nous ne pouvons ici que réitérer le besoin de nouveaux outils cryptographiques tenant compte de l'informatique quantique.

Annexe A

Introduction à l'informatique quantique

Nous décrirons ici les rudiments de l'informatique quantique. L'informatique quantique est un domaine récent de l'informatique, et aussi, d'une certaine manière, de la physique. Cette discipline n'est restée qu'une curiosité jusqu'à ce quelques résultats fort intéressants viennent titiller la curiosité des informaticiens. Le plus important est certainement l'algorithme de Shor, avec lequel la factorisation et le logarithme discret trouve une solution efficace sur un ordinateur quantique. D'autres résultats sont tout aussi intéressants, bien que ne nécessitant pas toujours l'ordinateur quantique. Par exemple la distribution de clefs à des fins cryptographiques peut être accomplie quantiquement, sans ordinateur quantique, et avec une sûreté impossible à atteindre par des protocoles classiques. Nous ne couvrirons ici que les bases mathématiques et les postulats de la physique quantique nécessaires à l'atteinte de notre objectif, qui est de présenter l'algorithme de Shor.

A.1 Le qubit

Tout comme l'ordinateur classique, l'ordinateur quantique possède une unité élémentaire d'information que nous appellerons **qubit**. Un qubit est vecteur sur $\mathbb{C}^2$ de norme égale à 1. Nous ne nous préoccuperons pas du sens physique de cette affirmation, mais que du formalisme mathématique. Donc un qubit est représenté par un vecteur $\binom{\alpha}{\beta}$ où α et β sont des nombres complexes,— $a + bi$ pour a et b réels.

Certains qubits de base méritent d'être désignés par des symboles particuliers :

$$\begin{aligned} |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad & |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \\ & |\nearrow\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad \text{et } |\searrow\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}. \end{aligned} \tag{A.1}$$

La notation «$|\ \rangle$» s'appelle la notation de Dirac. Elle ne signifie rien de plus que la notation vectorielle ordinaire, mais elle s'avère extrêmement pratique pour jongler avec les qubits. Naturellement, $|0\rangle$ et $|1\rangle$ sont orthonormaux. Ils forment donc une base de $\mathbb{C}^2$. Les qubits $|\nearrow\rangle$ et $|\searrow\rangle$ peuvent donc être exprimés en fonction de $|0\rangle$ et $|1\rangle$:

$$|\nearrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |\searrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{A.2}$$

La dernière équation nous permet de voir la différence principale entre un bit classique et un qubit. Alors qu'un bit classique n'est constitué que d'une seule valeur discrète, 0 ou 1, le qubit, lui, possède un spectre de possibilités beaucoup plus grand. Le qubit peut être dans une superposition d'états. Il est à la fois 0 et à la fois 1, selon des amplitudes bien déterminées. Donc, un qubit quelconque $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$, où $|\alpha|^2 + |\beta|^2 = 1$, est dans une superposition de α fois $|0\rangle$ et β fois $|1\rangle$. Les coefficients α et β sont appelés amplitudes. Il n'est pas quelque part à mi-chemin entre $|0\rangle$ et $|1\rangle$, il est les deux à la fois. Remarquons que la conditions $|\alpha|^2 + |\beta|^2 = 1$ nous assure que le vecteur $|\psi\rangle$ est de norme égale à 1.

Si $|\psi\rangle = \left(\begin{smallmatrix} \alpha \\ \beta \end{smallmatrix}\right)$ nous définirons $\langle\psi|$ comme étant égal à $(\bar{\alpha}, \bar{\beta})$. «$\langle\ |$» est donc le vecteur transposé et conjugué de «$|\ \rangle$». Naturellement $\langle\psi|\,|\psi\rangle = 1$. Nous utiliserons la notation simplifiée $\langle\psi|\,|\psi\rangle = \langle\psi|\psi\rangle$ pour le produit scalaire.

A.1.1 Opérations sur un qubit

Un qubit ne peut subir qu'une évolution dite unitaire que nous appellerons opérateur. Un opérateur est représenté par une matrice complexe U de dimension 2×2, telle que $U^\dagger U = \mathbb{I}_2$, où $U^\dagger = \overline{U}^T$. Une telle matrice est dite unitaire. Ceci implique que tout opérateur quantique peut être «défait», ou inversé :$|\psi\rangle = U^\dagger U |\psi\rangle$. De plus la composition d'opérateur quantique (multiplication de matrice), est stable, c'est-à-dire que la multiplication de deux opérateurs est un opérateur : si $U = U_1 U_2$ alors $U^\dagger U = \mathbb{I}_2$, où $U^\dagger = U_2^\dagger U_1^\dagger$.

Les matrices de Pauli sont les quatre opérateurs suivants :

$$\begin{aligned} \sigma_0 = \mathbb{I}_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \sigma_x = X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ \sigma_y = Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \sigma_z = Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \end{aligned} \tag{A.3}$$

Les opérateurs définissent des applications qui peuvent, dans les cas de X et Z, être réécrites ainsi :

$$\sigma_x : \begin{cases} |0\rangle & \longmapsto & |1\rangle \\ |1\rangle & \longmapsto & |0\rangle \end{cases} \qquad \sigma_z : \begin{cases} |0\rangle & \longmapsto & |0\rangle \\ |1\rangle & \longmapsto & -|1\rangle \end{cases} \tag{A.4}$$

L'opérateur de Walsh-Hadamard, $\mathrm{H} = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$, est certainement l'un des plus importants. Il représente l'application suivante :

$$\mathrm{H} : \begin{cases} |0\rangle & \longmapsto & \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |\nearrow\rangle \\ |1\rangle & \longmapsto & \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |\searrow\rangle \end{cases} . \tag{A.5}$$

De plus l'opérateur de Hadamard possède le fabuleuse propriété d'être son propre inverse, c'est-à-dire qu'$\mathrm{H}^2 = \mathbb{I}_2$, ou $\mathrm{H}^\dagger = \mathrm{H}$. Et donc

$$\mathrm{H} : \begin{cases} |\nearrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) & \longmapsto & |0\rangle \\ |\searrow\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) & \longmapsto & |1\rangle \end{cases} . \tag{A.6}$$

A.1.2 Mesure d'un qubit

L'information contenue dans un qubit n'est accessible qu'à travers une opération de mesure. Une mesure n'est pas un opérateur au sens défini à la section précédente, car cette opération n'est pas unitaire, et donc inversible. Il y a, de manière générale, une perte d'information quantique lors d'une mesure.

Dans le cas qui nous concerne, nous définirons une mesure $\mathcal{M}$ sur un espace de Hilbert de dimension 2 comme un ensemble de projecteurs tels que :

$$\sum_{P_i \in \mathcal{M}} P_i = \mathbb{I}_2 \ \text{ ainsi que } \ P_i P_j = 0 \text{ si } i \neq j.$$

Un projecteur P possède les propriétés d'être invariable lorsque multiplié par lui-même : $P^2 = P$; ainsi que d'être hermitien : $P^\dagger = P$. Nous verrons que cette propriété est fort intuitive. Les projecteurs canoniques, ou calculatoires, sont définis comme les matrices :

$$P_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \text{ et } P_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}. \tag{A.7}$$

L'application de la mesure calculatoire à un état quelconque $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ est définie ainsi :

$$\mathcal{M}\,|\psi\rangle = \begin{cases} P_0\,|\psi\rangle \mapsto \frac{P_0|\psi\rangle}{\sqrt{p_0}} = |0\rangle & \text{avec probabilité } p_0 = \langle\psi|\,P_0\,|\psi\rangle = |\alpha|^2 \\ P_1\,|\psi\rangle \mapsto \frac{P_1|\psi\rangle}{\sqrt{p_1}} = |1\rangle & \text{avec probabilité } p_1 = \langle\psi|\,P_1\,|\psi\rangle = |\beta|^2 \end{cases} \tag{A.8}$$

Si l'état $|\nearrow\rangle$ est mesuré dans la base calculatoire, nous obtiendrons avec probabilité $1/2$ l'état $|0\rangle$ et avec probabilité $1/2$ l'état $|1\rangle$. Les mêmes statistiques seraient obtenues avec l'état $|\searrow\rangle$. Il est donc impossible de différencier les états $|\nearrow\rangle$ et $|\searrow\rangle$ à l'aide d'une mesure dans la base canonique. Nous entendons par cela que si un ensemble de copies du vecteur $|\nearrow\rangle$ nous était donné, nous ne pourrions affirmer que cet ensemble n'est pas composé d'états $|\searrow\rangle$ si nous n'avons accès qu'à la mesure calculatoire.

Cette définition permet de définir une mesure comme une projection sur n'importe quelle base orthonormale de $\mathbb{C}^2$. Nous pouvons donc définir une mesure sur les vecteurs $|\nearrow\rangle$ et $|\searrow\rangle$. Cette nouvelle mesure, appelons-la $\mathcal{M}^+$, nous permettrait de différencier entre les états $|\nearrow\rangle$ et $|\searrow\rangle$. Mais elle ne nous permettrait pas de différencier les états $|0\rangle$ et $|1\rangle$. La «perte» d'information quantique est appelé réduction du paquet d'onde. L'état $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ se transformera en l'état classique $|0\rangle$ ou en l'état classique $|1\rangle$, pour la base calculatoire. Cette transformation est irréversible, puisqu'elle comporte un certain degré d'incertitude, que nous ne pouvons pas inverser de manière générale. Il est évident qu'une seconde application d'une mesure sur un état $|\psi\rangle$ ne modifie en rien le résultat de la première application. Après tout, $|0\rangle$ projeté dans la base calculatoire ne peut que devenir $|0\rangle$.

A.2 Deux qubits

À l'instar des bits classiques, une paire de qubits peut prendre 4 possibilités : $|00\rangle$, $|01\rangle$, $|10\rangle$ et $|11\rangle$. Un système quelconque de 2 qubits est défini comme un vecteur sur $\mathbb{C}^4$. Si $|\psi\rangle$ est un système quelconque de 2 qubits, alors $|\psi\rangle$ peut être écrit ainsi :

$$|\psi\rangle = \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \sigma\,|11\rangle = \sum_{i=0}^{2^2-1} \alpha_i\,|i\rangle \tag{A.9}$$

où $\sum_{i=0}^{2^2-1} |\alpha_i|^2 = 1$, cette condition impose au vecteur d'être de norme 1. Remarquons au passage que $|00\rangle = |0\rangle |0\rangle$. Cette opération, celle de juxtaposer deux qubits (deux systèmes $\in \mathbb{C}^2$) et d'obtenir un système décrit par un vecteur $\in \mathbb{C}^4$, s'appelle le produit tensoriel, que nous écrirons «$\otimes$». Donc $|00\rangle = |0\rangle |0\rangle = |0\rangle \otimes |0\rangle$. De manière générale, pour deux états $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ et $|\varphi\rangle = \gamma |0\rangle + \sigma |1\rangle$, alors

$$|\psi\rangle \otimes |\varphi\rangle = \begin{pmatrix} \alpha\gamma \\ \alpha\sigma \\ \beta\gamma \\ \beta\sigma \end{pmatrix} = \alpha\gamma |00\rangle + \alpha\sigma |01\rangle + \beta\gamma |10\rangle + \beta\sigma |11\rangle .$$

Théorème A.2.1 *Le produit tensoriel possède les propriétés suivantes :*

1. *Il n'est pas commutatif.*
2. *Il est associatif.*
3. $(A + B) \otimes (C + D) = A \otimes C + A \otimes D + B \otimes C + B \otimes D$.
4. $\lambda A \otimes \mu B = \lambda\mu(A \otimes B)$.
5. $(A \otimes B)(C \otimes D) = AC \otimes BD$.
6. $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$.

Le concept de mesure sur 2 qubits est similaire tout en étant plus complexe. Nous pouvons soit mesurer l'un des deux qubits, que nous appellerons mesure partielle, ou les deux qubits. Nous maintiendrons une définition similaire pour la mesure. Une mesure $\mathcal{M}$ est donc un ensemble de projecteur, P_i, orthogonaux deux à deux sur $\mathbb{C}^4$ tel que leurs somme soit l'identité. L'application d'une mesure à un système de deux qubits peut être décrite par par une équation similaire à l'équation (A.8), mais où il existe 4 possibilités au lieu de 2. Donc si $|\psi\rangle = (\alpha, \beta, \gamma, \sigma)^T$ alors

$$\mathcal{M} |\psi\rangle = \begin{cases} P_0 |\psi\rangle \mapsto \frac{P_0|\psi\rangle}{\sqrt{p_0}} = |00\rangle & \text{avec probabilité } p_0 = \langle\psi| P_0 |\psi\rangle = |\alpha|^2 \\ P_1 |\psi\rangle \mapsto \frac{P_1|\psi\rangle}{\sqrt{p_1}} = |01\rangle & \text{avec probabilité } p_1 = \langle\psi| P_1 |\psi\rangle = |\beta|^2 \\ P_2 |\psi\rangle \mapsto \frac{P_2|\psi\rangle}{\sqrt{p_2}} = |10\rangle & \text{avec probabilité } p_2 = \langle\psi| P_2 |\psi\rangle = |\gamma|^2 \\ P_3 |\psi\rangle \mapsto \frac{P_3|\psi\rangle}{\sqrt{p_3}} = |11\rangle & \text{avec probabilité } p_3 = \langle\psi| P_3 |\psi\rangle = |\sigma|^2 \end{cases} \tag{A.10}$$

où P_0, P_1, P_2 et $P_3 \in \mathbb{C}^4$.

Ne mesurer qu'un seul qubit est une opération équivalente à cumuler 2 des résultats de l'équation (A.10). Si nous ne mesurons que le premier qubit dans la base calculatoire, nous obtiendrons donc $|0\rangle$ avec probabilité $\alpha^2 + \beta^2$. Le système de deux qubit $|\psi'\rangle$ résultant sera donc $\frac{\alpha|00\rangle+\beta|01\rangle}{\sqrt{\alpha^2+\beta^2}}$. Ceci est donc équivalent à une mesure $\mathcal{M} = P_0 \otimes \mathbb{I}_2 + P_1 \otimes \mathbb{I}_2$ où P_0 et P_1 sont des projecteurs calculatoires dans $\mathbb{C}^2$. La définition du produit tensoriel n'est ici qu'une généralisation de celle décrite plus haut. Si $U = (u_{ij})$ où $0 \leq i, j < 2$ et V sont des matrices $\in \mathbb{C}^{2\times 2}$ alors

$$U \otimes V = \begin{pmatrix} u_{00}V & u_{01}V \\ u_{10}V & u_{11}V \end{pmatrix}$$

et $U \otimes V$ est une matrice $\in \mathbb{C}^{4\times 4}$. Le produit tensoriel de deux matrices unitaires génère une matrice unitaire ; donc un opérateur.

Soit l'état $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Cet état, l'un des quatre états de Bell, est fort intéressant puisqu'il ne peut pas être décrit comme le produit tensoriel de deux qubits distincts. C'est à dire qu'il n'existe pas α, β, γ et σ tels que $|\Phi^+\rangle = (\alpha\gamma, \alpha\sigma, \beta\gamma, \beta\sigma)^T$. Ce système de 2 qubits n'est donc pas équivalent à la juxtaposition de deux systèmes de 1 qubit. Nous dirons qu'un tel système est intriqué[1]. Un système intriqué implique une corrélation des résultats. Si nous mesurons le premier qubit de $|\Phi^+\rangle$ et que nous obtenons $|0\rangle$, l'état total du système se réduira à $|\phi'\rangle = \frac{1/\sqrt{2}|00\rangle+0|01\rangle}{1/\sqrt{2}} = |00\rangle$. Donc, si nous mesurons par la suite le second qubit, nous obtiendrons toujours $|0\rangle$. Le cas est parfaitement symétrique avec le résultat $|1\rangle$. Les résultats sont donc corrélés. Ce qui ne se serait pas produit avec une paire de qubits non intriqués. Les résultats seraient toujours indépendants et fonction des amplitudes de départ.

Les états de Bells sont :

$$\begin{aligned} |\beta_{00}\rangle = \left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\1\end{pmatrix}, \quad |\beta_{10}\rangle = \left|\Phi^-\right\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\-1\end{pmatrix}, \\ |\beta_{01}\rangle = \left|\Psi^+\right\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\1\\0\end{pmatrix}, \quad |\beta_{11}\rangle = \left|\Psi^-\right\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\-1\\0\end{pmatrix}, \end{aligned} \tag{A.11}$$

Ils sont tous intriqués. De plus, ils forment une base orthonormale de $\mathbb{C}^4$.

[1]En anglais «entangled», en allemand «verschränkt».

A.2.1 Opérateurs sur 2 qubits

Les opérateurs sur deux qubits sont des matrices $\in \mathbb{C}^{4\times4}$, telles que si U est un opérateur alors $U^\dagger U = \mathbb{I}_4$. Jusqu'ici, rien de nouveau. Les opérateurs sur 2 qubits peuvent être définis à l'aide du produit tensoriel d'opérateur agissant sur 1 qubit. Par exemple $\mathrm{H}\otimes\mathrm{H}$ appliqué à l'état $|00\rangle$ produira

$$(\mathrm{H}\otimes\mathrm{H})\,|00\rangle = \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\otimes\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle) = \frac{1}{2}\sum_{i=0}^{2^2-1}|i\rangle\,. \tag{A.12}$$

C'est à dire une superposition égale des vecteurs de la base canonique. Par superposition égale, nous entendons une combinaison linéaire des vecteurs de la base où toutes les amplitudes ont la même valeur.

La composition d'opérateurs générant des opérateurs, nous pouvons donc construire des opérateurs complexes sur 2 qubits à l'aide de la composition et du produit tensoriel. Soit l'opérateur suivant

$$\mathrm{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1\\ 0 & 0 & 1 & 0 \end{pmatrix} \text{ ou CNOT} : \begin{cases} |00\rangle & \longmapsto & |00\rangle\\ |01\rangle & \longmapsto & |01\rangle\\ |10\rangle & \longmapsto & |11\rangle\\ |11\rangle & \longmapsto & |10\rangle \end{cases}. \tag{A.13}$$

Cet opérateur, l'opérateur de négation contrôlée[2], ou le XOR quantique, est fort important en informatique quantique. Cet opérateur, à l'instar des états de Bells, ne peut pas être écrit comme le produit tensoriel de deux opérateurs agissant sur 1 qubit. Un opérateur n'étant pas un système physique dans le cadre décrit ici, nous ne pouvons donc pas lui appliquer le concept d'intrication. Mais ce genre d'opérateur non décomposable est généralement en relation étroite avec l'intrication des systèmes quantiques. Considérons l'opérateur $\mathrm{CNOT}(\mathrm{H}\otimes\mathbb{I}_2)$,— ceci consiste à appliquer d'abord l'opérateur $(\mathrm{H}\otimes\mathbb{I}_2)$ et ensuite l'opérateur CNOT. Si cet opérateur est appliqué au système $|00\rangle$ nous obtiendrons $|\Phi^+\rangle$. Nous pouvons décrire l'opérateur

[2] controlled-NOT

ainsi :

$$
\begin{aligned}
\mathrm{CNOT}(\mathrm{H} \otimes \mathbb{I}_2) &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \left(\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right) \\
&= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix} \\
&= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & -1 \\ 1 & 0 & -1 & 0 \end{pmatrix}
\end{aligned}
\tag{A.14}
$$

ou

$$
\mathrm{CNOT}(\mathrm{H} \otimes \mathbb{I}_2) : \begin{cases} |00\rangle & \longmapsto & |\Phi^+\rangle \\ |01\rangle & \longmapsto & |\Psi^+\rangle \\ |10\rangle & \longmapsto & |\Phi^-\rangle \\ |11\rangle & \longmapsto & |\Psi^-\rangle \end{cases}
\tag{A.15}
$$

Nous possédons donc une méthode simple pour générer les 4 états de Bells. Les états de Bells formant une base orthonormale de $\mathbb{C}^4$, nous pouvons donc mesurer dans cette base tout système quantique de 2 qubits. Cette mesure est cependant équivalente à un opérateur transformant les vecteurs de la base de Bell en vecteurs de la base canonique, à l'aide de l'opérateur $(\mathrm{H} \otimes \mathbb{I}_2)\mathrm{CNOT}$, suivi d'une mesure dans la base calculatoire.

L'opérateur CNOT applique une négation au second qubit conditionnellement au fait que le premier qubit soit dans l'état $|1\rangle$. De là lui vient son nom. Nous pouvons définir une opération logique contrôlée de manière générale ainsi :

$$
\text{C–}U : \left\{ |a\rangle\, |b\rangle \quad \longmapsto \quad |a\rangle \otimes U^a\, |b\rangle \right.
\tag{A.16}
$$

où a et $b \in \{0, 1\}$ sont classiques. Par linéarité, l'équation (A.16) décrit le comportement générale d'un opérateur U contrôlé. La notation matricielle est la suivante

$$
\text{C–}U = \begin{pmatrix} \mathbb{I}_2 & 0 \\ 0 & U \end{pmatrix} .
\tag{A.17}
$$

A.3 Circuits quantiques

A.3.1 Plus de deux qubits

Tous les concepts développés dans le cadre de systèmes à 1 qubit ou à 2 qubits se généralisent à des systèmes de n qubits.

Un système de n qubits est représenté par un vecteur $\in \mathbb{C}^{2^n}$ de norme égale à 1. On peut donc représenter un état $|\psi\rangle$ à l'aide d'une superposition des vecteurs canoniques :

$$|\psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle \tag{A.18}$$

où $\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$ et $|i\rangle = (a_0, a_1, \ldots, a_{2^n-1})^T$ où $i = j \Longrightarrow a_j = 1$ et $i \neq j \Longrightarrow a_j = 0$.

La notion de mesure est similaire, mais les projecteurs sont maintenant des projecteurs de dimension $2^n \times 2^n$, orthogonaux deux à deux, dont la somme est égale à l'identité.

Nous définirons, pour un opérateur U, le produit tensoriel de U avec lui même n fois ainsi :

$$U^{\otimes n} = U \otimes U^{\otimes(n-1)} \text{ et } U^{\otimes 1} = U. \tag{A.19}$$

Donc

$$U^{\otimes n} = \underbrace{U \otimes U \cdots \otimes U}_{n \text{ fois}}.$$

L'opérateur générant le système de n qubits consistant en une superposition égale de tous les vecteurs canoniques est simplement $\mathrm{H}^{\otimes n}$. L'intriquation est définie de la même manière, c'est à dire un état de n qubits ne pouvant être écrit comme le produit tensoriel de systèmes de moins de n qubits.

Le théorème suivant est d'une importance capitale en physique et en informatique quantique. Il exprime l'une des différences principales entre le monde classique et le monde quantique.

Théorème A.3.1 (Non-duplication quantique[3]) *Si $|\psi\rangle$ et $|\varphi\rangle$ sont des systèmes à n qubits, alors il n'existe pas d'opérateur U ni de système $|\varphi\rangle$ tels que $U(|\psi\rangle |\varphi\rangle) = |\psi\rangle |\psi\rangle$ pour un état $|\psi\rangle$ quelconque.*

[3] No-cloning theorem

Preuve :

Supposons qu'un opérateur U existe tel que $U(|\psi\rangle\,|\varphi\rangle) = |\psi\rangle\,|\psi\rangle$, pour un état $|\psi\rangle$ quelconque. Supposons qu'U soit capable de cloner $|\psi_1\rangle$ et $|\psi_2\rangle$. Alors nous pouvons écrire

$$\begin{aligned} U(|\psi_1\rangle\,|\varphi\rangle) &= |\psi_1\rangle\,|\psi_1\rangle \\ U(|\psi_2\rangle\,|\varphi\rangle) &= |\psi_2\rangle\,|\psi_2\rangle\,. \end{aligned} \tag{A.20}$$

Nous pouvons prendre le produit scalaire des deux équations et obtenir :

$$\begin{aligned} (\langle\psi_2|\,\langle\varphi|)U^\dagger U(|\psi_1\rangle\,|\varphi\rangle) &= \langle\psi_2|\,\langle\psi_2|\,|\psi_1\rangle\,|\psi_1\rangle \\ \langle\psi_2|\psi_1\rangle\,\underbrace{\langle\varphi|\varphi\rangle}_{1} &= (\langle\psi_2|\psi_1\rangle)^2 \\ \langle\psi_2|\psi_1\rangle &= (\langle\psi_2|\psi_1\rangle)^2. \end{aligned} \tag{A.21}$$

Cette dernière équation est une équation sur des scalaires que nous pouvons réécrire ainsi : $x = x^2$. Et évidement, elle n'a pour solution qu'$x = 0$ et $x = 1$. Ce qui implique que l'opérateur U ne peut dupliquer que des états quantiques qui sont soit colinéaires ou orthogonaux. Un opérateur U ne peut donc pas dupliquer un état $|\psi\rangle$ quelconque. *CQFD*

A.3.2 Circuits quantiques

Bien que plusieurs modèles d'ordinateurs quantiques existent, celui offrant la plus grande facilité d'approche pour les informaticiens est sans doute le circuit quantique. Il est constitué de fils où circule l'information (quantique ou classique), ainsi que de portes logiques implantant des opérateurs. Le théorème de non-duplication quantique ainsi que le principe de réversibilité obligent le circuit à avoir la même taille à l'entré et à la sortie.

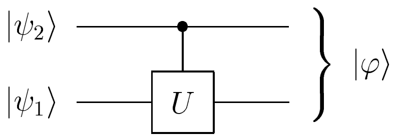
Le circuit le plus simple est certainement celui qui ne fait rien sur 1 qubit.

$$|\psi\rangle \;\text{———}\boxed{\mathbb{I}_2}\text{———}\; |\psi\rangle$$

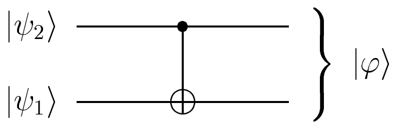
Naturellement l'opérateur $\mathbb{I}_2$ peut être remplacé par un autre opérateur :

$$|0\rangle \;\text{———}\boxed{\mathrm{H}}\text{———}\; |\nearrow\rangle \qquad\qquad |1\rangle \;\text{———}\boxed{\mathrm{H}}\text{———}\; |\searrow\rangle$$

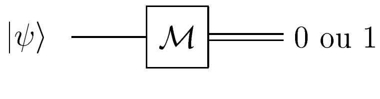
Nous décrirons le circuit accomplissant les opérateurs contrôlés ainsi :



où $|\varphi\rangle \in \mathbb{C}^4$. Plus particulièrement, nous écrirons pour CNOT :

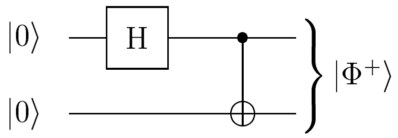


où $|\varphi\rangle \in \mathbb{C}^4$. Une mesure sera écrite comme un opérateur et l'information classique en émergeant sera décrite à l'aide d'un fil double.



Nous sommes maintenant prêts à présenter un premier circuit accomplissant une tâche intéressante : la téléportation quantique, figure A.1.

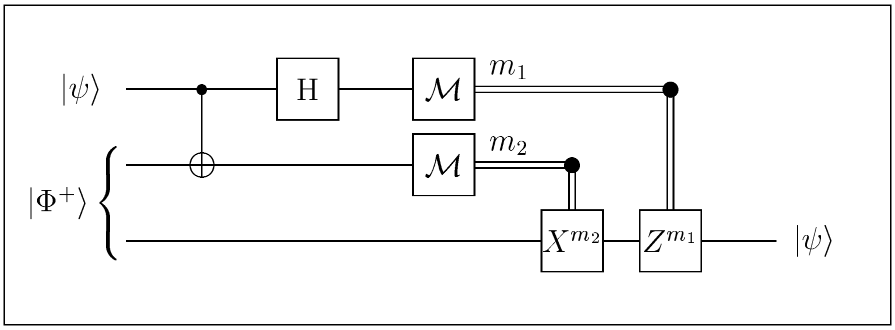
Ce circuit permet à deux partenaires de se communiquer des états quantiques. Ce résultat est fort surprenant étant donnée l'impossibilité de mesurer un état quantique quelconque pour en connaître les amplitudes. Supposons qu'Alice ait en sa possession les deux qubits du haut dans le circuit A.1, soit l'état $|\psi\rangle$ et la moitié de l'état $|\Phi^+\rangle$. Bob possédant, lui, le fil du bas, soit l'autre moitié de l'état $|\Phi^+\rangle$. Naturellement Alice et Bob purent préalablement se rencontrer pour fabriquer l'état $|\Phi^+\rangle$ à l'aide du circuit



Ceci étant fait, la procédure peut commencer. L'état à l'entrée du circuit est

$$|\psi_0\rangle = |\psi\rangle \left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}[\alpha\,|0\rangle\,(|00\rangle + |11\rangle) + \beta\,|1\rangle\,(|00\rangle + |11\rangle)] \tag{A.22}$$

FIG. A.1 – Circuit pour la téléportation



où $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$. Nous choisirons d'attribuer les deux qubits de gauche dans l'équation A.22 à Alice et le qubit de droite à Bob. Après l'application de l'opérateur CNOT, l'état global est devenu

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}[\alpha\,|0\rangle\,(|00\rangle + |11\rangle) + \beta\,|1\rangle\,(|10\rangle + |01\rangle)]. \tag{A.23}$$

Puis, après l'application de la porte logique H, l'état devient

$$|\psi_2\rangle = \frac{1}{2}[\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)]. \tag{A.24}$$

Nous pouvons réécrire $|\psi_2\rangle$ ainsi

$$\begin{aligned}|\psi_2\rangle = \frac{1}{2}[&|00\rangle\,(\alpha\,|0\rangle + \beta\,|1\rangle) + |01\rangle\,(\alpha\,|1\rangle + \beta\,|0\rangle)\\ &+ |10\rangle\,(\alpha\,|0\rangle - \beta\,|1\rangle) + |11\rangle\,(\alpha\,|1\rangle - \beta\,|0\rangle)],\end{aligned} \tag{A.25}$$

où naturellement, Alice possède toujours les deux qubits de gauche. Évidement, lorsqu'Alice mesurera ses 2 qubits dans la base canonique, elle obtiendra avec probabilité égale l'une des paires : $|00\rangle$,$|01\rangle$,$|10\rangle$ ou $|11\rangle$. Bob, lui, après la mesure, aura en sa possession l'un de quatre états possibles qui sera parfaitement déterminé par le résultat de la mesure faite par Alice. Donc, avec probabilité $1/4$, l'état total des 3 qubits après la mesure est

$$|\psi_3\rangle = \begin{cases} |00\rangle\,[\alpha\,|0\rangle + \beta\,|1\rangle] & \text{Si Alice a obtenu } |00\rangle \\ |01\rangle\,[\alpha\,|1\rangle + \beta\,|0\rangle] & \text{Si Alice a obtenu } |01\rangle \\ |10\rangle\,[\alpha\,|0\rangle - \beta\,|1\rangle] & \text{Si Alice a obtenu } |10\rangle \\ |11\rangle\,[\alpha\,|1\rangle - \beta\,|0\rangle] & \text{Si Alice a obtenu } |11\rangle \end{cases} \tag{A.26}$$

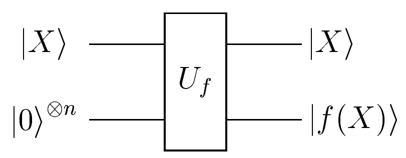
où les deux qubits d'Alice sont classiques. Bob a donc en sa possession un état qui peut être trivialement transformé, à l'aide des opérateurs σ_x et σ_z, en $|\psi\rangle$. Il a cependant besoin du résultat de la mesure appliquée à l'état $|\psi_2\rangle$ par Alice. Le premier qubit d'Alice indique un changement de signe et le second qubit une échange entre les valeurs $|0\rangle$ et $|1\rangle$. Si Alice a obtenu $|01\rangle$ ou $|11\rangle$, Bob doit appliquer l'opérateur de négation à son qubit afin d'échanger les amplitudes α et β, sinon il ne doit rien faire,— ce qui est équivalent à CNOT. Puis il doit changer la phase de son qubit conditionnellement au résultat du premier bit. C'est ce que fait la dernière porte du circuit. Et Bob obtient comme résultat un qubit identique au qubit d'entrée d'Alice. Le merveilleux de ce protocole consiste en la possibilité pour Bob et Alice à ne pas être dans la même pièce. Ils peuvent s'échanger au préalable les 2 qubits constituant $|\Phi^+\rangle$ puis s'éloigner autant qu'ils le désire avant de procéder à la téléportation. Alice n'a même pas besoin de savoir où se trouve Bob. Le résultat de la mesure effectuée par Alice peut être envoyé par les ondes hertziennes, ou même par le bon vieux courrier, à Bob qui peut, seul, compléter la procédure.

A.4 Parallélisme quantique

Ce que nous avons fait jusqu'ici est bien intéressant d'un point de vue mathématique, mais peut sembler plus ésotérique qu'utile dans une perspective informatique. Dans cette section, nous présenterons l'aspect qui différencie l'ordinateur quantique de l'ordinateur classique, ce qui donne au premier un avantage sur le second.

Un résultat important en informatique classique affirme que toute fonction $f : X \longrightarrow Y$ peut être implantée réversiblement. C'est- à-dire qu'il existe un circuit où toutes les portes logiques effectuent leurs calculs de manière réversible. La manière la plus simple, [3] ou [21], qui s'applique à toutes les fonctions, n'est pas nécessairement optimale pour toutes les fonctions f, mais elle n'exige pas une croissance exagérée du nombre de portes logiques par rapport au circuit original implantant f de manière non réversible. Le résultat global est le suivant, le circuit U implantant la fonction f accepte deux entrées $(X, 0)$. L'une contient la valeur sur laquelle la fonction doit être appliquée, X, et l'autre ne contient que des zéros. Le résultat à la sortie sera $(X, f(X))$. De cette manière, même les fonctions non injectives peuvent être inversées.

Ce qui nous intéresse ici, c'est que tout circuit U implantant une fonction f de manière classique, peut être implanté quantiquement de la manière suivante : Si $f : X \longmapsto Y$ où X nécessite m bits et Y n bits, alors



Qu'arrive-t-il si $|X\rangle$ est une superposition quelconque $|X\rangle = \sum_{i=0}^{2^m-1} \alpha_i |i\rangle$? La réponse est simple et surprenante : le circuit générera l'état global

$$\sum_{i=0}^{2^m-1} \alpha_i |i\rangle |f(i)\rangle . \tag{A.27}$$

Avec une seule utilisation du circuit, nous avons réussi à stocker dans le second registre toutes les valeurs possibles de l'image qui sont, d'ailleurs, intriquées avec leurs pré-images. Mais comment peut-on récupérer une information intéressante de cet embrouillamini ? C'est là toute la difficulté des algorithmes quantiques. Il est possible d'utiliser la sortie d'un tel circuit pour extraire efficacement une information qui serait autrement difficile à calculer.

A.5 L'algorithme de Shor

L'algorithme de Shor, [29], sert à calculer la période d'une fonction. C'est-à-dire que l'algorithme peut calculer, pour une fonction périodique $f : \mathbb{Z} \longrightarrow \mathbb{Z}$, le plus petit $r \in \mathbb{Z}$ tel que $\forall x, f(x) = f(x + r)$. Cette tâche est généralement difficile à calculer classiquement. La période d'un élément sur un groupe multiplicatif est un bon exemple de fonction que l'algorithme de Shor peut résoudre aisément. Il peut donc retrouver le plus petit $r \in \mathbb{Z}$ tel que $\forall \alpha, \alpha^r \equiv 1 \pmod p$ où p est un nombre premier,— l'algorithme fonctionne aussi si p n'est pas premier, nous calculerions alors l'ordre d'un élément sur un anneau. Cette capacité à calculer l'ordre d'un élément peut ensuite être utilisée pour factoriser ou pour calculer le logarithme discret,— ce qui nous permettrait entre autres d'attaquer le chiffre RSA ou le protocole d'échange de clefs de Diffie et Hellman,— tâche qui est toujours considérée comme impossible à réaliser classiquement dans des temps raisonnables.

L'algorithme utilise l'opérateur suivant, que nous appellerons : la transformation de Fourier quantique :

$$\text{TFQ} : |k\rangle \longmapsto \frac{1}{\sqrt{2^n}} \sum_{l=0}^{2^n-1} e^{2\pi i k l / 2^n} |l\rangle \tag{A.28}$$

où $|k\rangle$ et $|l\rangle$ sont des vecteurs de la base canonique de $\mathbb{C}^{2^n}$ et $i^2 = -1$. Cet opérateur est unitaire et peut être implanté avec un nombre raisonnable de portes quantiques, voir [29] ou [21] pour une description détaillée de la construction de la transformation de Fourier.

A.5.1 Factorisation

Supposons que nous possédions un oracle f nous retournant l'ordre d'un nombre modulo n : $\mathsf{O}(x) = r_x$. Nous pouvons écrire que $(x^{r_x/2} - 1)(x^{r_x/2} + 1) \equiv x^{r_x} - 1 \equiv 0 \pmod n$. Ce qui nous amène à conclure qu'étant donné que $(x^{r_x/2} - 1) > 1$, si $x > 1$, alors $\text{pgcd}(x^{r_x/2} - 1, n) | n$. Nous pourrions donc calculer un facteur de n. Ceci ne fonctionne naturellement que si r_x est pair et que $x \not\equiv -1 \pmod n$. Nous ne présenterons pas ici les détails algébriques, mais nous nous contenterons d'affirmer que la probabilité de succès lorsque la fonction f est appliquée sur un x choisi au hasard, où $1 < x < n-1$, est supérieure à $1 - 1/2^{k-1}$ où k est le nombre de facteurs premiers impairs de n. Donc, si un tel oracle existait, nous pourrions factoriser efficacement.

Nous utiliserons la technique décrite à la section A.4. Soit n un nombre à factoriser et soit $q = 2^{\lceil \log_2(n^2) \rceil}$,— $q = 2^t, t \in \mathbb{Z}$ tel que $n^2 \leq q < 2n^2$. Nous commencerons nos calculs avec l'état global

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle \, |0\rangle^{\otimes t} . \tag{A.29}$$

La fonction $f(a) = x^a \pmod n$ étant calculable en temps polynomial, il existe donc un circuit quantique efficace pouvant calculer l'état suivant à partir de l'état (A.29)

$$\frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a\rangle \, |x^a \pmod n\rangle . \tag{A.30}$$

Nous allons ensuite appliquer la transformation de Fourier sur le premier registre et obtenir la superposition

$$\frac{1}{q} \sum_{a=0}^{q-1} \sum_{c=0}^{q-1} e^{2\pi i a c/q} \, |c\rangle \, |x^a \pmod n\rangle \tag{A.31}$$

Nous mesurons finalement l'état des deux registres[4] dans la base canonique. Nous observerons alors $|c\rangle \left|x^k \pmod n\right\rangle$, où $0 \leq k < r_x$. Nous nous intéressons à la probabilité d'obtenir un état $|c\rangle \left|x^k \pmod n\right\rangle$ spécifique. Nous devons donc calculer la somme suivante :

$$\mathcal{P}(c, k) = \left| \frac{1}{q} \sum_{a : x^a \equiv x^k} e^{2\pi i a c/q} \right|^2 \tag{A.32}$$

[4]Nous aurions aussi pu mesurer le second registre de l'équation (A.30). Nous aurions alors obtenu une superposition $\sum_{j=0}^{A-1} |x_0 + j r_x\rangle \, |f(x_0)\rangle$ où $f(x_0)$ est le résultat obtenu lors de la mesure du second registre dans la base canonique et le premier registre est, lui, dans une superposition de tous les éléments ayant pour image $f(x_0)$. Nous aurions ensuite appliqué la transformation de Fourier au premier registre avant de le mesurer.

où nous prenons la somme pour tous les a, où $0 \leq a < q$, tels que $x^a \equiv x^k \pmod{n}$ et $\mathcal{P}(c,k)$ est la probabilité conjointe d'observer c et x^k. Étant donné $\mathsf{O}(x) = r_x$, cette somme peut être faite sur tous les a entre 0 et q tels que $a \equiv k \pmod{r_x}$. Donc, a est égal à $br_x + k$ pour un b judicieusement choisi. Nous pouvons donc réécrire l'équation (A.32) ainsi

$$\mathcal{P}(c,k) = \left| \frac{1}{q} \sum_{b=0}^{\lfloor (q-k-1)/r_x \rfloor} e^{2\pi i(br_x+k)c/q} \right|^2 . \tag{A.33}$$

Si $r_x c = tq + \{r_x c\}_q$ où $t \in \mathbb{Z}$ et $\{r_x c\}_q$ est le reste de $r_x c/q$ et $-q/2 \leq \{r_x c\}_q \leq q/2$, nous pouvons simplifier l'équation (A.33) ainsi :

$$\begin{aligned} \mathcal{P}(c,k) &= \left| \frac{1}{q} \sum_{b=0}^{\lfloor (q-k-1)/r_x \rfloor} \underbrace{e^{2\pi ikc/q} e^{2\pi itqb/q}}_{\text{magnitude de 1}} e^{2\pi ib\{r_x c\}_q/q} \right|^2 \\ &= \frac{1}{q^2} \left| \sum_{b=0}^{\lfloor (q-k-1)/r_x \rfloor} e^{2\pi ib\{r_x c\}_q/q} \right|^2 \end{aligned} \tag{A.34}$$

Posons $A = \lfloor (q-k-1)/r_x \rfloor + 1$ et $\gamma_c = 2\pi\{rc\}_q/q$. Alors cette somme peut être exprimée plus simplement, $\sum_{b=0}^{A-1} e^{ib\gamma_c}$, ce qui nous permet de reconnaître une série géométrique qui est égale à

$$\frac{e^{iA\gamma_c} - 1}{e^{i\gamma_c} - 1}. \tag{A.35}$$

Calculons la valeur de cette somme si $-\pi r_x/q \leq \gamma_c \leq \pi r_x/q$. Il y a exactement r_x valeurs de c, où $0 \leq c < q$, qui satisfont ces bornes. Cette affirmation peut être comprise en identifiant sur la droite des entiers toutes les positions qui sont un multiple de r_x ou de q entre 0 à $r_x q - 1$. À chaque multiple de q, (dq), il y a un multiple de r_x, (cr_x), tel que $-r_x/2 \leq cr_x - dq \leq r_x/2$. Ce qui est équivalent à $-r_x/2 \leq cr_x \pmod{q} \leq r_x/2$, ce qui implique que

$$\frac{-\pi r_x}{q} \leq \gamma_c \leq \frac{\pi r_x}{q}. \tag{A.36}$$

Étant donné que $A-1$ est plus petit que q/r_x nous pouvons affirmer d'une part que $0 < |e^{i\gamma_c} - 1| < |\gamma_c| < \pi/(A-1)$ et d'autre part $|e^{iA\gamma_c} - 1| > 2A|\gamma_c|/\pi$.

Le premier énoncé découle directement de l'équation (A.36). Il exprime le fait que l'arc de cercle sous-tendu par l'angle γ_c est plus grand que la corde sous-tendue par le même angle.

Reformulons le second énoncé ainsi : $g(\phi) = |e^{i\phi} - 1| > 2\phi/\pi$ pour $0 < \phi < \pi$. Alors, nous souvenant que $e^{i\phi}$ est un point sur le cercle de rayon 1, nous pouvons écrire que

$$\begin{aligned} g(\phi) =& \sqrt{(1-\cos(\phi)^2) + \sin^2(\phi)} \\ =& \sqrt{1 - 2\cos(\phi) + \cos^2(\phi) + \sin^2(\phi)} = \sqrt{2 - 2\cos(\phi)} > 0 \end{aligned}$$

La première dérivé de g, $g'(\phi) = \frac{\sin(\phi)}{\sqrt{2-2\cos(\phi)}} > 0$, nous indique que g est une fonction croissante.

La seconde dérivé de g, $= \frac{-(1-\cos(\phi))^2}{(2-2\cos(\phi))^{3/2}} < 0$ nous apprend que g est concave. La fonction g intersectant la fonction $h(\phi) = 2\phi/\pi$ en 0 et en π, nous en concluons que $g(\phi) > h(\phi)$ entre 0 et π.

Nous pouvons donc utiliser ces deux identités pour borner inférieurement l'équation (A.35) lorsque γ_c respecte la condition (A.36).

Donc

$$\begin{aligned} \left|\frac{e^{iA\gamma_c} - 1}{e^{i\gamma_c} - 1}\right| = \left|\frac{e^{i(A-1)\gamma_c} - 1}{e^{i\gamma_c} - 1} + e^{i(A-1)\gamma_c}\right| \geq \left|\frac{e^{i(A-1)\gamma_c} - 1}{e^{i\gamma_c} - 1}\right| - 1 \\ >& \frac{2(A-1)|\gamma_c|}{\pi|\gamma_c|} - 1 = \frac{2A}{\pi} - (2/\pi + 1) \\ >& \frac{2}{\pi}\left(\frac{q}{r_x} - 1\right) - (2/\pi + 1) = \frac{2q}{\pi r_x} - (4/\pi + 1) \\ >& \frac{2q}{\pi r} - 3. \end{aligned}$$

Donc

$$\begin{aligned} \mathcal{P}(c,k) >& \frac{1}{q^2}\left(\frac{2q}{\pi r_x} - 3\right)^2 > \frac{4q^2}{\pi^2 r_x^2} - \frac{12q}{\pi r_x} \\ >& \frac{4}{\pi^2 r_x^2} - \frac{12}{\pi r q} \\ >& \frac{1}{3r_x^2} \quad \text{pour un } n \text{ assez grand.} \end{aligned}$$

Donc la probabilité d'obtenir un c tel que la condition de l'équation (A.36) est vérifiée est supérieur à $\frac{1}{3r}$ lorsque le n à factoriser est suffisamment grand. Il ne nous reste plus qu'à montrer comment factoriser avec le c obtenu.

Nous savons par construction que

$$\frac{-r_x}{2} \leq r_x c - dq \leq \frac{r_x}{2}. \tag{A.37}$$

En divisant par $r_x q$ et en remaniant l'expression, nous obtenons

$$\left|\frac{c}{q} - \frac{d}{r_x}\right| \leq \frac{1}{2q}. \tag{A.38}$$

Nous connaissons c et q. Si nous pouvions calculez d/r_x tel que l'équation (A.38) soit satisfaite, nous aurions alors calculé la période. Nous pouvons affirmer qu'une seule fraction d/r_x tel que $r_x < n$ satisfait l'inégalité (A.38). Supposons, au contraire, que d_1/r_1 et d_2/r_2, où $r_1, r_2 < n \leq \sqrt{q}$, satisfassent (A.38). Alors nous pourrions écrire $|c/q - d_1/r_1| \leq 1/2q$ et $|c/q - d_2/r_2| \leq 1/2q$. Ce qui impliquerait, par l'inégalité triangulaire, que $|d_2/r_2 - d_1/r_1| \leq 1/q$. Donc $0 \leq r_1 d_2 - r_2 d_1 \leq r_1 r_2/q < 1$ ce qui nous amène à conclure que $r_1 d_2 - r_2 d_1 = 0$ et donc $d_1/r_1 = d_2/r_2$.

Nous devons donc calculer une fraction d/r_x tel que

$$\left|x - \frac{d}{r_x}\right| \leq \frac{1}{2q} \leq \frac{1}{2{r_x}^2}. \tag{A.39}$$

Par le théorème 2.4.2 nous savons que d/r_x est une réduite de c/q et par le théorème 2.4.1 nous savons que cette réduite est calculable en temps polynomial. Nous sommes donc en mesure de calculer p_n/q_n, une réduite d'ordre n, satisfaisant l'équation (A.39). Par construction, nous savons que r_x satisfait (A.38), nous en concluons donc que r_x est le dénominateur de la réduite p_n/q_n tel que $|c/q - p_n/q_n| \leq 1/2r_x^2$.

Si p_n et q_n n'ont pas de facteurs communs, ou que p_n n'a pas de facteurs communs avec r_x, alors nous avons calculé r_x qui est simplement égal q_n. Sinon, q_n est un facteur de r_x. Combien de c peuvent nous permettre de calculer r_x ? La théorie des nombres nous apprend qu'il y a exactement $\phi(r_x)$ valeurs possibles de d relativement premières à r_x. Nous savons que $\phi(r_x)/r_x > \upsilon/\log\log(r_x)$ où υ est une constante. La probabilité d'obtenir un état c nous permettant de factoriser est donc

$$\mathcal{P}(\text{c nous permette de factoriser}) > \frac{\phi(r_x)}{3r} > \frac{\upsilon}{\log\log(r_x)}. \tag{A.40}$$

Donc en répétant la procédure quantique $\mathcal{O}(\log\log(r_x))$ fois, notre probabilité de succès est supérieure à une constante proche de 1. Il est même possible d'augmenter la quantité de post-traitement classique après l'obtention de c et de diminuer l'espérance du nombre d'itérations quantiques à effectuer à une constante.

A.5.2 Le logarithme discret

L'algorithme calculant le logarithme discret est plus complexe que l'algorithme effectuant la factorisation. La preuve de sa complexité est aussi plus difficile. Nous ne donnerons ici que le début de la procédure. Le lecteur est donc encouragé à jeter un coup d'œil sur [29] s'il est friand de détails.

Considérons le corps $\mathbb{Z}_p$ et un générateur g de $\mathbb{Z}_p^*$. Nous cherchons alors à solutionner, pour tout $x \in \mathbb{Z}_p^*$, l'équation $g^r \equiv x \pmod p$. L'algorithme ressemble à celui de la factorisation mais utilise deux registres d'entrées dans une superposition égale de tous les nombres de 0 à $p-2$

$$\frac{1}{p-1}\sum_{a=0}^{p-2}\sum_{b=0}^{p-2} |a\rangle\,|b\rangle\,|0\rangle^{\otimes t} \tag{A.41}$$

où t est tel que $q = 2^t$ et $p < 2^t < 2p$. Ensuite, à l'aide d'un circuit unitaire, l'état suivant est calculé

$$\frac{1}{p-1}\sum_{a=0}^{p-2}\sum_{b=0}^{p-2} |a\rangle\,|b\rangle\,\left|g^a x^{-b} \pmod p\right\rangle. \tag{A.42}$$

La transformation de Fourier est ensuite appliquée de manière séparée aux deux premiers registres, l'état (A.42) étant transformé en

$$\frac{1}{q(p-1)}\sum_{c,d=0}^{q-1}\sum_{a,b=0}^{p-1} e^{\frac{2\pi i}{q}(ac+bd)}\,|c\rangle\,|d\rangle\,\left|g^a x^{-b} \pmod p\right\rangle. \tag{A.43}$$

Et puis on observe l'état dans la base canonique. Nous obtiendrons alors un état $|c\rangle\,|d\rangle\,\left|g^k\right\rangle$ avec probabilité

$$\mathcal{P}(c,d,k) = \left|\frac{1}{(p-2)q}\sum_{\substack{a,b\\ a-rb\equiv k}} e^{\frac{2\pi i}{q}(ac+bd)}\right|^2 \tag{A.44}$$

où cette somme est prise pour tous les a et b tels que $a-rb \equiv k \pmod{p-1}$. En faisant une restriction similaire à (A.36), nous pouvons montrer que cette probabilité est suffisamment grande, et qu'avec un nombre d'utilisations de la procédure quantique constant (mais grand) nous pouvons, à l'aide du développement en fraction continue et du théorème des restes chinois, calculer r.

Bibliographie

[1] Charles H. Bennett et Gilles Brassard. Quantum cryptography : Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984.

[2] Alain Bouvier, Michel George, et François Le Lionnais. *Dictionnaire des mathématiques.* Presses universitaires de France, seconde édition, 1983.

[3] Gilles Brassard. Notes du cours d'informatique quantique. Département d'informatique et de recherche opérationnelle, Université de Montréal, hiver 1999.

[4] Johannes A. Buchmann et Hugh C. Williams. A key-exchange system based on imaginary quadratic fields. *Journal of Cryptology : the journal of the International Association for Cryptologic Research*, 1(2) :107–118, 1988.

[5] Johannes A. Buchmann et Hugh C. Williams. A key-exchange system based on real quadratic fields. *Number Theory and Cryptography*, pages 9–25, 1990.

[6] Johannes A. Buchmann et Hugh C. Williams. A key-exchange system based on real quadratic fields. *CRYPTO 89 Proceedings*, pages 9–25, 1990.

[7] Duncan A. Buell. *Binary quadratic forms : Classical theory and modern computations.* springer-Verlag, 1989.

[8] Henri Cohen. *A Course In Computational Algebraic Number Theory.* springer-Verlag, 1993.

[9] Harvey Cohn. *Advanced number theory.* Dover, 1980.

[10] Whitfield Diffie et Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6) :644–654, 1976.

[11] Paul Dumais. *Hypothèses calculatoires en cryptographie quantique.* Thèse de doctorat, Université de Montréal, 2002.

[12] Paul Dumais, Dominic Mayers, et Louis Salvail. Perfectly concealing quantum bit commitment from any quantum one-way permutation. In *Advances in Cryptology, Eurocrypt 2000, Proceedings*, pages 300–315, 2000.

[13] Cynthia Dwork. Lattices and their application to cryptography. Lecture notes : `http://theory.stanford.edu/~csilvers/cs359/`.

[14] Hendrik. W. Lenstra Jr. Algorithms in algebraic number theory. *Bulletin of the american mathematical society*, 26(2) :211–244, avril 1992.

[15] Sean Hallgren. Polynomial-time quantum algorithms for pell's equation and the principal ideal problem. In ACM press, editor, *Proceedings of the 34th Annuual ACM Symposium on Theory of Computing*, pages 653–658, 2002.

[16] C. H. Hardy et E. M. Wright. *An Introduction to the Theory of Numbers.* Oxford University Press, London, 1979.

[17] Hendrik W. Lenstra Jr. On the calculation of regulators and class numbers of quadratic fields. *London mathematical society, Lecture Note series*, 56 :123–150, 1982.

[18] Michael J. Jacobson Jr. Computing discrete logarithms in quadratic orders. *Journal of Cryptology*, 13(4) :473–492, 2000.

[19] Donald E. Knuth. *The art of Computer Programming*, volume 2. Addison-Wesley, 1981.

[20] Richard A. Mollin. *Quadratics.* CRC Press, 1996.

[21] Michael A. Nielsen et Isaac L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, Cambridge, United Kingdom, 2000.

[22] Oskar Perron. *Die lehre von den kettenbrüchen*, volume 1. B. G. Teubner Verlagsgesellschaft, troisième édition, 1954.

[23] John Preskill. Lecture notes on quantum computing. `http://www.theory.caltech.edu/~preskill/ph229`.

[24] Michel Queysanne. *Algèbre.* Armand Colin, 1964.

[25] Renate Scheidler, Johannes A. Buchmann, et Hugh C. Williams. A key-exchange protocol using real quadratic fields. *Journal of Cryptology : the journal of the International Association for Cryptologic Research*, 7(3) :171–199, Summer 1994.

[26] Renate Scheidler, Andreas Stein, et Hugh C. Williams. Key-exchange in real quadratic congruence function fields. *Designs, Codes and Cryptography*, 7(1-2) :153–174, 1996.

[27] René J. Schoof. Quadratic fields and factorization. *Computational Methods in Number Theory*, pages 235–286, 1983.

[28] Donald Shanks. The infrastructure of a real quadratic field and its applications. *Proc. 1972 Number Theory Conference*, pages 217–224, 1972.

[29] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal of Computation*, 26(5) :1484–1509, October 1997.

[30] Douglas R. Stinson. *Cryptography, Theory and Practice*. CRC Press, Boca Raton, FL, première édition, 1995.

[31] Shigenori Uchiyama, Tatsuaki Okamoto et Keisuke Tanaka. Quantum public-key cryptosystems. *Lecture Notes in Computer Science :Advances in Cryptology - CRYPTO 2000*, pages 147–165, 2000.

[32] Hugh C. Williams et M. C. Wunderlich. On the parallel generation of the residues for the continued fraction factoring algorithm. *Mathematics of Computation*, 48 :405–423, 1987.

[33] Hugh C. Williams et M. C. Wunderlich. Some computational results on a problem concerning powerful numbers. *Mathematics of Computation*, 50 :619–632, 1988.

[34] Hong Zhu. Survey of computational assumptions used in cryptography broken or not by Shor's algorithm. Mémoire de maîtrise, Université McGill, Montréal, Québec Décembre 2001.

Table des figures

Table des matières