Un algorithme de résolution des équations quadratiques en dimension 5 sans factorisation

Pierre Castel

UNIVERSITÉ DE CAEN BASSE–NORMANDIE

U.F.R de Sciences

ÉCOLE DOCTORALE SIMEM

THÈSE

Présentée par

M. Pierre CASTEL

Et soutenue

le 7 octobre 2011

En vue de l'obtention du

DOCTORAT de l'UNIVERSITÉ de CAEN

Spécialité : Mathématiques et leurs interactions

Arrêté du 07 août 2006

TITRE :

Un algorithme de résolution des équations quadratiques en dimension 5 sans factorisation

MEMBRES du JURY :

M. Andreas Enge, Directeur de Recherche INRIA, Université Bordeaux 1
M. Fabien Laguillaumie, Maître de Conférences, Université de Caen Basse–Normandie
M. Reynald Lercier, Ingénieur de l'Armement, HDR, DGA, Université de Rennes 1
M. Claus–Peter Schnorr, Professeur, Goethe Universität, Allemagne *(rapporteur)*
M. Denis Simon, Professeur, Université de Caen Basse–Normandie *(directeur)*
M. Peter Stevenhagen, Professeur, Universiteit Leiden, Pays–Bas *(rapporteur)*

Remerciements

Je suis sincèrement heureux et honoré d'adresser mes premiers remerciements à Denis Simon qui a encadré mon mémoire de Master puis cette thèse. Denis a été pour moi un excellent directeur de thèse, toujours de bonne humeur et disponible. Il m'a toujours soutenu et encouragé durant ces années autant sur le plan professionnel que personnel. Il a su faire preuve d'une grande ouverture d'esprit notamment face à certaines idées parfois capillotractées j'en conviens. À ses cotés, j'ai appris à cerner le coté ludique et pédagogique de mathématiques parfois très compliquées. À travers lui, je remercie aussi sa famille pour avoir supporté qu'il reste parfois tard à travailler avec moi au bureau.

J'adresse mes remerciements à Claus–Peter Schnorr et Peter Stevenhagen qui on accepté la lourde tâche de rapporteur pour cette thèse. J'éprouve un profond respect pour leur travail.

Je remercie également les autres membres de mon jury : Andreas Enge, Fabien Laguillaumie avec qui j'ai eu l'opportunité d'organiser le séminaire de cryptologie de Caen et Reynald Lercier qui m'a invité à exposer à Rennes.

Merci à Brigitte Vallée et à tous les membres de l'ANR Lareda pour m'avoir permis de découvrir en profondeur l'algorithme LLL.

J'ai effectué ce travail au sein du Laboratoire de Mathématiques Nicolas Oresme dont je souhaite remercier tous les membres, enseignants–chercheurs et personnel administratif.

Je souhaite également remercier l'ensemble des doctorants du LMNO, la bonne ambiance qui règne entre les jeunes chercheurs n'y est pas pour rien dans ce travail. Je remercie plus particulièrement Benjamin Beeker et Philippe Regnault ; la caféine nous aura permis d'aller jusqu'au bout !

J'adresse mes remerciements au personnel de l'école doctorale SIMEM : Lamri Adoui qui s'est toujours montré intéressé par mes remarques et suggestions, Sandrine Soro qui a à chaque fois pris le temps de répondre à mes questions.

Merci au personnel de la bibliothèque universitaire de s'être toujours arrangé pour le mieux face à mes (trop ?) nombreux retards de prêt. Sans cela, la suspension aurait été très longue ! (la durée exacte est trop honteuse pour être donnée).

Un grand merci à ma famille sans qui je ne serais jamais arrivé jusqu'ici. Leur soutien inconditionnel a toujours été une source de motivation.

J'adresse mes plus profonds remerciements à Virginie sans qui cette thèse n'aurait pas été ce qu'elle est. Merci d'avoir supporté mes envies nocturnes de travail et mes soirées en compagnie de pari–gp. Merci aussi pour avoir relu cette thèse sans tout comprendre et de m'avoir écouté lorsque je parlais de toutes ces choses compliquées.

Je remercie aussi mes amis, Virois et Caennais, de ne pas m'avoir laissé tombé lorsque je leur ai dit que je faisais une thèse de mathématiques et d'avoir compris que je devais régulièrement rester enfermé chez moi avec mon ordinateur.

J'ai également une pensée pour Guillaume B. qui a su m'initier aux joies du logiciel libre et qui continue à me porter secours dans les cas extrêmes.

Enfin, j'adresse un merci à ceux qui ont eu une influence dans ce travail et que j'aurais éventuellement pu oublier. Ce n'est que partie remise...

Table des matières

Notations

$\mathbb{N}$ ..... l'ensemble des entiers naturels.
$\mathbb{Z}$ ..... l'ensemble des entiers relatifs.
$\mathbb{Q}$ ..... l'ensemble des rationnels.
$\mathbb{R}$ ..... l'ensemble des réels.
$\mathbb{C}$ ..... l'ensemble des nombres complexes.
$\mathcal{P}$ ..... l'ensemble des nombres premiers.
p ..... un nombre premier.
$\mathbb{F}_p$ ..... le corps fini à p éléments.
Q_n ..... la matrice d'une forme quadratique de dimension n.
$\mathrm{Co}(Q_n)$ ..... la comatrice de Q_n.
$a \wedge b$ ..... le pgcd de deux entiers a et b.
$a \stackrel{?}{=} b$ ..... un test d'égalité entre a et b.
$\sharp A$ ..... le cardinal de l'ensemble A.
$v_p(x)$ ..... la valuation p–adique de x.
Id_n ..... la matrice identité de taille n.
$a := b$ ..... on affecte la valeur b à a.
$\Re(z)$ ..... la partie réelle du nombre complexe z.
$\Im(z)$ ..... la partie imaginaire du nombre complexe z.
$[\![a, b]\!]$ ..... les entiers compris entre a et b.
$\lfloor a \rfloor$ ..... la partie entière inférieure de a.
${}^tA$ ..... la transposée le matrice A.
$\omega(n)$ ..... le nombre de facteurs premiers de n.
$\mathcal{M}_{n,m}(\mathbb{K})$ ..... l'ensemble des matrices de taille $n \times m$ à coefficients dans $\mathbb{K}$.
$\mathcal{M}_n(\mathbb{K})$ ..... l'ensemble des matrices carrées de taille n à coefficients dans $\mathbb{K}$.

Chapitre 1

Introduction

Comme son titre l'indique, dans cette thèse, je propose un algorithme de résolution des équations quadratiques en dimension 5 sans factorisation. Afin de comprendre de quoi il retourne, commençons par donner une idée générale de la définition des mots du titre :

Algorithme : ce mot provient de Al Khwarizmi, surnom du mathématicien arabe Muhammad Ibn Musa (XI^{e} siècle) né à Khwarizem, en Ouzbekistan. Un algorithme est une suite finie de règles à appliquer dans un ordre déterminé à un nombre fini de données pour arriver en nombre fini d'étapes à un certain résultat. Un exemple simple d'algorithme est celui de l'addition de deux nombres écrits en base 10. On commence par additionner les chiffres des unités, on écrit ensuite le dernier chiffre de cette somme, on note dans la colonne suivante une éventuelle retenue puis on continue avec le chiffre des dizaines etc. Un autre exemple très simple est celui de la recette de cuisine ! Il suffit de suivre les étapes dans l'ordre pour obtenir un certain mets.

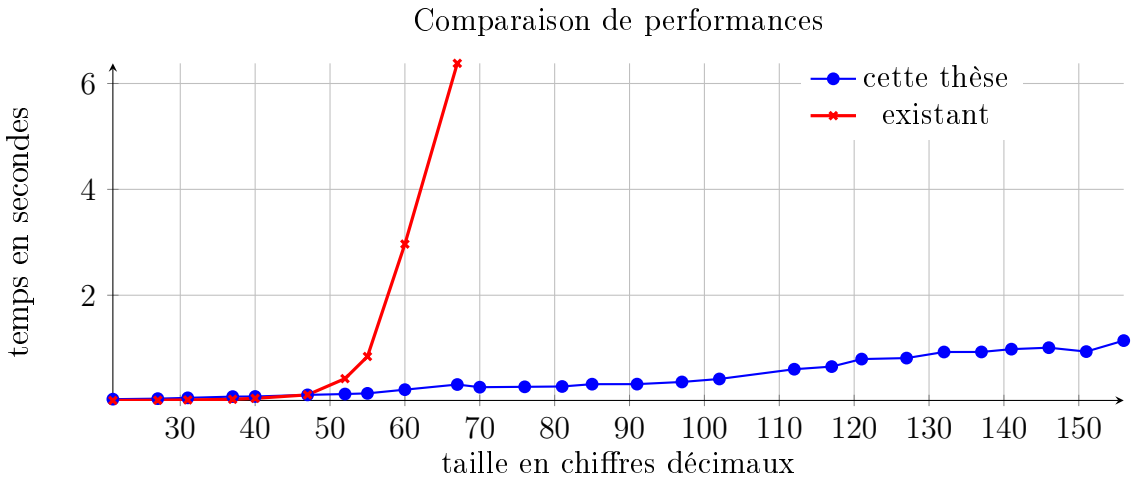
Équation quadratique en dimension 5 : on commence par donner le sens de l'expression « équation quadratique ». Une *équation* est quelque chose de bien connu, il s'agit d'une égalité mathématique au sens large dans laquelle se trouvent une ou plusieurs inconnues généralement notées x, y ou bien z. Une équation du second degré est une équation dans laquelle les variables apparaissent au carré. Un exemple bien connu d'équation de degré 2 est le suivant : $ax^2+bx+c=0$ où $a \neq 0$, b et c sont des nombres réels. Le mot *quadratique* signifie ici que lorsqu'une variable apparaît seule, elle est au carré, sinon elle est multipliée par une autre variable et le coefficient qui les accompagne est pair dans le cas entier. Par exemple $x^2 - 2xy + y^2 = 0$ et $x^2 + 5y^2 - 7z^2 + 4xy + 6xz + 18yz = 0$ sont des équations quadratiques ; par contre $x^2 + x^2z^2 + 3xy = 0$ ne l'est pas. Enfin le terme *dimension* 5 indique que les équations considérées seront en 5 variables. Une équation type sera donc de la forme $ax^2 + by^2 + cz^2 + ds^2 + et^2 = 0$ où a, b, c, d et e sont des entiers relatifs et x, y, z, s, t les inconnues.

Factorisation : tout entier se décompose de manière unique à l'ordre près des facteurs en un produit de nombres premiers. Il s'agit du théorème fondamental de l'arithmétique. Il existe des nombres appelés nombres premiers, qui ne sont divisibles que par 1 et par eux–mêmes. Il s'agit des nombres premiers ; par exemple 2, 3, 5,

7, 11, 13, 17, 19, 23 et 29 sont les dix premiers nombres premiers. Le théorème fondamental de l'arithmétique nous dit que tout nombre entier s'exprime de manière unique comme un produit de ces entiers ; par exemple $12 = 2 \times 2 \times 3$, $123 = 3 \times 41$. Trouver la factorisation d'un entier signifie trouver la décomposition sous forme d'un produit de nombres premiers de cet entier. Il s'agit d'un problème très simple, mais qui est nettement plus difficile qu'il n'y paraît. L'algorithme de factorisation le plus performant à ce jour (le *Number Field Sieve*[1]) a mis un peu plus de 3 ans pour trouver les facteurs d'un entier de 232 chiffres alors que celui–ci était égal au produit de deux nombres premiers seulement !

Si l'on remet ensemble les définitions données, on obtient la chose suivante : dans cette thèse, je propose une liste d'instructions à suivre permettant de trouver une solution à une équation en 5 variables dans laquelle toutes ces variables apparaissent au carré et qui ne demande pas trop de temps. Simple non ?

Voici une comparaison entre un algorithme déjà existant et celui que je propose dans cette thèse :



1. Crible de Corps de Nombres

1.1 Introduction générale

Dans cette thèse, je propose un nouvel algorithme pour résoudre des équations quadratiques en dimension 5 sur les entiers ou les rationnels sans utiliser la factorisation. Des algorithmes existent déjà pour résoudre ce genre d'équation, voir [CR03] ou [Sim05a]. Cependant ces algorithmes nécessitent de factoriser le déterminant de la matrice associée, donc leur complexité est essentiellement celle d'un algorithme de factorisation, c'est–à–dire sous–exponentielle dans le meilleur des cas. L'algorithme décrit dans cette thèse est d'une complexité nettement meilleure que les méthodes précédemment citées. Sa complexité est polynomiale en la taille du déterminant de la forme de départ. Il s'agit d'un algorithme probabiliste reposant sur l'hypothèse de Riemann pour les fonctions zêta de Dedekind d'un corps de nombres.

Afin de donner l'explication détaillée de cet algorithme, le cheminement de ce manuscrit va suivre celui de l'algorithme.

Le chapitre 2 recense les connaissances préliminaires nécessaires à la compréhension de ce travail. Il s'agit de résultats issus de la théorie des formes quadratiques, des définitions et propriétés des formes normales d'Hermite et de Smith, de l'hypothèse de Riemann. Une partie est consacrée à l'algorithme de Pollard–Schnorr [PS87]. Cet algorithme permet aussi de résoudre des équations quadratiques, mais en dimension 2 et modulo un entier m. Le point fort de cet algorithme est qu'il ne nécessite pas de factorisation ; ce qui est très intéressant pour celui qui sera développé dans cette thèse. Ce premier chapitre se termine en donnant des algorithmes existant pour les autres dimensions.

Le chapitre 3 est une description complète et détaillée de l'algorithme, sa structure suit celle de l'algorithme en question. On commence par expliquer ce qu'est la complétion d'une forme et les propriétés vérifiées par son déterminant. Il faut ensuite s'inquiéter du devenir de la signature de la nouvelle forme en question : quelles sont les propriétés qu'elle vérifie et quelles sont les conditions qu'elle doit vérifier pour le bon fonctionnement de l'algorithme. Puis on explique ce qu'est la minimisation d'une forme quadratique : quelle est l'incidence de l'existence d'un diviseur élémentaire différent du déterminant de la matrice de la forme, comment procéder afin de se ramener au cas où celui–ci est égal à 1. On explique ensuite comment réduire la forme afin que son déterminant soit impair. Ensuite, la preuve de cet algorithme donne le fonctionnement général de celui–ci. C'est dans cette section que tous les morceaux de ce puzzle sont remis en ordre. Ce chapitre se termine en donnant des idées pour généraliser cet algorithme aux dimensions supérieures ainsi que quelques exemples détaillés de chacune des parties décrites.

Le chapitre 4 consiste en l'analyse de cet algorithme. Je commence par donner un exemple de calcul de discriminant d'un corps de nombres composé d'extensions de degré 2. Je donne ensuite une majoration de ce discriminant pour le cas général d'un compositum d'extensions quadratiques. Il faut après cela estimer la proportion de nombres premiers vérifiant les conditions imposées par le déterminant de la forme complétée. On effectue pour cela une étude théorique des bornes puis une étude numérique afin d'optimiser celle–ci. On analyse ensuite la répartition de ces nombres. Vient ensuite l'analyse de complexité de l'algorithme. Cette analyse se dé-

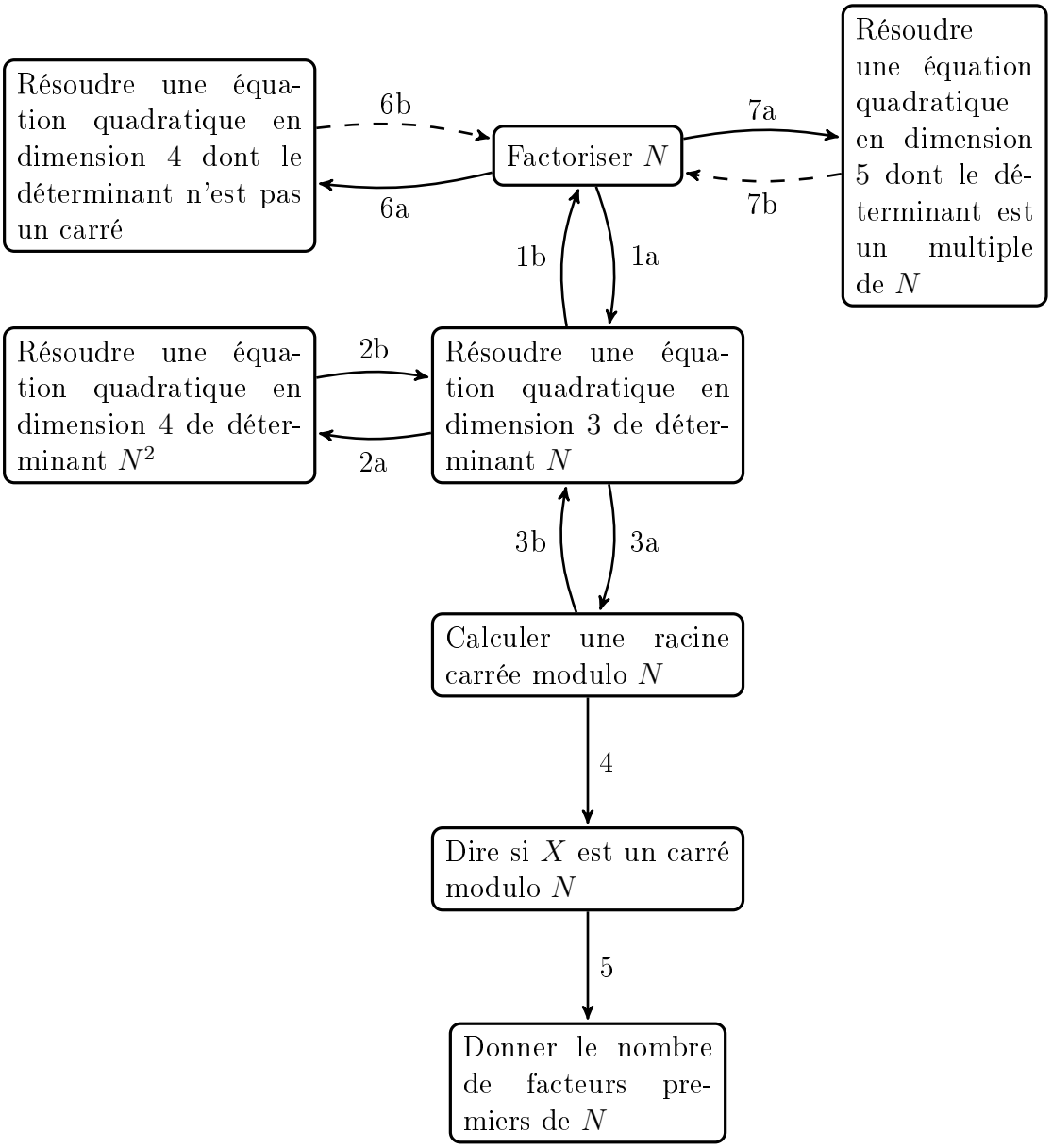
compose en l'analyse successive des étapes de minimisation, de complétion, des tests de friabilité, de la fin de l'algorithme et enfin cela est regroupé afin de donner la complexité globale de l'algorithme. La section qui suit la complexité donne une idée des améliorations possibles de cet algorithme. On termine ce chapitre en donnant les résultats de quelques expériences menées afin d'obtenir un graphique des performances de l'algorithme de cette thèse ainsi qu'une comparaison avec celui développé par Simon.

À la fin de ce manuscrit, on trouvera une annexe. Cette annexe donne un graphique des valeurs prises par la fonction $\pi(X, n)$ définie dans la section 4.2.2 du chapitre 4. On y trouvera également le rapport entre l'estimation donnée et la vraie valeur de la fonction en question.

La section qui va suivre complète cette présentation de la thèse en donnant des motivations pour l'algorithme décrit ici. Le point de départ de cette thèse était la factorisation des entiers, je donne ici une liste non exhaustive des liens qui existent entre les formes quadratiques et la factorisation des entiers.

1.2 Les liens avec la factorisation

Les formes quadratiques ont de multiples liens avec la factorisation des entiers. Nous recensons les liens qui nous intéressent à l'aide du diagramme suivant en supposant que l'on travaille sur les entiers ou les rationnels.



Une flèche entre deux éléments de ce diagramme signifie que si l'on sait faire l'un alors on peut faire l'autre. Expliquons plus précisément ces différents liens.

1- Équations quadratiques en dimension 3

Le lien 1a est une conséquence directe de l'article de Simon [Sim05b]. Dans cet article, Simon donne un algorithme permettant de résoudre des équations quadratiques en dimension 3. Cet algorithme consiste à effectuer des minimisations sur la forme quadratique de départ par rapport à chacun des facteurs premiers du déterminant. Un fois ces minimisations effectuées, il reste une forme quadratique, à laquelle on applique l'algorithme LLL ce qui la rend diagonale, de déterminant ± 1, donc trouver une solution est évident. Il existe également un autre algorithme, donné par Cremona et Rusin dans [CR03].

Le lien 1b est développé dans [Cas08]. Dans ce mémoire, j'avais donné un algorithme, qui à partir d'une forme quadratique bien choisie, permet de trouver la factorisation d'un entier. Le principe de l'algorithme est d'obtenir une congruence de deux carrés modulo l'entier à factoriser. Pour cela, on commence par tirer au hasard des entiers α et β dont on souhaite que le carré modulo N soit congru à un nombre premier. On note les carrés respectifs p et p'. On considère ensuite les trois équations quadratiques en dimension 3 suivantes, que l'on regarde ensuite modulo N :

$$\begin{aligned} x^2 - py^2 - Nz^2 &= 0 & \qquad x^2 - py^2 &\equiv 0 \pmod{N} \\ x^2 - p'y^2 - Nz^2 &= 0 & \qquad x^2 - p'y^2 &\equiv 0 \pmod{N} \\ x^2 - pp'y^2 - Nz^2 &= 0 & \qquad x^2 - pp'y^2 &\equiv 0 \pmod{N} \end{aligned}$$

On a $\alpha^2 \equiv p \pmod{N}$ et $\beta^2 \equiv p' \pmod{N}$ et on note (x_0, y_0), (x_1, y_1) et (x_2, y_2) les solutions respectives des équations précédentes, il vient alors :

$$\begin{aligned} x^2 - (\alpha y)^2 &\equiv 0 \pmod{N} & \qquad \left(\frac{x_0}{y_0}\right)^2 &\equiv p \pmod{N} \\ x^2 - (\beta y)^2 &\equiv 0 \pmod{N} & \qquad \left(\frac{x_1}{y_1}\right)^2 &\equiv p' \pmod{N} \\ x^2 - (\alpha\beta y)^2 &\equiv 0 \pmod{N} & \qquad \left(\frac{x_2}{y_2}\right)^2 &\equiv pp' \pmod{N} \end{aligned}$$

On obtient ainsi l'égalité suivante :

$$(\alpha\beta)^2 \equiv \left(\frac{x_0 x_1}{y_0 y_1}\right)^2 \equiv \left(\frac{x_2}{y_2}\right)^2 \pmod{N}$$

qui nous permet éventuellement de trouver un facteur de N (voir le principe général en 3). Il s'agit d'un algorithme probabiliste dans le sens ou il faut dans un premier temps trouver des éléments dont le carré modulo N est un nombre premier et dans un second temps, il faut de plus que les équations quadratiques associées aient des solutions.

Cet algorithme fonctionne dans la mesure ou l'on est capable de trouver une solution à la troisième équation quadratique de dimension 3 de départ. Il s'agit donc d'une preuve du fait que s'il est possible de résoudre rapidement des équations quadratiques en dimension 3, alors il est possible de factoriser de manière efficace.

2- Équations quadratiques en dimension 4 lorsque le déterminant est un carré

Il est connu qu'une équation quadratique de dimension 3 se ramène à la forme suivante :

$$x^2 - ay^2 - bz^2 = 0 \tag{1.1}$$

En ce qui concerne la dimension 4, lorsque le déterminant est un carré, il est toujours possible de se ramener à la forme suivante :

$$x^2 - ay^2 - bz^2 + abt^2 = 0 \tag{1.2}$$

Une fois les équations ramenées sous ces formes respectives, les coefficients a et b des équations (1.1) et (1.2) coïncident puisque dans le premier cas le déterminant vaut $N = ab$ et dans l'autre cas il vaut $(ab)^2 = N^2$.

Le lien 2a est alors simple : si l'on dispose d'une solution pour l'équation (1.1) on obtient une solution de (1.2) en posant $t = 0$.

En ce qui concerne le lien 2b, si la solution de (1.2) donnée vérifie $t = 0$, il n'y a rien à faire ; cette solution sera également solution de (1.1). Dans le cas où $t \neq 0$, on commence par écrire la forme quadratique dans une base dont le dernier vecteur est solution. La matrice de la forme est alors du type :

$$\begin{bmatrix} 0 & \alpha & * & * \\ \alpha & * & * & * \\ * & * & * & * \\ * & * & * & * \end{bmatrix}$$

À l'aide calculs de pgcd, il est possible d'obtenir un changement de base pour lequel la matrice est de la forme :

$$Q = \left[\begin{array}{c|ccc} 0 & 0 & 0 & \alpha \\ \hline 0 & \multicolumn{2}{c}{\multirow{2}{*}{Q_2}} & * \\ 0 & & & * \\ \hline \alpha & * & * & * \end{array}\right]$$

où α est un entier et Q_2 une forme quadratique de dimension 2.

Or on sait que le déterminant de la forme de départ est un carré et on a la relation :

$$\det Q = -\alpha^2 \det Q_2$$

Ainsi, $\det Q_2$ est également un carré. On peut alors utiliser la méthode classique pour trouver un vecteur isotrope pour la forme Q_2. En effectuant un changement de base à l'aide de ce vecteur isotrope, la matrice de la forme est alors du type :

$$\left[\begin{array}{ccc|c} 0 & 0 & 0 & \alpha \\ 0 & 0 & \beta & * \\ 0 & \beta & * & * \\ \hline \alpha & * & * & * \end{array}\right]$$

On note que les deux premiers vecteurs de la base dans laquelle la matrice est écrite sont à la fois isotropes et orthogonaux. Donc en effectuant une combinaison linéaire de ces deux vecteurs de sorte que la dernière coordonnée du résultat soit nulle, on obtient un vecteur isotrope pour la forme de départ.

3- Calcul de racines carrées

3a Si l'on suppose connue la factorisation d'un entier N, il est facile de trouver la racine carrée modulo N de n'importe quel élément si elle existe. En effet, on commence par décomposer N en produit de facteurs premiers :

$$N = \prod_{i=1}^{r} p_i^{\alpha_i} \ ,p_i \in \mathcal{P}$$

Si a est l'élément en question, on commence par calculer une racine carrée de a modulo chacun des p_i via un algorithme de calcul de racine carrée tel celui de Shanks (voir [Coh96, p32]), puis on relève cette racine en une modulo $p_i^{\alpha_i}$ via un lift de Hensel. Une fois toutes les racines obtenues, il faut les combiner en utilisant le lemme Chinois afin d'en obtenir une modulo N.

3b Le lien entre la factorisation d'un entier donné et le calcul de racines carrées modulaires est connu depuis fort longtemps. En effet une grande partie des algorithmes de factorisation reposent sur le principe suivant :

Si l'on connait deux entiers a et b non nuls, tels que $a \neq \pm b$ et vérifiant :

$$a^2 \equiv b^2 \pmod{N}$$

alors il est possible d'en déduire un facteur de N en calculant $\gcd(a-b, N)$ ou $\gcd(a+b\,, N)$. En effet, la congruence précédemment citée se factorise en $(a-b)(a+b)$ d'où le calcul des diviseurs communs. Le fait d'avoir une congruence de deux carrés nous ramène donc au calcul de racine carrée. En effet, si certaines méthodes de factorisation sont basées sur cette identité, elles diffèrent dans la manière d'obtenir les deux entiers a et b en question. On peut en citer plusieurs :

Dixon L'idée de cet algorithme est de tirer aléatoirement des entiers x_i, de les mettre au carré modulo N, on a alors $x_i^2 \equiv a_i \pmod{N}$. Ensuite on tente de factoriser a_i sur une base de nombres premiers fixée en amont. On se constitue alors une liste d'éléments a_i repérés par la parité de leurs coordonnées sur la base d'entiers fixés. Il suffit alors de trouver une combinaison linéaire des coordonnées des a_i telle que celle–ci soit nulle modulo 2. Si on réussit, cela signifie que l'on a trouvé un élément qui est un carré modulo N et dont on connait une racine carrée sans avoir eu besoin de factoriser N. Il reste alors simplement à appliquer le principe de départ.

Quadratic Sieve On commence par considérer le polynôme

$$Q(a) = \left(\left\lfloor \sqrt{N} \right\rfloor + a\right)^2 - N$$

On remarque que $Q(a) \equiv x^2 \pmod{N}$ pour $x = \left\lfloor \sqrt{N} \right\rfloor + a$. Cette fois–ci, on ne va pas tenter de tirer des éléments aléatoirement dans un intervalle donné, mais on va directement cribler sur un intervalle. Supposons que l'on ait un entier m tel que $m \mid Q(a)$, alors pour tout entier k, $m \mid Q(a+km)$. Pour trouver un tel entier a, s'il existe, on essaie de résoudre l'équation $x^2 \equiv N \pmod{m}$ ce qui est aisé lorsque m est bien choisi. Puis on prend $a = x - \left\lfloor \sqrt{N} \right\rfloor \pmod{N}$. On fait ensuite varier le k dans un intervalle d'entiers donnés. Une fois cela effectué, chacune des relations obtenues est propice à l'utilisation du principe général énoncé, donc on cherche une combinaison linéaire modulo 2 comme précédemment.

4- Savoir si un élément est un carré

Ce lien est évident. En effet, si la factorisation de l'entier N est connue, il suffit de calculer les symboles de Jacobi pour chaque nombre premier p divisant N.

5- Donner le nombre de facteurs premiers d'un entier

Si l'on suppose que l'on est capable de dire si un entier donné est un carré ou pas modulo N, il existe une méthode probabiliste relativement simple pour avoir une estimation du nombre de facteurs premiers de N. Le principe de cette méthode est basé sur le fait qu'il y a autant de carrés que de non carrés dans $(\mathbb{Z}/p\mathbb{Z})^*$ pour tout nombre premier p. L'idée est donc de tirer aléatoirement un certain nombre d'entiers dans $\mathbb{Z}/N\mathbb{Z}$ puis de regarder la proportion P d'entre eux contenant les carrés. Comme il y autant de carrés que de non carrés modulo p mais pas modulo N, la proportion P se rapproche de $\frac{1}{2^k}$ pour un certain k qui est exactement le nombre de facteurs premiers de N. On calcule alors $\frac{-\log P}{\log 2}$ qui est égal au k cherché.

6- Équations quadratiques en dimension 4 lorsque le déterminant n'est pas un carré

6a Le lien 6a est une conséquence de l'article de Simon [Sim05a]. Il y décrit un article pour traiter le cas des équations quadratiques en dimension 4. L'algorithme proposé nécessite de connaitre la factorisation du déterminant afin de pouvoir effectuer des minimisations sur la matrice de la forme pour trouver une solution.

6b Ce lien est un cas intermédiaire entre la dimension 3 et la dimension 5. L'étude de celui–ci nécessiterait un travail supplémentaire qui n'a pas été effectuée dans cette thèse.

7- Équations quadratiques en dimension 5

7a Le lien 7a est une conséquence de l'article de Simon [Sim05a]. Dans cet article, il donne un algorithme pour résoudre des équations quadratiques en dimension 5. Cet algorithme nécessite de connaitre la factorisation du déterminant de la forme correspondante. Nous détaillons plus précisément cela dans la partie 2.6.

7b Le lien 7b est la question à l'origine de cette thèse : « Est–il possible d'obtenir la factorisation d'un entier en résolvant des équations quadratiques de dimension 5 bien choisies ? ». Ce lien est similaire au lien 1b. Dans le cas 1b, la réponse est claire et affirmative ; il y a équivalence entre savoir résoudre des équations quadratiques en dimension 3 et factoriser un entier. Cette thèse donne un élément de réponse très important pour le lien 7b : elle donne un algorithme qui permet de résoudre des équations quadratiques en dimension 5 *sans utiliser d'algorithme de factorisation.* Si le lien 7b existait, alors on pourrait facilement factoriser.

Chapitre 2

Préliminaires

Ce chapitre regroupe les notions élémentaires nécessaires à la compréhension des chapitres suivants. Comme cette thèse donne un algorithme pour résoudre des équations quadratiques, nous commençons par donner les définitions de base ainsi que les principaux résultats de la théorie des formes quadratiques. Nous donnons ensuite le résultat probablement le plus important de cette théorie, à savoir le théorème de Hasse–Minkowski. Les formes normales de Smith et d'Hermite sont également très utilisées tout au long de ce document, nous en donnons donc les définitions ainsi que quelques résultats utiles autour de celles–ci. Ensuite, un autre point central de l'algorithme proposé dans cette thèse est l'algorithme de Pollard–Schnorr ; nous en énonçons donc une version sans trop entrer dans les détails. Enfin, nous donnons un tour d'horizon des méthodes qui existent déjà pour résoudre des équations quadratiques de dimension 3 à 6.

2.1 Formes quadratiques et définitions associées

Nous donnons quelques définitions absolument nécessaires à la compréhension de ce qui va suivre. Ces définitions sont largement inspirées de [Ser95].

Pour commencer, la définition d'une forme quadratique :

Définition 2.1.1 (Forme quadratique)**.** *Soit V un module sur un anneau commutatif A. Une application $Q : V \longrightarrow A$ est appelée* forme quadratique *sur V si :*

- *on a $Q(ax) = a^2 Q(x)$ pour $a \in A$ et $x \in V$*
- *l'application $(x, y) \longmapsto Q(x + y) - Q(x) - Q(y)$ est une forme bilinéaire*

Un tel couple (V, Q) est appelé un *module quadratique.*

Dans tout ce qui va suivre, sauf mention explicite du contraire, on se placera dans le cas où l'anneau A est un corps de caractéristique différente de 2. Le A–module V est alors un A–espace vectoriel que l'on supposera de dimension finie.

On posera :

$$Q(x, y) = \frac{1}{2}\left(Q(x + y) - Q(x) - Q(y)\right)$$

Remarque : On note qu'avec cette notation, on a :

$$Q(x, x) = Q(x)$$

Lorsque la caractéristique est différente de 2, cela a bien un sens de parler de forme quadratique. L'application $(x, y) \longmapsto Q(x, y)$ est une forme bilinéaire symétrique sur V ; on l'appelle le *produit scalaire* associé à Q.

Définition 2.1.2 (Matrice d'une forme quadratique)**.** *Soit $(e_i)_{1 \leq i \leq n}$ une base de V. On appelle matrice de Q par rapport à cette base la matrice $A = (a_{i,j})$, où $a_{i,j} = Q(e_i, e_j)$. C'est une matrice symétrique. Si $x = \sum x_i e_i$ est un élément de V, on a :*

$$Q(x) = \sum_{i,j} a_{i,j} x_i x_j \ ,$$

ce qui montre que $Q(x)$ est une « forme quadratique » en $x_1, \ldots, x_n$ au sens usuel.

Remarque : Si l'on modifie la base (e_i) au moyen d'une matrice inversible G, la matrice A' de Q par rapport à la nouvelle base est :

$$A' = {}^t G A G$$

On a en particulier :

$$\det A' = \det A \det G^2$$

On note ainsi que le déterminant de Q est défini à un carré près.

Définition 2.1.3. *Soit $n > 0$ un entier. On désigne par $Sym(n, \mathbb{Z})$ l'ensemble des matrices carrées de déterminant non nul, symétriques, de taille $n \times n$ à coefficients entiers.*

Dans la suite, nous utiliserons également la notation suivante, si on désigne par X le vecteur colonne ayant pour coordonnées les coefficients de $x = \sum x_i e_i$, la notation vectorielle associée pour $Q(x)$ sera :

$$^tXQX$$

C'est–à–dire que Q désignera la forme quadratique Q mais aussi sa matrice A dans la base $(e_i)_{1\leq i\leq n}$. Cela nous permettra d'avoir des notations plus claires et de rendre certains calculs plus compréhensibles.

Définition 2.1.4. *Un élément x d'un module quadratique (V, Q) est* isotrope *si l'on a $Q(x) = 0$. Un sous–module U de V est dit isotrope si tous ses éléments sont isotropes.*

Définition 2.1.5. *On appelle* plan hyperbolique *tout module quadratique ayant une base formée de deux éléments isotropes x, y tels que $Q(x, y) \neq 0$.*

Définition 2.1.6 (Orthogonalité)**.** *Soit (V, Q) un module quadratique. Deux éléments x, y de V sont dits* orthogonaux *si $Q(x, y) = 0$. L'ensemble des éléments orthogonaux à une partie H de V est noté H^0, c'est un sous espace vectoriel de V. Si V_1 et V_2 sont deux sous espaces vectoriels de V, on dit que V_1 et V_2 sont* orthogonaux *si $V_1 \subset V_2^0$. L'orthogonal V^0 de V tout entier est appelé* radical *(ou* noyau*) de V, et noté* $\operatorname{rad} V$*. Sa codimension s'appelle le* rang *de Q. Si $V^0 = 0$, on dit que Q est* non dégénérée *; cela équivaut à dire que le déterminant de Q est non nul.*

Proposition 2.1.7. *Soit x un élément isotrope non nul d'un module quadratique non dégénéré (V, Q). Il existe alors un sous–espace U de V qui contient x et qui est un plan hyperbolique.*

Démonstration. La preuve est disponible dans [Ser95, p55]. □

Définition 2.1.8. *Une base $(e_1, \ldots, e_n)$ d'un module quadratique (V, Q) est dite orthogonale si elle est formée d'éléments deux à deux orthogonaux.*

Remarque : Cela revient à dire que la matrice de Q par rapport à cette base est une matrice diagonale :

$$\begin{bmatrix} a_1 & 0 & & 0 \\ 0 & a_2 & & 0 \\ & & \ddots & \\ 0 & 0 & & a_n \end{bmatrix}$$

Si $x = \sum x_i e_i$, on a alors :

$$Q(x) = a_1 x_1^2 + \cdots + a_n x_n^2$$

Théorème 2.1.9. *Tout module quadratique (V, Q) possède une base orthogonale.*

Démonstration. La démonstration de ce théorème est disponible dans [Ser95, p55]. □

Définition 2.1.10. *Si Q réelle, non dégénérée est écrite dans une base dans laquelle sa matrice est diagonale, et si on note r le nombre de coefficients positifs, s le nombre de coefficients négatifs ; on appelle* signature *de Q le couple (r, s).*

Proposition 2.1.11. *La signature d'une forme quadratique réelle ne dépend pas de la base dans laquelle elle est écrite.*

Démonstration. La démonstration de ce résultat est détaillée dans [Ser95, p64]. □

Définition 2.1.12. *Si r ou s est nul, Q est dite* définie *(*positive si $s = 0$, négative si $r = 0$*). Sinon elle est dite* indéfinie.

Définition 2.1.13 (Équivalence)**.** *Deux formes quadratiques Q et Q' sont dites* équivalentes *si les modules correspondants sont isomorphes.*

Remarque : Si A et A' sont les matrices de Q et Q', cela revient à dire qu'il existe une matrice inversible G telle que :

$$A' = {}^tGAG$$

Dans les définitions et résultats qui vont suivre, le corps de base utilisé sera un corps p–adique $\mathbb{Q}_p$, où p désigne un nombre premier.

Soit (V, Q) un module quadratique de rang n, on note Δ la classe de $\det(Q)$ dans $\mathbb{Q}_p/\mathbb{Q}_p^{*2}$. Si $e = (e_1, \ldots, e_n)$ est une base orthogonale de V, et si l'on pose $a_i = Q(e_i, e_i)$, on a :

$$\Delta = a_1 \ldots a_n \text{ dans } \mathbb{Q}_p/\mathbb{Q}_p^{*2}$$

Dans la suite, on notera souvent par la même lettre un élément de $\mathbb{Q}_p^*$ et sa classe modulo $\mathbb{Q}_p^{*2}$.

Rappelons également la définition du symbole de Hilbert :

Définition 2.1.14. *Soient $\mathbb{K}$ un corps et a, b deux éléments de $\mathbb{K}^*$. On pose :*

$(a, b) = 1$ *si l'équation $z^2 - ax^2 - by^2 = 0$ a une solution non triviale dans $\mathbb{K}$*
$(a, b) = -1$ *sinon*

le nombre (a, b) est appelé symbole de Hilbert *de a et b relativement à $\mathbb{K}$.*

Remarque : Lorsque le corps considéré est un corps p–adique, on notera ce symbole $(a, b)_p$ et s'il s'agit de $\mathbb{R}$ $(a, b)_\infty$

Proposition 2.1.15. *Soient $a,\ b \in \mathbb{K}^*$*

– *Si $\mathbb{K} = \mathbb{R}$, on a :*

$$\begin{aligned} (a, b) &= 1 && \text{si } a > 0 \text{ ou } b > 0 \\ (a, b) &= -1 && \text{sinon} \end{aligned}$$

– *Si $\mathbb{K} = \mathbb{Q}_p$, on écrit $a = p^\alpha u$, $b = p^\beta v$ avec $u,\ v \in \mathbb{Z}_p^*$, et on a :*

– *si* $p \neq 2$ *:*

$$(a,b) = (-1)^{\alpha\beta\epsilon(p)} \left(\frac{u}{p}\right)^{\beta} \left(\frac{v}{p}\right)^{\alpha}$$

– *si* $p = 2$ *:*

$$(a,b) = (-1)^{\epsilon(u)\epsilon(v)+\alpha\omega(v)+\beta\omega(u)}$$

Sachant que $\epsilon(u) = \frac{u-1}{2} \pmod 2$, $\omega(u) = \frac{u^2-1}{8} \pmod 2$ *et* $\left(\frac{u}{p}\right)$ *désigne le symbole de Legendre modulo p.*

Remarque : La fonction ϵ ci–dessus n'est définie que pour des entiers impairs (naturels ou p–adiques).

Démonstration. La preuve de cette proposition est disponible dans [Ser95, p39]. □

Plus de précisions sur le symbole de Hilbert sont disponibles dans [Ser95, p37] ou bien dans [Cas08, p37]. On pose alors :

$$\epsilon_p(Q) = \prod_{i<j} (a_i, a_j)_p$$

Remarque : On a bien sûr $\epsilon_p(Q) = \pm 1$.

Théorème 2.1.16. *Le nombre* $\epsilon_p(Q)$ *ne dépend pas de la base e.*

Démonstration. Plus de détails sont disponibles dans [Ser95, p64]. □

De ce théorème découle alors le fait suivant :

Proposition 2.1.17. *Si Q est une forme quadratique à n variables sur* $\mathbb{Q}_p$*, et si Q est équivalente à* $a_1x_1^2 + \cdots + a_nx_n^2$ *les deux éléments :*

$$\Delta = a_1 \dots a_n \text{ dans } \mathbb{Q}_p/\mathbb{Q}_p^{*2}$$
$$\epsilon_p(Q) = \prod_{i<j} (a_i, a_j)_p \text{ dans } \{\pm 1\}$$

sont des invariants de la classe d'équivalence de Q.

Remarque : $\epsilon_p(Q)$ est appelé invariant de Witt de Q en p.

Définition 2.1.18. *On dit qu'une forme Q* représente *un élément a s'il existe un élément x,* $x \neq 0$ *tel que* $Q(x) = a$*. En particulier, Q représente* 0 *si et seulement si le module quadratique correspondant contient un élément isotrope non nul.*

Soit donc maintenant une forme quadratique f non dégénérée et de dimension n sur $\mathbb{Q}_p$; soient Δ son déterminant et $\epsilon = \epsilon_p(Q)$. Le théorème suivant nous donne les conditions pour qu'une forme quadratique représente 0.

Théorème 2.1.19. *Pour que f représente 0 sur $\mathbb{Q}_p$, il faut et il suffit que :*

i) $n = 2$ *et* $\Delta = -1$ *dans* $\mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$

ii) $n = 3$ *et* $(-1, -\Delta)_p = \epsilon$

iii) $n = 4$ *et, soit* $\Delta \neq 1$,*soit* $\Delta = 1$ *et* $\epsilon = (-1, -1)_p$

iv) $n \geq 5$

Remarque : On note que toute forme quadratique d'au moins 5 variables représente 0. Ce théorème donne immédiatement le corollaire suivant :

Corollaire 2.1.20. *Soit* $a \in \mathbb{Q}_p^*/\mathbb{Q}_p^{*2}$. *Pour que f représente a, il faut et il suffit que :*

i) $n = 1$ *et* $a = \Delta$

ii) $n = 2$ *et* $(a, -\Delta) = \epsilon$

iii) $n = 3$ *et, soit* $a \neq -\Delta$, *soit* $a = -\Delta$ *et* $(-1, -\Delta) = \epsilon$

iv) $n \geq 4$

Les démonstrations des deux précédents résultats sont détaillées dans [Ser95, p66].

2.2 Hasse–Minkowski

Nous expliquons ici le principe de Hasse–Minkowski. Ce principe est fondamental et permet de savoir si une équation quadratique admet des solutions ou pas. Ce principe est résumé en le théorème suivant :

Théorème 2.2.1 (Hasse–Minkowski)**.** *Pour qu'une forme quadratique f non dégénérée représente 0 sur $\mathbb{Q}$, il faut et il suffit que f représente 0 sur $\mathbb{Q}_p$ pour tout nombre premier p et sur $\mathbb{R}$.*

Démonstration. voir [Ser95, Théorème 8 p.73] □

Ce théorème est aussi connu sous le nom de principe *local–global*, c'est–à–dire qu'une forme quadratique représente 0 globalement (ie sur $\mathbb{Q}$) si et seulement si elle représente 0 partout localement (ie sur $\mathbb{Q}_p$ pour tout nombre premier p et sur $\mathbb{R}$). Un corollaire immédiat est le suivant :

Corollaire 2.2.2 (Meyer)**.** *Une forme quadratique f sur $\mathbb{Q}$ de rang supérieur ou égal à 5 représente 0 si et seulement si elle est indéfinie.*

Démonstration. Il s'agit d'une conséquence directe des résultats précédents 2.2.1 et 2.1.19. En effet comme f est de rang ≥ 5, f représente 0 partout localement. En appliquant l'autre théorème, on voit qu'il suffit que f représente 0 sur $\mathbb{R}$ et pour cela, il suffit que f soit indéfinie. □

Proposition 2.2.3. *Soit f une forme quadratique de dimension $n \geq 3$ sur $\mathbb{Z}$. Pour que f représente 0 sur $\mathbb{Q}$, il faut et il suffit que f représente 0 sur $\mathbb{Q}_p$ pour tout nombre premier p qui divise $2 \det f$ et sur $\mathbb{R}$.*

Démonstration. Nous allons montrer que pour tout nombre premier p ne divisant pas $2 \det f$, l'équation $f(x) = 0$ admet toujours des solutions sur $\mathbb{Q}_p$. On note Q la matrice de f. On a ainsi $\det Q = \det f$. Soit p un nombre premier ne divisant pas $2 \det Q$. Soit $\overline{Q}$ la réduction de Q modulo p. Comme $p \neq 2$, $\mathbb{Z}/p\mathbb{Z}$ est un corps de caractéristique différente de 2, donc d'après [Ser95, p55, théorème 1], il existe une matrice $G_1 \in \mathcal{M}_n(\mathbb{Z}/p\mathbb{Z})$ telle que ${}^tG_1 Q G_1$ est diagonale et les coefficients diagonaux ne sont pas divisibles par p. En relevant sur $\mathbb{Z}$ la matrice G_1, on obtient une matrice $G_2 \in \mathcal{M}_n(\mathbb{Z})$ telle que :

$$Q^{(2)} = {}^tG_2 Q G_2 \equiv \begin{bmatrix} a_1 & & & 0 \\ & a_2 & & \\ & & \ddots & \\ 0 & & & a_n \end{bmatrix} \pmod{p}$$

et $Q^{(2)}$ est équivalente à Q. Distinguons maintenant les cas selon la dimension.

- $n = 3$: si $a_1 \equiv 0 \pmod{p}$ alors on a un vecteur isotrope modulo p, donc une solution de l'équation sur $\mathbb{Q}_p$ via un lift de Hensel. Sinon, on se ramène au cas $a_1 = 1 \pmod{p}$ et on calcule le symbole de Hilbert modulo p. Or les coefficients a_i ne sont pas divisibles par p, donc un utilisant la proposition 2.1.15 on voit que le symbole vaut 1.
- $n = 4$: si $\det Q$ n'est pas un carré p–adique il y a des solutions. Sinon, il faut vérifier que $\epsilon_p(Q) = (-1,-1)_p$. Comme $p \neq 2$, en utilisant la proposition 2.1.15, on sait que $(-1,-1)_p = 1$. Il faut donc vérifier que l'invariant ϵ_p de Q vaut 1. On sait que :
$$\epsilon_p(Q) = \prod_{i<j} (a_i, a_j)_p$$
Comme les coefficients diagonaux de $Q^{(2)}$ ne sont pas divisibles par p, les exposants α et β de la proposition 2.1.15 valent 0, donc chacun des symboles de Hilbert $(a_i, a_j)_p$ vaut 1. On a ainsi $\epsilon_p(Q) = 1 = (-1,-1)_p$ d'où l'existence de solutions.
- $n \geq 5$: il n'y a rien à démontrer pour ce cas puisque le théorème de Hasse–Minkowski 2.2.1 assure l'existence de solutions pour $n \geq 5$.

□

2.3 Formes normales d'Hermite et de Smith

Ces définitions et propriétés sont largement inspirées de [Coh96].

Forme normale d'Hermite

Théorème 2.3.1 (Forme Normale d'Hermite d'une matrice, HNF)**.**
Soit $A \in \mathcal{M}_{n,m}(\mathbb{Z})$ une matrice. Alors il existe une unique matrice H, appelée HNF

de A et une matrice $U \in GL_n(\mathbb{Z})$ telles que :

$$H = AU$$

$$H = \begin{bmatrix} 0 & 0 & \dots & 0 & * & * & \dots & * \\ 0 & 0 & \dots & 0 & 0 & * & \dots & * \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 & * \end{bmatrix}$$

$$\forall 1 \leq i \leq n \; h_{i,i} > 0, \forall j > i, 0 \leq m_{ij} < m_{ii}$$

Démonstration. Voir [Coh96, p67]. □

Remarque : Un algorithme permettant de calculer la forme normale d'Hermite d'une matrice est détaillé dans [Coh96, p68]. Un autre algorithme est également donné dans [Ili89], sa complexité y est aussi détaillée et cet algorithme permet en outre d'obtenir la matrice U du théorème 2.3.1.

Nous donnons maintenant une utilisation de la forme normale d'Hermite. L'algorithme qui va suivre permet de compléter une famille contenant un seul vecteur de $\mathbb{Z}^n$ en une base de $\mathbb{Z}^n$ de déterminant ± 1. L'idée est d'utiliser la forme normale d'Hermite d'un vecteur considéré comme une matrice de taille $1 \times n$ afin d'avoir une matrice de taille $n \times n$, de déterminant égal à ± 1 et dont la dernière colonne est le vecteur de départ. On rappelle qu'un vecteur est dit *primitif* si le plus grand commun diviseur des coordonnées est 1.

Algorithme 2.3.1: Complétion base

Données : $X \in \mathbb{Z}^n$, primitif
Résultat : B une base de $\mathbb{Z}^n$ dont le dernier vecteur est X

1 **début**
2 Calculer la forme normale d'Hermite de X. Soient H et U les matrices telles que $H = XU$.
3 $B := U^{-1}$
4 **retourner** B
5 **fin**

Démonstration. La preuve de cet algorithme réside dans le fait que la forme normale d'Hermite d'un vecteur est un vecteur dont toutes les coordonnées sont nulles, sauf une qui vaut le pgcd des coefficients du vecteur. Donc lorsque le vecteur est primitif, ce coefficient vaut 1. Ainsi, la dernière colonne de la matrice B en question est égale au vecteur X de départ. □

Remarque : Lorsque le vecteur X contient une coordonnée égale à 1, disons la $i^{\text{ème}}$, il n'est pas nécessaire d'utiliser la forme normale de Hermite. Il suffit de prendre la matrice identité dans laquelle on remplace la $i^{\text{ème}}$ colonne par le vecteur lui–même puis d'échanger la première et la $i^{\text{ème}}$ colonne.

Forme normale de Smith

Théorème 2.3.2 (Forme Normale de Smith d'une matrice, SNF)**.**
Soit $A \in \mathcal{M}_n(\mathbb{Z})$ une matrice de déterminant non nul. Alors il existe une unique matrice D, appelée SNF de A et 2 matrices U, $V \in GL_n(\mathbb{Z})$ telles que :

$$D = UAV$$

$$D = \begin{bmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{bmatrix} \quad \forall 1 \leq i \leq n \ d_i \in \mathbb{Z}, \ d_i > 0$$

où $d_n \mid d_{n-1} \mid \dots d_2 \mid d_1$ sont les diviseurs élémentaires de A.

Démonstration. voir [Coh96, p75]. □

Remarque : Un algorithme permettant de calculer la forme normale de Smith d'une matrice est détaillé dans [Coh96, p77]. Comme pour la forme normale d'Hermite, un autre algorithme est détaillé dans [Ili89] et il permet d'obtenir les matrices U et V du théorème 2.3.2

Lemme 2.3.3. *Soit $A \in Sym(n, \mathbb{Z})$. Soient U, V et D les matrices données par la forme normale de Smith de A vérifiant $D = UAV$ où U, $V \in GL_n(\mathbb{Z})$, D est diagonale à coefficients entiers. Notons $d_1, \dots, d_n$ les coefficients diagonaux de la matrice D. Alors, si $d_k \neq 1$ et $d_{k+1} = 1$, A admet un noyau de dimension k modulo d_k. De plus, une base de ce noyau est donnée par les k premières colonnes de la matrice V.*

Démonstration. On remarque tout d'abord que comme $d_k \neq 1$ et $d_{k+1} = 1$, par la condition de divisibilité sur les diviseurs élémentaires de A, on a $d_i = 1$ pour $k+1 \leq i \leq n$. On a $D = UAV$. Ainsi,

$$\begin{aligned} AV &= U^{-1}UAV \\ &= U^{-1}D \\ &= U^{-1} \begin{bmatrix} d_1 & & & & & \\ & \ddots & & & & \\ & & d_k & & & \\ & & & 1 & & \\ & & & & \ddots & \\ & & & & & 1 \end{bmatrix} \end{aligned}$$

Si on note $\{e_i\}_{1 \leq i \leq n}$ la base canonique, on remarque que :

$$\forall 1 \leq i \leq k, \ AVe_i \equiv 0 \pmod{d_k}$$

étant donné qu'on a la condition de divisibilité suivante sur les diviseurs élémentaires de A :

$$d_k \mid d_{k-1} \mid \cdots \mid d_2 \mid d_1$$

On a alors montré que les k premières colonnes de V forment une famille libre du noyau de A modulo d_k. De plus, comme U et V sont unimodulaires, la dimension ne peut pas être plus grande que k, donc elle est exactement égale à k. □

Remarque : On remarque que grâce à ce lemme, il nous suffit de calculer la forme normale de Smith de la matrice en question afin de savoir si un tel noyau existe et d'en obtenir une base.

Définition 2.3.4. *Pour une matrice $M \in \mathcal{M}_n(\mathbb{Z})$ de déterminant non nul, on notera $d_1(M), \ldots, d_n(M)$ les diviseurs élémentaires de la matrice M (donnés par sa forme normale de Smith).*

Remarque : Dans les cas où cela ne sera pas ambigu, on les notera $d_1, \ldots, d_n$ au lieu de $d_1(M), \ldots, d_n(M)$.

On introduit la notation suivante, qui raffine la définition 2.1.3 :

Définition 2.3.5. *Soit n un entier strictement positif. On désigne par $Sym^*(n, \mathbb{Z})$ l'ensemble des éléments M de $Sym(n, \mathbb{Z})$ vérifiant $d_2(M) = 1$.*

2.4 L'hypothèse de Riemann

On donne ici la définition de la fonction zêta de Riemann afin de donner un énoncé de l'hypothèse de Riemann pour les fonctions zêtas de Dedekind des corps de nombres. Ces définitions sont issues de [Lan86, p159].

La fonction ζ de Riemann est définie de la façon suivante :

$$\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s}$$

et il est connu que lorsque $\Re(s) > 1$, on a :

$$\zeta(s) = \prod_{p \in \mathcal{P}} \frac{1}{1 - p^{-s}}$$

On considère maintenant un corps de nombres $\mathbb{K}$, tel que $[\mathbb{K} : \mathbb{Q}] = n$. Si $\mathfrak{p}$ est un idéal premier de $\mathbb{K}$ tel que $\mathfrak{p} \mid p$ et si $\mathcal{N}(\mathfrak{p}) = p^{f_\mathfrak{p}}$ où $f_\mathfrak{p} = \deg \mathfrak{p}$ est le degré résiduel de $\mathfrak{p}$ dans $\mathbb{K}$, alors on a :

$$\sum_{\mathfrak{p} \mid p} f_\mathfrak{p} \leq n$$

On définit ensuite la *fonction zeta de Dedekind de* $\mathbb{K}$ par :

$$\zeta_\mathbb{K}(s) = \sum_{\mathfrak{p}} \frac{1}{\mathcal{N}(\mathfrak{p})^s}$$

On a aussi :

$$\zeta_{\mathbb{K}}(s) = \prod_{\mathfrak{p}} \frac{1}{1 - \mathcal{N}(\mathfrak{p})^{-s}}$$

L'hypothèse de Riemann pour la fonction zêta de Dedekind d'un corps de nombres est alors semblable à celle pour la fonction zêta « classique » de Riemann : les zéros non triviaux sont situés sur la droite verticale $\Re(s) = \frac{1}{2}$.

2.5 L'algorithme de Pollard et Schnorr

L'algorithme de Pollard et Schnorr [PS87] est une méthode permettant de résoudre en temps polynomial et sans factorisation des équations du type :

$$x^2 + ky^2 \equiv m \pmod{n} \tag{2.1}$$

où m, n sont des entiers.

En 1984, Ong, Schnorr et Shamir avaient proposé un schéma de signature basé sur les équations quadratiques [OSS84]. La sécurité de ce schéma était basée sur le fait que résoudre des équations quadratiques du type (2.1) est aussi difficile que de factoriser le module n. Cependant, en 1987, dans [PS87], Pollard et Schnorr ont proposé un algorithme résolvant ce type d'équation sans factoriser le module n, ce qui a totalement brisé ce schéma de signature.

Cet algorithme est basé sur la propriété de multiplicativité de la norme dans les corps de nombres quadratiques. C'est–à–dire sur l'identité :

$$(x_1^2 + ky_1^2)(x_2^2 + ky_2^2) = X^2 + kY^2 \tag{2.2}$$

où

$$\begin{aligned} X &= x_1x_2 \pm ky_1y_2 \\ Y &= x_1y_2 \mp x_2y_1 \end{aligned}$$

ici dans le corps $\mathbb{Q}(\sqrt{-k})$. Le principe réside également dans le fait qu'il est possible dans l'équation (2.1) d'interchanger les rôles de k et m. En posant $x' = \frac{x}{y} \pmod{n}$, $y' = \frac{1}{y} \pmod{n}$, on obtient $x'^2 - my'^2 \equiv -k \pmod{n}$. L'idée développée est alors de remplacer le m de départ par un m' plus petit. La structure de l'algorithme est

la suivante :

Algorithme 2.5.1: Pollard–Schnorr [PS87]

Données : n, k, m
Résultat : une solution (x, y) de l'équation $x^2 + ky^2 \equiv m \pmod{n}$

1 **début**
2 **si** *n est une puissance d'un premier* **alors**
3 résoudre (2.1) en calculant des racines carrées dans $(\mathbb{Z}/n\mathbb{Z})^*$
4 **fin si**
5 remplacer m par un m' équivalent vérifiant $0 < m' \leq \sqrt{\frac{4k}{3}}$ si $k > 0$ et $0 < |m'| \leq \sqrt{|k|}$ si $k < 0$
6 **si** *m' est un carré ou $m' = k$* **alors**
7 résoudre $x^2 + ky^2 \equiv m' \pmod{n}$ avec $y = 0$ ou $x = 0$ et aller en 11
8 **fin si**
9 appliquer l'algorithme récursivement pour résoudre $x'^2 - m'y'^2 \equiv -k \pmod{n}$ de sorte que $y' \wedge n = 1$
10 résoudre $x^2 + ky^2 \equiv m' \pmod{n}$ en posant $x = \frac{x'}{y'} \pmod{n}$ et $y = \frac{1}{y'} \pmod{n}$
11 en déduire une solution de l'équation de départ
12 **retourner** (x, y)
13 **fin**

L'étape 5 est la clef de cet algorithme. Elle consiste à trouver un entier m' tel que :

$$0 < m' \leq \sqrt{\frac{4k}{3}} \qquad \text{dans le cas } k > 0$$
$$0 < |m'| \leq \sqrt{|k|} \qquad \text{dans le cas } k < 0$$

et tel que l'on puisse déduire d'une solution de l'équation :

$$x^2 + ky^2 \equiv m' \pmod{n}$$

une solution de l'équation

$$x^2 + ky^2 \equiv m \pmod{n}$$

Afin d'effectuer la réduction, on commence par choisir un entier m_0, premier, tel que $\left(\frac{-k}{m_0}\right) = 1$ puis on résoud l'équation $x_0^2 = -k \pmod{m_0}$. La méthode proposée dans [PS87] est de choisir aléatoirement une paire d'entiers $(u, v) \pmod{n}$ avec $u^2 + kv^2 \in (\mathbb{Z}/n\mathbb{Z})^*$, poser $m_0 = m(u^2 + kv^2) \pmod{n}$, puis essayer de résoudre l'équation $x_0^2 = -k \pmod{m_0}$ au moyen d'un algorithme probabiliste de calcul de racine carrée modulaire qui trouve la racine carrée avec probabilité $\frac{1}{2}$ pourvu que m_0 soit premier. Si l'hypothèse de Riemann est vraie (voir section 2.4), il faut essayer en moyenne $\mathcal{O}(\log n)$ paires (u, v) avant de trouver un m_0 premier et x_0. Lorsque l'on dispose de x_0, m_0, u et v il faut alors résoudre :

$$x'^2 + ky'^2 \equiv m_0 \pmod{n} \tag{2.3}$$

En effet, si l'on connait les variables précédemment citées ainsi qu'une solution (x'', y'') de (2.3), on a :

$$\begin{aligned} x''^2 + ky''^2 &\equiv m_0 \pmod{n} \\ (x''^2 + ky''^2)(u^2 + kv^2) &\equiv m_0^2 m^{-1} \pmod{n} \end{aligned}$$

on utilise ensuite l'identité (2.2), on obtient alors X et Y vérifiant :

$$X^2 + kY^2 \equiv m_0^2 m^{-1} \pmod{n}$$

en posant ensuite $x = Xmm_0^{-1}$ et $y = Ymm_0^{-1}$, il vient :

$$\begin{aligned} x^2 + ky^2 &\equiv (Xmm_0^{-1})^2 + k(Ymm_0^{-1})^2 && \pmod{n} \\ &\equiv X^2 m^2 (m_0^{-1})^2 + kY^2 m^2 (m_0^{-1})^2 && \pmod{n} \\ &\equiv m^2 (m_0^{-1})^2 (X^2 + kY^2) && \pmod{n} \\ &\equiv m^2 (m_0^{-1})^2 m_0^2 m^{-1} && \pmod{n} \\ &\equiv m && \pmod{n} \end{aligned}$$

ce qui nous donne une solution de (2.1). Il reste maintenant à résoudre l'équation (2.3.) Pour cela, on effectue l'étape de réduction ; on définit les entiers

$$m_1,\ x_1,\ m_2,\ x_2,\ \ldots,\ x_{I-1},\ m_I = m'$$

de la façon suivante :

$$\begin{aligned} x_0^2 + k &= m_0 m_1 \\ x_1 &= \min\left(x_0 \pmod{m_1},\ m_1 - (x_0 \pmod{m_1})\right) \\ &\vdots \\ x_i^2 + k &= m_i m_{i+1} \\ x_{i+1} &= \min\left(x_i \pmod{m_{i+1}},\ m_{i+1} - (x_i \pmod{m_{i+1}})\right) \\ &\vdots \\ x_{I-1}^2 + k &= m_{I-1} m_I \end{aligned}$$

on effectue cette réduction jusqu'à l'obtention d'un entier $i = I$ tel que :

$$\begin{aligned} x_{I-1} \leq m_I \leq m_{I-1} \qquad & \text{si } k > 0 \\ |m_I| \leq \sqrt{|k|} \qquad & \text{si } k < 0 \end{aligned}$$

une fois ces égalités obtenues, on multiplie les équations :

$$x_i^2 + k = m_i m_{i+1} \qquad \text{pour } i = 0, 1, \ldots, I-1$$

et en utilisant l'identité (2.2), on obtient deux entiers s et t tels que :

$$s^2 + kt^2 = m_0 \left(m_1 m_2 \ldots m_{I-1}\right)^2 m_I$$

ou bien, en posant $U = \frac{s}{M}$, $V = \frac{t}{M}$, $M = m_1 m_2 \dots m_I \pmod n$, on a :

$$U^2 + kV^2 \equiv m_0 m_I^{-1} \pmod n \tag{2.4}$$

Maintenant, si on dispose d'une solution de l'équation suivante :

$$x^2 + ky^2 \equiv m_I \pmod n$$

on peut alors multiplier (2.3) et (2.4) et résoudre (2.1) en utilisant une fois encore l'identité (2.2). Cette étape de réduction se termine donc en stockant les valeurs de U et V. On réitère alors le processus pour avoir une solution de (2.4). En effet, le m de départ a été remplacé par un m_I plus petit.

La complexité annoncée dans [PS87] est la suivante :

Théorème 2.5.1. *Supposons que GRH est vraie. Alors l'algorithme probabiliste 2.5.1 prend en entrée des entiers k, m, et n tels que $\gcd(km, n) = 1$ et donne une solution de l'équation $x^2 + ky^2 \equiv m \pmod n$ en $\mathcal{O}\left((\log n)^2 \left|\log\log|k|\right|\right)$ opérations arithmétiques sur des entiers de taille $\mathcal{O}(\log n)$ bits.*

2.6 Algorithmes existants

Dans cette section, je donne une liste non exhaustive des algorithmes existant pour résoudre des équations quadratiques en différentes dimensions.

2.6.1 Dimension 3

Le cas des équations quadratiques de cette dimension fait l'objet du mémoire de master [Cas08]. Rappelons–en brièvement le principe.

On dispose d'une forme quadratique de dimension 3 dont on souhaite obtenir un vecteur isotrope non trivial. L'algorithme développé par Simon dans [Sim05b] se décompose en les étapes suivantes :

1. Décomposer le déterminant de la matrice de la forme quadratique en produit de facteurs premiers.
2. Effectuer des minimisations sur la forme pour chacun des nombres premiers composant le déterminant.
3. Appliquer l'algorithme LLL pour réduire la forme.
4. On est alors ramené à une forme quadratique diagonale, de déterminant égal à ± 1.
5. Calculer une solution pour cette forme.
6. Effectuer le changement de base pour obtenir une solution pour la forme de départ

2.6.2 Dimension 4

Dans le cas de la dimension 4, il y a deux cas différents : soit le déterminant de la forme quadratique en question est un carré, soit il n'en n'est pas un. Si c'est un carré, il est alors possible de généraliser la méthode décrite pour la dimension 3. Lors de l'étape de minimisation, cette méthode réduit les puissances des nombres premiers deux par deux, donc si le déterminant de la forme est un carré, on se ramène alors à une forme diagonale dont le déterminant vaut ± 1. Il est donc aisé de trouver une solution.

Si le déterminant de la forme n'est pas un carré, il y a plus de travail à effectuer. La méthode développée dans [Sim05a] consiste à augmenter la dimension de la forme en question de 2 de sorte d'obtenir une forme avec les bons invariants. Il faut pour cela calculer la 2–partie du groupe de classes en utilisant l'algorithme décrit dans [BS96]. Une fois cela calculé, il faut ensuite trouver la forme ayant les bons invariants de Witt, puis décomposer et minimiser la forme.

2.6.3 Dimension 5 et plus

Pour ce qui est des dimensions 5 et plus, dans [Sim05a] Simon donne une algorithme permettant de résoudre ces équations en différenciant les cas selon la parité de la dimension. Pour chacun des cas, la factorisation du déterminant est requise. Lorsque la dimension est supérieure ou égale à 5 et impaire, le principe est le suivant :

1. Calculer la signature (r, s) de la forme. Si r ou s est nul, il n'y a pas de solution.
2. Effectuer des minimisations sur la forme pour chacun des nombres premiers composant le déterminant.
3. Appliquer l'algorithme LLL pour réduire la forme.
4. Si le déterminant vaut ± 1, utiliser l'algorithme [Sim05a, algorithm 2] afin de trouver un sous espace totalement isotrope pour la forme. En déduire un pour la forme de départ.
5. Poser $\delta = -8\,|\det Q|$ et calculer un système de générateurs du 2–Sylow du groupe de classes $\mathcal{C}l(\delta)$ à l'aide de l'algorithme donné dans [BS96].
6. Trouver une forme ayant les bons invariants locaux de Witt de dimension 2.
7. Augmenter la dimension de la forme de départ de 2 en ajoutant la forme précédemment trouvée. Effectuer des minimisations sur cette nouvelle forme.
8. En considérant des intersections de sous espaces isotropes de la bonne dimension, déduire un sous espace isotrope pour la forme de départ.

Lorsque la dimension est supérieure ou égale à 6 et paire, la méthode est similaire à celle énoncée et diffère à partir de l'étape 5. Dans ce cas–ci, on ne va pas chercher une forme avec les bons invariants, on va augmenter la dimension de la forme de départ de 1 en ajoutant $-Id$. Puis de la même manière que précédemment, on cherche un sous espace isotrope pour la forme de départ en considérant des intersections de sous–espaces isotropes pour la forme augmentée.

Comme il est décrit dans l'article correspondant, les performances de cette méthode sont limitées par le fait que la factorisation du déterminant de la forme est

requise. La complexité est donc sous–exponentielle. Cependant, si on met de coté la partie factorisation du déterminant, elle semble être polynomiale en la taille des coefficients.

Chapitre 3

Algorithme

Dans ce chapitre, je donne les détails de fonctionnement du résultat principal de cette thèse, à savoir un algorithme qui permet de trouver un vecteur isotrope pour une forme quadratique de dimension 5 non dégénérée et indéfinie, sans avoir recours à un quelconque algorithme de factorisation. Le principe est de compléter la matrice de la forme en question pour en obtenir une de dimension 6 pour laquelle trouver une solution est « facile », et d'en déduire une solution pour la forme de départ. On aboutira alors à l'algorithme 3.0.1 qui est le suivant :

Algorithme 3.0.1: Résolution(Q_5)

Données : Q_5 : forme quadratique de dimension 5 non dégénérée et indéfinie
Résultat : X : vecteur non nul de $\mathbb{Z}^5$ vérifiant ${}^tXQ_5X = 0$

1 **début**
2 Appliquer l'algorithme de minimisation 3.4.5 à Q_5
3 Appliquer les algorithmes de réduction de la partie paire 3.4.6 et 3.4.7 à la forme obtenue en 2
4 Appliquer l'algorithme de complétion 3.3.1 à la forme obtenue en 3 jusqu'à ce que le déterminant de la forme complétée Q_6 soit égal à $\pm 2p$ où $p \in \mathcal{P}$ et $p \neq 2$
5 Trouver une solution à l'équation ${}^tXQ_6X = 0$
6 Décomposer Q_6 en $Q_6 = H \oplus Q_4$ où H est un plan hyperbolique
7 Trouver une solution à l'équation ${}^tXQ_4X = 0$
8 Décomposer Q_4 en $Q_4 = H' \oplus Q_2$ où H' est un plan hyperbolique
9 En déduire une solution S de ${}^tXQ_5X = 0$
10 **retourner** S
11 **fin**

et dont la preuve sera faite dans la section 3.5.

On commence donc par expliquer comment on complète cette matrice, quel est son déterminant, quelles sont les conditions vérifiées par ce déterminant. On détaille ensuite les étapes de minimisation à effectuer sur la forme de départ et pourquoi il faut les faire. La fin de ce chapitre donne la version complète de l'algorithme en question ainsi que sa preuve.

Dans ce qui va suivre, on utilisera les notations suivantes :

À $Q_n \in \mathrm{Sym}(n, \mathbb{Z})$, on associe Q_{n+1} comme étant la matrice complétée de Q_n de la manière suivante :

$$Q_{n+1} = \begin{bmatrix} Q_n & X \\ {}^tX & z \end{bmatrix} \qquad\qquad X = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

où $x_i \in \mathbb{Z}$ et $z \in \mathbb{Z}$. On note également $\Delta_n = \det Q_n$ et $\Delta_{n+1} = \det Q_{n+1}$.

3.1 Déterminant de la forme complétée

Commençons d'abord par rappeler la définition de la comatrice et la valeur de ses coefficients :

Définition 3.1.1 (Cofacteur). *Soit $A = (a_{ij})$ une matrice carrée de taille n. On appelle $(i,j)^{ème}$ cofacteur de A le produit de $(-1)^{i+j}$ et du déterminant de la matrice A à laquelle on a éliminé la $i^{ème}$ ligne ainsi que la $j^{ème}$ colonne. Autrement dit :*

$$Cof_{i,j} = (-1)^{i+j} \times \det \begin{bmatrix} & & & & j & & & \\ a_{1,1} & a_{1,2} & \dots & a_{1,j-1} & a_{1,j} & a_{1,j+1} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,j-1} & a_{2,j} & a_{2,j+1} & \dots & a_{2,n} \\ \vdots & & & \vdots & & & & \\ a_{i-1,1} & \dots & \dots & a_{i-1,j-1} & a_{i-1,j} & a_{i-1,j+1} & & a_{i-1,n} \\ a_{i,1} & - & - & a_{i,j-1} & a_{i,j} & a_{i,j+1} & - & a_{i,n} \\ a_{i+1,1} & & & a_{i+1,j-1} & a_{i+1,j} & a_{i+1,j+1} & & a_{i-1,n} \\ \vdots & & & & & & & \\ a_{n,1} & a_{n,2} & \dots & a_{n,j-1} & a_{n,j} & a_{n,j+1} & \dots & a_{n,n} \end{bmatrix} i$$

Définition 3.1.2 (Comatrice). *Soit A une matrice carrée de taille n. On appelle comatrice de A, notée $\mathrm{Co}(A)$ la matrice composée des cofacteurs de la matrice A.*

Remarque : On rappelle rapidement que la comatrice intervient dans le calcul de l'inverse d'une matrice. Si la matrice A est inversible, on a :

$$A^{-1} = \frac{1}{\det A} \, {}^t\mathrm{Co}(A)$$

ou bien, on a l'égalité suivante, valable même si la matrice A n'est pas inversible :

$$A \, {}^t\mathrm{Co}(A) = \det A \times Id_n$$

La formule qui va suivre est relativement simple mais joue un rôle fondamental pour la suite de l'algorithme :

Proposition 3.1.3 (Déterminant de la matrice complétée). *Soit Q_n une matrice symétrique de dimension n. Si on désigne par Q_{n+1} la forme quadratique obtenue en ajoutant à Q_n une ligne et une colonne de la façon suivante :*

$$Q_{n+1} = \begin{bmatrix} & & & x_1 \\ & Q_n & & \vdots \\ & & & x_n \\ x_1 & \dots & x_n & z \end{bmatrix}$$

et si on désigne par X le vecteur formé des coefficients x_i pour $1 \leq i \leq n$, alors le déterminant Δ_{n+1} de Q_{n+1} vérifie :

$$\Delta_{n+1} = \Delta_n z - {}^tX \operatorname{Co}(Q_n) X$$

où Δ_n désigne le déterminant de Q_n.

Démonstration. On notera dans la suite $X = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$ et $Q_n = [a_{i,j}]_{1 \leqslant i,j \leqslant n}$, avec $a_{i,j} = a_{j,i}$ pour tous i, j. On commence par développer le déterminant de cette matrice selon la dernière colonne :

$$\Delta_{n+1} = \sum_{i=1}^{n} (-1)^{n+1+i} x_i \det \widehat{Q_i} \; + \Delta_n z$$

où $\widehat{Q_i}$ représente la matrice Q_{n+1} à laquelle on a enlevé la $i^{\text{ème}}$ ligne ainsi que la dernière colonne. On développe maintenant $\det \widehat{Q_i}$ selon la dernière ligne, ce qui donne :

$$\det \widehat{Q_i} = \sum_{j=1}^{n} (-1)^{n+j} x_j \det \widehat{Q_{i,j}}$$

où $\widehat{Q_{i,j}}$ désigne la matrice $\widehat{Q_i}$ à laquelle on a enlevé la dernière ligne ainsi que la $j^{\text{ème}}$ colonne. On remarque qu'en fait $\det \widehat{Q_{i,j}}$ représente exactement le $(i,j)^{\text{ème}}$ cofacteur de Q_n au signe près. On a ainsi :

$$\det \widehat{Q_i} = \sum_{j=1}^{n} (-1)^{n+j} x_j \, (-1)^{i+j} \operatorname{Co}(Q_n)_{i,j}$$

Fort de ces remarques, on remet tout en place dans la formule de départ :

$$\begin{aligned}
\Delta_{n+1} &= \sum_{i=1}^{n} \left((-1)^{n+i+1} x_i \left(\sum_{j=1}^{n} (-1)^{n+j} x_j \, (-1)^{i+j} \operatorname{Co}(Q_n)_{i,j} \right) \right) + \Delta_n z \\
&= \sum_{i=1}^{n} \left(\sum_{j=1}^{n} (-1)^{n+i+1} \, (-1)^{n+j} \, (-1)^{i+j} x_i x_j \operatorname{Co}(Q_n)_{i,j} \right) + \Delta_n z \\
&= -\sum_{i=1}^{n} \left(\sum_{j=1}^{n} x_i x_j \operatorname{Co}(Q_n)_{i,j} \right) + \Delta_n z
\end{aligned}$$

D'où :

$$\Delta_{n+1} = \Delta_n z - {}^tX \operatorname{Co}(Q_n) X \tag{3.1}$$

□

3.2 Congruence du déterminant

Pour commencer, on rappelle la définition 2.3.5 de $\mathrm{Sym}^*(n,\mathbb{Z})$: soit n un entier strictement positif. On désigne par $\mathrm{Sym}^*(n,\mathbb{Z})$ l'ensemble des éléments M de $\mathrm{Sym}(n,\mathbb{Z})$ vérifiant $d_2(M)=1$.

Théorème 3.2.1 (Congruence du déterminant dans $\mathbb{Z}$)**.** *Soit $Q_n \in Sym^*(n,\mathbb{Z})$ de déterminant Δ_n. Alors il existe un entier δ premier avec Δ_n, et $\alpha \in \mathbb{Z}$ tels que :*

$$ {}^tX\,\mathrm{Co}(Q_n)X \equiv \delta\alpha^2 \pmod{\Delta_n} \text{ pour tout } X \in \mathbb{Z}^n $$

De plus, α peut être donné par la première coordonnée de $Y = {}^tVX$ où V est donnée par la forme normale de Smith de Q_n.

Démonstration. Soient U, V et D les matrices données par la décomposition en forme normale de Smith de Q_n vérifiant $D = UQ_nV$. Comme Q_n appartient à l'ensemble $\mathrm{Sym}^*(n,\mathbb{Z})$, D est de la forme :

$$ D = \begin{bmatrix} |\Delta_n| & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{bmatrix} $$

La matrice V est unimodulaire, on effectue un changement de base selon V. Cela nous donne :

$$ {}^tVQ_nV \equiv \left[\begin{array}{c|ccc} 0 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & Q_{n-1} & \\ 0 & & & \end{array}\right] \pmod{\Delta_n} $$

On a alors, en passant à la comatrice :

$$ \mathrm{Co}({}^tVQ_nV) \equiv \left[\begin{array}{c|ccc} \Delta_{n-1} & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & 0 & \\ 0 & & & \end{array}\right] \pmod{\Delta_n} \tag{3.2} $$

où Δ_{n-1} désigne le déterminant de la matrice symétrique Q_{n-1}. Montrons que Δ_{n-1} est premier avec Δ_n :

Le changement de base V étant unimodulaire, la matrice ${}^tVQ_nV$ est de même déterminant que Q_n. Sa première colonne (ainsi que sa première ligne) est divisible par Δ_n. Donc, si on cherche à calculer le déterminant en effectuant un développement en cofacteurs selon la première colonne, on obtient $\Delta_n = \lambda_{1,1}\Delta_n \times \det(Q_{n-1}) + \sum_{i=2}^{n} \lambda_{i,1}\Delta_n \det(Q_{i,1})$ où $Q_{i,1}$ désigne la matrice extraite de Q_n à laquelle on a enlevé la $i^{\text{ème}}$ ligne et la première colonne et λ_{ij} des entiers apparaissant dans les coefficients de la matrice. On note que les coefficients de la première ligne de chacune des

matrices $Q_{i,1}$ sont divisibles par Δ_n. On obtient alors une relation du type : $\Delta_n = \lambda_{1,1}\Delta_n \times \det(Q_{n-1}) + \sum_{i=2}^{n} \mu_{i,1}\Delta_n^2$ où $\mu_{i,1} \in \mathbb{Z}$. En simplifiant par $\Delta_n \neq 0$, on obtient :

$$1 = \lambda_{1,1} \det(Q_{n-1}) + \Delta_n \sum_{i=2}^{n} \mu_{i,1}$$

On a ainsi une combinaison linéaire de $\det(Q_{n-1})$ et de Δ_n valant 1, d'où $\Delta_n \wedge \det(Q_{n-1}) = 1$.

On note par ailleurs que :

$$\begin{aligned} \mathrm{Co}({}^tVQ_nV) &= \Delta_n \, {}^t({}^tVQ_nV)^{-1} \\ &= \Delta_n({}^tVQ_nV)^{-1} \\ &= V^{-1}(\Delta_n Q_n^{-1}) \, {}^tV^{-1} \\ &\text{en utilisant (3.2),} \\ &= V^{-1} \mathrm{Co}(Q_n) \, {}^tV^{-1} \end{aligned}$$

En posant alors $X = {}^tV^{-1}Y$, avec $Y = \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix}$ il vient :

$$\begin{aligned} {}^tX \, \mathrm{Co}\,(Q_n)X &= {}^t({}^tV^{-1}Y) \, \mathrm{Co}(Q_n)({}^tV^{-1}Y) \\ &= {}^tY \, \mathrm{Co}({}^tVQ_nV)Y \\ &\equiv \Delta_{n-1}y_1^2 \pmod{\Delta_n} \end{aligned}$$

En posant $\delta = \Delta_{n-1}$ et $\alpha = y_1$, il vient alors :

$${}^tX \, \mathrm{Co}(Q_n)X \equiv \delta\alpha^2 \pmod{\Delta_n}$$

□

3.3 Signature de la forme complétée

On donne ici une formule pour connaître la signature de la forme complétée.

3.3.1 Pourquoi vouloir imposer la signature ?

Dans la procédure de complétion de la matrice de la forme quadratique, le vecteur X est choisi aléatoirement et le z est fixé en fonction de la signature. Cependant il peut être nécessaire de contrôler le signe du déterminant de la forme obtenue. En effet, le succès de l'algorithme réside en partie dans le succès de l'algorithme de Simon à trouver des solutions à des équations quadratiques bien choisies. Pour que la réussite soit garantie, il faut commencer par s'assurer de l'existence de telles solutions. C'est en partie ce que nous permet le fait de pouvoir contrôler la signature de la forme complétée.

3.3.2 Comment choisir la signature ?

Lemme 3.3.1. *Soit $Q_n \in Sym(n,\mathbb{Z})$, indéfinie, de signature (r,s). Soit $\overline{\beta}$ un représentant de la classe de ${}^tX\,\mathrm{Co}(Q_n)X$ modulo Δ_n. On pose $z := \frac{{}^tX\,\mathrm{Co}(Q_n)X - \overline{\beta}}{\Delta_n}$ et $Q_{n+1} = \begin{bmatrix} Q_n & X \\ {}^tX & z \end{bmatrix}$. Alors la signature de Q_{n+1} varie selon le choix de $\overline{\beta}$ de la façon suivante :*

Signature de Q_{n+1}	$\overline{\beta} > 0$	$\overline{\beta} < 0$
$\det(Q_n) > 0$	$(r, s+1)$	$(r+1, s)$
$\det(Q_n) < 0$	$(r+1, s)$	$(r, s+1)$

De plus on a $\overline{\beta} = -\Delta_{n+1}$.

Démonstration. D'après 3.1.3, le déterminant de Q_{n+1} est donné par :

$$\Delta_{n+1} = \Delta_n z - {}^tX\,\mathrm{Co}(Q_n)X$$

On a défini les quantités suivantes :

$$\begin{aligned} \beta &= {}^tX\,\mathrm{Co}(Q_n)X \\ \overline{\beta} &= \text{un représentant de la classe de } \beta \text{ modulo } \Delta_n \\ &= \beta - z\Delta_n \\ &= -\Delta_{n+1} \end{aligned}$$

Comme le lien entre Q_n et Q_{n+1} est l'ajout d'une ligne et d'une colonne, si on considère la restriction de Q_{n+1} à l'espace engendré par les n premiers vecteurs de la base on obtient exactement la forme Q_n. Ainsi, compléter Q_n en lui ajoutant une ligne et une colonne ne change pas sa signature sur son espace de base. On peut donc connaître la signature de Q_{n+1} à partir de celle de Q_n en considérant les signes de Δ_n et de Δ_{n+1}.

Si la signature de Q_n est (r,s), on peut, grâce au signe de Δ_{n+1}, connaître la signature de Q_{n+1} puisque $sgn(\Delta_n) = (-1)^s$. Ainsi :

- Si $\Delta_n > 0$, on a $s \equiv 0 \pmod 2$. En prenant $\overline{\beta} > 0$, on obtient $\Delta_{n+1} < 0$. On a donc changé le signe du déterminant. Donc la signature de Q_{n+1} est $(r, s+1)$.
- Si Δ_n est positif, en prenant $\overline{\beta} < 0$, on a $\Delta_{n+1} > 0$. Donc la signature de Q_{n+1} est $(r+1, s)$.
- Si $\Delta_n < 0$, on a $s \equiv 1 \pmod 2$. Donc si on choisi $\overline{\beta} > 0$, on aura $\Delta_{n+1} < 0$ et donc la signature de Q_{n+1} sera $(r+1, s)$.
- Si $\Delta_n < 0$ et que l'on choisi $\overline{\beta} < 0$, on aura $\Delta_{n+1} > 0$, et donc la signature de Q_{n+1} sera $(r, s+1)$.

Cela se résume alors par le tableau suivant :

Signature de Q_{n+1}	$\overline{\beta} > 0$ $(\Delta_{n+1} < 0)$	$\overline{\beta} < 0$ $(\Delta_{n+1} > 0)$
$\det(Q_n) > 0$ $(s \equiv 0 \pmod 2)$	$(r, s+1)$	$(r+1, s)$
$\det(Q_n) < 0$ $(s \equiv 1 \pmod 2)$	$(r+1, s)$	$(r, s+1)$

□

L'algorithme de résolution va nécessiter que la signature (u, v) de Q_{n+1} vérifie $u \geq 2$ et $v \geq 2$. C'est pourquoi l'algorithme de complétion qui va suivre opère le choix de la valeur de $\overline{\beta}$ en ce sens. L'algorithme permettant de contrôler la signature de la forme complétée est donc le suivant :

Algorithme 3.3.1: Complétion(Q_n)

Données : Q_n : une forme quadratique de dimension n, non dégénérée et indéfinie ; $k \geq 1$ un entier

Résultat : Q_{n+1} : une forme quadratique de dimension $n+1$, non dégénérée, indéfinie et de signature (r, s) vérifiant $r \geq 2$, $s \geq 2$ et de la forme : $\begin{bmatrix} Q_n & X \\ {}^tX & z \end{bmatrix}$ et vérifiant $|\det Q_{n+1}| < k\,|\Delta_n|$

1 **début**
2 Calculer la signature de la forme Q_n. On la note (r, s).
3 Choisir un vecteur X entier aléatoirement dans $[\![0, |\Delta_n|[\![^n$
4 $\beta := {}^tX\,\mathrm{Co}(Q_n)X$, $\overline{\beta} := \beta \pmod{\Delta_n}$ avec $0 \leq \overline{\beta} < |\Delta_n|$
5 **si** $r = 1$ **alors**
6 **si** $\Delta_n > 0$ **alors**
7 $\overline{\beta} := \overline{\beta} - |\Delta_n|$
8 **fin si**
9 **fin si**
10 **si** $s = 1$ **alors**
11 $\overline{\beta} := \overline{\beta} - \Delta_n$
12 **fin si**
13 $z := \dfrac{\beta - \overline{\beta}}{\Delta_n}$
14 Ajouter un multiple aléatoire de $|\Delta_n|$ à $\overline{\beta}$ de sorte que $|\det Q_{n+1}| < k\,|\Delta_n|$ tout en respectant la condition sur la signature et mettre z à jour
15 **retourner** $Q_{n+1} = \begin{bmatrix} Q_n & X \\ {}^tX & z \end{bmatrix}$
16 **fin**

Remarques :

1. On note qu'en sortie de cet algorithme, le déterminant de la forme complétée est toujours égal à $-\overline{\beta}$. Ceci est une conséquence directe de la façon dont a été effectué le choix du z (voir la démonstration du lemme 3.3.1).

2. Lorsque l'on utilisera cet algorithme, on répètera la boucle principale jusqu'à ce que le $\overline{\beta}$ soit de la forme $2 \times p$ où $p \in \mathcal{P}$ impair. Ce choix est dû à une condition d'existence d'une solution lors du passage en dimension 4 et sera explicité lors de la preuve de l'algorithme de résolution 3.0.1.

3.4 Minimisations

Avant d'expliquer ce que signifie dans cette thèse le terme « minimisation », commençons d'abord par regarder la nature des valeurs prises par le déterminant de la forme complétée :

Lemme 3.4.1 (Valeurs prises par Δ_{n+1})**.** *Soit $Q_n \in Sym(n, \mathbb{Z})$ de déterminant Δ_n. Alors quels que soient $X \in \mathbb{Z}^n$ et $z \in \mathbb{Z}$, $d_2(Q_n)$ divise Δ_{n+1}.*

Démonstration. La formule 3.1.3 du calcul du déterminant de la matrice complétée est la suivante :

$$\Delta_{n+1} = \Delta_n z - {}^tX \operatorname{Co}(Q_n) X$$

Considérons la forme normale de Smith de Q_n : il existe alors deux matrices U, V de $GL_n(\mathbb{Z})$ et une matrice D diagonale à coefficients entiers telles que $D = UQ_nV$ où les coefficients diagonaux de D se divisent successivement (voir 2.3.2). On s'intéresse aux valeurs prises par le déterminant de la matrice Q_{n+1}, c'est–à–dire aux valeurs de $-{}^tX \operatorname{Co}(Q_n) X$ modulo Δ_n. On a :

$$\begin{aligned}
D &= UQ_nV \\
Q_n &= U^{-1}DV^{-1} \\
\operatorname{Co}(Q_n) &= \operatorname{Co}(V^{-1}) \operatorname{Co}(D) \operatorname{Co}(U^{-1}) \\
&= \det(V) \det(U)\, {}^tV \operatorname{Co}(D)\, {}^tU \\
&= \pm\, {}^t\big(U\, {}^t\operatorname{Co}(D) U\big) \\
&= \pm\, {}^t(U \operatorname{Co}(D) V)
\end{aligned}$$

La matrice D est alors de la forme :

$$D = \begin{bmatrix} d_1 & & & & & \\ & d_2 & & & & \\ & & \ddots & & & \\ & & & d_k & & \\ & & & & \ddots & \\ & & & & & d_n \end{bmatrix}$$

où $d_n \mid d_{n-1} \mid \cdots \mid d_2 \mid d_1$. On a notamment $d_1 = kd_2$ où $k \neq 0 \in \mathbb{N}$. Donc nécessairement, la comatrice de D est de la forme :

$$\operatorname{Co}(D) = \begin{bmatrix} d_2 \prod_{i=3}^n d_i & & & & \\ & kd_2 \prod_{i=3}^n d_i & & & \\ & & d_1 d_2 \prod_{i=4}^n d_i & & \\ & & & \ddots & \\ & & & & \prod_{i=1}^{n-1} d_i \end{bmatrix}$$

Comme tous les coefficients diagonaux de $\mathrm{Co}(D)$ sont des multiples de d_2, on a :

$$\begin{aligned} {}^tX\,\mathrm{Co}(Q_n)X &= \pm\ {}^tX\ {}^t(U\,\mathrm{Co}(D)V)X \\ &\equiv 0 \pmod{d_2} \end{aligned}$$

On a ainsi $\Delta_{n+1} = -\ {}^tX\,\mathrm{Co}(Q_n)X \pmod{\Delta_n}$.
Donc on a également $\Delta_{n+1} \equiv 0 \pmod{d_2}$. □

Remarque : On note ce lemme est également valable pour n'importe quel diviseur de d_2.

3.4.1 Calcul des d_i

Comme le suggère le lemme 3.4.1, si l'entier $d_2(Q_n)$ en question n'est pas factorisable il n'est pas possible par complétion de Q_n d'obtenir une forme Q_{n+1} dont le déterminant est factorisable. La solution à ce problème est alors la suivante :

1. Calculer $d_2(Q_n)$
2. Effectuer une minimisation sur la matrice Q_n afin de se ramener à $d_2(Q_n) = 1$ avant d'entamer la complétion.

Minimiser Q_n signifie donc se ramener à une matrice équivalente pour laquelle $d_2 = 1$. Le but de cette section est donc de donner les algorithmes permettant de se ramener au cas où $d_2 = 1$.

Les algorithmes qui vont suivre sont valables pour effectuer une minimisation lorsque la forme donnée est de dimension 5.

3.4.2 Cas où $d_5 \neq 1$

Proposition 3.4.2. *Soit $Q_5 \in Sym(5, \mathbb{Z})$ telle que $d_5 \neq 1$. Alors il existe deux matrices G et Q_f à coefficients entiers telles que :*

$$\begin{aligned} d_5 Q_f &= {}^tGQ_5G \\ \det Q_f &= \frac{1}{d_5^5} \det Q_5 \end{aligned}$$

Démonstration. Lorsque $d_5 \neq 1$, la matrice entière est divisible par d_5. La minimisation à effectuer consiste alors simplement à diviser la matrice par d_5 et le changement de base correspondant est $G = Id_5$. □

L'algorithme de minimisation est alors le suivant :

Algorithme 3.4.1: Minimisation $5(Q_5,\, m)$

Données : $Q_5 \in \mathrm{Sym}(5,\mathbb{Z})$ telle que $d_5(Q_5) \neq 1$; $m \in \mathbb{Z}$ un entier différent de 1 divisant $d_5(Q_5)$

Résultat : Q_f : forme équivalente à Q_5 et telle que $\det Q_f = \frac{1}{m} \det Q_5$; G : changement de base associé tel que $d_5 Q_f = {}^tGQ_5G$

```
1 début
2     G := Id_5
3     Q_f := (1/m) Q_5
4     retourner Q_f, G
5 fin
```

3.4.3 Cas où $d_4 \neq 1$ et $d_5 = 1$

Proposition 3.4.3. *Soit $Q_5 \in Sym(5,\mathbb{Z})$ telle que $d_4(Q_5) \neq 1$ et $d_5(Q_5) = 1$. Alors il existe deux matrices G et Q_f à coefficients entiers telles que :*

$$d_4 Q_f = {}^tGQ_nG$$
$$\det Q_f = \frac{1}{d_4^3} \det Q_n$$

Démonstration. À l'aide des matrices données par la forme normale de Smith de Q_5, $D = UQ_nV$ (voir 2.3.3), on commence par écrire Q_5 dans une base dans laquelle les 4 premières lignes et colonnes de Q_5 sont divisibles par d_4. Dans cette base Q_5 est de la forme :

$$\left[\begin{array}{cccc:c} d_4* & d_4* & d_4* & d_4* & d_4* \\ d_4* & d_4* & d_4* & d_4* & d_4* \\ d_4* & d_4* & d_4* & d_4* & d_4* \\ d_4* & d_4* & d_4* & d_4* & d_4* \\ \hdashline d_4* & d_4* & d_4* & d_4* & * \end{array}\right]$$

où les $*$ représentent des entiers.

Il nous suffit alors de multiplier la dernière ligne ainsi que la dernière colonne par d_4, puis de diviser la matrice obtenue par d_4. Cela revient à multiplier à droite et à gauche cette matrice par la matrice suivante :

$$H = \begin{bmatrix} 1 & & & & \\ & 1 & & 0 & \\ & & 1 & & \\ & 0 & & 1 & \\ & & & & d_4 \end{bmatrix}$$

On effectue une réduction à l'aide de l'algorithme LLL afin de contrôler la taille de la sortie. La matrice G du théorème est alors la matrice du changement de base complétée que l'on multiplie par la matrice précédente, soit $V \times H$. □

L'algorithme correspondant est alors le suivant :

Algorithme 3.4.2: Minimisation $4(Q_5, m)$

Données : $Q_5 \in \mathrm{Sym}(5, \mathbb{Z})$ telle que $d_4(Q_5) \neq 1$ et $d_5(Q_5) = 1$; m un entier différent de 1 divisant $d_4(Q_5)$

Résultat : Q_f : forme équivalente à Q_5 telle que $\det Q_f = \frac{1}{m^3} \det Q_n$; G : changement de base associé tel que $mQ_f = {}^tGQ_nG$

1 **début**
2 $V :=$ matrice V de la forme normale de Smith de Q_5
3 Soit H la matrice diagonale telle que pour $1 \leq i \leq 4$, $H_{i,i} = 1$ et $H_{5,5} = m$
4 $G := V \times H$; $Q' := \frac{1}{m}\, {}^tGQ_nG$
5 Appliquer l'algorithme LLL pour réduire Q'. On note Q_f la forme renvoyée et G' le changement de base associé.
6 $G := G \times G'$
7 **retourner** Q_f, G
8 **fin**

3.4.4 Cas où $d_3 \neq 1$ et $d_4 = 1$

Proposition 3.4.4. *Soit $Q_5 \in Sym(5, \mathbb{Z})$ telle que $d_3(Q_5) \neq 1$ et $d_4(Q_5) = 1$. Alors il existe deux matrices G et Q_f à coefficients entiers telles que :*

$$d_3 Q_f = {}^tGQ_5G$$
$$\det Q_f = \frac{1}{d_3} \det Q_5$$

Démonstration. La démonstration de cette proposition est essentiellement la même que celle de la proposition 3.4.3. La différence réside dans le fait que ce sont les 3 premières lignes ainsi que les 3 premières colonnes qui sont divisibles par d_3 après le changement de base effectué à l'aide de la matrice V de la forme normale de Smith de Q_5. □

De la même manière que pour la preuve, l'algorithme de minimisation associé à cette preuve est essentiellement identique à l'algorithme 3.4.2 :

Algorithme 3.4.3: Minimisation $3(Q_5,\, m)$

Données : $Q_5 \in \mathrm{Sym}(5,\mathbb{Z})$ telle que $d_3(Q_5) \neq 1$ et $d_4(Q_5) = 1$; m un entier différent de 1 divisant $d_3(Q_5)$

Résultat : Q_f : forme équivalente à Q_5 telle que $\det Q_f = \frac{1}{m} \det Q_5$; G : changement de base associé tel que $mQ_f = {}^tGQ_5G$

1 **début**
2 V :=matrice V de la forme normale de Smith de Q_5
3 Soit H la matrice diagonale telle que pour $1 \leq i \leq 3$, $H_{i,i} = 1$ et $H_{4,4} = H_{5,5} = m$
4 $G := V \times H$; $Q' := \frac{1}{m}\, {}^tGQ_5G$
5 Appliquer l'algorithme LLL pour réduire Q'. On note Q_f la forme renvoyée et G' le changement de base associé.
6 $G := G \times G'$
7 **retourner** Q_f, G
8 **fin**

3.4.5 Cas où $d_2 \neq 1$ et $d_3 = 1$

Dans l'algorithme qui va suivre, on se sert d'une variante de l'algorithme de Gram–Schmidt. La version originale est celle décrite dans [Coh96, p82]. La différence avec la version originale est la suivante : on travaille modulo un entier m fixé en entrée. Si on rencontre un entier ayant un pgcd différent de 1, m au cours de l'algorithme, on renvoie cet entier. Si au cours de la procédure on trouve un vecteur dont la norme est nulle ou divisible par m alors on ne continue pas et on renvoie ce vecteur. Enfin le changement de base correspondant est renvoyé sous forme d'une matrice à coefficients entiers compris entre 0 et $m-1$, triangulaire supérieure avec des 1 sur la diagonale.

Dans le cas où il existe un entier $m \neq 1$ qui divise $d_2(Q_5)$ et tel que $d_3(Q_5) = 1$,

l'algorithme suivant permet de minimiser Q_5 :

Algorithme 3.4.4: Minimisation 2(Q_5, m)

Données : $Q_5 \in \mathrm{Sym}(5,\mathbb{Z})$ telle que $d_2(Q_5) \neq 1$ et $d_3(Q_5) = 1$; m un entier différent de 1 divisant $d_2(Q_5)$

Résultat : Q_f : forme équivalente à Q_5 ; G : changement de base associé tel que $m'Q_f = {}^tGQ_5G$ où $1 < m' \mid m$

1 **début**
2 Calculer la forme normale de Smith de Q_5 avec l'algorithme de [Ili89].
3 $G := V$; $Q := {}^tGQ_5G$
4 Soit Q_3 le bloc 3×3 extrait en bas à droite de Q
5 Appliquer la variante de l'algorithme de Gram–Schmidt à (voir ci–dessus) à Q_3 et m
6 Si Gram–Schmidt renvoie un vecteur, le stocker dans S et aller en 10. Si Gram–Schmidt renvoie un entier m', recommencer en 5 avec $m = m'$.
7 On note D_3 la matrice obtenue et G_3 le changement de base correspondant
8 On note $d = D_3[1,1] \wedge m$. Si $d \neq 1$, recommencer en 5 avec $m = d$
9 Utiliser l'algorithme de Pollard–Schnorr 2.5.1 pour résoudre l'équation : $X^2 + \frac{D_3[2,2]}{D_3[1,1]}Y^2 \equiv -\frac{D_3[3,3]}{D_3[1,1]} \pmod m$. On note S une solution.
10 $S := [S, 1]$
11 Soit H une matrice 3×3 telle que sa première colonne soit égale à S de sorte que ses colonnes forment une base de $\mathbb{Z}^3$. Cela peut être obtenu via l'algorithme 2.3.1
12 $G_3 := G_3 \times H$
13 Soit $\widetilde{G}$ la matrice 5×5 diagonale par blocs telle que le bloc 2×2 en haut à gauche soit l'identité et le bloc 3×3 en bas à droite soit égal à G_3.
14 $G := G \times \widetilde{G}$; $Q' := \frac{1}{m}\,{}^tGQ_5G$.
15 Appliquer l'algorithme LLL pour réduire Q'. On note Q_f la forme renvoyée et G' le changement de base associé.
16 $G := G \times G'$
17 **retourner** Q_f, G
18 **fin**

La preuve de cet algorithme consiste en la proposition suivante :

Proposition 3.4.5. *Soit $Q_5 \in Sym(5,\mathbb{Z})$ telle que $d_2(Q_5) \neq 1$ et $d_3(Q_5) = 1$. Soit $m \in \mathbb{Z}$ un entier différent de 1 divisant $d_2(Q_5)$. Alors il existe deux matrices Q_f et G, G unimodulaire, à coefficients entiers telles que :*

$$\begin{aligned} mQ_f &= {}^tGQ_5G \\ \det Q_f &= \tfrac{1}{m}\det Q_5 \end{aligned}$$

Démonstration. On commence par calculer la forme normale de Smith $D = UQ_5V$

de Q_5. En appliquant le changement de base donné par la matrice V, on obtient :

$$ {}^tVQ_5V = \left[\begin{array}{c:c} mM_{2,2} & mM_{2,3} \\ \hdashline mM_{3,2} & Q_3 \end{array}\right] $$

La principale étape de cette minimisation va consister à trouver une base dans laquelle le coefficient situé en haut à gauche du bloc 3×3 va être divisible par m. Cela va alors nous permettre d'effectuer un autre changement de base afin de pouvoir réduire complètement la matrice par la suite. On extrait ce bloc 3×3 que l'on note Q_3. On a donc :

$$ {}^tVQ_5V = \left[\begin{array}{c:c} mM_{2,2} & mM_{2,3} \\ \hdashline mM_{3,2} & Q_3 \end{array}\right] $$

Afin d'obtenir une base dans laquelle le coefficient en question va être congru à 0 modulo m, il faut tout d'abord effectuer une orthogonalisation de Gram–Schmidt de Q_3. Ce procédé est appliqué directement modulo l'entier m en utilisant la variante citée en début de section. Comme m n'est pas nécessairement un nombre premier, il est possible que l'on obtienne un vecteur dont la norme est divisible par m. Dans ce cas, il n'est pas nécessaire de passer par l'algorithme de Pollard–Schnorr, on effectue directement le changement de base correspondant. Sinon, on obtient un base dans laquelle Q_3 est de la forme :

$$ \begin{bmatrix} a & & 0 \\ & b & \\ 0 & & c \end{bmatrix} \pmod{m} $$

On cherche une base dans laquelle le « nouveau » a va être divisible par m. Autrement dit, on cherche un vecteur $X = \begin{bmatrix} x \\ y \\ z \end{bmatrix}$ tel que :

$$ ax^2 + by^2 + cz^2 \equiv 0 \pmod{m} $$

Si a n'est pas premier avec m, cela signifie que l'on a trouvé un facteur de m. Il faut donc reprendre la minimisation en utilisant ce facteur à la place de m. Nous sommes maintenant dans le cas où a est premier avec m. On peut alors écrire :

$$ \begin{aligned} & x^2 + \frac{b}{a}y^2 + \frac{c}{a}z^2 \equiv 0 \pmod{m} \\ \iff & x^2 + \frac{b}{a}y^2 \equiv \frac{-c}{a}z^2 \pmod{m} \end{aligned} $$

Il est désormais possible d'utiliser l'algorithme de Pollard et Schnorr [PS87] et dont le principe est expliqué dans le section 2.5, puisque celui–ci permet de résoudre des équations du type :

$$X^2 + kY^2 \equiv M \pmod{N}$$

sans avoir besoin de la factorisation du module N. Afin de nous ramener exactement à ce type d'équation, on choisit de prendre $z = 1$.

On pourrait choisir de prendre n'importe quel z tel que $\frac{-c}{a}z^2$ soit premier avec m.

L'algorithme de Pollard et Schnorr nous donne alors un vecteur S solution de cette équation. On construit alors une base de $\mathbb{Z}^3$ en ajoutant à S la valeur de z choisie. La complétion de la famille contenant seulement le vecteur S en une base de $\mathbb{Z}^3$ se fait à l'aide de l'algorithme 2.3.1. Cet algorithme donne un changement de base unimodulaire. Dans cette nouvelle base, Q_3 s'écrit alors :

$$\begin{bmatrix} m* & * & * \\ * & * & * \\ * & * & * \end{bmatrix}$$

Notons G la matrice de changement de base qui nous a permis d'obtenir la forme précédente de la matrice Q_3. Il nous faut maintenant replacer la nouvelle version de Q_3 dans notre forme quadratique de départ. Le changement de base à effectuer est alors le suivant :

$$G' = \left[\begin{array}{cc:ccc} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ \hdashline 0 & 0 & \multicolumn{3}{c}{\multirow{3}{*}{G}} \\ 0 & 0 & & & \\ 0 & 0 & & & \end{array}\right]$$

Dans la base G', Q_5 est alors de la forme :

$$\left[\begin{array}{c:ccc} mM_{2,2} & \multicolumn{3}{c}{mM_{2,3}} \\ \hdashline & m* & * & * \\ mM_{3,2} & * & * & * \\ & * & * & * \end{array}\right]$$

Une fois Q_5 sous cette forme, il suffit de la multiplier à droite et à gauche par :

$$\begin{bmatrix} 1 & & & \\ & 1 & & 0 \\ & & 1 & \\ & 0 & & m \\ & & & & m \end{bmatrix}$$

Puis de diviser le résultat par m. On a ainsi multiplié le déterminant par m^4 puis on l'a divisé par m^5. On applique ensuite l'algorithme LLL afin de contrôler la taille de la sortie de cet algorithme. Le résultat obtenu finalement correspond à la matrice Q_f annoncée. Le changement de base correspondant est le produit des changements de base utilisés au long de la preuve. □

3.4.6 Algorithme de minimisation

On récapitule alors l'ensemble de ces algorithmes de minimisation dans l'algorithme qui va suivre.

Algorithme 3.4.5: Minimisation(Q_5)

Données : $Q_5 \in \mathrm{Sym}(5,\mathbb{Z})$
Résultat : $Q_t \in \mathrm{Sym}^*(5,\mathbb{Z})$ équivalente à Q_5 ; B : le changement de base associé

1 **début**
2 $Q_t := Q_5$
3 Calculer D forme normale de Smith de Q_5
4 **si** $d_1 = \det Q_5$ **alors**
5 aller en 28
6 **fin si**
7 **si** $d_5 \neq 1$ **alors**
8 $i := 5$
9 **fin si**
10 Soit $i \leq 5$ tel que $d_i \neq 1$ avec $d_{i+1} = 1$ et $d_i = d_5$ si $d_5 \neq 1$
11 $B := Id_5$
12 **tant que** $d_1 \neq \det(Q_t)$ **faire**
13 **suivant** i **faire**
14 **cas où** $i = 5$
15 Appliquer l'algorithme 3.4.1 à Q_t et d_i
16 **cas où** $i = 4$
17 Appliquer l'algorithme 3.4.2 à Q_t et d_i
18 **cas où** $i = 3$
19 Appliquer l'algorithme 3.4.3 à Q_t et d_i
20 **cas où** $i = 2$
21 Appliquer l'algorithme 3.4.4 à Q_t et d_i
22 **fin d'alternative**
23 Soient Q_f et G les matrices renvoyées
24 $Q_t := Q_f$; $B := B \times G$
25 Calculer la forme normale de Smith D de Q_t
26 Soit d_i le coefficient diagonal de la SNF de Q_t tel que $d_i \neq 1$ avec $d_{i+1} = 1$ et $d_i = d_5$ si $d_5 \neq 1$
27 **fin tq**
28 **retourner** Q_t, B
29 **fin**

Remarque : Cet algorithme nécessite de calculer la forme normale de Smith à chaque étape. Pour la calculer, on utilise de préférence l'algorithme décrit dans [Ili89] car celui–ci semble être optimisé et donne les matrices U et V correspondantes.
Remarque : On notera que dans cet algorithme, on utilise les algorithmes précédemment décrits non pas avec un entier divisant le coefficient d_i de la forme normale de Smith, mais avec d_i lui–même. Utiliser un simple diviseur nuirait complètement

à la performance de l'algorithme puisqu'il faudrait alors se servir d'un algorithme de factorisation.

Cet algorithme termine puisqu'à chaque étape, le déterminant de la matrice de départ est divisé par un facteur non trivial.

À la sortie de l'algorithme, on obtient une forme quadratique avec $d_2 = 1$. On obtient également la matrice du changement de base qui permet de passer de cette forme à celle de départ. Une solution pour la forme de départ s'obtient donc à partir d'une solution de la forme renvoyée par l'algorithme en utilisant le changement de base donné.

3.4.7 Réduction de la partie paire

Lemme 3.4.6. *Soit $Q_5 \in Sym^*(5,\mathbb{Z})$, indéfinie. Soit v le quotient dans la division euclidienne de la valuation 2–adique de $\det Q_5$ par 2. Alors il existe deux matrices Q' et G telles que :*

$$\begin{aligned} \det G &= \frac{1}{2^v} \\ Q' &= {}^tGQ_5G \\ v_2(\det Q') &= 0 \text{ ou } 1 \end{aligned}$$

et $Q' \in Sym^*(5,\mathbb{Z})$.

Démonstration. Si $\det Q_5$ est impair, il suffit de prendre $G = Id_5$ et $Q' = Q_5$. Supposons que $v_2(\det Q_5) \neq 0$. Dans ce cas, la forme normale de Smith de Q_5 nous donne trois matrices U, V et D telles que :

$$D = UQ_5V$$

avec U, V unimodulaires à coefficients entiers et D est diagonale avec $d_{1,1} = |\det Q|$ et les autres coefficients diagonaux sont tous égaux à 1 puisque $d_2(Q_5) = 1$. On effectue un changement de base selon la matrice V. Alors la première ligne ainsi que la première colonne de la matrice $Q'' = {}^tVQV$ sont divisibles par $2^{v_2(\det Q)}$. Soient alors v le quotient de la division euclidienne de $v_2(\det Q)$ par 2, F la matrice diagonale telle que le premier coefficient en haut à gauche est égal à $\frac{1}{2^v}$ et les autres a 1. Alors si $v_2(\det Q)$ est pair, le déterminant de ${}^tFQ''F = Q'$ est impair, sinon, le déterminant de Q' est divisible par 2 mais pas par 4. On prend donc $G = V \times F$. Reste à montrer que $Q' \in \mathrm{Sym}^*(5,\mathbb{Z})$. On sait que $Q_5 \in \mathrm{Sym}^*(5,\mathbb{Z})$. Le changement de base donnée par le calcul de la forme normale de Smith est unimodulaire, donc les facteurs invariants n'ont pas changés après ce changement de base. La dernière opération consiste à travailler sur la première colonne de la matrice et selon une puissance de 2, donc les facteurs invariants ne changent pas, donc $Q' \in \mathrm{Sym}^*(5,\mathbb{Z})$. Ce qui termine cette démonstration. □

L'algorithme de minimisation correspondant à ce lemme est donc le suivant :

Algorithme 3.4.6: Réduction de la partie paire - 1

Données : $Q_5 \in \mathrm{Sym}^*(5,\mathbb{Z})$ indéfinie, de dimension 5 de déterminant Δ_5
Résultat : $Q' \in \mathrm{Sym}^*(5,\mathbb{Z})$ indéfinie, de déterminant égal à $2^k n$ où n est impair et $k \equiv v_2(Q_5) \pmod 2$, Q' équivalente à Q_5 ; G le changement de base associé.

début
  si $\Delta_5 \equiv 1 \pmod 2$ **alors**
    retourner Q_5, Id_5
  fin si
  Poser $G = Id_5$
  Soit v_2 la valuation 2–adique de Δ_5
  Soit v le quotient dans la division euclidienne de v_2 par 2
  Soient U, V et D les matrices données par la forme normale de Smith de Q_5 telles que $D = UQ_5V$
  $Q' := {}^tVQ_5V$; $G := G \times V$
  Soit H la matrice diagonale telle que $H_{11} = \frac{1}{2^v}$ et $H_{ii} = 1$ sinon
  $Q' := {}^tHQ'H$; $G := G \times H$
  retourner Q', G
fin

Lemme 3.4.7. *Soit $Q_5 \in Sym^*(5,\mathbb{Z})$, indéfinie et telle que $\det Q_5 = 2 \times k$ où $k \in \mathbb{Z}$ impair. Alors il existe deux matrices Q' et G telles que :*

$$\begin{aligned} \det G &= \frac{1}{2^3} \\ Q' &= 2 \times {}^tGQ_5G \\ \det Q' &\equiv k \pmod 2 \end{aligned}$$

où $Q' \in Sym^*(5,\mathbb{Z})$.

Démonstration. Comme dans la démonstration du lemme précédent, on commence par calculer la forme normale de Smith de Q_5. Il existe donc trois matrices à coefficients entiers U, V et D telles que $D = UQ_5V$, où U et V sont unimodulaires et D est diagonale. Comme $d_2(Q_5) = 1$, on sait que le coefficient en haut à gauche de D est exactement au signe près le déterminant de Q_5. On effectue un changement de base selon la matrice V. On obtient donc une matrice Q' de la forme suivante :

$$Q' = {}^tVQV = \left[\begin{array}{c|cc|cc} 2* & \multicolumn{2}{c|}{2*} & & \\ \hline & \multicolumn{2}{c|}{\multirow{2}{*}{Q_1}} & * & * \\ 2* & \multicolumn{2}{c|}{} & * & * \\ \hline & * & * & * & * \\ & * & * & * & * \end{array}\right]$$

On s'intéresse alors à la forme quadratique Q_1 qui n'est autre que la restriction de la forme quadratique Q' au sous–espace vectoriel engendré par les second et

troisième vecteurs de la base. On note cette forme $\begin{bmatrix} a & b \\ b & c \end{bmatrix}$. On cherche maintenant à effectuer un changement de base sur cette forme de sorte que dans la nouvelle base, le coefficient correspondant à a soit divisible par 2. C'est–à–dire que l'on cherche un couple (x, y) d'entiers vérifiant :

$$ax^2 + 2bxy + cy^2 \equiv 0 \pmod 2$$

Ce qui revient à résoudre :

$$ax^2 + cy^2 \equiv 0 \pmod 2$$

Pour résoudre cette équation, il suffit de considérer la congruence de a et de c modulo 2. En effet, si $(a, c) \equiv (1, 1) \pmod 2$, on prend $(x, y) = (1, 1)$, si $(a, c) \equiv (1, 0) \pmod 2$, on prend $(x, y) = (0, 1)$. Si a est déjà pair, on ne change rien. On effectue ensuite le changement de base correspondant sur Q'. On obtient alors une matrice de la forme :

$$\left[\begin{array}{c|cccc} 2* & & 2* & & \\ \hline & 2* & * & * & * \\ 2* & * & * & * & * \\ & * & * & * & * \\ & * & * & * & * \end{array}\right]$$

On multiplie ensuite cette matrice par 2 avant d'effectuer une minimisation, on a alors une matrice de la forme :

$$\left[\begin{array}{c|cccc} 4* & & 4* & & \\ \hline & 4* & 2* & 2* & 2* \\ 4* & 2* & 2* & 2* & 2* \\ & 2* & 2* & 2* & 2* \\ & 2* & 2* & 2* & 2* \end{array}\right]$$

Les premiers changements de base étant unimodulaires et le déterminant de Q_5 divisible une seule fois par 2, le déterminant de cette matrice est donc divisible par 2^6 (mais pas par 2^7). On effectue alors un premier changement de base qui consiste à diviser les deux premières lignes ainsi que les deux premières colonnes par 2. La matrice obtenue est alors de la forme :

$$\begin{bmatrix} * & * & 2* & 2* & 2* \\ * & * & * & * & * \\ 2* & * & 2* & 2* & 2* \\ 2* & * & 2* & 2* & 2* \\ 2* & * & 2* & 2* & 2* \end{bmatrix}$$

et son déterminant est divisible par 2^2. On calcule alors la forme normale de Smith de cette matrice et on effectue le changement de base selon la matrice V obtenue. Comme le déterminant est un multiple de 4, on a alors deux possibilités :

Soit le noyau modulo 2 est de dimension 1 ; dans ce cas, la première ligne et la première colonne sont divisibles par 2 et le coefficient en haut à gauche de la matrice

est divisible par 4. On peut alors effectuer un changement de base consistant à multiplier le premier vecteur de la base par $\frac{1}{2}$.

Soit le noyau est de dimension 2. Dans ce cas, les deux premières lignes ainsi que les deux premières colonnes sont divisibles par 2. On s'intéresse alors au bloc 2×2 situé en haut à gauche de cette matrice, il s'agit de la restriction de notre forme à l'espace engendré par les deux premiers vecteurs de la base. On va alors effectuer un changement de base, de sorte que le coefficient en haut à gauche soit divisible par 4. Si on note cette forme $2ax^2 + 4bxy + 2cy^2$, il nous suffit de résoudre l'équation :

$$ax^2 + cy^2 \equiv 0 \pmod 2$$

Ce qui se fait comme expliqué précédemment. Une fois le changement de base effectué, il suffit alors d'effectuer un dernier changement de base consistant à multiplier par $\frac{1}{2}$ le premier vecteur. Dans cette nouvelle base, le déterminant de la forme quadratique est alors impair.

Reste maintenant à montrer que $Q' \in \mathrm{Sym}^*(5, \mathbb{Z})$. Les déterminants des changements de bases effectués sont de déterminant une puissance de 2, donc inversibles modulo les autres facteurs premiers du déterminant. Ainsi le rang de la matrice n'a pas changé modulo les autres facteurs premiers, donc $Q' \in \mathrm{Sym}^*(5, \mathbb{Z})$. □

Remarque : Ces deux lemmes s'utilisent ensemble. Dans la pratique, on commence par minimiser la forme quadratique de départ afin de se ramener au cas où $d_5(Q_5) = 1$. On utilise ensuite les deux lemmes précédents afin que le déterminant devienne impair.

Ces deux lemmes nous donnent alors un algorithme qui permet d'obtenir une forme quadratique dont le déterminant est impair avec $d_2 = 1$ et équivalente à Q_5, c'est–à–dire dont une solution nous donne une solution pour la forme de départ avec un simple changement de base.

Proposition 3.4.8 (Réduction de la partie paire)**.** *Il existe un algorithme qui étant donnée une matrice $Q_5 \in Sym^*(5, \mathbb{Z})$ indéfinie, de déterminant Δ_5 ; renvoie une matrice de $Sym^*(5, \mathbb{Z})$ indéfinie de déterminant impair ainsi que le changement de base associé.*

Cet algorithme nous est donné par les deux lemmes précédents.

Algorithme 3.4.7: Réduction de la partie paire - 2

Données : $Q_5 \in \mathrm{Sym}^*(n,\mathbb{Z})$ indéfinie avec $\det Q_5 = \Delta_5 = 2^k n$ ou n est impair et $k = 0$ ou 1

Résultat : Q', une matrice de $\mathrm{Sym}^*(5,\mathbb{Z})$ de déterminant impair et équivalente à Q_5 ; G le changement de base associé.

1 **début**
2 **si** $\Delta_5 \equiv 1 \pmod 2$ **alors**
3 **retourner** Q_5,Id_5
4 **fin si**
5 $G := Id_5$
6 Soit v la valuation 2–adique de Δ_5
7 Soient U, V et D les matrices données par la forme normale de Smith de Q_5 telles que $D = UQ_5V$
8 $Q' := {}^tVQV$; $G := G \times V$
9 **si** $(q'_{2,2}, q'_{3,3}) \equiv (1,1) \pmod 2$ **alors**
10 $H := Id_5$; $H[3,2] := 1$ puis $Q' := {}^tHQ'H$; $G := G \times H$
11 **fin si**
12 **si** $(q'_{2,2}, q'_{3,3}) \equiv (1,0) \pmod 2$ **alors**
13 $H := \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}$ puis $Q' := {}^tHQ'H$; $G := G \times H$
14 **fin si**
15 $Q' := 2 \times Q'$
16 $P := Id_5$; $P[2,2] := \frac{1}{2}$
17 $Q' := {}^tPQ'P$; $G := G \times P$
18 Soient U', V' et D' les matrices données par le calcul de la forme normale de Smith de Q' telles que $D = UQ'V$
19 $Q' := {}^tV'Q'V'$; $G := G \times V'$
20 **si** $q'_{1,1} \equiv 0 \pmod 4$ **alors**
21 $R := Id_5$; $R[1,1] := \frac{1}{2}$. $Q' := {}^tRQ'R$; $G := G \times R$
22 **retourner** Q',G
23 **fin si**
24 Répéter les étapes 9 à 14 avec $(q'_{1,1}, q'_{2,2})$
25 $R := Id_5$; $R[1,1] := \frac{1}{2}$. $Q' := {}^tRQ'R$; $G := G \times R$
26 **retourner** Q',G
27 **fin**

3.5 Preuve de l'algorithme

Théorème 3.5.1. *Soit Q_5 une forme quadratique de dimension 5 non dégénérée, indéfinie et à coefficients entiers. L'algorithme 3.0.1 donne une solution $X \in \mathbb{Z}^5$ non triviale de l'équation ${}^tXQ_5X = 0$ sans factoriser le déterminant de Q_5.*

Remarque : Le principe de l'algorithme repose en partie sur le fait que celui développé par Simon dans [Sim05b] est très efficace pour résoudre ce type d'équations dès que la factorisation du déterminant de la forme en question est connue. Ce théorème montre qu'il existe un algorithme efficace même lorsque la factorisation du déterminant est inconnue ou bien impossible à réaliser en un temps raisonnable.

Démonstration. La preuve de ce théorème suit le cheminement de l'algorithme en question. Il se décompose selon les étapes suivantes, numérotées comme dans l'algorithme 3.0.1 :

2 Minimisations

3 Réduction de la partie paire

4 Choix de la signature et complétion de Q_5 en imposant la forme du déterminant

5 Calcul d'une solution pour Q_6

6 Calcul d'un plan hyperbolique

7 Calcul d'une solution pour Q_4

8 Calcul d'un plan hyperbolique

9 Calcul d'une solution pour Q_5

L'enchainement de ces étapes donnera l'algorithme en lui–même et un récapitulatif sera donné à la fin de cette preuve.

L'idée générale de l'algorithme est la suivante : comme l'algorithme de Simon [Sim05b] est efficace lorsque la factorisation du déterminant est facile ou bien connue, nous allons chercher à construire une forme quadratique de dimension 6 de sorte que son déterminant soit égal à $\pm 2p$ avec p premier et sur laquelle on pourra utiliser l'algorithme de Simon. Une fois cette étape effectuée, il nous faudra en déduire une solution de l'équation de départ.

Étape 2 : on applique l'algorithme 3.4.5 qui est expliqué dans la section 3.4. À l'issue de cette étape, on obtient une forme $Q_5^{(2)} \in \mathrm{Sym}^*(5,\mathbb{Z})$ équivalente à Q_5 ainsi qu'une matrice inversible G_2 et un rationnel non nul $\lambda^{(2)}$ tels que $Q_5^{(2)} = \lambda^{(2)}\,{}^tG_2Q_5G_2$.

Étape 3 : on applique successivement les algorithmes 3.4.6 et 3.4.7 à $Q_5^{(2)}$ de manière à obtenir un déterminant impair. À l'issue de cette étape, on obtient une forme $Q_5^{(3)} \in \mathrm{Sym}^*(5,\mathbb{Z})$ équivalente à Q_5 ainsi qu'une matrice inversible G_3 et un rationnel non nul $\lambda^{(3)}$ tels que $Q_5^{(3)} = \lambda^{(3)}\,{}^tG_3Q_5^{(2)}G_3$ et le déterminant Δ_5 de $Q_5^{(3)}$ est impair.

Étape 4 : on applique l'algorithme 3.3.1 en choisissant le paramètre k selon les valeurs données dans le théorème 4.2.8 (par exemple $k = 10^6$ convient toujours) jusqu'à ce que le déterminant de la matrice renvoyée soit égal à $\pm 2p$ avec p premier impair. Le théorème 4.2.8 montre qu'un tel choix est toujours possible et le théorème 4.3.8 montre que le nombre moyen d'essais à effectuer est en $\mathcal{O}(\log \Delta_5)$. À l'issue de cette étape, on obtient une forme Q_6 dont la restriction au sous espace engendré par les 5 premiers vecteurs de la base est égale à $Q_5^{(3)}$, dont le déterminant est égal à $\pm 2p$ avec p premier impair et dont la signature (r, s) vérifie $r \geq 2$ et $s \geq 2$.
Remarque : Dans la pratique, le choix $k = 3$ convient pour les grandes valeurs de Δ_5.

Étape 5 : on utilise l'algorithme de Simon décrit dans [Sim05b], et on obtient un vecteur non nul T de $\mathbb{Z}^6$ vérifiant :

$$^tTQ_6T = 0$$

En divisant par le pgcd des coefficients, on se ramène au cas où T est primitif.

Étape 6 : l'étape 6 consiste à exhiber un plan hyperbolique qui contient T. Le résultat suivant de Serre [Ser95, p.55, Proposition 3.] nous assure l'existence d'un tel plan hyperbolique :

Proposition 3.5.2 (Serre)**.** *Soit x un élément isotrope non nul d'un module quadratique non dégénéré (V, Q). Il existe alors un sous–espace de U de V qui contient x et qui est un plan hyperbolique.*

Expliquons comment obtenir ce plan hyperbolique. On écrit la matrice de Q_6 dans une base commençant par le vecteur isotrope T précédemment obtenu. On utilise pour cela l'algorithme 2.3.1 et on note G_4 une matrice unimodulaire dont la première colonne est constituée des coordonnées du vecteur T. On définit $Q_6^{(1)}$ de la manière suivante :

$$Q_6^{(1)} = {}^tG_4Q_6G_4 = \begin{bmatrix} 0 & * & * & * & * & * \\ * & * & * & * & * & * \\ * & * & * & * & * & * \\ * & * & * & * & * & * \\ * & * & * & * & * & * \\ * & * & * & * & * & * \end{bmatrix}$$

où les $*$ représentent des entiers relatifs. Soit maintenant G_5 une matrice unimodulaire telle que $(Q_6^{(1)}[1,2], Q_6^{(1)}[1,3], Q_6^{(1)}[1,4], Q_6^{(1)}[1,5], Q_6^{(1)}[1,6])G_5 = (a, 0, 0, 0, 0)$ où a est le pgcd des coefficients $(Q_6^{(1)}[1,2], Q_6^{(1)}[1,3], Q_6^{(1)}[1,4], Q_6^{(1)}[1,5], Q_6^{(1)}[1,6])$. On a $a = 1$ puisque a divise la première ligne ainsi que la première colonne de $Q_6^{(1)}$, donc $a^2 \mid \det(Q_6^{(1)})$, or $\det(Q_6^{(1)}) = \pm 2p$ avec p premier, donc $a = 1$. Une matrice G_5 est donnée par la forme normale d'Hermite de :

$$(Q_6^{(1)}[1,2], Q_6^{(1)}[1,3], Q_6^{(1)}[1,4], Q_6^{(1)}[1,5], Q_6^{(1)}[1,6])$$

On peut poser $G_6 = \begin{bmatrix} 1 & 0 \\ 0 & G_5 \end{bmatrix}$. On a alors :

$$Q_6^{(2)} = {}^tG_6 Q_6^{(1)} G_6 = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & b_2 & b_3 & b_4 & b_5 & b_6 \\ 0 & b_3 & * & * & * & * \\ 0 & b_4 & * & * & * & * \\ 0 & b_5 & * & * & * & * \\ 0 & b_6 & * & * & * & * \end{bmatrix}$$

Soit alors G_7 la matrice suivante :

$$G_7 = \begin{bmatrix} 1 & \left[\frac{-b_2}{2}\right] & -b_3 & -b_4 & -b_5 & -b_6 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

On a $\det(G_7) = 1$, et

$$Q_6^{(3)} = {}^tG_7 Q_6^{(2)} G_7 = \left[\begin{array}{cc:cccc} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & \alpha & 0 & 0 & 0 & 0 \\ \hdashline 0 & 0 & \multicolumn{4}{c}{\multirow{4}{*}{Q_4}} \\ 0 & 0 & & & & \\ 0 & 0 & & & & \\ 0 & 0 & & & & \end{array}\right]$$

où $Q_4 \in \mathrm{Sym}(4, \mathbb{Z})$. On note aussi que :

$$\det Q_4 = -\det Q_6$$

Le α dans cette matrice vaut soit 0, soit 1 selon la parité du coefficient b_2 mais il n'interviendra pas dans la suite. On regroupe alors les changements de base effectués et on note $G_8 = G_4 \times G_6 \times G_7$. On a alors $Q_6^{(3)} = {}^tG_8 Q_6 G_8$. L'obtention des matrices $Q_6^{(3)}$ et G_8 terminent l'étape 6.

Étape 7 : Le travail va maintenant s'effectuer sur la forme Q_4. Celle–ci est de déterminant égal à $-\det(Q_6)$ donc toujours égal à $\pm 2p$ avec p premier. Montrons que l'équation ${}^tRQ_4R = 0$ admet une solution non triviale. On utilise le théorème de Hasse–Minkowski 2.2.1 ainsi que le résultat suivant :

Théorème 3.5.3. *Soit f une forme quadratique sur $\mathbb{Q}_p$ non dégénérée et de dimension 4. Pour que f représente 0 sur $\mathbb{Q}_p$, il faut et il suffit que son déterminant ne soit pas un carré p–adique où bien que son déterminant soit un carré p–adique et que son invariant ϵ soit égal au symbole de Legendre $(-1,-1)_p$.*

On sait que Q_4 est indéfinie. En effet, la matrice $Q_5^{(3)}$ a été complétée de sorte que sa signature, notée (r, s), vérifie $r \geq 2$ et $r \geq 2$. On a décomposé Q_6 en la somme (au sens des formes quadratiques) d'un plan hyperbolique avec une autre forme quadratique Q_4, or la signature d'une forme quadratique sur un plan hyperbolique est $(1, 1)$ et $Q_6^{(3)}$ a la même signature que Q_6 donc la signature de la forme Q_4 restante est :

$$sgn(Q_4) = (r - 1, s - 1)$$

D'après la relation énoncée précédemment, on a $r - 1 \geq 1$ et $s - 1 \geq 1$, donc Q_4 est bien encore indéfinie. Cela nous assure donc l'existence d'une solution sur $\mathbb{R}$.

Il nous faut maintenant nous assurer de l'existence d'une solution sur $\mathbb{Q}_\ell$ pour tout nombre premier ℓ. Soit ℓ un nombre premier impair ne divisant pas $\det Q_4$. Alors dans ce cas, d'après la proposition 2.2.3, on sait que des solutions existent. Il reste à considérer les cas où ℓ divise $\det Q_4$ et $\ell = 2$. $\det Q_4 = \pm 2p$ n'est pas un carré dans $\mathbb{Q}_2$ ni $\mathbb{Q}_p$ (les valuations sont impaires et $p \neq 2$). Donc il existe des solutions locales.

Ces remarques nous permettent d'être sûrs que l'équation ${}^tRQ_4R = 0$ admet bien une solution non triviale. Comme mentionné précédemment, le déterminant de cette forme est égal à $\pm 2p$ avec p premier. Donc il est possible d'utiliser une seconde fois l'algorithme de Simon pour résoudre cette équation. Soit donc R une telle solution. En divisant par le pgcd des coefficients, on se ramène au cas où R est primitif.

Étape 8 : On écrit ensuite la matrice de Q_4 dans une base unimodulaire dont le premier vecteur est R. Soit donc B_1 une matrice unimodulaire dont la première colonne est égale au vecteur R. On définit alors $Q_4^{(1)}$:

$$Q_4^{(1)} = {}^tB_1Q_4B_1 = \begin{bmatrix} 0 & * & * & * \\ * & * & * & * \\ * & * & * & * \\ * & * & * & * \end{bmatrix}$$

où les $*$ représentent des entiers relatifs. On effectue alors les mêmes opérations que celles de l'étape 6 sur cette matrice, on note alors B le changement de base tel que :

$$ {}^tBQ_4B = \left[\begin{array}{cc:cc} 0 & 1 & 0 & 0 \\ 1 & \beta & 0 & 0 \\ \hdashline 0 & 0 & \multicolumn{2}{c}{\multirow{2}{*}{Q_2}} \\ 0 & 0 & & \end{array}\right]$$

où $\beta = 0$ ou 1.

Étape 9 : Le travail ayant été effectué sur la matrice Q_4 extraite de $Q_6^{(3)}$, il nous faut replacer les changements de base effectués. On pose alors :

$$G_9 = \left[\begin{array}{cc:cccc} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ \hdashline 0 & 0 & \multicolumn{4}{c}{\multirow{4}{*}{B}} \\ 0 & 0 & & & & \\ 0 & 0 & & & & \\ 0 & 0 & & & & \end{array}\right]$$

et on pose également :

$$P = G_8 \times G_9$$

On a alors obtenu une matrice P telle que :

$${}^tPQ_6P = \left[\begin{array}{cc:cc:c} 0 & 1 & \multicolumn{2}{c:}{\multirow{2}{*}{0}} & \multirow{2}{*}{0} \\ 1 & \alpha & \multicolumn{2}{c:}{} & \\ \hdashline \multicolumn{2}{c:}{\multirow{2}{*}{0}} & 0 & 1 & \multirow{2}{*}{0} \\ \multicolumn{2}{c:}{} & 1 & \beta & \\ \hdashline 0 & 0 & \multicolumn{2}{c:}{0} & Q_2 \end{array}\right]$$

où $\alpha,\ \beta = 0$ ou 1.

Si on désigne par P_1 et P_3 la première et la troisième colonnes de la matrice P, on remarque que ce sont des vecteurs solutions de l'équation ${}^tXQ_6X = 0$ mais aussi que ce sont des vecteurs orthogonaux pour la forme quadratique Q_6. Donc toute combinaison linéaire de P_1 et P_3 est encore une solution. On note J une combinaison non triviale telle que la dernière coordonnée est nulle et U tel que :

$$J = \left[\begin{array}{c} U \\ \hdashline 0 \end{array}\right] \text{ où } U \in \mathbb{Z}^5$$

On sait donc que ${}^tJQ_6J = 0$, mais on regarde le détail des calculs :

$$\begin{aligned} {}^tJQ_6J &= \left[\begin{array}{c:c} {}^tU & 0 \end{array}\right] \left[\begin{array}{c:c} Q_5^{(3)} & X \\ \hdashline {}^t\bar{X} & z \end{array}\right] \left[\begin{array}{c} U \\ \hdashline 0 \end{array}\right] \\ &= {}^tUQ_5^{(3)}U \\ &= 0 \end{aligned}$$

Ainsi, U est une solution non triviale de l'équation ${}^tUQ_5^{(3)}U = 0$. En posant $S = G_2G_3U$, on obtient :

$${}^tSQ_5S = 0$$

Ce qui nous donne une solution de l'équation.

□

3.6 Dimension > 5

L'algorithme proposé est prévu pour résoudre des équations quadratiques de dimension 5. La question qui vient naturellement est la suivante : peut–on généraliser aux dimensions supérieures ? Plusieurs pistes sont possibles :

- Comme l'algorithme est prévu pour la dimension 5, une piste possible est de restreindre l'équation à une autre de dimension 5. Cela peut être fait en isolant un sous–espace de dimension 5 sur lequel la forme en question a la bonne signature. La question devient donc maintenant : comment isoler ce sous–espace de manière efficace ?
- La procédure de complétion utilisée est valable quelle que soit la dimension de la matrice. La formule de congruence reste valable également. Le seul soucis restant concerne les procédures de minimisation. Dans le présent ouvrage, ces procédures sont spécifiques à la dimension 5. Il faudrait donc chercher une manière de généraliser ces procédures de minimisations, peut–être en séparant les cas ou la dimension est paire ou impaire.

3.7 Exemples détaillés

Je donne ici des exemples illustrant les différents algorithmes précédemment énoncés. Il y aura tout d'abord un exemple donnant le fonctionnement détaillé des étapes de minimisation et de réduction de la partie paire du déterminant ; puis un autre donnant le fonctionnement de la partie complétion de la matrice et enfin un dernier expliquant la partie résolution de l'algorithme.

3.7.1 Minimisation et réduction de la partie paire

On souhaite trouver une solution à l'équation :

$$ {}^tXQX = 0 $$

Avec

$$ Q = \begin{bmatrix} 2460 & -2460 & 1740 & -840 & 1650 \\ -2460 & -1890 & -300 & -615 & 450 \\ 1740 & -300 & 2670 & 600 & 270 \\ -840 & -615 & 600 & 2370 & 3000 \\ 1650 & 450 & 270 & 3000 & 68 \end{bmatrix} $$

On a $\det Q = 178927612016805000$. On commence donc par calculer la forme normale de Smith de Q. Celle–ci, notée SNF_Q vaut :

$$ SNF_Q = \begin{bmatrix} 13253897186430 & 30 & 30 & 15 & 1 \end{bmatrix} $$

On remarque que le quatrième coefficient de SNF_Q vaut 15 et que le cinquième vaut 1, donc il s'agit du cas où $d_4 = 15$ et $d_5 = 1$. On effectue donc un changement de base de sorte que les quatre premières lignes ainsi que les quatre premières colonnes de la matrice de Q dans cette nouvelle base soient divisibles par 15. Ce changement

de base est donné par la matrice opérant sur les lignes dans le calcul de la forme normale de Smith de Q. On la note V. On a alors :

$$V = \begin{bmatrix} 2842265821 & 337544268 & -6272013568 & 1590397374 & -2850018524 \\ -2697265852 & -320324236 & 5952042872 & -1509262257 & 2704623046 \\ -2076372137 & -246587602 & 4581919861 & -1161839533 & 2082035751 \\ -1004692022 & -119316086 & 2217048788 & -562178084 & 1007432469 \\ 1451876055 & 172423155 & -3203847525 & 812401095 & -1455836263 \end{bmatrix}$$

En effectue alors ce changement de base, puis comme indiqué dans l'algorithme 3.4.2, on multiplie la dernière ligne ainsi que la dernière colonne par 15 et on divise la matrice entière par 15. La nouvelle matrice est alors celle obtenue de l'opération :

$$Q' = \frac{1}{15}\, {}^tVQV$$
$$\det Q' = \frac{1}{15^3} \det Q$$

Son déterminant vaut $\det Q = 53015588745720$, soit le déterminant de départ divisé par 15^3. On calcule alors une nouvelle fois la forme normale de Smith de cette matrice. On obtient :

$$SNF_{Q'} = \begin{bmatrix} 13253897186430 & 2 & 2 & 1 & 1 \end{bmatrix}$$

Cette fois–ci, on repère que $d_3 = 2$ et $d_4 = 1$. On utilise alors l'algorithme 3.4.3, ce qui se passe de la même manière que précédemment au détail près qu'il faut multiplier les deux dernières colonnes ainsi que les deux dernières lignes par 2 avant d'effectuer la division. La matrice de changement de base associée aux deux opérations précédentes est la suivante :

$$G = \begin{bmatrix} 15 & -4 & 0 & 0 & 0 \\ -111411593817900 & 29709758351456 & 0 & 226 & 0 \\ -787008905175 & 209869041380 & 1 & 0 & 0 \\ -7416253302150 & 1977667547240 & 0 & 0 & 2 \\ -132662196252330 & 35376585667305 & 0 & 240 & 0 \end{bmatrix}$$

Cette matrice est donc telle que l'on ait :

$$Q'' = \frac{1}{15 \cdot 2}\, {}^tGQG$$
$$\det Q'' = \frac{1}{15^3 \cdot 2} \det Q$$

Comme après chaque minimisation, on calcule la forme normale de Smith de Q''. On a :

$$SNF_{Q''} = \begin{bmatrix} 13253897186430 & 2 & 1 & 1 & 1 \end{bmatrix}$$

On note cette fois ci que $d_2 = 2$ et $d_3 = 1$. On utilise alors l'algorithme 3.4.4. Cet algorithme nous donne le changement de base correspondant à la minimisation

effectuée. La matrice globale des opérations de minimisation est la suivante :

$$G = \begin{bmatrix} 0 & 0 & 7 & 22 & 0 \\ 0 & 226 & -51992077114988 & -163403670932888 & 0 \\ 0 & 0 & -367270822414 & -1154279727590 & 2 \\ 2 & 0 & -3460918207670 & -10877171509820 & 0 \\ 0 & 240 & -61909024917720 & -194571221170050 & 0 \end{bmatrix}$$

Cette matrice est telle que l'on a :

$$Q''' = \frac{1}{15 \cdot 2 \cdot 2}\, {}^tGQG$$
$$\det Q''' = \frac{1}{15 \cdot 2 \cdot 2} \det Q$$

La forme normale de Smith de Q''' est :

$$SNF_{Q'''} = \begin{bmatrix} 13253897186430 & 1 & 1 & 1 & 1 \end{bmatrix}$$

Cette fois–ci, on a $d_1 \neq 1$ et $d_2 = 1$ donc l'étape de minimisation s'achève. Il faut ensuite effectuer une réduction pour enlever la partie paire du déterminant afin de s'assurer l'existence d'une solution lors du passage en dimension 4. Le déterminant de Q''' vaut 13253897186430 et sa valuation en 2 vaut 1. On applique donc l'algorithme 3.4.7. On récupère alors la matrice de changement de base G, regroupant toujours la totalité des opérations précédentes et qui vérifie :

$$Q'''' = \frac{1}{15 \cdot 2 \cdot 2}\, {}^tGQG$$
$$\det Q'''' = \frac{1}{15 \cdot 2 \cdot 2} \det Q$$
$$\det Q'''' \equiv 1 \pmod 2$$

Et comme annoncé dans l'algorithme 3.4.7, Q'''' appartient à l'ensemble $\mathrm{Sym}^*(5, \mathbb{Z})$ et son déterminant est impair. Comme on dispose de la matrice permettant de revenir à la forme quadratique de départ, il ne reste plus qu'à résoudre l'équation :

$${}^tXQ''''X = 0$$

3.7.2 Complétion

La matrice choisie ici remplit les conditions fixées pour permettre le bon fonctionnement de l'algorithme, à savoir que pour la forme quadratique Q_5 dont la matrice est donnée ci–dessous, elle est indéfinie, appartient à $\mathrm{Sym}^*(5, \mathbb{Z})$ et de déterminant impair. Nous avons :

$$Q_5 = \begin{bmatrix} 5 & -1 & 4 & 0 & 6 \\ -1 & 4 & -5 & 8 & 2 \\ 4 & -5 & 2 & 8 & 0 \\ 0 & 8 & 8 & 9 & -1 \\ 6 & 2 & 0 & -1 & 6 \end{bmatrix}$$

$$\det Q_5 = 30737$$

La première étape consiste à calculer la signature de la forme quadratique en question. On a :

$$sgn\,(Q) = (3,2)$$
$$\det Q > 0$$

Il s'agit du cas le plus favorable de l'algorithme 3.3.1. On complète alors la matrice. Dans le cadre cet exemple, le vecteur de complétion :

$$X = \begin{bmatrix} -4974 \\ -10916 \\ -7292 \\ -9909 \\ 6710 \end{bmatrix}$$

et le z pris égal à :

$$z = -22176388$$

donnent un déterminant pour la matrice complétée égal à :

$$\det Q_6 = -15874 = -1 \times 2 \times 7937$$

ce qui correspond bien à un déterminant de la forme $\pm 2p$ avec p premier.

3.7.3 Calcul d'une solution

Afin d'expliquer avec plus de clarté l'algorithme et de permettre au lecteur de faire les calculs lui–même, je détaille ici le fonctionnement de la partie calcul d'une solution avec une matrice dont les coefficients sont de plus petite taille que précédemment. La matrice choisie ici remplit les conditions fixées pour permettre le bon fonctionnement de l'algorithme, à savoir que la forme quadratique Q_5 dont la matrice est donnée ci–dessous est indéfinie, appartient à $\mathrm{Sym}^*(5,\mathbb{Z})$ et de déterminant impair. L'étape de complétion de cette matrice a donné le vecteur Y ainsi que la matrice Q_6 qui sont également donnés. Nous avons ainsi :

$$Q_5 = \begin{bmatrix} 5 & -1 & 4 & 0 & 6 \\ -1 & 4 & -5 & 8 & 2 \\ 4 & -5 & 2 & 8 & 0 \\ 0 & 8 & 8 & 9 & -1 \\ 6 & 2 & 0 & -1 & 6 \end{bmatrix}$$

$$\det Q_5 = 30737$$

$$X = \begin{bmatrix} -4974 \\ -10916 \\ -7292 \\ -9909 \\ 6710 \end{bmatrix}$$

$$z = -22176388$$

$$Q_6 = \begin{bmatrix} 5 & -1 & 4 & 0 & 6 & -4974 \\ -1 & 4 & -5 & 8 & 2 & -10916 \\ 4 & -5 & 2 & 8 & 0 & -7292 \\ 0 & 8 & 8 & 9 & -1 & -9909 \\ 6 & 2 & 0 & -1 & 6 & 6710 \\ -4974 & -10916 & -7292 & -9909 & 6710 & -22176388 \end{bmatrix}$$

$$\det Q_6 = -15874 = -1 \times 2 \times 7937$$

Connaissant alors la factorisation du déterminant de la matrice Q_6, on utilise l'algorithme de Simon afin d'obtenir une solution de l'équation ${}^tXQ_6X = 0$.

La solution donnée est la suivante :

$$S_1 = \begin{bmatrix} 6071 & 2194 & -1927 & -3005 & -5067 & -2 \end{bmatrix}$$

Il faut maintenant décomposer Q_6 en $H \oplus Q_4$ où H est un plan hyperbolique. Pour cela, on commence par considérer une matrice G unimodulaire dont la première colonne est exactement le vecteur S_1. Pour obtenir cette matrice, il suffit de considérer la forme normale d'Hermite de S_1. L'algorithme de Simon donnant un vecteur solution dont le pgcd des coefficients vaut 1, la forme normale d'Hermite de S_1 nous donne une matrice V unimodulaire telle que :

$$S_1 \times V = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Donc on a :

$$S_1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \end{bmatrix} \times V^{-1}$$

Ainsi, comme V est unimodulaire, V^{-1} l'est aussi, et l'égalité précédente nous assure que la dernière colonne de V^{-1} est exactement le vecteur S_1. Il suffit donc d'échanger la première et la dernière colonne de V^{-1} afin d'obtenir la matrice G cherchée. Dans notre cas, la matrice G cherchée est la suivante :

$$G = \begin{bmatrix} 6071 & 0 & 0 & 0 & 0 & -3035 \\ 2194 & 1 & 0 & 0 & 0 & 0 \\ -1927 & 0 & 1 & 0 & 0 & 0 \\ -3005 & 0 & 0 & 1 & 0 & 0 \\ -5067 & 0 & 0 & 0 & 1 & 0 \\ -2 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

On note alors Q'_6 la matrice de la forme Q_6 écrite dans la base donnée par G. Soit $Q'_6 = {}^tGQ_6G$. Soit maintenant G_2 une matrice unimodulaire telle que :

$$\begin{bmatrix} Q'_6[1,2] & Q'_6[1,3] & Q'_6[1,4] & Q'_6[1,5] & Q'_6[1,6] \end{bmatrix} \times G_2 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Cette matrice est donnée par la forme normale d'Hermite de

$$\begin{bmatrix} Q'_6[1,2] & Q'_6[1,3] & Q'_6[1,4] & Q'_6[1,5] & Q'_6[1,6] \end{bmatrix}$$

La matrice de Q_6 dans cette base est alors :

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -3 & 0 & 1 & 1 \\ 0 & 0 & 0 & 36 & -18 & 1 \\ 0 & 0 & 1 & -18 & 95 & 0 \\ 0 & 0 & 1 & 1 & 0 & -2 \end{bmatrix}$$

Et le changement de base correspondant est :

$$\begin{bmatrix} -6071 & 18213 & -6072 & -78923 & 118387 & -6071 \\ -2194 & 6581 & -2195 & -28517 & 42794 & -2196 \\ 1927 & -5781 & 1927 & 25052 & -37573 & 1926 \\ 3005 & -9015 & 3005 & 39065 & -58598 & 3005 \\ 5067 & -15200 & 5068 & 65869 & -98806 & 5067 \\ 2 & -6 & 2 & 26 & -39 & 2 \end{bmatrix}$$

Une fois ce changement effectué, on a décomposé notre forme Q_6 sous la forme $H \oplus Q_4$ où H est un plan hyperbolique et Q_4 une forme quadratique de dimension 4 :

$$\left[\begin{array}{cc:cccc} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ \hdashline 0 & 0 & -3 & 0 & 1 & 1 \\ 0 & 0 & 0 & 36 & -18 & 1 \\ 0 & 0 & 1 & -18 & 95 & 0 \\ 0 & 0 & 1 & 1 & 0 & -2 \end{array}\right]$$

et on a :

$$Q_4 = \begin{bmatrix} -3 & 0 & 1 & 1 \\ 0 & 36 & -18 & 1 \\ 1 & -18 & 95 & 0 \\ 1 & 1 & 0 & -2 \end{bmatrix}$$

Il faut alors effectuer le même genre d'opérations que précédemment sur la forme Q_4. Un vecteur isotrope pour Q_4 donné par l'algorithme de Simon est le suivant :

$$S_2 = \begin{bmatrix} -10 \\ -3 \\ -2 \\ 6 \end{bmatrix}$$

La matrice des changements à opérer sur Q_4 est la suivante :

$$\begin{bmatrix} -10 & 26 & 18509 & 149 \\ -3 & 8 & 5717 & 46 \\ -2 & 5 & 3729 & 30 \\ 6 & -15 & -11698 & -94 \end{bmatrix}$$

Une fois les transformations effectuées sur Q_4, la nouvelle matrice de Q_4 est la suivante :

$$\left[\begin{array}{cc:cc} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ \hdashline 0 & 0 & -15874 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right]$$

On observe bien la décomposition de Q_4 en $H \oplus Q_2$. La matrice de changement de base comprenant la totalité des opérations effectuées est alors :

$$\begin{bmatrix} -6071 & 18213 & 24289 & -106256 & -51105758 & -412902 \\ -2194 & 6581 & 8737 & -38296 & -18391310 & -148593 \\ 1927 & -5781 & -7724 & 33763 & 16249062 & 131281 \\ 3005 & -9015 & -12019 & 52585 & 25289718 & 204325 \\ 5067 & -15200 & -20273 & 88685 & 42655345 & 344628 \\ 2 & -6 & -8 & 35 & 16833 & 136 \end{bmatrix}$$

et la matrice de Q_6 dans cette base est :

$$\left[\begin{array}{cccc:cc} 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ \hdashline 0 & 0 & 0 & 0 & -15874 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right]$$

comme annoncé dans l'algorithme, on remarque que le premier et le troisième vecteur de cette base sont isotropes et orthogonaux pour Q_6. On les note E et F.

$$E = \begin{bmatrix} -6071 \\ -2194 \\ 1927 \\ 3005 \\ 5067 \\ 2 \end{bmatrix} \qquad F = \begin{bmatrix} 24289 \\ 8737 \\ -7724 \\ -12019 \\ -20273 \\ -8 \end{bmatrix}$$

On effectue alors une combinaison linéaire de ces deux vecteurs de sorte que la dernière coordonnée du résultat soit nulle. On la note alors $\widetilde{S}$.

$$\widetilde{S} = -8 \times E - 2 \times F = \begin{bmatrix} -10 \\ 78 \\ 32 \\ -2 \\ 10 \\ 0 \end{bmatrix}$$

On extrait alors les cinq premières coordonnées de ce vecteur qui forment une solu-

tion de l'équation de départ. On peut vérifier que :

$$\begin{bmatrix} -10 & 78 & 32 & -2 & 10 \end{bmatrix} \times \begin{bmatrix} 5 & -1 & 4 & 0 & 6 \\ -1 & 4 & -5 & 8 & 2 \\ 4 & -5 & 2 & 8 & 0 \\ 0 & 8 & 8 & 9 & -1 \\ 6 & 2 & 0 & -1 & 6 \end{bmatrix} \times \begin{bmatrix} -10 \\ 78 \\ 32 \\ -2 \\ 10 \end{bmatrix} = 0$$

Chapitre 4

Analyse

Dans ce chapitre, nous proposons une analyse de l'algorithme 3.0.1 décrit dans le chapitre 3. Afin d'effectuer une analyse rigoureuse, nous allons tout d'abord avoir besoin d'estimer le discriminant d'un corps de nombres engendré par des racines carrées. Pour ce calcul, nous commencerons par étudier un cas particulier puis nous verrons le cas général. Ensuite, afin de pouvoir estimer la réussite de la procédure de complétion, nous devrons estimer la quantité de nombre premiers congrus à un carré modulo un entier N ainsi que la répartition de ceux–ci. Enfin nous en viendrons à l'étude la complexité de l'algorithme en question. On s'intéressera d'abord aux étapes de minimisation et de complétion puis on donnera une méthode pour tester la friabilité d'un entier. Enfin, nous terminerons ce chapitre en donnant la complexité globale de cet algorithme ainsi que les résultats de quelques expériences.

4.1 Calcul du discriminant du corps

Soient $p_1, \ldots, p_t$ des nombres premiers impairs. On définit ℓ_i de la manière suivante :

$$\ell_i = \begin{cases} p_i & \text{si } p_i \equiv 1 \pmod 4 \\ -p_i & \text{si } p_i \equiv 3 \pmod 4 \end{cases}$$

de sorte que $\ell_i \equiv +1 \pmod 4$ $\forall i$.

On cherche à calculer le discriminant, ou du moins une majoration du discriminant du corps de nombres L donné par :

$$L = \mathbb{Q}\left(\sqrt{\ell_1}, \ldots, \sqrt{\ell_t}\right)$$

4.1.1 Cas général

On démontre le résultat général suivant :

Théorème 4.1.1. *Soient $p_1, \ldots, p_n \in \mathcal{P}$ des nombres premiers. On note L le corps de nombres $\mathbb{Q}\left(\sqrt{\ell_1}, \ldots, \sqrt{\ell_n}\right)$ et d_L son discriminant. Alors si $\forall i \in [\![1, n]\!]\, p_i \equiv 1 \pmod 4$, on a :*

$$d_L \leq \left(\prod_{i=1}^{n} p_i\right)^{2^{n-1}}.$$

Démonstration. On utilise les notations suivantes : $p_1, \ldots, p_t$ sont des nombres premiers impairs, ℓ_i est définit de la manière suivante :

$$\ell_i = \begin{cases} p_i & \text{si } p_i \equiv 1 \pmod 4 \\ -p_i & \text{si } p_i \equiv 3 \pmod 4 \end{cases}$$

de sorte que $\ell_i \equiv +1 \pmod 4$ $\forall i$ et L est le corps de nombres suivant :

$$L = \mathbb{Q}\left(\sqrt{\ell_1}, \ldots, \sqrt{\ell_t}\right)$$

Pour une extension du type $\mathbb{Q}\left(\sqrt{\ell}\right)$, il est connu [IR90, p.189] qu'une base de l'anneau des entiers d'une telle extension est donnée par :

$$\mathcal{B} = \left\{1, \sqrt{\ell}\right\} \text{ si } \ell \equiv 3 \pmod 4$$

$$\mathcal{B} = \left\{1, \frac{1+\sqrt{\ell}}{2}\right\} \text{ si } \ell \equiv 1 \pmod 4$$

Dans le premier cas, la matrice du groupe de Galois est la suivante :

$$\begin{bmatrix} 1 & \sqrt{\ell} \\ 1 & -\sqrt{\ell} \end{bmatrix}$$

et dans le second cas :

$$\begin{bmatrix} 1 & \frac{1+\sqrt{\ell}}{2} \\ 1 & -\frac{1+\sqrt{\ell}}{2} \end{bmatrix}$$

Comme les entiers ℓ_i ont étés choisis tous congrus à 1 modulo 4, nous sommes dans le second cas. Ainsi le discriminant du corps de nombres $\mathbb{Q}\left(\sqrt{\ell_i}\right)$ vaut $\left(\sqrt{\ell_i}\right)^2$ et on a $\left[\mathbb{Q}\left(\sqrt{\ell_i}\right) : \mathbb{Q}\right] = 2$. Le théorème se montre par récurrence sur le nombre de racines qui composent le corps L de l'énoncé. Si $n = 1$, nous venons de montrer que la formule est vraie. Supposons maintenant que la formule soit vraie pour ≥ 1 racines. On a alors :

$$d_L \leq \left(\prod_{i=1}^{n} p_i\right)^{2^{n-1}}$$

On pose $L' = \mathbb{Q}\left(\sqrt{\ell_1}, \ldots, \sqrt{\ell_n}\right)\left(\sqrt{\ell_{n+1}}\right)$ où $\ell_{n+1} = \pm p_{n+1}$ selon que p_{n+1} soit équivalent à 1 ou 3 modulo 4 où un nombre premier ne divisant pas $\prod_{i=1}^{n} \ell_i$ et $\ell_{n+1} \equiv 1 \pmod 4$. On a $[L : Q] = 2^{n-1}$, et $\left[\mathbb{Q}\left(\sqrt{\ell_{n+1}}\right) : \mathbb{Q}\right] = 2$. On utilise alors la proposition 17 de [Lan86, p68] : Les corps L et $\mathbb{Q}\left(\sqrt{\ell_{n+1}}\right)$ ont des discriminants premiers entre eux puisque $\ell_{n+1} \nmid \prod_{i=1}^{n} \ell_i$ et les ℓ_i sont tous congrus à 1 modulo 4. Ainsi, on a :

$$\begin{aligned} d_{L'} &= \left(\left(\prod_{i=1}^{n} \ell_i\right)^{2^{n-1}}\right)^2 \times (\ell_i)^2 \\ &= \left(\prod_{i=1}^{n+1} \ell_i\right)^{2^n} \end{aligned}$$

Et comme $\ell_{n+1} = \pm p_{n+1}$, on obtient la majoration annoncée.

□

4.2 Estimation de premiers congrus à un carré

4.2.1 Estimation asymptotique

Soit n un entier impair sans facteur carré. Soit δ un entier inversible modulo n. On cherche à estimer la quantité de nombres premiers p ne divisant pas n, plus petits que X tels que :

$$\exists x \in \mathbb{Z},\ p \equiv \delta x^2 \pmod n$$

C'est à dire que l'on cherche à connaitre :

$$\pi_\delta(n, X) = \sharp\left\{p \in \mathcal{P}; p \nmid n; p < X; \exists x,\ p \equiv \delta x^2 \pmod n\right\}$$

Le résultat utilisé est essentiellement le suivant :

Soient K est un corps de nombres algébriques sur $\mathbb{Q}$, L une extension normale de K de groupe de Galois $G = \mathcal{G}al(L/K)$, d_L désigne le discriminant de L, n_L est le degré de l'extension $[L/\mathbb{Q}]$. Si $\mathfrak{p}$ désigne un idéal premier de K non–ramifié dans L, on note avec le symbole d'Artin $\left[\frac{L/K}{\mathfrak{p}}\right]$ la classe de conjugaison des automorphismes de Frobenius correspondant aux idéaux premiers $p \mid \mathfrak{p}$. Pour chaque classe de conjugaison C de G, on définit :

$$\widetilde{\pi}_C(X, L/K) = \sharp\left\{\mathfrak{p}; \mathfrak{p} \text{ n'est pas ramifié dans } L, \left[\frac{L/K}{\mathfrak{p}}\right] = C, \mathcal{N}_{K/\mathbb{Q}}(\mathfrak{p}) \leq X\right\}$$

Le résultat est alors :

Théorème 4.2.1 (Théorème de Tchebotarev)**.** *Il existe une constante positive absolue calculable c_1 telle que, si GRH est vraie pour la fonction zeta de Dedekind de L, alors pour tout X strictement supérieur à 2, on a :*

$$\left|\widetilde{\pi}_C(X, L/K) - \frac{|C|}{|G|}\operatorname{Li}(X)\right| \leq c_1\left(\frac{|C|}{|G|}X^{\frac{1}{2}}\log\left(|d_L|\,X^{n_L}\right) + \log\left(|d_L|\right)\right)$$

Ce théorème est énoncé dans [LO77] et la formulation de l'hypothèse de Riemann généralisée pour la fonction zeta de Dedekind d'un corps de nombres est donnée dans le chapitre 2, section 2.4. La fonction Li est la fonction logarithme intégral donnée par l'expression :

$$\operatorname{Li}(x) = \int_2^x \frac{dt}{\log(t)}$$

Dans la suite, nous allons utiliser ce théorème afin d'estimer $\pi_\delta(n, X)$ et démontrer le résultat suivant :

Théorème 4.2.2. *Soit n un entier sans facteur carré et impair. Notons $\pi_\delta(X, n)$ le nombre de nombres premiers p plus petits que X pour lesquels il existe un entier relatif x tel que $p \equiv \delta x^2 \pmod{n}$. Si GRH est vraie pour la fonction zeta de Dedekind de L, alors :*

$$\left|\pi_\delta(X, n) - \frac{1}{2^{\omega(n)}}\operatorname{Li}(n)\right| \leq c_1\left(\frac{1}{2}\sqrt{X}\log(nX^2) + 2^{\omega(n)-1}\log(n)\right)$$

où c_1 est donnée par le théorème 4.2.1 et $\omega(n)$ désigne le nombre de facteurs premiers de n.

Démonstration. Notons $n = \prod_{i=1}^{t} p_i$ sa décomposition en produit de nombres premiers. On suppose également que :

$$\begin{array}{ll} \forall\ 1 \leq i \leq s & p_i \equiv 1 \pmod 4 \\ \forall\ s+1 \leq i \leq t & p_i \equiv 3 \pmod 4 \end{array}$$

Et on pose :

$$\ell_i = \pm p_i \equiv +1 \pmod 4$$

Montrons le lemme suivant :

Lemme 4.2.3.

$$p \equiv \delta x^2 \pmod{n} \Leftrightarrow \left(\frac{\delta}{p}\right) = \left(\frac{\ell_i}{p}\right) \textit{ pour } 1 \leq i \leq t$$

Démonstration. Avoir $p \equiv \delta x^2 \pmod{n}$ revient, à l'aide du lemme Chinois, à dire que :

$$\forall\ 1 \leq i \leq t,\ p \equiv \delta x^2 \pmod{\ell_i}$$

Comme δ est inversible modulo n, cette relation s'écrit avec le symbole de Legendre :

$$\forall\ 1 \leq i \leq t,\ \left(\frac{p\delta^{-1}}{p_i}\right) = +1$$

Ou bien encore :

$$\forall\ 1 \leq i \leq t,\ \left(\frac{p}{\ell_i}\right) = \left(\frac{\delta}{p_i}\right)$$

On remarque cependant que si $1 \leq i \leq s$, $\ell_i \equiv 1 \pmod 4$, on a alors :

$$\left(\frac{p}{\ell_i}\right) = (-1)^{\frac{(p-1)(\ell_i-1)}{4}} \left(\frac{\ell_i}{p}\right) = (-1)^{p-1} \left(\frac{\ell_i}{p}\right)$$

Mais n étant impair, on obtient alors :

$$\left(\frac{p}{\ell_i}\right) = \left(\frac{\ell_i}{p}\right)$$

De la même manière, si $s+1 \leq i \leq t$, $\ell_i \equiv 3 \pmod 4$, donc

$$\left(\frac{p}{\ell_i}\right) = (-1)^{\frac{(p-1)(\ell_i-1)}{4}} \left(\frac{\ell_i}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{\ell_i}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{\ell_i}{p}\right) = \left(\frac{-\ell_i}{p}\right)$$

Donc, dans ce cas :

$$\left(\frac{p}{\ell_i}\right) = \left(\frac{-\ell_i}{p}\right)$$

On a ainsi la relation annoncée. □

Dans notre cas, L va être le corps de nombres suivant :

$$L = \mathbb{Q}\left(\sqrt{\ell_1}, \ldots, \sqrt{\ell_s}, \sqrt{\ell_{s+1}}, \ldots, \sqrt{\ell_t}\right)$$

Notons d_L le discriminant de ce corps. Le théorème 4.1.1 nous donne l'égalité suivante :

$$|d_L| \leq \left(\left|\prod_{i=1}^{t} \ell_i\right|\right)^{2^{t-1}}$$

Soit $\mathfrak{p}$ un idéal premier de K. Dans notre cas, on a $K = \mathbb{Q}$, donc on le note désormais p au lieu de $\mathfrak{p}$. Donc on a en fait $p \in \mathcal{P}$ au sens propre du terme. Dire

que p n'est pas ramifié dans L signifie que $p \nmid d_L$, donc que p est différent de p_i pour tout i compris entre 1 et t.

D'après la nature de L, on voit que :

$$\mathcal{G}al\left(L/\mathbb{Q}\right) \simeq \prod_{i=1}^{t} \mathcal{G}al\left(\mathbb{Q}\left(\sqrt{\ell_i}\right)/\mathbb{Q}\right)$$

C'est–à–dire que l'on a une correspondance entre l'application qui à $\mathfrak{p}$ associe $\mathcal{F}rob_{\mathfrak{p}}$ et l'application qui à $\mathfrak{p}$ associe le t–uplet des $\mathcal{F}rob_{\mathfrak{p}}$ restreints au corps de nombres $\mathbb{Q}\left(\sqrt{\epsilon_i \ell_i}\right)$. Dans notre cas, ces restrictions sont exactement les applications qui à $p \in \mathcal{P}$ associent le symbole de Jacobi $\left(\frac{\ell_i}{p}\right)$ selon la valeur de i. Le symbole d'Artin du théorème 4.2.1 correspond alors au t–uplet de ces symboles de Jacobi (voir [Jan73, p99]).

Appliquons maintenant le théorème 4.2.1 à notre cas en réécrivant la signification de $\widetilde{\pi}$:

$$\begin{aligned} \pi_\delta\left(X,n\right) &= \sharp\left\{p \in \mathcal{P},\ p \nmid n,\ p \leq X,\ \forall 1 \leq i \leq t,\ \left(\tfrac{\delta}{p_i}\right) = \left(\tfrac{\ell_i}{p}\right)\right\} \\ &= \sharp\left\{p \in \mathcal{P},\ p \nmid n,\ p \leq X, \exists x,\ p = \delta x^2 \pmod{n}\right\} \\ &= \widetilde{\pi}_C\left(X, L/\mathbb{Q}\right) \end{aligned}$$

où $C = \left(\left(\frac{\delta}{p_1}\right), \left(\frac{\delta}{p_2}\right), \ldots, \left(\frac{\delta}{p_t}\right)\right)$.

La classe de conjugaison du théorème correspond exactement à un choix précis d'un t–uplet de symboles de Jacobi car en général $C(p) = \left(\left(\frac{\ell_1}{p}\right), \ldots, \left(\frac{\ell_t}{p}\right)\right)$, le degré de l'extension est 2^t et le cardinal du groupe de Galois de L est 2^t. En appliquant le théorème 4.2.1, il vient donc :

$$\begin{aligned} \left|\pi_\delta\left(X, d_L\right) - \tfrac{1}{2^t}\,\mathrm{Li}\left(X\right)\right| &\leq c_1\left(\tfrac{1}{2^t}\sqrt{X}\log\left(|d_L|\right) + \log(|d_L|)\right) \\ &\leq c_1\left(\tfrac{1}{2}\sqrt{X}\log\left(\textstyle\prod_{i=1}^{t}\ell_i\ X^2\right) + 2^{t-1}\log\left(\textstyle\prod_{i=1}^{t}\ell_i\right)\right) \end{aligned}$$

D'où :

$$\left|\pi_\delta\left(X,n\right) - \frac{1}{2^t}\,\mathrm{Li}(X)\right| \leq c_1\left(\frac{1}{2}\sqrt{X}\log\left(nX^2\right) + 2^{t-1}\log(n)\right) \tag{4.1}$$

Ici, t représente finalement le nombre de facteurs premiers de n on a donc $t = \omega(n)$. Ce qui nous donne le résultat annoncé. □

Corollaire 4.2.4. *Soit n un entier impair, sans facteur carré différent de 3, 15. Notons $\pi_\delta(n)$ le nombre de nombres premiers p plus petits que n pour lesquels il existe un entier relatif x tel que $p \equiv \delta x^2 \pmod{n}$. Alors, si GRH est vraie pour la fonction zeta de Dedekind de L, on a :*

$$\left|\pi_\delta(n) - \frac{1}{2^{\omega(n)}}\,\mathrm{Li}(n)\right| \leq 2c_1\sqrt{n}\log(n)$$

où c_1 est donnée par le théorème 4.2.1.

Démonstration. C'est un corollaire du théorème précédent, il s'agit dans l'asymptotique de prendre $X = n$. On a alors :

$$\left|\pi_\delta(n,n) - \frac{1}{2^{\omega(n)}}\operatorname{Li}(n)\right| \leq c_1\left(\frac{3}{2}\sqrt{n}\log(n) + 2^{\omega(n)-1}\log(n)\right)$$

On démontre le lemme suivant :

Lemme 4.2.5. *Soit n un entier strictement supérieur à 1, sans facteur carré différent de 3. Alors on a :*

$$2^{\omega(n)} \leq \sqrt{n}$$

Démonstration. On décompose n en produit de facteurs premiers :

$$n = \prod_{i=1}^{t} p_i^{\alpha_i},\ p_i \in \mathcal{P},\ \alpha_i \in \mathbb{N}$$

Si $3 \nmid n$, alors comme n est impair et sans facteur carré, on a $\alpha_i = 1$ et $p_i \geq 4$ pour tout i, donc :

$$n \geq 4^{\omega(n)}$$

donc, en passant à la racine, il vient :

$$\sqrt{n} \geq 2^{\omega(n)}$$

Si $3 \mid n$, alors comme $n \neq 3$, on a $p_i \geq 4$ pour tout i et comme $n \neq 15$, la puissance de 5, si $5 \mid n$, est supérieure ou égale à 2, donc $\sqrt{n} \geq 5$, donc le résultat est encore vrai. D'où le lemme. □

En utilisant ce lemme, on a alors :

$$\left|\pi_\delta(n,n) - \frac{1}{2^{\omega(n)}}\operatorname{Li}(n)\right| \leq c_1\left(\frac{3}{2}\sqrt{n}\log(n) + \frac{1}{2}\sqrt{n}\log(n)\right)$$

Ce qui nous donne :

$$\left|\pi_\delta(n,n) - \frac{1}{2^{\omega(n)}}\operatorname{Li}(n)\right| \leq 2c_1\sqrt{n}\log(n)$$

□

Dans l'article [Ser81], il est indiqué en remarque qu'il est possible de prendre $c_1 = 2$. Avec ce raffinement, le résultat devient alors :

Théorème 4.2.6. *Soit n un entier sans facteur carré différent de 3, 15. Notons $\pi_\delta(n)$ le nombre de nombres premiers p plus petits que n pour lesquels il existe un entier relatif x tel que $p \equiv \delta x^2 \pmod{n}$. Alors, si GRH est vraie pour la fonction zeta de Dedekind de L, on a :*

$$\left|\pi_\delta(n) - \frac{1}{2^{\omega(n)}}\operatorname{Li}(n)\right| \leq 4\sqrt{n}\log(n)$$

Remarque : On note que dans cet énoncé, l'estimation donnée ne dépend absolument pas de δ.
Remarque : En améliorant le lemme 4.2.5, on peut remplacer le 4 du théorème précédent par une constante inférieure, mais jamais inférieure à 3. Le théorème suivant nous sera utile pour l'analyse de l'algorithme. Il s'agit d'une autre version du résultat précédent.

Théorème 4.2.7. *Soit n un entier sans facteur carré. Notons $\pi_\delta(n)$ le nombre de nombres premiers p plus petits que n pour lesquels il existe un entier relatif x tel que $p \equiv \delta x^2 \pmod{n}$. Alors, si GRH est vraie pour la fonction zeta de Dedekind de L, on a :*

$$\left|\pi_\delta\left(\frac{n}{2}, n\right) - \frac{1}{2^{\omega(n)}}\operatorname{Li}\left(\frac{n}{2}\right)\right| \leq \frac{3}{\sqrt{2}}\log(n) + 2^{\omega(n)}\log(n)$$

Démonstration. Il s'agit d'un raffinement du théorème 4.2.2. Il faut également tenir compte de la remarque stipulant que la constante c_1 peut être prise égale à 2. □

4.2.2 Estimation numérique

Le théorème 4.2.7 donne un équivalent asymptotique pour la fonction $\pi_\delta\left(\frac{n}{2}, n\right)$. Cependant afin d'avoir une idée réelle de ce qu'il se passe dans le cas pratique, il est nécessaire d'avoir un raffinement des valeurs de cette fonction.

Théorème 4.2.8. *Soit n un entier impair, on définit la fonction suivante :*

$$\psi(n) = \frac{1}{2}\frac{1}{2^{\omega(n)}}\operatorname{Li}\left(\frac{n}{2}\right)$$

Alors on a :

- *Pour $k = 4 \times 10^4$: $\pi_\delta\left(\frac{n}{2}k, n\right) \geq \psi(n)\ \forall\ n \geq 10^{7,7}$*
- *Pour $k = 10^5$: $\pi_\delta\left(\frac{n}{2}k, n\right) \geq \psi(n)\ \forall\ 10^{7,7} > n \geq 10^{5,9}$*
- *Pour $k = 10^6$: $\pi_\delta\left(\frac{n}{2}k, n\right) \geq \psi(n)\ \forall\ 10^{5,9} > n \geq 10^{3,275}$*
- *Pour $k = 6$: $\pi_\delta\left(\frac{n}{2}k, n\right) \geq \psi(n)\ \forall\ 10^{3,275} > n \geq 3$*

Démonstration. L'estimation asymptotique nous donne l'inégalité suivante :

$$\left|\pi_\delta\left(\frac{n}{2}, n\right) - \frac{\operatorname{Li}\left(\frac{n}{2}\right)}{2^{\omega(n)}}\right| \leq \sqrt{\frac{n}{2}}\log\left(n\left(\frac{n}{2}\right)^2\right) + 2^{\omega(n)}\log(n) \tag{4.2}$$

On souhaite connaître la valeur numérique de n pour laquelle il existe une proportion non négligeable d'éléments dans l'ensemble de cardinal $\pi_\delta\left(\frac{n}{2}, n\right)$. On définit alors les fonctions suivantes :

$$f(x) = \frac{1}{2}\frac{1}{g(x)}\operatorname{Li}\left(\frac{x}{2}\right) - \sqrt{\frac{x}{2}}\log\left(\frac{x^3}{4}\right) - g(x)\log(x) \tag{4.3}$$

et $g(x)$ est une fonction telle que :

$$g(x) \geq 2^{\omega(x)}$$

La fonction f ainsi définie mesure la différence entre l'équivalent asymptotique et le terme reste. Afin de s'assurer de l'existence d'une proportion conséquente d'entiers appartenant à l'ensemble de cardinal $\pi_\delta\left(\frac{n}{2}, n\right)$, le terme équivalent de l'inégalité (4.2) est affecté d'un coefficient $\frac{1}{2}$.

On souhaite maintenant avoir une expression pour la fonction $g(x)$. On sait que l'entier n du théorème 4.2.2 est impair. On suppose donc que $n > 3$ et que $3 \mid n$. On écrit alors la décomposition en facteurs premiers de n :

$$n = \prod_{i=1}^{\omega(n)} p_i^{\alpha_i}$$

Comme $3 \mid n$, on peut alors minorer n de la façon suivante :

$$n \geq 3 \times 5^{\omega(n)-1}$$

Ce qui nous donne :

$$\begin{aligned} n &\geq \frac{3}{5} 5^{\omega(n)} \\ \log\left(\frac{5}{3}n\right) &\geq \omega(n)\log(5) \\ \frac{\log\left(\frac{5}{3}n\right)}{\log(5)} &\geq \omega(n) \\ \left(2^{\log\left(\frac{5}{3}n\right)}\right)^{\frac{1}{\log(5)}} &\geq 2^{\omega(n)} \\ \left(\frac{5}{3}n\right)^{\frac{\log(2)}{\log(5)}} &\geq 2^{\omega(n)} \end{aligned}$$

On pose ainsi :

$$g(x) = \left(\frac{5}{3}x\right)^{\frac{\log(2)}{\log(5)}}$$

On cherche alors une valeur de x pour laquelle on a $f(x) > 0$. À l'aide du logiciel de calcul GP, on obtient que $f(x) > 0$ pour $x \geq 10^{81}$. On élargit alors un peu la définition de la fonction f en introduisant un paramètre k. Par rapport à l'estimation donnée par le théorème 4.2.2, la paramètre k nous autorise à chercher des nombres premiers inférieurs ou égaux à $\frac{n}{2} \times k$ au lieu de $\frac{n}{2}$. On ne change donc pas fondamentalement la fonction π_δ, on s'autorise simplement à avoir de plus grands nombres premiers. L'inégalité (4.2) devient alors :

$$\left|\pi_\delta\left(\frac{n}{2}k, n\right) - \frac{\mathrm{Li}\left(\frac{n}{2}k\right)}{2^{\omega(n)}}\right| \leq \sqrt{k}\sqrt{\frac{n}{2}}\log\left(n\left(\frac{n}{2}\right)^2 k^2\right) + 2^{\omega(n)}\log(n) \tag{4.4}$$

La fonction f donnée par l'égalité (4.3) devient alors :

$$f(x) = \frac{1}{2}\frac{1}{g(x)}\,\mathrm{Li}\left(\frac{x}{2}k\right) - \sqrt{k}\sqrt{\frac{x}{2}}\log\left(\frac{x^3}{4}k^2\right) - g(x)\log(x) \tag{4.5}$$

En prenant $k = 4 \times 10^4$ et $g(x) = \left(\frac{5}{3}x\right)^{\frac{\log(2)}{\log(5)}}$, on obtient que $f(x) > 0$ pour $x \geq 10^{39}$. Il est désormais possible de raffiner cette valeur en effectuant le raisonnement suivant :

- on suppose que $n \leq 10^{39}$
- alors on sait que $\omega(n) \leq 25$
- on pose alors $g(x) = 2^{25}$
- on a alors $f(n) > 0$ pour $n \geq 10^{20}$ et $k = 4 \times 10^4$

En itérant ce processus plusieurs fois successives, on obtient une meilleure borne. Ces itérations sont résumées dans le tableau suivant :

itération	$n \leq .$	$\omega(n) \leq .$	$f(n) > 0$ pour $n \geq .$	$k = .$
1	–	$\left(\frac{5}{3}x\right)^{\frac{\log(2)}{\log(5)}}$	10^{39}	4×10^4
2	10^{39}	25	10^{20}	4×10^4
3	10^{20}	15	10^{13}	4×10^4
4	10^{13}	11	10^{10}	4×10^4
5	10^{10}	9	$10^{8,5}$	4×10^4
6	$10^{8,5}$	8	$10^{7,7}$	4×10^4
7	$10^{7,7}$	7	$10^{6,57}$	10^5
8	$10^{6,57}$	6	$10^{5,9}$	10^5
9	$10^{5,9}$	6	$10^{4,79}$	10^6
10	$10^{4,79}$	5	$10^{4,05}$	10^6
11	$10^{4,05}$	4	$10^{3,275}$	10^6

Remarque : Prendre $k = 1$ redonne la fonction f définie en (4.3). Cette même approche en gardant $k = 1$ nous aurait permis de descendre jusqu'à $n \leq 10^{15,887}$, ce qui est nettement trop pour pouvoir lancer un calcul exhaustif.

Sachant que $10^{3,275} < 1884$, il est maintenant envisageable de déterminer de façon exacte les valeurs de la fonction π_δ. On définit alors la fonction suivante :

$$\pi(X, n) = \min_{\substack{\delta \wedge n = 1 \\ 1 \leq \delta < n}} \left(\pi_\delta\left(X, n\right)\right) \tag{4.6}$$

Puis on calcule les valeurs exactes de $\pi\left(\frac{n}{2}k, n\right)$.

Comme le montrent les valeurs données dans l'annexe A.1, prendre $k = 1$ laisse encore quelques valeurs nulles. Pour s'assurer qu'aucune valeur ne soit nulle, il faut aller jusque $k = 3$. La section A.2 de l'annexe A donne un graphique des valeurs de la fonction $\pi(X, n)$ pour $X = 3n$, $3 \leq n \leq 10^{3,275}$, n entier impair ainsi que le

rapport entre la valeur exacte et l'asymptotique donnée. On pourra ainsi constater qu'en choisissant $k = 3$, on assure l'existence des entiers cherchés pour les petites valeurs de n. □

Remarque : Dans la pratique, on n'utilisera pas le facteur k décrit précédemment. Les expériences menées montrent qu'il y a toujours suffisamment de nombres premiers de la bonne forme. Pour ce qui est des matrices ayant un « petit » déterminant, comme le montrent les graphiques de la section 4.6.2, il est préférable de factoriser ce déterminant et d'utiliser directement l'algorithme de Simon.

4.3 Répartition des premiers

On se propose dans cette section d'étudier la répartition des valeurs prises par le déterminant de la matrice de la forme complétée. On commence par fixer quelques notations qui seront valables pour toute la section qui va suivre.

Soit Q_5 une matrice symétrique à coefficients entiers. On note Δ_5 son déterminant. On suppose que Δ_5 est impair, sans facteur carré et positif. On note Q_6 la matrice symétrique complétée, Δ_6 son déterminant. Soit $\delta \in \mathbb{Z}$ premier avec Δ_5 ; on note :

$$\begin{aligned}
\mathcal{P} &= \{p \in \mathbb{N}, p \text{ est un nombre premier}\} \\
\mathcal{C}_{\delta,2} &= \left\{ x \in \mathbb{N}; x \leq \frac{\Delta_5}{2}, \exists \alpha \in \mathbb{Z}\ x \equiv 2^{-1}\delta\alpha^2 \pmod{\Delta_5} \right\} \\
\mathcal{C'}_{\delta,2} &= \{x \in \mathcal{C}_\delta, x \wedge \Delta_5 = 1\}
\end{aligned}$$

Dans tout ce qui va suivre, choisir aléatoirement signifie choisir aléatoirement en suivant la loi uniforme.

Lemme 4.3.1. *Dans le calcul du déterminant de la forme complétée Q_6, choisir aléatoirement un vecteur $X \in [\![0, \Delta_5[\![^5$ revient à choisir aléatoirement un $y_1 \in [\![0, \Delta_5[\![$ tel qu'il existe un $\alpha \in \mathbb{Z}/\Delta_5\mathbb{Z}$ vérifiant $y_1 \equiv \delta\alpha^2 \pmod{\Delta_5}$, où δ est premier avec Δ_5 et fixé.*

Démonstration. La démonstration du théorème 3.2.1 nous donne directement ce résultat. Il s'agit maintenant de vérifier que le y_1 est aléatoire lui aussi. Toujours dans cette même démonstration, si on note V la matrice donnée par le calcul de la forme normale de Smith de Q_5 agissant sur les colonnes, on pose $Y = {}^tV^{-1}X$ où X est un vecteur aléatoirement choisi. Comme le déterminant de V vaut 1, on sait que le vecteur Y est encore aléatoire. Cela correspond à un simple changement de base. Maintenant, y_1 est la première coordonnée de ce vecteur, donc elle est elle aussi aléatoire. □

Lemme 4.3.2. *Soit m un entier aléatoirement choisi dans l'intervalle $[\![0, \Delta_5[\![$. Alors la probabilité que cet entier soit premier avec Δ_5 est :*

$$\frac{\varphi(\Delta_5)}{\Delta_5}$$

Démonstration. Il suffit de remarquer qu'il y a exactement $\varphi(\Delta_5)$ entiers plus petits que Δ_5 et premiers avec Δ_5. □

Lemme 4.3.3. *Considérons la fonction suivante :*

$$\varphi_2(n) = \sharp\left\{x \in \mathbb{N},\ 0 \leq x \leq \frac{n}{2},\ x \wedge n = 1\right\}$$

Alors pour tout $n > 2$, on a :

$$\varphi_2(n) = \frac{\varphi(n)}{2}$$

Démonstration. Soit $a \in \mathbb{N}$ vérifiant $a \wedge n = 1$ et $\frac{n}{2} \leq a < n$. Alors $-a + n$ vérifie $0 < -a + n \leq \frac{n}{2}$ et $(-a + n) \wedge n = 1$ puisque $a \wedge n = 1$. Donc pour chaque élément compris entre $\frac{n}{2}$ et n et premier avec n, on peut construire un élément premier à n et compris entre 0 et $\frac{n}{2}$, d'où le résultat annoncé. Le cas $n = 2$ est à part, car il s'agit du seul cas où $\frac{n}{2} \wedge n = 1$. □

Lemme 4.3.4. *On a :*

$$\sharp\left(\mathcal{P} \cap \mathcal{C'}_{\delta,2}\right) = \pi_{\frac{\delta}{2}}\left(\frac{\Delta_5}{2}, \Delta_5\right)$$

Démonstration. Il suffit de remarquer que l'intersection entre les deux ensembles concernés correspond exactement à la définition de la fonction $\pi_\delta(X, n)$ précédemment donnée. □

Lemme 4.3.5. *On a :*

$$\sharp\mathcal{C'}_{\delta,2} = \frac{\varphi(\Delta_5)}{2^{\omega(\Delta_5)+1}}$$

Démonstration. On sait d'après le lemme 4.3.3 que le nombre d'entiers plus petits que $\frac{\Delta_5}{2}$ et premiers avec lui est exactement $\frac{\varphi(\Delta_5)}{2}$.

On sait aussi qu'à chaque élément x de cet ensemble correspond un élément de la forme α^2. Mais chaque élément de la forme α^2 possède exactement $2^{\omega(\Delta_5)}$ racines carrées ; car cela correspond à un choix de racine carrée parmi 2 modulo chacun des facteurs premiers de Δ_5. Comme on souhaite dénombrer les éléments x, il ne faut en considérer qu'une seule. D'où le résultat. □

Lemme 4.3.6. *Soit α un entier aléatoirement choisi dans l'intervalle $[\![0, \Delta_5]\!]$. Alors la probabilité que l'élément $x \equiv 2^{-1}\delta\alpha^2 \pmod{\Delta_5}$ correspondant appartienne à l'ensemble $\mathcal{C'}_{\delta,2}$ est :*

$$P\left(x \in \mathcal{C'}_{\delta,2}\right) = \frac{\varphi(\Delta_5)}{2\Delta_5}$$

Démonstration. Comme α est choisi aléatoirement dans l'intervalle entier $[\![0, \Delta_5]\!]$ et que $x = 2^{-1}\delta\alpha^2 \pmod{\Delta)_5}$, on sait que x appartient à l'ensemble

$$\left\{x \in \mathbb{N},\ x \leq \Delta_5,\ \exists\alpha \in \mathbb{Z}\ x \equiv 2^{-1}\delta\alpha^2 \pmod{\Delta)_5}\right\}$$

L'élément x est alors inférieur ou égal à $\frac{\Delta_5}{2}$ avec probabilité $\frac{1}{2}$. C'est–à–dire que dans ces conditions, on a $x \in \mathcal{C}_{\delta,2}$ avec probabilité $\frac{1}{2}$.

Si $x \in \mathcal{C}_{\delta,2}$, dire que $x \in \mathcal{C'}_{\delta,2}$ signifie avoir $x \wedge \Delta_5 = 1$, ou encore que x est inversible modulo Δ_5. Or on a $x = 2^{-1}\delta\alpha^2 \pmod{\Delta}_5$ où $2 \wedge \Delta_5 = 1$, $\delta \wedge \Delta_5 = 1$. La condition est alors équivalente à avoir α inversible modulo Δ_5. Comme il y a $\varphi(\Delta_5)$ éléments inversibles modulo Δ_5, on en déduit que la probabilité que α soit inversible modulo Δ_5 est $\frac{\varphi(\Delta_5)}{\Delta_5}$. Ce qui nous donne le résultat annoncé. □

Lemme 4.3.7. *Soit $x \in \mathcal{C'}_{\delta,2}$. Alors la probabilité que x soit premier est :*

$$P\left(x \in \mathcal{P}\right) = \frac{2\,\mathrm{Li}(\frac{\Delta_5}{2})}{\varphi(\Delta_5)}$$

Démonstration. On a, grâce aux lemmes précédents et à l'estimation :

$$\pi_\delta\left(\frac{\Delta_5}{2}, \Delta_5\right) = \mathrm{Li}\left(\frac{\Delta_5}{2}\right)/2^{\omega(\Delta_5)} + o\left(\sqrt{\frac{\Delta_5}{2}}\log\left(\frac{\Delta_5^3}{4}\right) + 2^{\omega(\Delta_5)}\right)$$

que :

$$\begin{aligned} P\left(x \in \mathcal{P}\right) &= \frac{\sharp(\mathcal{P} \cap \mathcal{C'}_{\delta,2})}{\sharp(\mathcal{C'}_{\delta,2})} \\ &= \frac{\mathrm{Li}(\frac{\Delta_5}{2})/2^{\omega(\Delta_5)}}{\varphi(\Delta_5)/2^{\omega(\Delta_5)+1}} \\ &= \frac{2\,\mathrm{Li}(\frac{\Delta_5}{2})}{\varphi(\Delta_5)} \end{aligned}$$

□

Proposition 4.3.8. *Soit $X \in [\![0, \Delta_5[\![^5$ un vecteur aléatoirement choisi. Alors le déterminant de la forme complétée Q_6 est égal à $2 \times p$ avec p premier avec une probabilité de :*

$$P(\Delta_6 \in 2 \times \mathcal{P}) = \frac{\mathrm{Li}(\frac{\Delta_5}{2})}{\Delta_5} \sim \frac{1}{2\log\Delta_5}$$

Démonstration. En utilisant les lemmes précédents, on sait que choisir ce vecteur X de manière aléatoire revient à choisir également de manière aléatoire un élément $y_1 \in [\![0, \Delta_5]\!]$ tel qu'il existe un $\alpha \in \mathbb{Z}/\Delta_5\mathbb{Z}$ vérifiant $y_1 \equiv 2^{-1}\delta\alpha^2 \pmod{\Delta_5}$, où δ est premier avec Δ_5. Choisir ce y_1 revient à choisir l'élément α correspondant. On combine alors les deux lemmes précédents. On souhaite que x soit à la fois un élément de $\mathcal{C'}_{\delta,2}$ et un nombre premier. On effectue alors le produit des probabilités de ces deux évènements et on obtient le résultat annoncé. □

Remarque : Cette proposition nous permet d'avoir une estimation sur le nombre de tentatives de complétions à faire avant d'obtenir un vecteur donnant la « bonne » forme quadratique. L'équivalent naturel de $\mathrm{Li}(x)$ étant $\dfrac{x}{\log(x)}$, il nous faudra alors en moyenne $2\log(\Delta_5)$ essais. Cette estimation est notamment confirmée par des mesures dont les résultats sont visibles en section 4.6.3.

4.4 Complexité

On souhaite maintenant estimer la complexité de l'algorithme décrit dans le chapitre 3. Le cheminement de cette section va suivre celui de l'algorithme 3.0.1.

Définition 4.4.1. *Soient f et g deux fonctions. On dit que $g = \widetilde{\mathcal{O}}(f)$ si il existe un réel $\alpha \geq 0$ tel que*

$$g = \mathcal{O}\left(f \log(f)^{\alpha}\right)$$

Définition 4.4.2. *Pour une matrice M ou un vecteur V, on note :*

$$||M|| = \max_{i,j} \{|m_{i,j}|\}$$

$$||V|| = \max_{i} \{|v_i|\}$$

Dans les sections qui vont suivre, le terme *complexité* désigne le nombre moyen d'opérations binaires effectuées.

4.4.1 Minimisations

Nous allons commencer par donner la complexité de chacun des algorithmes de minimisation de la section 3.4 selon la dimension du noyau correspondant.

Lemme 4.4.3. *Soient Q_5 une matrice symétrique à coefficients entiers, de déterminant non nul Δ_5, LLL–réduite, de dimension 5 et $m \in \mathbb{Z}$ un entier divisant Δ_5. On suppose que $m \mid d_2(Q_5)$ et que $d_3(Q_5) = 1$. Alors la complexité de l'algorithme 3.4.4 pour minimiser Q_5 par rapport à m est :*

$$\widetilde{\mathcal{O}}\left(\log(|\Delta_5|)^6\right)$$

et Q_f, G vérifient :

$$\log(||Q_f||) \leq \widetilde{\mathcal{O}}\left(\log(|\Delta_5|)\right)$$

$$\log(||G||) \leq \widetilde{\mathcal{O}}\left(\log(|\Delta_5|)^6\right)$$

Démonstration. La preuve de ce lemme est une analyse de complexité des différents étapes de la preuve du théorème 3.4.5. Le calcul de la forme normale de Smith de Q_5 se fait en temps :

$$\widetilde{\mathcal{O}}\left(\log(||Q_5||)^2\right)$$

et la sortie est du même ordre de grandeur.

Une fois le changement de base effectué, on applique une orthogonalisation de Gram–Schmidt modulo m à la matrice 3×3 extraite en bas à droite. La taille des coefficients est de l'ordre de m et la dimension est 3. Cette partie requiert $\mathcal{O}(1)$ étapes, chacune de complexité de l'ordre de celle d'une multiplication d'entiers de la taille de m. Ce qui se fait en temps :

$$\widetilde{\mathcal{O}}\left(\log(m)\right)$$

La partie suivante consiste en la résolution d'une équation quadratique modulaire. Si l'entier m est une puissance d'un premier, la résolution se résume en le calcul d'une racine carré dans $\mathbb{Z}/m\mathbb{Z}$, ce qui se fait en temps $\widetilde{\mathcal{O}}(\log(m))$ en utilisant l'algorithme de Shanks (voir [Coh96]). Dans le cas où m n'est pas une puissance d'un premier, on utilise l'algorithme de Pollard et Schnorr [PS87] dont la complexité est

$$\widetilde{\mathcal{O}}\left(\log(m)^3\right)$$

Comme la dernière coordonnée du vecteur S vaut 1, l'algorithme 3.3.1 donne la matrice H en temps

$$\widetilde{\mathcal{O}}(1)$$

De plus, la taille de H est telle que

$$\log(||H||) \leq \widetilde{\mathcal{O}}\left(\log(m)^2\right)$$

Les étapes 12, 13 et 14 ne comportent pas d'opération couteuse, il s'agit de changements de bases dont la matrice est donnée par les calculs précédents. Il faut également effectuer des multiplications d'entiers de taille $\widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)^2\right)$, mais cette complexité reste inférieure aux termes déjà énoncés.

On applique l'algorithme LLL à la matrice Q' dont la taille est $\widetilde{\mathcal{O}}(\log(m)^2) = \widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)^2\right)$. Cela se fait en temps

$$\widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)^6\right)$$

en utilisant la version de Simon donnée dans [Sim05b].
Remarque : En utilisant la version de Nguyen et Stehlé donnée dans [NS09], on obtiendrai

$$\widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)^4\right)$$

La complexité de cet algorithme correspond à celle de la partie dominante, ce qui nous donne :

$$\widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)^6\right)$$

Enfin, la taille de la sortie est donnée par l'analyse de LLL (voir [Sim05b]). □

Lemme 4.4.4. *Soient Q_5 une matrice symétrique à coefficients entiers, de déterminant non nul Δ_5, LLL–réduite, de dimension 5 et $m \in \mathbb{Z}$ un entier divisant Δ_5. On suppose que $m \mid d_3(Q_5)$ et que $d_4(Q_5) = 1$. Alors la complexité de l'algorithme 3.4.3 pour minimiser Q_5 par rapport à m est :*

$$\widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)^6\right)$$

et Q_f, G vérifient :

$$\log(||Q_f||) \leq \widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)\right)$$

$$\log(||G||) \leq \widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)^6\right)$$

Démonstration. La base décrite dans cet algorithme est encore celle donnée par le calcul de la forme normale de Smith. Ce calcul se fait en temps :

$$\widetilde{\mathcal{O}}\left(\log\left(||Q_5||\right)^2\right)$$

et la sortie est du même ordre de grandeur. La suite de l'algorithme consiste en un changement de base dont la matrice est explicitement donnée. La complexité de ce changement est donc $\mathcal{O}\left(\log\left(|\Delta_5|\right)^2\right)$. Enfin, on applique l'algorithme LLL sur la matrice Q' qui est de taille $\widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)^2\right)$, ce qui se fait en temps :

$$\widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)^6\right)$$

Enfin, la taille de la sortie est donnée par l'analyse de LLL (voir [Sim05b]). □

Lemme 4.4.5. *Soient Q_5 une matrice symétrique à coefficients entiers, de déterminant non nul, LLL–réduite, de dimension 5 et $m \in \mathbb{Z}$ un entier divisant $\det(Q_5)$. On suppose que $m \mid d_4(Q_5)$ et $d_5(Q_5) = 1$. Alors la complexité de l'algorithme 3.4.2 pour minimiser Q_5 par rapport à m est :*

$$\widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)^6\right)$$

et Q_f, G vérifient :

$$\log\left(||Q_f||\right) \leq \widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)\right)$$

$$\log\left(||G||\right) \leq \widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)^6\right)$$

Démonstration. La preuve est la même que celle du lemme 4.4.4. □

Lemme 4.4.6. *Soient Q_5 une matrice symétrique à coefficients entiers, de déterminant non nul, LLL–réduite, de dimension 5 et $m \in \mathbb{Z}$ un entier divisant $\det(Q_5)$. On suppose que $m \mid d_5(Q_5)$. Alors la complexité de l'algorithme 3.4.1 pour minimiser Q_5 par rapport à m est :*

$$\widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)\right)$$

et $G = Id_5$.

Démonstration. Il s'agit simplement de diviser la matrice Q_5 par m. Cela se fait en temps :

$$\widetilde{\mathcal{O}}\left(\log(m)\right) = \widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)\right)$$

□

Proposition 4.4.7. *Soit Q_5 une matrice symétrique à coefficients entiers, de déterminant non nul, de dimension 5 sur $\mathbb{Z}$ de déterminant Δ_5. La complexité de l'algorithme 3.4.5 pour obtenir une forme quadratique équivalente à Q_5 et appartenant à $Sym^*(5,\mathbb{Z})$ est :*

$$\widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)^7\right)$$

et Q_f, G vérifient :

$$\log\left(||Q_f||\right) \leq \widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)\right)$$
$$\log\left(||G||\right) \leq \widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)^7\right)$$

Démonstration. La complexité d'une étape de minimisation est majorée par la complexité du cas le plus onéreux. Cela se fait donc en temps :

$$\widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)^6\right)$$

Le nombre d'étapes nécessaires à l'algorithme 3.4.5 pour obtenir une matrice vérifiant $d_2 = 1$ est majoré par le nombre de facteurs premiers de Δ_5, donc par

$$\widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)\right)$$

Pour obtenir le changement de base global, il faut effectuer le produit des changements de base donnés par les différents algorithmes. Cela prend un temps nettement inférieur à celui des minimisations. Le temps requis par l'algorithme est donc

$$\widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)^7\right)$$

Enfin, la taille de la sortie est donnée par l'analyse de LLL (voir [Sim05b]). □

4.4.2 Complétion

L'étape suivante dont on doit évaluer la complexité est l'étape de complétion de la matrice la forme quadratique Q_5.

Théorème 4.4.8. *Soit Q_5 une matrice symétrique, à coefficients entiers, de déterminant non nul Δ_5 et vérifiant $d_1(Q_5) = \Delta_5$ et $d_2(Q_5) = 1$. Alors, sous GRH, la complexité de l'algorithme 3.3.1 pour obtenir une forme de déterminant égal à $\pm 2p$ où $p \in \mathcal{P}$ est :*

$$\widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)^5\right)$$

et la sortie est en :

$$\widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)\right)$$

Démonstration. L'algorithme 3.3.1 nous donne la formule exacte du déterminant de la matrice complétée. En combinant ce résultat avec le théorème 3.2.1, on obtient que le déterminant de la matrice complétée est congru à un certain entier δ premier avec Δ_5 multiplié par un autre entier au carré :

$$\Delta_6 \equiv \delta\alpha^2 \pmod{\Delta_5}$$

Ce qui nous donne donc :

$${}^tX\,\mathrm{Co}(Q_5)X \equiv \delta\alpha^2 \pmod{\Delta_5}$$

Dans l'algorithme, on cherche de tels entiers qui sont égaux à $2p$ où $p \in \mathcal{P}$.

La question du nombre de vecteurs X à essayer avant d'obtenir un bon déterminant devient alors la suivante : quelle est la proportion de nombres premiers plus petits que $\frac{\Delta_5}{2}$ qui sont congrus à un entier multiplié par un carré donné dans $\mathbb{Z}/\Delta_5\mathbb{Z}$?

La réponse nous est donnée par le théorème 4.2.7 ainsi que les lemmes de la section 4.3. Il nous suffit de les appliquer à Δ_5. On obtient donc :

$$\left|\pi_\delta\left(\frac{\Delta_5}{2}, \Delta_5\right) - \frac{1}{2^{\omega(\Delta_5)}}\,\mathrm{Li}\left(\frac{\Delta_5}{2}\right)\right| \leq \frac{3}{\sqrt{2}}\log(\Delta_5) + 2^{\omega(\Delta_5)}\log(\Delta_5)$$

L'équivalent naturel de la fonction logarithme intégral est $\dfrac{x}{\log(x)}$. L'estimation obtenue est donc de l'ordre de :

$$\frac{\Delta_5}{2^{\omega(\Delta_5)+1}\log(\Delta_5)}$$

Cette estimation est une proportion, donc le nombre moyen correspond à l'inverse de cette quantité. De plus, on a :

$$2^{\omega(\Delta_5)+1} \leq |\Delta_5|$$

Ce qui nous donne un nombre moyen de :

$$\widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)\right)$$

étapes.

À chaque étape, il faut choisir un vecteur X dont les coordonnées sont de taille $\widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)\right)$. Cela se fait donc en temps :

$$\widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)\right)$$

Ensuite, il faut calculer le déterminant correspondant ce qui prends le même temps. Enfin il faut effectuer un test de primalité sur ce déterminant. On considère le test de primalité AKS. Celui–ci est décrit dans [CP05, p213] et sa complexité pour un entier n est en $\widetilde{\mathcal{O}}\left(\log(n)^{4+o(1)}\right)$ d'après [Ber03]. On peut également utiliser l'algorithme de Miller [Mil76] dont la validité dépend de GRH et dont la complexité est en $\widetilde{\mathcal{O}}\left(\log(n)^4\right)$. Chacun des entiers de la forme complétée Q_6 est majoré par $|\Delta_5|$, donc le déterminant de Q_6 est majoré par $|k\Delta_5|$. La complexité d'un test de primalité est donc dans le cas de cet algorithme en :

$$\widetilde{\mathcal{O}}\left(\log\left(|k\Delta_5|\right)^4\right)$$

L'ensemble des complexités étant majoré par la dernière énoncée, l'algorithme 3.3.1 requiert donc un temps :

$$\widetilde{\mathcal{O}}\left(\log\left(|k\Delta_5|\right)^5\right)$$

Comme il a été dit lors de la preuve de l'algorithme 3.0.1, $k = 10^6$ convient toujours. La complexité de cet algorithme devient alors :

$$\widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)^5\right)$$

Comme k est une constante fixée, la sortie est en :

$$\widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)\right)$$

□

Remarque : Dans le théorème précédent, le corps utilisé pour GRH est celui défini page 69, à savoir une extension multiquadratique.

Remarque : Dans la pratique, on ne cherche pas forcément à ce que le déterminant de la matrice complétée soit égal à $2p$ $p \in \mathcal{P}$, mais seulement qu'il soit facilement factorisable. Cela est dû au fait que l'algorithme de résolution des équations quadratiques de Simon requiert la factorisation du déterminant de la matrice. Dans cette optique, le nombre de vecteurs X éligibles est supérieur à l'estimation annoncée.

4.4.3 Fin de l'algorithme

Lemme 4.4.9. *La complexité des étapes 5 à 9 de l'algorithme 3.0.1 est de l'ordre de :*

$$\widetilde{\mathcal{O}}\left(P\left(\log\left(|\Delta_5|\right)\right)\right)$$

et la sortie est de l'ordre de :

$$\widetilde{\mathcal{O}}\left(P\left(\log\left(|\Delta_5|\right)\right)\right)$$

où P est un polynôme non explicite donné par la complexité de l'algorithme de Simon en dimensions 6 et 4.

Démonstration. La fin de l'algorithme consiste en la partie où l'on utilise l'algorithme de Simon en dimensions 6 puis 4 et où après chaque utilisation de cet algorithme, on effectue un changement de base par algèbre linéaire afin d'obtenir une base constituée de deux plans hyperboliques orthogonaux et d'un troisième plan. Le détail de ces étapes est donné dans la démonstration du théorème 3.5.1.

Étape 5 : il s'agit d'utiliser l'algorithme de Simon [Sim05b] afin de trouver un vecteur isotrope pour la forme complétée Q_6. Nous allons procéder à une analyse simple de l'algorithme de Simon. Dans cet algorithme, on commence par effectuer des étapes de minimisation modulo chacun des facteurs premiers du déterminant de la forme Q_6. Ces étapes de minimisation sont du même type que celles effectuées dans l'algorithme 3.4.5. Cependant, comme on a $\det\left(Q_6\right) = \pm 2p$, le nombre d'étapes de minimisation à effectuer est au plus égal à 2 puisque le déterminant n'a que 2 facteurs premiers. Ces étapes prennent donc un temps polynomial en $\log\left(|\Delta_5|\right)$. Ensuite, une étape clef de l'algorithme est le calcul de la 2–partie du groupe de classe $\mathcal{C}l_2\left(-8\,|\Delta_6|\right)$. Cela est fait en utilisant l'algorithme de Bosma et Stevenhagen [BS96] ou celui de Shanks [Sha71]. En étudiant [Lag80], la complexité de ces algorithmes est

$$\widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)^5\right)$$

On note que comme on a $|\det\left(Q_6\right)| \leq |k\Delta_5|$ et que k est fixé, on a $\log\left(|\Delta_6|\right) = \mathcal{O}\left(\log\left(|\Delta_5|\right)\right)$.

La fin de cet algorithme nécessite l'utilisation de l'algorithme LLL pour réduire une forme quadratique, cela se fait en temps :

$$\widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)^6\right)$$

La complexité de cette étape est alors :

$$\widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)^6\right)$$

et la sortie est en

$$\widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)^6\right)$$

Les étapes restantes consistent en de l'algèbre linèaire, des minimisations ainsi que des applications de l'algorithme LLL ce qui reste polynomial en $\log\left(|\Delta_5|\right)$, voir la section 4.4.1.

□

4.4.4 Complexité globale

Théorème 4.4.10. *Sous GRH, la complexité de l'algorithme 3.0.1 afin d'obtenir une solution à l'équation* ${}^tXQ_5X = 0$ *est :*

$$\widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)^7 + P\left(\log\left(|\Delta_5|\right)\right)\right)$$

où P est un polynôme non explicite donné par la complexité de l'algorithme de Simon en dimensions 6 *et* 4.

Démonstration. On reprend les complexités annoncées dans les sections précédentes. Il nous suffit de les additionner pour obtenir le nombre d'étapes global de l'algorithme au complet.
La proposition 4.4.7 nous donne la complexité de la partie minimisation de l'algorithme :

$$\widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)^7\right)$$

et les matrices renvoyées Q_f, G vérifient :

$$\log\left(||Q_f||\right) \leq \widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)\right)$$

$$\log\left(||G||\right) \leq \widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)^7\right)$$

Le théorème 4.4.8 nous donne celle de la partie complétion :

$$\widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)^5\right)$$

Enfin, le lemme 4.4.9 nous donne celle de la fin de l'algorithme :

$$\widetilde{\mathcal{O}}\left(P\left(\log\left(|\Delta_5|\right)\right)\right)$$

et la sortie est de l'ordre de :

$$\widetilde{\mathcal{O}}\left(P\left(\log\left(|\Delta_5|\right)\right)\right)$$

où P est un polynôme non explicite donné par la complexité de l'algorithme de Simon en dimensions 6 et 4. En effectuant cette somme, on obtient un nombre d'étapes égal à :

$$\widetilde{\mathcal{O}}\left(\log\left(|\Delta_5|\right)^7 + P\left(\log\left(|\Delta_5|\right)\right)\right)$$

□

Remarque : Le corps utilisé pour GRH est celui défini page 69, à savoir une extension multiquadratique.

4.5 Optimisations possibles

Cette section regroupe des perspectives possibles afin d'optimiser l'algorithme proposé dans cette thèse.

Algorithme de Pollard–Schnorr

L'algorithme de Pollard–Schnorr est largement utilisé dans le cas de la minimisation de la forme quadratique lorsque le coefficient d_2 de sa forme normale de Smith est différent de 1 et que le d_3 vaut 1. Il est vraisemblablement possible d'améliorer la complexité de cet algorithme en utilisant l'algorithme LLL afin de réduire la forme quadratique utilisée pour résoudre l'équation.

Déterminant de la forme complétée

Dans l'algorithme décrit dans le présent document, on cherche à compléter la forme d'origine en une de dimension 1 de plus telle que son déterminant soit égal à 2 fois un nombre premier. Cette condition est imposée par le fait que dans la suite, on se restreint à une autre forme de même déterminant au signe près et de dimension 4. La condition d'existence d'une solution en dimension 4 impose que le déterminant de cette forme soit égal à une puissance impaire de 2 fois un nombre premier. Dans cette thèse, nous nous sommes limités à prendre $2 \times p$ car cela simplifie énormément la partie analyse. Cependant, en prenant une puissance impaire de 2 fois un nombre premier, les chances d'obtenir un « bon » déterminant sont plus grandes ce qui améliore la complexité de l'algorithme. Le graphique de la page 92 montre que dans ce cas le nombre moyen de tentatives de complétion est inférieur à celui du cas où l'on choisit un déterminant égal à $2 \times p$.

Forme normale de Smith

L'algorithme de minimisation 3.4.5 nécessite le calcul de la forme normale de Smith de la forme après chaque minimisation. On utilise la forme normale de Smith afin d'obtenir les diviseurs élémentaires de la matrice en question pour pouvoir minimiser par la suite. Un optimisation possible serait de trouver un moyen d'obtenir ces diviseurs sans avoir à calculer à chaque étape la forme normale de Smith de la matrice. Cela permettrait une grande amélioration de la complexité de l'étape de minimisation de l'algorithme.

Test de pseudo–primalité

Lors de l'étape de complétion, on cherche à obtenir un déterminant égal à $2 \times p$ où $p \in \mathcal{P}$. Cependant, pour chaque vecteur que l'on essaie, il faut effectuer un test de primalité du déterminant. Une optimisation possible est de remplacer ce test par un test de pseudo–primalité. Cela permet de gagner un temps considérable lors de cette étape. D'un point de vue de l'algorithme, on considère par la suite que cet entier est premier ; cela ne nuit pas vraiment à la bonne marche de l'algorithme, car

la probabilité de tomber sur un diviseur d'un entier pseudo–premier est très faible lorsque l'entier en question est suffisamment grand.

L^2 pour les formes indéfinies

Dans l'algorithme, il est régulièrement fait appel à l'algorithme LLL pour réduire la forme. Une amélioration possible est d'utiliser la version L^2 proposée par Stehlé et Nguyen dans [NS09] en l'adaptant au cas indéféni plutôt que de prendre la version de Simon dans [Sim05b].

4.6 Les expériences

L'ensemble des calculs suivants a été effectué en gp. L'ordinateur utilisé est un core 2 duo cadencé à 2.66GHZ équipé de 4Go de mémoire vive.

4.6.1 Tirage d'une forme quadratique

Afin d'évaluer les performances de l'algorithme, il faut définir une manière de choisir une forme quadratique aléatoirement. Deux méthodes similaires sont utilisées ici. La première est basique et donne des formes quadratiques n'ayant que très rarement un noyau de dimension supérieure à 1. La seconde est similaire à la première mais permet dans la plupart des cas d'obtenir une forme quadratique avec un noyau de dimension 2 ou plus modulo l'un des facteurs premiers du discriminant. L'algorithme correspondant à la première méthode est le suivant :

Algorithme 4.6.1: Forme Aléatoire 1

Données : un intervalle I ; un entier n
Résultat : une matrice symétrique aléatoire Q de taille $n \times n$

```
1 début
2     pour i de 1 à n faire
3         pour j de 1 à i faire
4             Q_{i,j} = Q_{j,i} := a où a est un entier pris aléatoirement dans I
5         fin pour
6     fin pour
7     retourner Q = (Q + {}^tQ)\2 où \ désigne la division entière
8 fin
```

L'algorithme suivant correspond à la seconde méthode précédemment décrite :

Algorithme 4.6.2: Forme Aléatoire 2

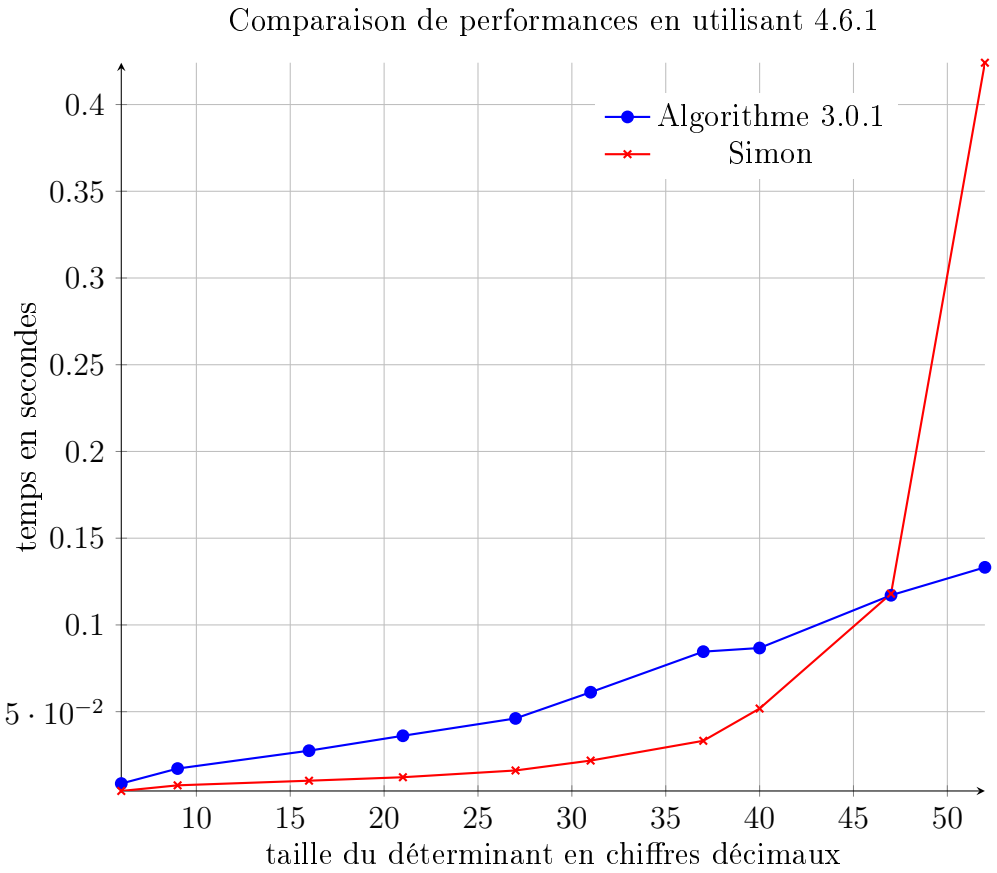
Données : un intervalle I ; un entier n
Résultat : une matrice symétrique aléatoire Q de taille $n \times n$

début
  Choisir un entier k compris entre 1 et n
  Choisir un entier m aléatoirement dans I
  pour i *de* 1 *à* n **faire**
    pour j *de* 1 *à* i **faire**
      $Q_{i,j} = Q_{j,i} := a$ où a est un entier pris aléatoirement dans I
    fin pour
  fin pour
  pour i *de* 1 *à* k **faire**
    Multiplier la ligne i de Q par m
    Multiplier la colonne i de Q par m
  fin pour
  $Q := (Q + {}^tQ)\backslash 2$ où $\backslash$ désigne la division entière
  pour i *de* 1 *à* k **faire**
    pour j *de* 1 *à* k **faire**
      $Q_{i,j} := Q_{i,j}\backslash m$ où $\backslash$ désigne la division entière
      $Q_{i,j} := Q_{i,j}\backslash 2$ où $\backslash$ désigne la division entière
    fin pour
  fin pour
  retourner Q
fin

Cette procédure permet, dans la plupart des cas de produire une matrice symétrique de déterminant non nul dont le facteur d_2 est différent de 1.

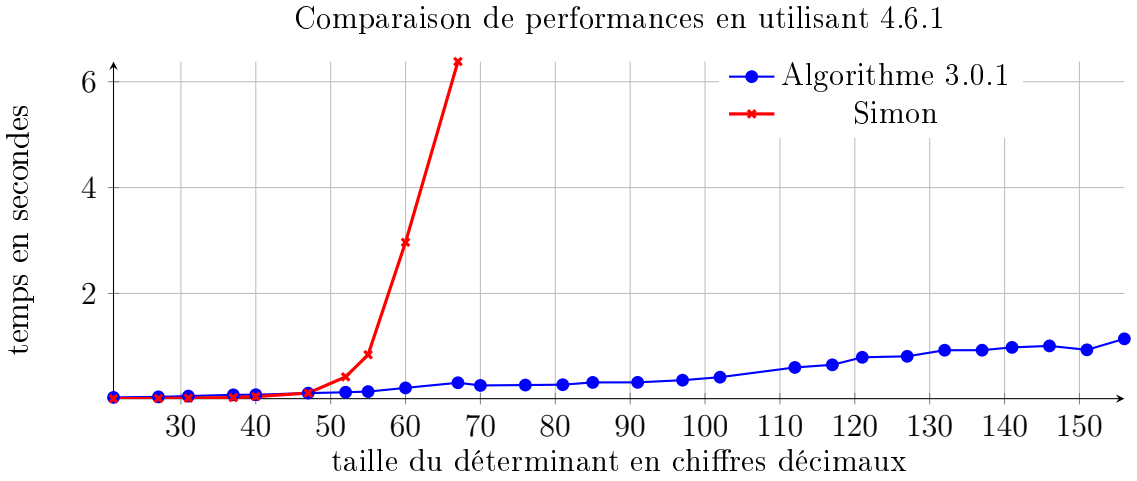
4.6.2 Performances de l'algorithme

Le graphique suivant donne la comparaison entre l'algorithme proposé dans cette thèse et celui de Simon. Les mesures sont faites en tirant aléatoirement des matrices de formes quadratiques et en faisant varier la taille des coefficients à l'aide de l'algorithme 4.6.1. Les sept premières mesures correspondent à la moyenne sur 1000 itérations, les restantes sur 100. Les mêmes matrices sont utilisées pour chacun des deux algorithmes.



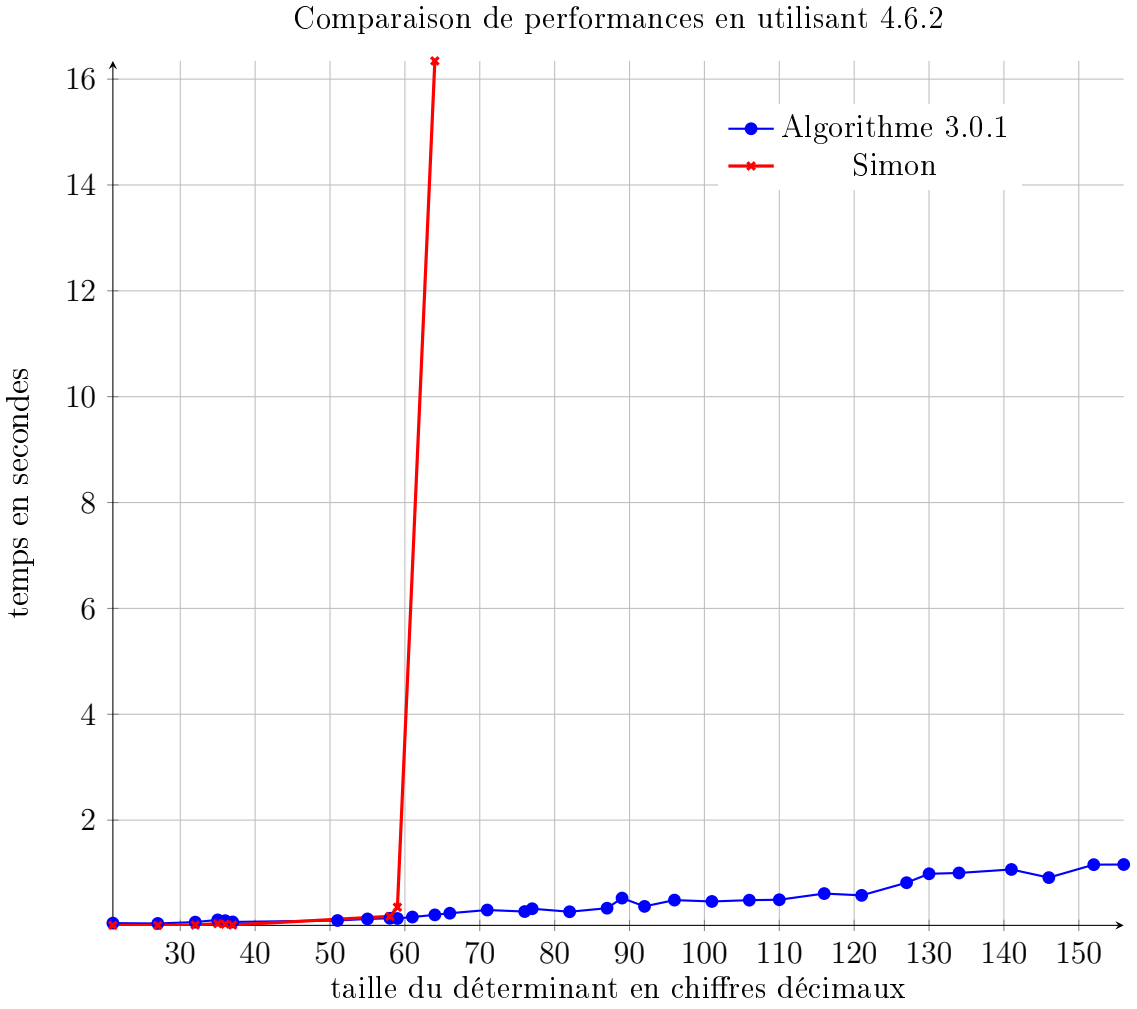
On remarque que l'algorithme de Simon reste plus performant pour des petites valeurs du discriminant. En effet, factoriser un petit discriminant n'est pas couteux. Cependant, lorsque l'arrive vers des discriminants ayant 45 chiffres décimaux, la complexité augmente de manière exponentielle.

Le même graphique, mais avec plus de mesures. Les sept premières sont faites sur 1000 itérations, les autres seulement sur 100.



Ce graphique fait apparaître de manière très nette l'utilisation de la factorisation dans l'algorithme de Simon. Les performances de l'algorithme proposé dans cette thèse sont nettement supérieures à celles de celui de Simon à partir du moment où le déterminant de la forme quadratique considérée n'est plus factorisable facilement.

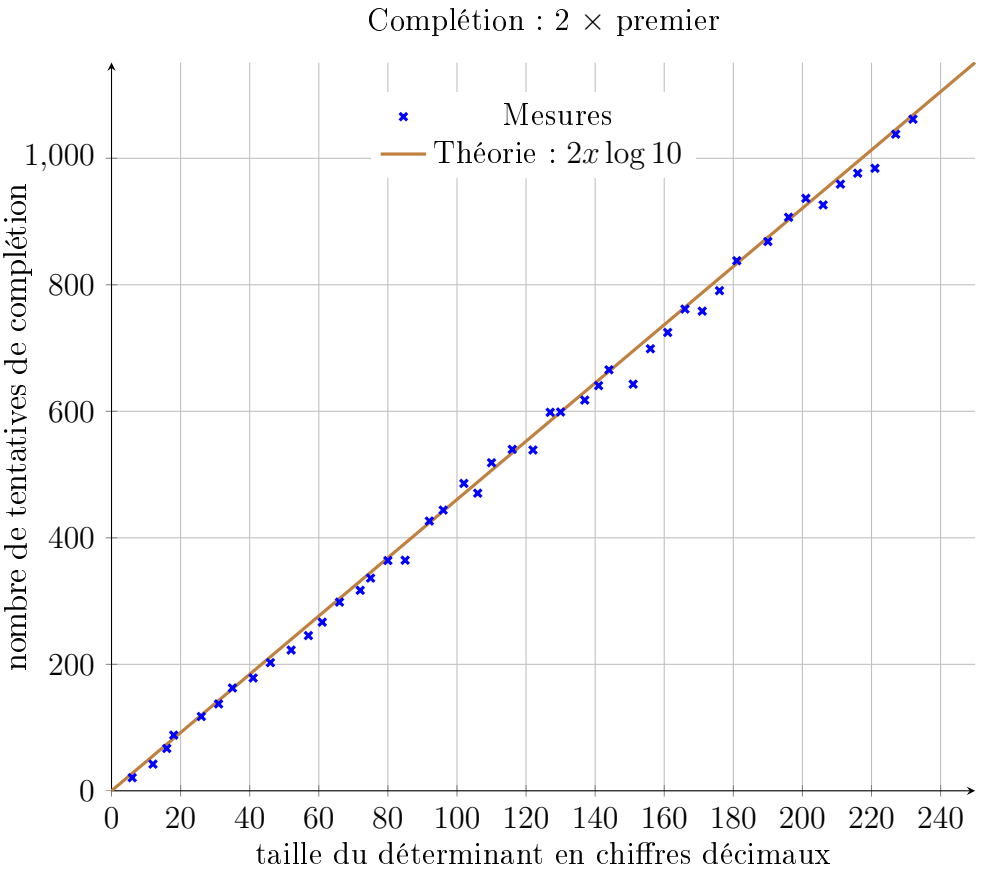
Sur ce graphique, les formes sont choisies en utilisant l'algorithme 4.6.2. Chaque mesure correspond à une moyenne effectuée sur 100 formes quadratiques dont la taille des coefficients est la même.



Ce graphique montre que même si les formes quadratiques utilisées ont un noyau, l'algorithme reste nettement plus performant. L'utilisation de l'algorithme de Pollard et Schnorr ne joue pas un rôle fondamental dans la complexité de la méthode proposée. Une autre valeur a été obtenue pour l'algorithme de Simon, mais celle–ci ne figure pas sur ce graphique. Il s'agit de la moyenne pour 100 valeurs avec un déterminant de taille 89 chiffres décimaux : le temps moyen mis est de l'ordre de 235 secondes soit environ 4 minutes. La même mesure pour l'algorithme 3.0.1 donne un temps moyen de 0.537 secondes. Ce qui confirme très nettement les performances de l'algorithme proposé dans cette thèse.

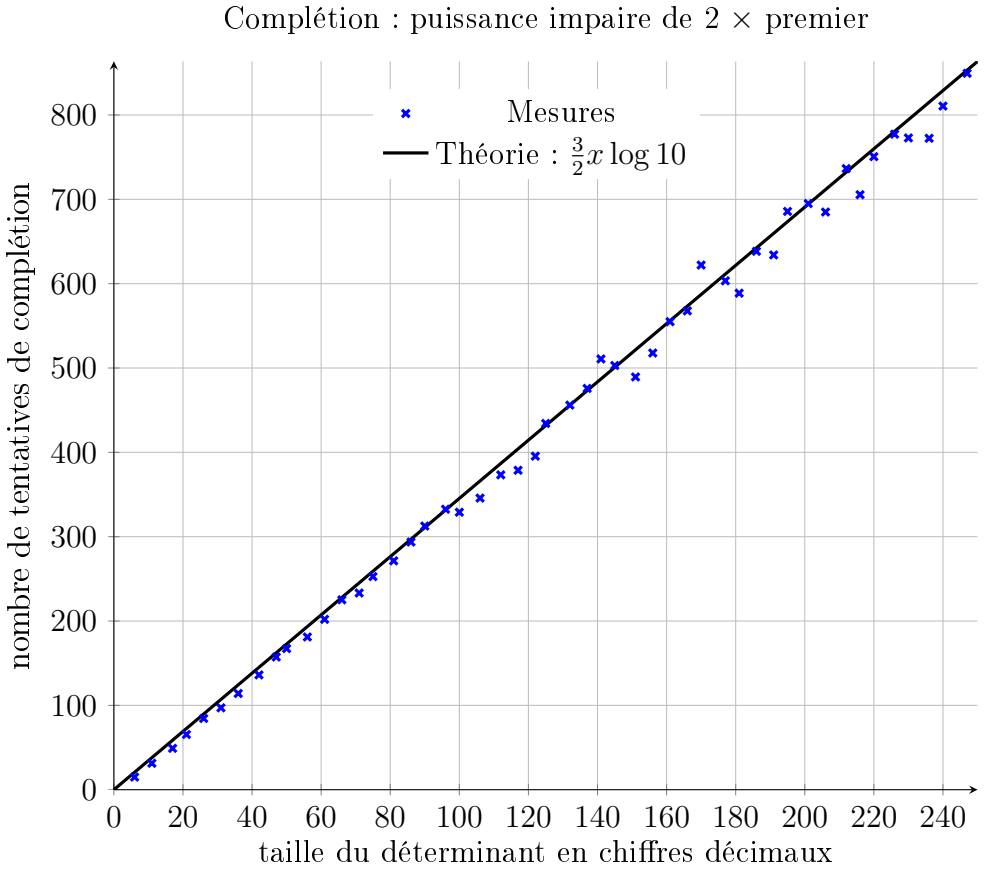
4.6.3 Procédure de complétion

Le graphique suivant donne un aperçu du nombre moyen de tentatives de complétion afin d'obtenir une forme quadratique de dimension 6 dont le déterminant est égal à 2 fois un nombre premier. Chaque valeur correspond à une moyenne effectuée sur 1000 matrices.



On note que conformément au résultat 4.3.8 le nombre moyen d'essais à effectuer suit le logarithme du déterminant.

Ce graphique ci donne le nombre moyen de tentatives de complétion afin d'obtenir une forme quadratique dont le déterminant est égal à une puissance impaire de 2 multipliée par un nombre premier. Chaque valeur est une moyenne effectuée sur 1000 mesures.



Cette mesure est utile dans le sens où, pour s'assurer de l'existence d'une solution lors de la dimension 4, la condition à remplir n'est pas que le déterminant soit 2 fois un nombre premier mais une puissance impaire de 2 fois un nombre premier. Comme on pouvait l'attendre, il faut moins de tentatives de complétion lorsque l'on élargit cette condition de la sorte. La courbe théorique tracée ici n'a pas été rigoureusement prouvée dans cette thèse. Mais une démonstration prouverai sans doute ce résultat, il s'agit d'effectuer la somme sur les puissances impaires de $\frac{1}{2}$ d'où le facteur $\frac{3}{2}$.

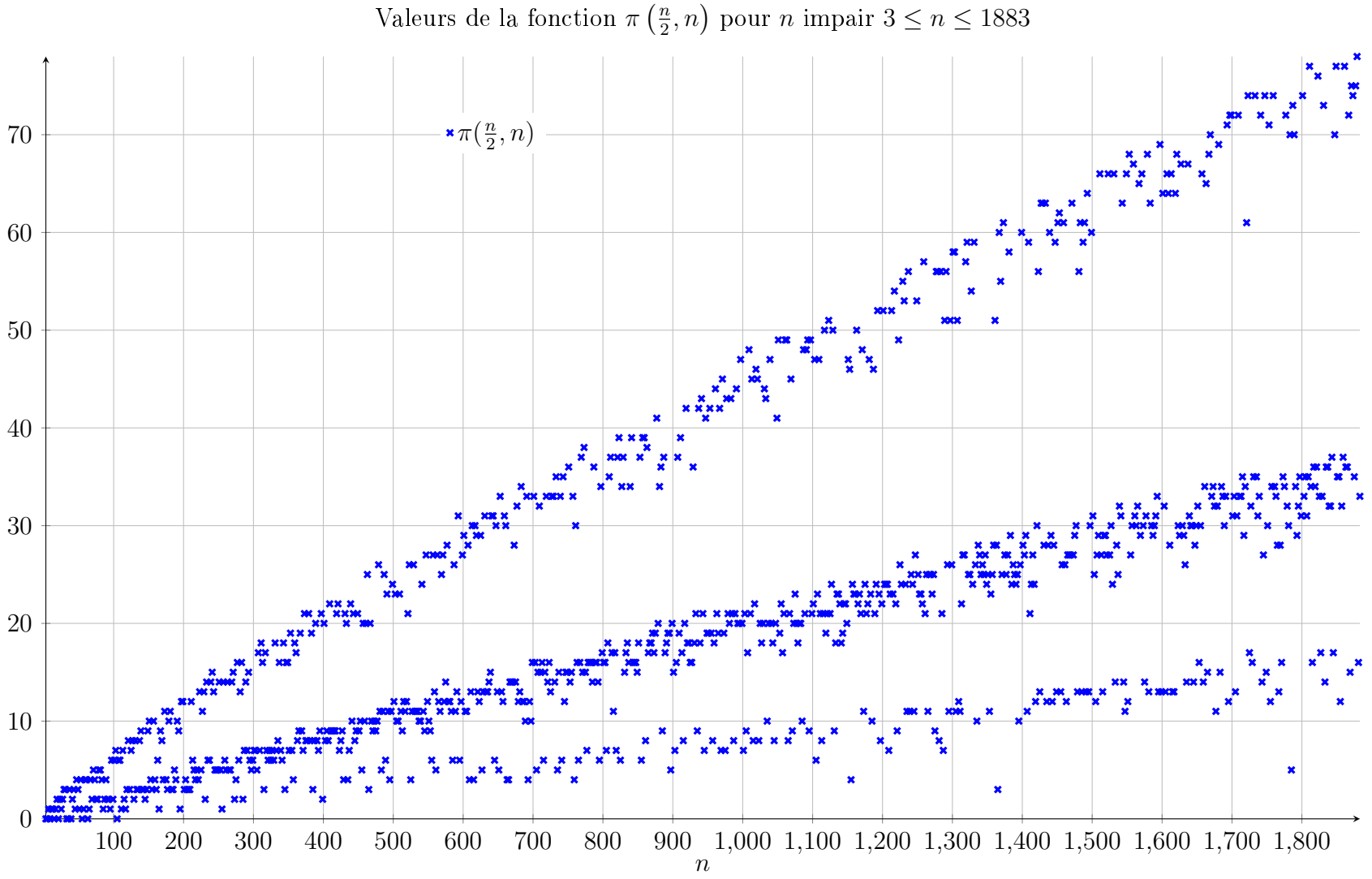
Annexe A

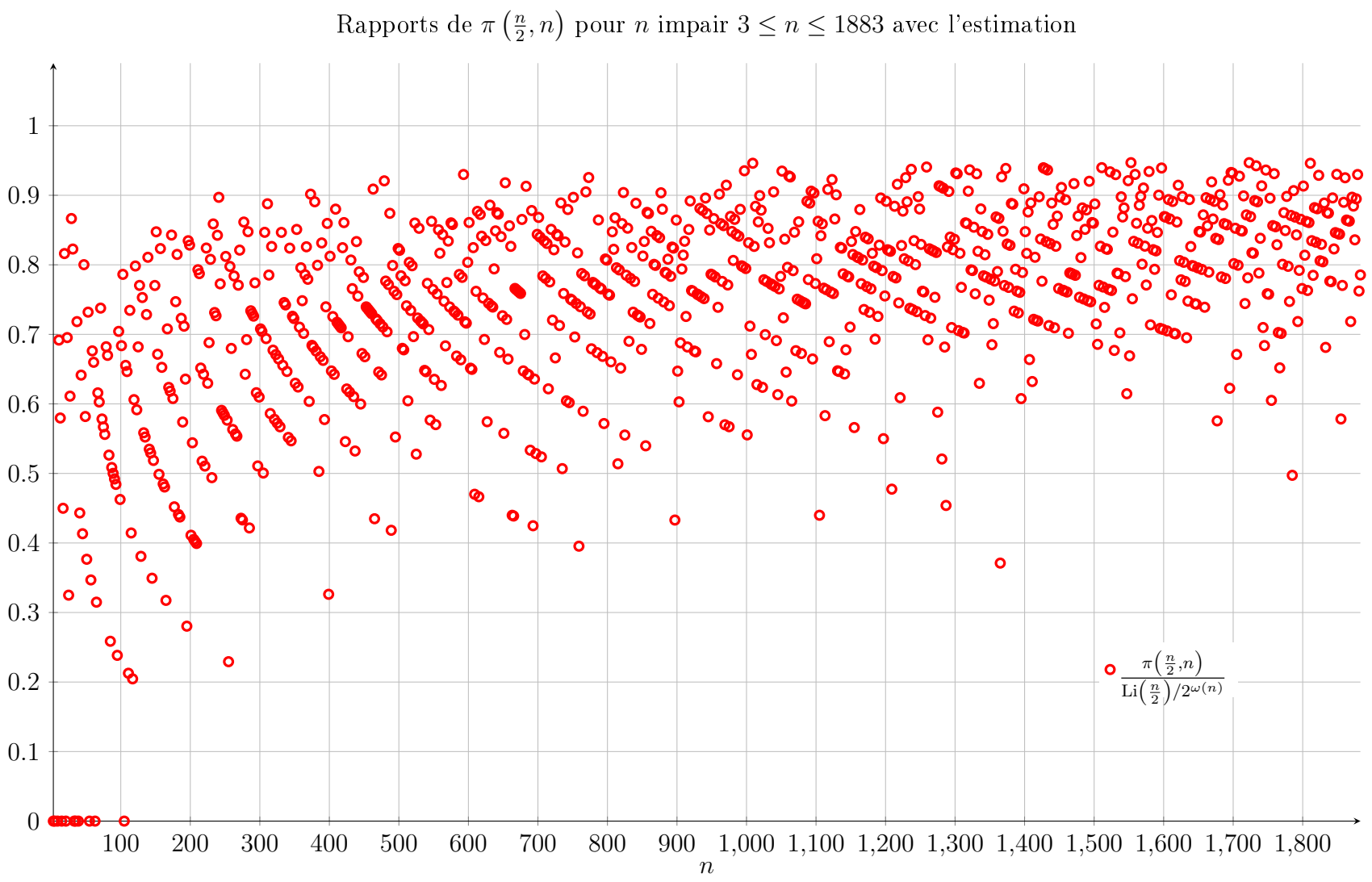
Valeurs de la fonction $\pi(X, n)$

Voici les valeurs de la fonction définie dans la section 4.2.2. Les valeurs sont données sous forme graphiques et sont calculées pour un entier n impair compris entre 3 et 1883. Ces bornes sont suffisantes pour compléter l'asymptotique fournie par le théorème 4.2.2.

A.1 $\pi\left(\frac{n}{2}, n\right)$

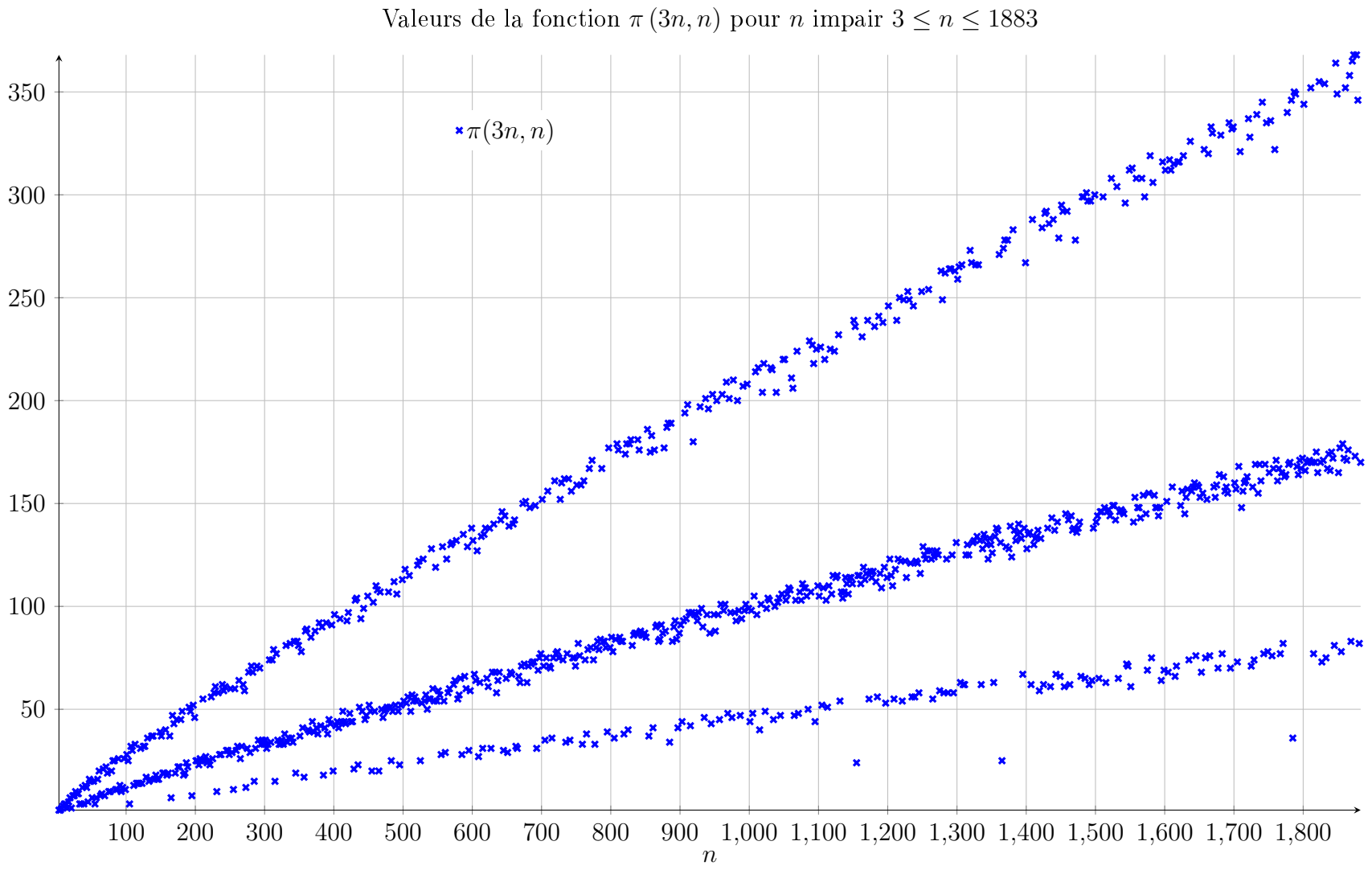
Voici les valeurs de la fonction $\pi\left(\frac{n}{2}, n\right)$ (voir équation (4.6)) pour n entier impair compris entre 3 et 1883.

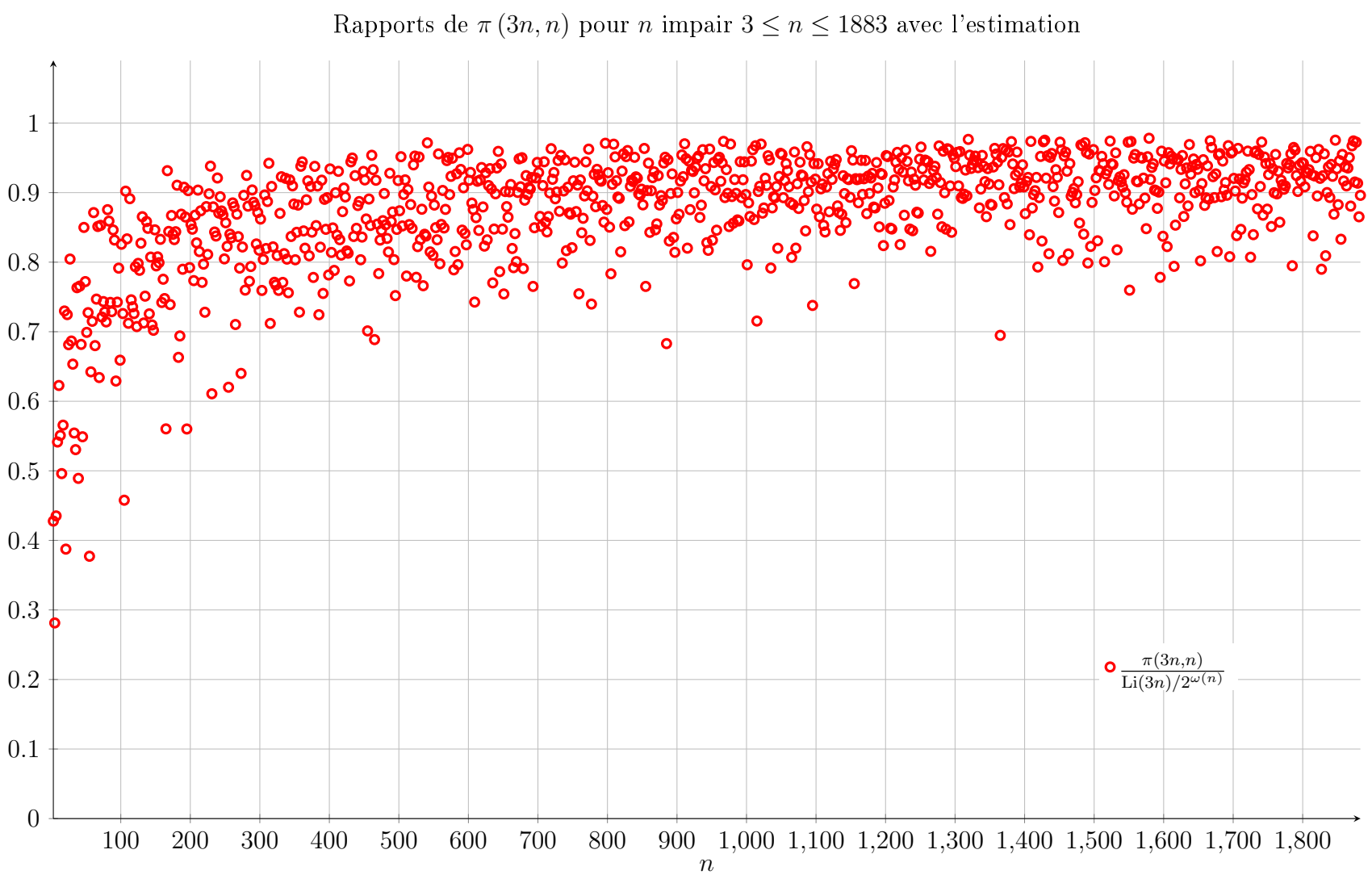

Valeurs de la fonction $\pi\left(\frac{n}{2}, n\right)$ pour n impair $3 \leq n \leq 1883$
$\pi(\frac{n}{2}, n)$
0
10
20
30
40
50
60
70
100
200
300
400
500
600
700
800
900
1,000
1,100
1,200
1,300
1,400
1,500
1,600
1,700
1,800
n

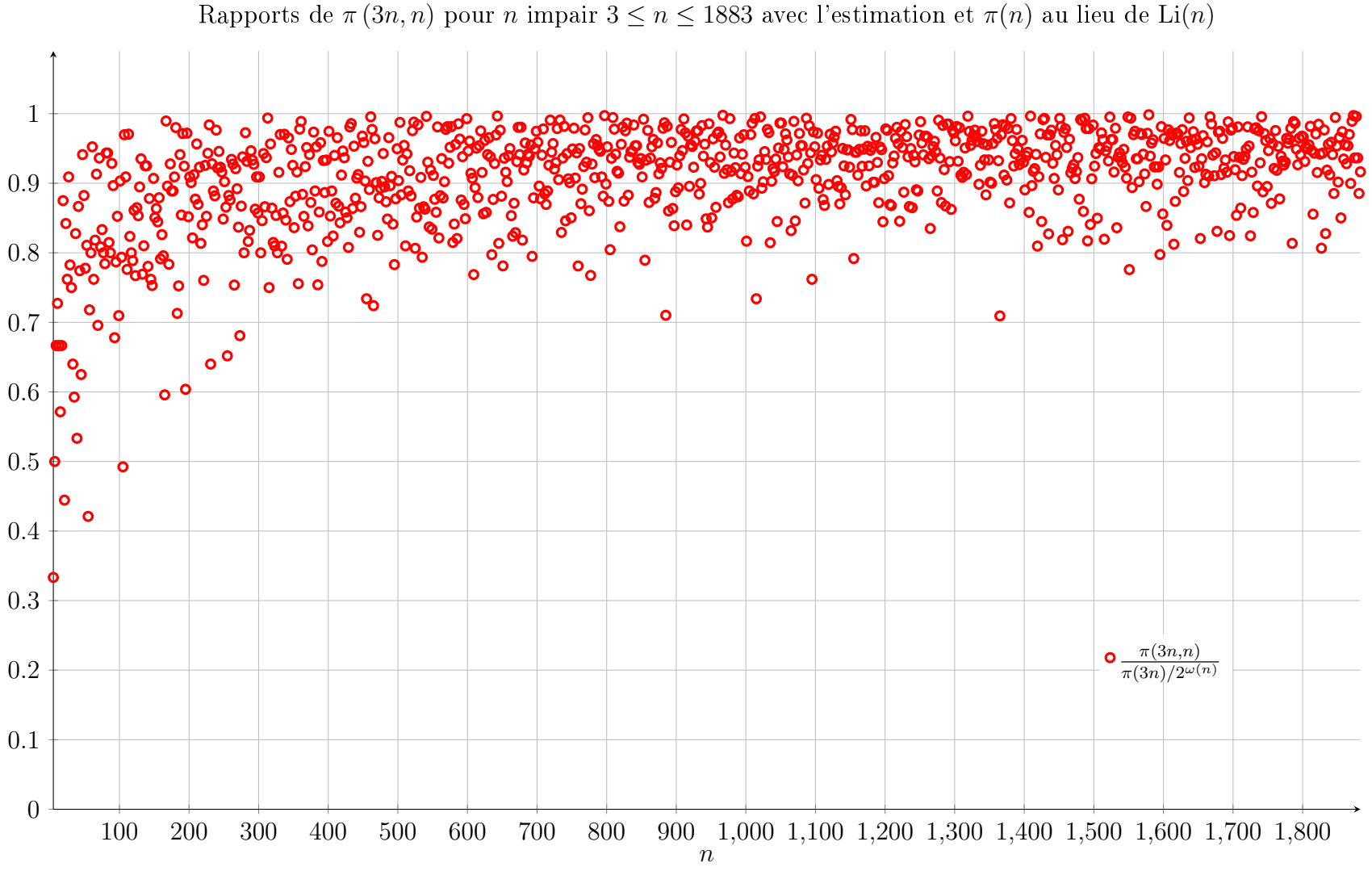

Rapports de $\pi\left(\frac{n}{2}, n\right)$ pour n impair $3 \leq n \leq 1883$ avec l'estimation
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
100
200
300
400
500
600
700
800
900
1,000
1,100
1,200
1,300
1,400
1,500
1,600
1,700
1,800
n
$\frac{\pi\left(\frac{n}{2},n\right)}{\mathrm{Li}\left(\frac{n}{2}\right)/2^{\omega(n)}}$

A.2 $\pi(3n, n)$

Voici les valeurs de la fonction $\pi(3n, n)$ (voir équation (4.6)) pour n entier impair compris entre 3 et 1883. Le second graphique de rapports utilise directement la fonction de comptage des nombres premiers au lieu de la fonction $\mathrm{Li}(x)$. Ils sont donc plus précis.


Valeurs de la fonction $\pi(3n, n)$ pour n impair $3 \leq n \leq 1883$
$\pi(3n, n)$
350
300
250
200
150
100
50
100
200
300
400
500
600
700
800
900
1,000
1,100
1,200
1,300
1,400
1,500
1,600
1,700
1,800
n


Rapports de $\pi(3n, n)$ pour n impair $3 \leq n \leq 1883$ avec l'estimation
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
100
200
300
400
500
600
700
800
900
1,000
1,100
1,200
1,300
1,400
1,500
1,600
1,700
1,800
n
$\frac{\pi(3n,n)}{\mathrm{Li}(3n)/2^{\omega(n)}}$


Rapports de $\pi(3n, n)$ pour n impair $3 \leq n \leq 1883$ avec l'estimation et $\pi(n)$ au lieu de $\mathrm{Li}(n)$
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
100
200
300
400
500
600
700
800
900
1,000
1,100
1,200
1,300
1,400
1,500
1,600
1,700
1,800
n
$\frac{\pi(3n,n)}{\pi(3n)/2^{\omega(n)}}$

Liste des Algorithmes

Bibliographie

[AEM87] L.M. Adleman, D.R. Estes, and K.S. McCurley. Solving bivariate quadratic congruences in random polynomial time. *Mathematics of Computation*, 48(177) :17–28, 1987.

[Ber00] Daniel J. Bernstein. How to find small factors of integers. *Accepted to Mathematics Of Computation ; being now revamped*, 2000.

[Ber03] Daniel J. Bernstein. Proving primality in essentially quartic time. `http://cr.yp.to/papers.html`. 2003.

[Ber04] Daniel J. Bernstein. How to find smooth parts of integers. May 2004.

[Bre89] David M. Bressoud. *Factorization and primality testing*. 1989.

[BS96] Wieb Bosma and Peter Stevenhagen. On the computation of quadratic 2–class groups. *J. Théor. nombres Bordeaux*, 8(2) :283–313, 1996.

[Bue89] D.A. Buell. *Binary Quadratic Forms : classical theory and modern computations*. 1989.

[Cas78] J.W.S. Cassels. *Rational Quadratic Forms*. L.M.S. Monographs, 1978.

[Cas08] Pierre Castel. Formes quadratiques et factorisation. Master's thesis, Laboratoire de Mathématiques Nicolas Oresme, juillet 2008.

[CC82] T. J. Chou and G. E. Collins. Algorithms for the solution of systems of linear diophantine equations. *SIAM J. Comput.*, 11 :687–708, 1982.

[CG06] Pierre Castel and Virginie Gamblin. Résidus quadratiques généralisés. Master's thesis, Université de Caen Basse-Normandie, juin 2006.

[Coh96] H. Cohen. *A Course in Computational Algebraic Number Theory*. Springer, 1996.

[Cox89] David A. Cox. *Primes of the form $x^2 + ny^2$*. John Wiley and Sons, 1989.

[CP05] R.E. Crandall and C. Pomerance. *Prime numbers : a computational perspective*. Springer Verlag, 2005.

[CR03] J. E. Cremona and D. Rusin. Efficient solution of rational conics. *Math. Comput.*, 72(243) :1417–1441, 2003.

[Gau89] Carl Friedrich Gauss. *Disquisitiones Arithmeticæ*. Springer-Verlag, 1989.

[HM91] James L. Hafner and Kevin S. Maccurley. Asymptotically fast triangularization of matrices over rings. *SIAM J. Comput.*, 20(6) :1068–1083, December 1991.

[Ili89] Costas S. Iliopoulos. Worst–case complexity bounds on algorithms for computing the canonical structure of finite abelian groups and the hermite and smith normal forms of an integer matrix. *SIAM J. Comput.*, 18(4) :658–669, August 1989.

[IR90] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*, volume 84. Springer-Verlag, graduate texts in mathematics edition, 1990.

[Jan73] Gerald J. Janusz. *Algebraic Number Fields*, volume 55 of *Pure and Applied Mathematics*. Academic Press, 1973.

[Lag80] J.C. Lagarias. On the computational complexity of determining the solvability or unsolvability of the equation $x^2 - dy^2 = -1$. *Trans. of the AMS*, 260(2) :485–508, August 1980.

[Lan86] Serge Lang. *Algebraic Number Theory*. 1986.

[LO77] J.C. Lagarias and A.M. Odlyzko. Effective versions of the chebotarev density theorem. In *Algebraic Number Fields*, pages 409–464. A. Frölich, 1977.

[Mil76] G.L. Miller. Riemann's hypothesis and tests for primality. *Journal of Computer and System Sciences*, 13(3) :300–317, 1976.

[NS09] Phong Q. Nguyen and Damien Stehlé. An LLL algorithm with quadratic complexity. *SIAM J. Comput.*, 39(3) :874–903, 2009.

[OSS84] H. Ong, C.P. Schnorr, and A. Shamir. An efficient signature scheme based on quadratic equations. In *16th Symp. on the Theory of Computing*, pages 208–216. Washington, 1984.

[PS87] John M. Pollard and Claus P. Schnorr. An efficient solution of the congruence $x^2 + ky^2 = m \pmod{n}$. *IEEE Transactions on Information Theory*, IT-33(5) :702–709, 1987.

[Rie94] Hans Riesel. *Prime Numbers and Computer Methods for Factorization*. 1994.

[Ser81] Jean-Pierre Serre. Quelques applications du théorème de densité de chebotarev. *Publications Mathématiques de l'IHES*, 54 :123–201, 1981.

[Ser95] Jean-Pierre Serre. *Cours d'arithmétique*. Presses Universitaires de France, 3$^{\text{eme}}$ edition, 1995.

[Sha71] D. Shanks. Gauss's ternary form reduction and the 2–sylow subgroup. *Math. Comp.*, 25(116) :837–853, 1971.

[Sim05a] Denis Simon. Quadratic equations in dimension 4, 5 and more. preprint, 2005.

[Sim05b] Denis Simon. Solving quadratic equations using reduced unimodular quadratic forms. *Mathematics of Computation*, 74(251) :1531–1543, January 2005.

[Sim06] Denis Simon. On the parametrization of solutions of quadratic equations. (Sur la paramétrisation des solutions des équations quadratiques.). 2006.

[UH39] Uspensky and Heaslet. *Elementary Number Theory*. 1939.

Un algorithme de résolution des équations quadratiques en dimension 5 sans factorisation

Résumé de la thèse :
Cette thèse en théorie algorithmique des nombres présente un nouvel algorithme probabiliste pour résoudre des équations quadratiques sur $\mathbb{Z}$ ou $\mathbb{Q}$ en dimension 5 sans utiliser de factorisation. Il est d'une complexité nettement meilleure que les algorithmes existant pour résoudre ce genre d'équations et repose sur deux algorithmes : celui de Simon et celui de Pollard et Schnorr. Après quelques rappels sur la théorie des formes quadratiques, on explique comment fonctionne cet algorithme. La suite consiste en l'analyse détaillée de cet algorithme pour laquelle on utilisera une version effective du théorème de densité de Tchebotarev.

An algorithm for solving dimension 5 quadratic equations without factorisation

Abstract :
This thesis in algorithmic number theory presents a new probabilistic algorithm for solving dimension 5 quadratic equations over $\mathbb{Z}$ or $\mathbb{Q}$ without using any factorisation. It has a much better complexity than existing algorithms and is based on two other algorithms : one from Simon and the other from Pollard and Schnorr. After a survey on the theory of quadratic forms, we explain how this algorithm works. What follows is a detailed analysis of the complexity of the algorithm for which we will use an effective version of the Tchebotarev density theorem.

Mots–clés :
- *Indexation RAMEAU :* théorie algorithmique des nombres, équations du second degré, formes quadratiques, nombres premiers, factorisation, corps quadratiques, groupes de classes (Mathématiques)
- *Indexation libre :* principe local–global, Hasse–Minkowski, vecteur isotrope, plan hyperbolique

Discipline : Mathématiques et leurs interactions
Laboratoire de Mathématiques Nicolas Oresme, CNRS UMR 6139
Université de Caen Basse–Normandie BP 5186
14032 CAEN Cedex, FRANCE