Université de Caen Basse-Normandie
CNRS UMR 6139
UFR Sciences

Laboratoire de Mathématiques Nicolas Oresme

HABILITATION à DIRIGER les RECHERCHES

présentée par

Denis SIMON

intitulée

Équations quadratiques, courbes elliptiques et polynômes non unitaires

soutenue le 28 novembre 2005

devant le jury composé de :

Francesco	**AMOROSO**	Professeur à l'Université de Caen.
Karim	**BELABAS**	Professeur à l'Université Bordeaux I.
John	**BOXALL**	Professeur à l'Université de Caen.
Henri	**COHEN**	Professeur à l'Université Bordeaux I.
Jean	**COUGNARD**	Professeur à l'Université de Caen, directeur.
Hendrik W.	**LENSTRA**	Professeur à l'Université de Leiden (Pays-Bas).
Jean–François	**MESTRE**	Professeur à l'Université Paris VII.

après avis des rapporteurs :

Henri	**COHEN**	Professeur à l'Université Bordeaux I.
John	**CREMONA**	Professeur à l'Université de Nottingham (Angleterre).
Hendrik W.	**LENSTRA**	Professeur à l'Université de Leiden (Pays-Bas).

LMNO, BP 5186, Université de Caen, 14 032 Caen cedex, FRANCE +33.(0)2.31.56.73.22
lmno@math.unicaen.fr http ://www.math.unicaen.fr/lmno/

Table des matières

Table des Matières **2**

I Présentation Générale **5**
1 Description des résultats obtenus 5
1.1 Autour de la thèse 5
1.2 Autour des polynômes non unitaires 6
1.3 Autour des équations quadratiques 7
2 Projets de recherche 8

Liste des travaux présentés **11**

II Équations aux normes **13**
1 Le résultat principal 14
2 Extensions galoisiennes 14
3 Extensions non galoisiennes 15

III Polynômes non unitaires **17**
1 L'anneau invariant d'un polynôme non unitaire 17
2 La classe invariante 19
3 Décomposition des idéaux 19

IV Équations quadratiques **21**
1 Points rationnels sur les coniques 22
2 Paramétrisation des coniques et groupes de classes 25
3 Équations quadratiques en dimension supérieure 27

V Courbes Elliptiques **33**
1 2–descente 34
2 4–descente et 3–descente 36

Bibliographie **37**

Chapitre I

Présentation Générale

1 Description des résultats obtenus

Mes activités de recherche sont centrées principalement sur l'étude des propriétés arithmétiques des invariants des polynômes à coefficients entiers et la résolution algorithmique des équations diophantiennes, en particulier les courbes elliptiques, les équations aux normes et les équations quadratiques.

Même si ces deux axes utilisent des outils communs (en particulier ceux de la théorie algébrique des nombres), ils sont relativement parallèles et il serait artificiel de leur chercher une intersection, à part peut-être celle que constitue la théorie de Gauss des groupes de classes de formes quadratiques binaires.

Tous mes travaux sont imprégnés de ma conviction que l'on peut faire des mathématiques, même théoriques, à partir d'expériences et sont illustrés de nombreux exemples numériques.

1.1 Autour de la thèse

Motivé par la présence à Bordeaux de deux spécialistes, l'un H. Cohen en théorie algorithmique des nombres algébriques, l'autre J. Cremona en 2–descente sur les courbes elliptiques sur $\mathbb{Q}$, mon sujet de thèse ([T1]) s'est rapidement orienté vers la détermination algorithmique du rang des courbes elliptiques sur les corps de nombres. Je me suis alors aperçu que, dans l'ensemble, les deux aspects se combinaient naturellement bien. Mais un nouveau problème algorithmique est apparu, celui de la résolution des équations de Legendre dans les corps de nombres. En exprimant cette équation sous la forme d'une équation aux normes dans une extension relative de corps de nombres, j'ai pu la résoudre algorithmiquement en démontrant un résultat théorique nouveau sur la nature des solutions en termes de S–unités ([T3]) : j'utilise pour cela différentes notions de groupes de classes relatifs et des méthodes issues de la cohomologie. S'agissant là d'un résultat intéressant, même indépendamment des courbes elliptiques, j'ai proposé d'inclure le programme correspondant dans le logiciel `pari/gp` ([T13]). J'ai ainsi pu proposer le premier algorithme pour la 2–descente sur les courbes elliptiques définies sur un corps de nombres général. La description de cet algorithme a subi de nombreuses améliorations et simplifications entre ma thèse

[T1] et la publication ultérieure de l'article [T4]. En particulier, je simplifie les formules qui permettent de construire le groupe de Selmer et je diminue considérablement le nombre d'étapes nécessaires pour la minimisation des quartiques qui représentent les éléments du groupe de Selmer. Dans un travail ultérieur, non publié, je me suis rendu compte que ces formules simplifiées permettaient de travailler simultanément sur des familles entières de courbes elliptiques : les tordues quadratiques. En effet, pour ces familles, une grande partie de l'algorithme de la 2–descente est commune, la partie restante étant souvent plus rapide. Le programme que j'ai écrit en `gp` ([T14] et [T15]) permet ainsi de calculer le rang de courbes elliptiques, qui sont tout à fait hors de portée des autres programmes existants, même sur $\mathbb{Q}$, comme le programme `mwrank` de Cremona.

Indépendamment, je me suis aussi intéressé pendant ma thèse ([T1]) aux valeurs minimales des discriminants des polynômes à coefficients entiers, en fonction de leur degré et de leur signature. J'ai proposé des constructions tout à fait originales ([T2]), qui m'ont permis de battre un grand nombre de records antérieurs ([T12]) et de construire des milliers de polynômes intéressants pour des degrés $d \leqslant 50$. Deux questions se sont alors posées :

- Que donnerait une généralisation de ces idées au cas des polynômes à deux variables ? Probablement la construction de courbes géométriques remarquables, mais cette question reste ouverte.
- Pourquoi la quasi–totalité des polynômes construits sont–ils unitaires ?

1.2 Autour des polynômes non unitaires

Pour envisager la question précédente, j'ai étudié les propriétés arithmétiques des polynômes non unitaires. Pour simplifier la situation, je me suis contenté de considérer les polynômes irréductibles. Le cas général doit pouvoir s'en déduire, au moins en partie. On peut voir les polynômes à une variable comme des formes binaires, sur lesquelles agit le groupe $SL_2(\mathbb{Z})$. Comme le discriminant est un invariant pour cette action, ce cadre est plus naturel que celui des polynômes unitaires, qui n'a d'autre action que la translation par $\mathbb{Z}$. Dans le cas du degré 2, la théorie des classes de formes quadratiques de Gauss, la situation est idéale. On connaît tous les invariants, et on peut les décrire en termes de corps quadratiques, d'anneaux d'entiers et de groupes de classes d'idéaux. S'il est bien connu comment associer un corps de nombres à un polynôme non unitaire, il est moins connu comment on peut lui associer un anneau d'entiers dans ce corps de nombres. Dans [T5], j'ai proposé pour cela de suivre une construction de Dedekind. Cet anneau ne change pas lorsque $SL_2(\mathbb{Z})$ agit sur les polynômes, c'est donc une bonne généralisation du cas quadratique. On peut ainsi généraliser la notion d'anneau d'entiers monogène. En utilisant cette construction, j'ai généralisé un résultat de M.N. Gras, sur la monogénéité des anneaux d'entiers dans les extensions cycliques de $\mathbb{Q}$, de degré premier. Cette généralisation donnait un résultat plus précis, y compris à propos des polynômes unitaires.

Dans [T6], j'ai poussé plus loin la construction et j'ai réussi à associer à un polynôme non unitaire, une classe dans le groupe de classes d'idéaux de l'anneau d'entier associé. Malheureusement, j'ai montré que cette tentative de généralisation de la théorie de Gauss n'en conservait pas toutes les propriétés, ce qui la rendait peut-être moins intéressante.

Tout du moins, elle donnait une nouvel invariant, plus précis que le discriminant et l'anneau d'entiers associé, qui permettait dans certains cas de montrer que deux formes ne sont pas équivalentes.

J'étais convaincu que la voie que je venais de prendre était la source de nombreuses généralisations et même d'améliorations, car le contexte me semblait plus naturel que celui des polynômes unitaires. Au cours d'échanges avec R. Dvornicich et I. Delcorso à Pise, j'ai dû transmettre cette conviction, car après une semaine nous avions le projet de démontrer plusieurs résultats dans cette direction. C'est ainsi que nous avons généralisé ([T9]) au cas des ordres non maximaux définis par des polynômes non unitaires, les critères de décomposition des nombres premiers et le critère de Dedekind sur la p–maximalité. Nous avons aussi généralisé la notion d'indice d'un corps de nombres.

Mais ma conviction ne s'arrête pas là et j'espère encore obtenir d'autres résultats...

1.3 Autour des équations quadratiques

Dans l'algorithme de la 2–descente sur les courbes elliptiques, une des étapes consiste à résoudre des équations quadratiques ternaires, dont les coefficients peuvent être gigantesques, mais dont le déterminant, connu à l'avance, est souvent très petit. Les méthodes connues pour résoudre ces équations utilisent presque systématiquement les formes quadratiques diagonales, ce qui génère l'incontournable difficulté de factoriser des entiers ayant des milliers de chiffres, y compris lorsque l'on travaille sur $\mathbb{Q}$. C'est alors que j'ai compris que l'on ne pourrait pas décrire d'algorithme efficace pour chercher des points rationnels sur les courbes de genre 1 tant que l'on n'en disposait pas d'un pour les courbes de genre 0. Je me suis alors concentré sur la résolution rapide des équations quadratiques ternaires à coefficients dans $\mathbb{Q}$. En comparant les algorithmes existants (Lagrange, Gauss, Cremona,...), j'ai réussi à écrire un nouvel algorithme rapide, qui ne se ramène pas au cas diagonal et n'utilise pas d'autre factorisation que celle du déterminant ([T7] et [T16]). L'algorithme se fait en deux étapes principales : minimisation et réduction. La minimisation consiste à utiliser la connaissance des facteurs premiers du déterminant pour se ramener au cas où le déterminant vaut -1, quitte à augmenter la taille des coefficients. La réduction consiste à réduire la taille des coefficients jusqu'à l'obtention d'un 0. Pour la réduction, j'ai proposé une modification de l'algorithme LLL pour les formes quadratiques indéfinies. Les bornes que j'ai obtenues dans [T7] pour la qualité de la réduction montrent que l'on peut ainsi résoudre rapidement toutes les équations quadratiques unimodulaires en dimension $n \leqslant 6$. Appliqué au cas des équations issues de la 2–descente sur les courbes elliptiques définies sur $\mathbb{Q}$, cela donne un résultat particulièrement surprenant, au point que mon algorithme a rapidement été adopté par les différents spécialistes de la 2–descente (notamment pour `magma`).

Cependant, pour les courbes elliptiques, une nouvelle difficulté apparaissait : il n'était pas suffisant d'avoir une solution, on les voulait toutes, sous forme paramétrée. Bien sûr, il existe un moyen géométrique très simple pour cela, mais la paramétrisation obtenue n'était pas satisfaisante, car elle introduisait des facteurs parasites gigantesques qu'il fallait éliminer. Dans [T4], j'avais déjà proposé un moyen d'en éliminer une partie, mais je me suis

rendu compte ([T8]) qu'il existait un moyen très simple de fabriquer une paramétrisation qui ne les introduisait pas ! Non seulement cette paramétrisation était optimale pour cette application, mais elle avait en plus de très belles propriétés. En effet, j'ai montré le lien entre cette paramétrisation des solutions d'une équation quadratique ternaire et l'extraction d'une racine carrée dans un certain groupe de classes. Comme cette extraction de racine carrée est à la base de l'algorithme pour déterminer la 2–partie du groupe de classes des formes quadratiques de discriminant donné (algorithme de Gauss, Shanks, Bosma–Stevenhagen), mon résultat permet une nouvelle interprétation de cet algorithme.

Après avoir ainsi obtenu une version plus satisfaisante de l'algorithme de la 2–descente sur les courbes elliptiques, je me suis orienté vers les généralisations possibles. Ayant appris que l'une des étapes de la 3–descente sur les courbes elliptiques ([T18]) nécessitait la résolution d'une équation quadratique en dimension 8, j'ai cherché à résoudre les équations quadratiques pour des dimensions n plus grandes que 3. J'ai commencé par la dimension 4, en espérant que l'aspect algorithmique se comporterait comme la théorie et qu'il suffirait de distinguer successivement les trois cas $n = 3$, puis $n = 4$ et enfin $n \geqslant 5$. Contrairement au cas $n = 3$, je n'ai trouvé dans la littérature qu'un seul algorithme pour $n = 4$ et il était particulièrement inefficace (mais parfait pour la théorie !). L'idée naturelle de tenter une minimisation/réduction ne suffisait pas à cause de la minimisation qui n'était tout simplement jamais possible pour une simple question de parité. C'est dans un article de Cassels que j'ai trouvé l'idée de passer en dimension 6, en rajoutant une forme quadratique binaire bien choisie dans un groupe de classes de discriminant donné. Grâce à l'algorithme décrit plus haut, cela était possible et la minimisation se faisait correctement en dimension 6. En combinant avec mon algorithme de réduction des formes indéfinies, j'ai ainsi obtenu le premier algorithme efficace pour la résolution des équations quadratiques en dimension 4 ([T11] et [T17]). Il restait encore une difficulté à franchir pour atteindre les dimensions $n \geqslant 5$. Pour ces dimensions, la minimisation pouvait se faire en dimension $n+3$. Expérimentalement, la réduction fonctionnait correctement sans modification, mais les bornes prouvées dans [T7] étaient insuffisantes, y compris pour $n = 5$. Dans [T10], j'ai obtenu de nouvelles bornes, suffisantes pour montrer que l'algorithme de réduction permettait de résoudre les équations quadratiques unimodulaires pour toutes les dimensions $n \leqslant 9$. Je pouvais enfin démontrer ([T11]) un algorithme général pour toutes les dimensions $n \geqslant 5$.

2 Projets de recherche

J'ai déjà cité quelques projets de recherche dans la première partie, comme la construction de polynômes en deux variables de petit discriminant ou la généralisation de nouvelles propriétés aux polynômes non unitaires. Je voudrais ici en évoquer d'autres.

Par exemple, il serait intéressant de généraliser la résolution des équations quadratiques à d'autres corps de nombres que $\mathbb{Q}$. Cependant, comme mon approche utilise largement la géométrie des nombres, il semblerait nécessaire d'avoir des idées radicalement nouvelles pour les corps non euclidiens.

Une autre généralisation de ces résultats est envisageable. En effet, on peut les voir

comme une version algorithmique de la preuve de principe local/global de Hasse pour les formes quadratiques sur $\mathbb{Q}$, où l'on utilise deux outils successifs : la minimisation puis la réduction. Mon projet est d'utiliser cette même stratégie pour d'autres problèmes de théorie des nombres pour lesquels le principe de Hasse est vrai, afin de proposer des méthodes effectives de résolution et des algorithmes efficaces. Par exemple, j'ai déjà des résultats partiels ([T19]) pour les équations aux normes dans les extensions cubiques cycliques sur $\mathbb{Q}(\zeta_3)$. Ce cas particulier est aussi une étape pour la 3–descente sur les courbes elliptiques ([T18]). On peut envisager plus généralement toutes les équations aux normes dans les extensions cycliques, ou encore la trivialisation des algèbres simples.

Je cite enfin un projet beaucoup plus ambitieux concernant les courbes elliptiques. En effet, si la 2–descente sur les courbes elliptiques est aujourd'hui algorithmiquement bien maîtrisée, ce n'est pas encore le cas de la 3-descente ou de la 5-descente et plus généralement de la p-descente. En collaboration avec J.E. Cremona, T. Fisher, C. O'Neil et M. Stoll, nous avons le projet de combler ce manque ([T18]). Les difficultés sont à la fois théoriques et algorithmiques. Nous avons déjà réussi à franchir quelques étapes décisives et nous sommes donc assez optimistes pour les suivantes, en particulier pour la 3-descente. Actuellement, la difficulté majeure que nous rencontrons est la représentation d'algèbres simples comme algèbres de matrices, qui est un cas particulier du problème général du calcul effectif dans les groupes de Brauer des corps de nombres. Si nos espoirs aboutissent, cela constituerait une avancée majeure dans le domaine des courbes elliptiques, mais aussi de la géométrie algébrique et des algèbres semi-simples.

Parmi les projets que j'ai cités, certains sont déjà bien avancés, d'autres sont reportés à un futur plus ou moins proche. Dans tous les cas, je m'attends à ce que les résultats ainsi obtenus, qu'ils soient positifs ou négatifs, m'ouvrent davantage de nouvelles pistes qu'ils n'en ferment. Ainsi, le nombre de questions que je souhaite étudier augmente de jour en jour.

Liste des travaux présentés

[T1] Thèse de Doctorat, Université Bordeaux I (21/12/1998) *Équations dans les Corps de Nombres et Discriminants Minimaux*, disponible sur `www.math.unicaen.fr/∼simon/maths/these_resume.html`.

• **Articles publiés** :

[T2] *Construction de polynômes de petits discriminants*, Comptes Rendus de l'Académie des Sciences, Paris, t. **329**, Série I (1999), 465–468.

[T3] *Solving norm equations in relative number fields using S–units*, Math. Comp. Vol **71** No 239 (2002), 1287–1305.

[T4] *Computing the rank of elliptic curves over number fields*, London Mathematical Society Journal of Computation and Mathematics, Vol **5** (2002), 7–17.

[T5] *The Index of Nonmonic Polynomials*, Indagationes Mathematicae, N.S., **12** (4) (2001), 505–517.

[T6] *La classe invariante d'une forme binaire*, Comptes Rendus Mathématiques, Volume **336**, Issue 1, 1 (Janvier 2003), 7–10.

[T7] *Solving quadratic equations using reduced unimodular quadratic forms*, Math. Comp., Vol **74** No 251 (2005), 1531–1543.

• **Articles acceptés** :

[T8] *Sur la paramétrisation des équations quadratiques*, accepté au Journal de Théorie des Nombres de Bordeaux (Juillet 2005).

[T9] *The decomposition of primes in nonmaximal orders*, (avec R. Dvornicich et I. Delcorso, Pise), accepté à Acta Arithmetica (Août 2005).

• **Articles soumis** :

[T10] *Reduced unimodular quadratic forms in low dimension*, soumis au LMS Journal of Computation and Mathematics (2005).

[T11] *Quadratic equations in dimensions* 4, 5, *and more*, soumis à Math. Comp. (2005).

• **Publication de tables et de programmes informatiques** :

En complément à ces publications, j'ai également mis des tables et des programmes à la disposition du public sur mon site internet `www.math.unicaen.fr/∼simon` :

[T12] Tables de milliers de polynômes contenant les records de petits discriminants pour plusieurs degrés et signatures.

[T13] Programme de résolution des équations aux normes dans les corps de nombres.

[T14] Programme de calcul du rang des courbes elliptiques dans les corps de nombres.

[T15] Programme de calcul du rang des courbes elliptiques sur $\mathbb{Q}$.

[T16] Programme de résolution des équations quadratiques ternaires sur $\mathbb{Q}$.

[T17] Programme de résolution des équations quadratiques $\mathbb{Q}$, en dimensions 4, 5 et plus.

• **Travaux en cours** :

[T18] *Explicit 3-descent on an elliptic curve*, avec J.E. Cremona, T. Fisher, C. O'Neil, et M. Stoll.

[T19] *Résolution des équations aux normes cubiques cycliques sur* $\mathbb{Q}(\zeta_3)$.

Chapitre II

Équations aux normes

Les résultats de ce chapitre sont issus de ma thèse [T1] et de l'article correspondant [T3]. L'algorithme que l'on peut en déduire pour résoudre les équations aux normes est inclus dans `pari/gp` ([T13]).

On aborde ici la résolution explicite des équations du type $\mathcal{N}_{L/K}(x) = a$, où L/K est une extension quelconque de corps de nombres, et a un élément non nul du corps K.

En écrivant a sous la forme $a = \alpha/b$ avec $b \in \mathbb{Z}$ et α un entier algébrique de K, on voit que l'équation est équivalente à $\mathcal{N}_{L/K}(x) = b^{d-1}\alpha$ où $d = [L : K]$ est le degré de l'extension. Ainsi, on peut supposer que a est un entier algébrique.

Un point de vue classique consiste à chercher les solutions entières, ce qui peut se faire par exemple en bornant la valeur absolue des coefficients. C'est ce que développent [Siegel 1973] pour les extensions galoisiennes, [Fincke et Pohst 1983] pour les extensions de $\mathbb{Q}$ et [Fieker, Jurk et Pohst 1997] pour les extensions relatives. On peut aussi utiliser un point de vue plus algébrique pour montrer l'existence d'une solution rationnelle, comme [Bartels 1980] pour les extensions cycliques ou, mieux, pour déterminer une telle solution, comme [Garbanati 1980] pour les extensions abéliennes ou [Fieker 1997] pour les extensions galoisiennes.

Ces deux points de vue sont très différents. En particulier, si l'on peut montrer qu'il n'existe pas de solution entière, cela ne prouve absolument pas qu'il n'existe pas de solution rationnelle. Considérons l'exemple fondamental suivant : $L/K = \mathbb{Q}(\sqrt{34})/\mathbb{Q}$ et $a = -1$. L'unité fondamentale $u = 6\sqrt{34} + 35$ est de norme $+1$, donc a ne peut pas être la norme d'un entier algébrique (de L). Pourtant, on a $\mathcal{N}_{L/K}((\sqrt{34} + 5)/3) = -1$.

Je donne ici une description algébrique des solutions rationnelles dans le cas d'une extension relative quelconque. Mes principaux résultats donnent une description des numérateurs et surtout des dénominateurs possibles pour les solutions. Plus précisément, je donne une liste finie d'idéaux premiers à partir de laquelle on peut construire une solution. Cette construction se fait en appliquant plusieurs fois l'algorithme de l'idéal principal dans le corps L. Si la construction échoue, cela prouve que l'équation n'a pas de solution du tout. L'algorithme correspondant à cette construction a été implanté en `pari` dans les fonctions `bnfisnorm` et `rnfisnorm` de `gp` (voir [T13]).

1 Le résultat principal

Soit S un ensemble fini d'idéaux premiers du corps de base K. On dit qu'un élément $a \in K^*$ (resp. $x \in L^*$) est une S–unité si les seuls idéaux premiers apparaissant dans la décomposition de a (resp. x) sont dans S (resp. au dessus d'un idéal premier de S). On note $\mathbb{U}_{K,S}$ le groupe des S–unités de K et $\mathbb{U}_{L,S}$ celui de L. On cherche les solutions de notre équation sous la forme de S–unités, pour un ensemble S bien choisi. Naturellement, les idéaux premiers qui divisent a ont une contribution dans ce problème et nous supposerons que S les contient, autrement dit, nous supposerons que a est une S–unité. On utilise aussi la notion de S–entier : on dit qu'un nombre algébrique est un S–entier lorsque son dénominateur ne contient que des idéaux premiers de S.

Il est clair que la norme d'une S–unité de L est une S–unité de K, c'est–à–dire que

$$\mathcal{N}_{L/K}(\mathbb{U}_{L,S}) \subset \mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S} \ .$$

L'exemple fondamental que nous venons d'envisager montre que l'inclusion réciproque n'est pas vraie en général (ici avec $S = \emptyset$) : une S–unité qui est une norme n'est pas toujours la norme d'une S–unité.

Le résultat principal montre que l'on a une égalité dès que S contient un ensemble fini S_0 explicite qui ne dépend que de l'extension L/K. Ainsi, pour résoudre l'équation $\mathcal{N}_{L/K}(x) = a$, il est suffisant de considérer les idéaux premiers divisant a, ainsi que les idéaux premiers de S_0.

Théorème I *Soit L/K une extension de corps de nombres. Il existe un ensemble fini S_0 d'idéaux premiers de K, ne dépendant que de L/K, tel que*

$$\textit{si } S \supset S_0 \textit{ alors } \mathcal{N}_{L/K}(\mathbb{U}_{L,S}) = \mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S} \ .$$

Un tel S_0 est décrit explicitement en termes d'idéaux ramifiés et de certains groupes de classes. Quand S ne contient pas S_0, il est encore possible de donner des informations sur le quotient $(\mathcal{N}_{L/K}(L^*) \cap \mathbb{U}_{K,S})/\mathcal{N}_{L/K}(\mathbb{U}_{L,S})$. Ces informations sont plus précises quand l'extension est galoisienne, et même cyclique.

2 Extensions galoisiennes

Dans le cas d'une extension galoisienne, l'énoncé du résultat est particulièrement simple :

Théorème II (Cas galoisien) *On suppose que L/K est une extension galoisienne. Si S_0 engendre le groupe de classes relatif $\mathrm{Cl}_i(L/K)$, alors pour tout $S \supset S_0$, on a*

1– Un S–entier est une norme si et seulement si c'est la norme d'un S–entier.

2– Une S–unité est une norme si et seulement si c'est la norme d'une S–unité.

Le groupe de classes relatif $\mathrm{Cl}_i(L/K)$ est le quotient du groupe de classes ordinaire $Cl(L)$ obtenu de la manière suivante : le groupe des idéaux fractionnaires de K s'injecte naturellement dans celui de L, ce qui induit une application de $\mathrm{Cl}(K)$ dans $\mathrm{Cl}(L)$, dont on

note l'image $i(\mathrm{Cl}(K))$; le groupe $\mathrm{Cl}_i(L/K)$ est le quotient $\mathrm{Cl}(L)/i(\mathrm{Cl}(K))$. On obtient une version plus simple, mais plus faible, du théorème en remplaçant $\mathrm{Cl}_i(L/K)$ par $\mathrm{Cl}(L)$. Pour les S–unités, un argument très simple permet d'améliorer le résultat :

Théorème III *Le théorème I est vrai si S_0 engendre la $[L : K]$–partie du groupe de classes relatif $\mathrm{Cl}_i(L/K)$.*

Dans le cas d'une extension quadratique, on a donc montré que la connaissance de la 2–partie du groupe de classes permet de résoudre les équations aux normes. La théorie des genres donne une réciproque à cela et dans la partie IV.2, nous verrons comment la connaissance des solutions des équations aux normes permet de reconstruire toute la 2–partie du groupe de classes.

3 Extensions non galoisiennes

Pour les extensions non galoisiennes, la situation est nettement plus compliquée et il n'est plus suffisant de considérer le groupe de classes de l'extension L/K.

Soit $\mathfrak{L}/K$ la clôture galoisienne de L/K. On note G le groupe de Galois de $\mathfrak{L}/K$ et H le sous–groupe de G correspondant à l'extension $\mathfrak{L}/L$. Pour tout sous–groupe D de G, on note $\mathfrak{L}^D$ le sous–corps de $\mathfrak{L}$ stable par D (par exemple $\mathfrak{L}^D = L$).

Dans le cas où les degrés $[L : K]$ et $[\mathfrak{L} : L]$ sont premiers entre eux, le critère reste relativement simple :

Théorème IV *On suppose que $[L : K]$ et $[\mathfrak{L} : L]$ sont premiers entre eux. Le théorème I est vrai si S_0 engendre la $[L : K]$–partie du groupe de classes relatif $\mathrm{Cl}_i(\mathfrak{L}/K)$.*

Ce critère simple s'applique en particulier à toutes les extensions de degré premier, mais aussi à bien d'autres types d'extensions.

Dans le cas où $[L : K]$ et $[\mathfrak{L} : L]$ ne sont pas premiers entre eux, le critère est plus restrictif, et il faut considérer les idéaux premiers ramifiés, ainsi que de nouveaux groupes de classes.

Théorème V *Soit S_0 un ensemble fini d'idéaux premiers de K, contenant les premiers ramifiés de L/K, et engendrant la $[L : K]$–partie du groupe de classes relatif $\mathrm{Cl}_i(\mathfrak{L}/K)$.*

De plus, pour tout nombre premier p divisant à la fois $[L : K]$ et $[\mathfrak{L} : L]$, et pour tout sous–groupe cyclique D de G d'ordre p^a tel que $D \cap H \neq \{1\}$, on suppose que S_0 engendre aussi la p–partie du groupe de classes relatif $\mathrm{Cl}_i(\mathfrak{L}^D/K)$.

Sous ces conditions, le théorème I est vrai.

On peut se convaincre de la nécessité de toutes ces conditions à partir des nombreux exemples que je donne dans [T3]. Je donne aussi dans cet article de nombreux cas où l'on peut simplifier les hypothèses, par exemple pour les extensions de $\mathbb{Q}$.

Chapitre III

Polynômes non unitaires

Les polynômes entiers ayant un degré et un discriminant fixés sont utiles dans de nombreuses applications, parmi lesquelles l'étude des groupes de classes des corps quadratiques (ce sont les classes de formes quadratiques de Gauss, voir [Gauss 1953] ou [Cox 1989]) ou la recherche d'espaces homogènes donnés par des polynômes quartiques dans l'algorithme de la 2–descente sur les courbes elliptiques (voir [Cremona 1997 a]).

L'objectif de cette série de travaux [T5], [T6], [T9] (et même [T2], mais l'approche est très différente et je ne reviendrai pas sur cet aspect ici) est de pouvoir déduire un maximum de renseignements de nature algébrique ou arithmétique sur les polynômes non unitaires. Je veux éviter de recourir à une transformation pour les rendre unitaires, car ils peuvent alors perdre une quantité significative d'information. Afin de pouvoir considérer ces polynômes dans un autre contexte, par exemple celui de la 4–descente sur les courbes elliptiques (voir §V.2), une telle étude est nécessaire.

1 L'anneau invariant d'un polynôme non unitaire

Soit P un polynôme unitaire à coefficients entiers de degré n. Si θ est une racine de P, θ est un entier algébrique et le système d'entiers algébriques $1, \theta, \ldots, \theta^{n-1}$ est de discriminant $\mathrm{Disc}P$. La question très classique de savoir si un anneau d'entiers d'un corps de nombres K est engendré sur $\mathbb{Z}$ par une telle base de puissances, c'est-à-dire si on a $\mathbb{Z}_K = \mathbb{Z}[\theta]$, est étudiée dans [Győry 1998]. On dit alors que l'anneau des entiers est monogène. Cela revient à trouver des polynômes unitaires tels que $\mathrm{Disc}P = \mathrm{Disc}K$. L'ensemble des P est clairement stable par translation $P(X) \mapsto P(X+c)$, qui ne change ni le coefficient dominant, ni le discriminant. On peut aussi chercher les polynômes satisfaisant $\mathrm{Disc}P = f^2\mathrm{Disc}K$, où $f = \mathrm{Ind}\, P$ est l'indice de P.

Mais le discriminant d'un polynôme est un invariant pour l'action d'un groupe bien plus grand que le seul groupe des translations (isomorphe à $\mathbb{Z}$). En effet, si $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, et $P \in \mathbb{Z}[X]$ est de degré n, alors $P_M = P((aX+b)/(cX+d)) \cdot (cX+d)^n$ est encore dans $\mathbb{Z}[X]$ et $\mathrm{Disc}P = \mathrm{Disc}P_M$. De plus, P et P_M engendrent le même corps de nombres

et ont le même indice. Le discriminant est donc un invariant pour l'action de $SL_2(\mathbb{Z})$. Comme cette action ne préserve pas le coefficient dominant des polynômes, chercher des polynômes entiers de discriminant donné doit naturellement se faire modulo cette action et il faut donc aussi considérer les polynômes non unitaires. S'il existe un polynôme entier (non nécessairement unitaire) ayant un discriminant donné, alors l'action de $SL_2(\mathbb{Z})$ montre qu'il y en une infinité. Toutefois, modulo cette action, il n'y a qu'un nombre fini de classes de polynômes ayant un discriminant fixé : voir [Birch et Merriman 1972].

Quand le polynôme P n'est pas unitaire, de coefficient dominant a_0, l'élément θ n'est en général pas entier. Bien sûr, on peut remplacer θ par $a_0\theta$ pour obtenir un entier algébrique et prendre ses puissances successives, mais le discriminant du système correspondant est multiplié par une grande puissance de a_0. La construction suivante d'un anneau d'entiers de discriminant Disc$P$ à partir de P est bien connue (voir par exemple [Hancock 1964, art. 14, p. 25], ou [Hurwitz 1895] ou encore [Cohen 1993, Ex. 4.15 p. 216]), mais elle semble peu utilisée.

Soit $P = a_0X^n + \cdots + a_n$ un polynôme entier de degré n. Pour plus de simplicité, je suppose ici que l'anneau de base est $\mathbb{Z}$ et que P est irréductible. On travaille alors dans le corps de nombres $K = \mathbb{Q}[X]/P(X)$, dont l'anneau des entiers est noté $\mathbb{Z}_K$. On note θ l'image de X dans $K = \mathbb{Q}[X]/P(X)$. Dans [T5], je travaille dans un cadre plus général.

On définit les polynômes entiers

$$\begin{aligned} P_0 &= a_0 \\ P_1 &= a_0X + a_1 \\ &\vdots \\ P_{n-1} &= a_0X^{n-1} + a_1X^{n-2} + \cdots + a_{n-1} \end{aligned}$$

Les nombres $P_0(\theta), \ldots, P_{n-1}(\theta)$ sont des entiers algébriques de K. On note $\mathbb{Z}_P$ le $\mathbb{Z}$–module engendré par $1, P_1(\theta), P_2(\theta), \ldots, P_{n-1}(\theta)$ (attention, on a bien pris 1 à la place de $P_0 = a_0$). Lorsque P est unitaire, on a $\mathbb{Z}_P = \mathbb{Z}[\theta]$. Dans [T9], on montre plus généralement que $\mathbb{Z}_P = \mathbb{Z}[\theta] \cap \mathbb{Z}[\theta^{-1}]$. Ce module est en fait un sous–anneau de $\mathbb{Z}_K$ et son discriminant est exactement Disc$P$. Dans [T5], je montre que l'anneau $\mathbb{Z}_P$ ne change pas lorsque P est transformé en P_M pour $M \in SL_2(\mathbb{Z})$, d'où son nom d'*anneau invariant*. Il s'agit donc d'un invariant plus fin que le discriminant de P. On a par exemple,

$$\mathrm{Disc}P = [\mathbb{Z}_K : \mathbb{Z}_P]^2 \mathrm{Disc}K \ .$$

S'il est bien connu que tous les anneaux d'entiers des corps quadratiques sont de la forme $\mathbb{Z}[\theta]$, cela n'est plus vrai pour les corps cubiques. Toutefois, grâce à une construction de [Delone et Feddeev 1940], on voit qu'ils sont tous de la forme $\mathbb{Z}_P$. De telles constructions n'existent plus en dimension supérieure et, dans [T5], je montre que, dans certains corps, on ne peut pas avoir $\mathbb{Z}_K = \mathbb{Z}_P$. Plus précisément, je montre le théorème :

Théorème I *Soit $K/\mathbb{Q}$ une extension cyclique de degré premier $l \geqslant 5$ de conducteur $f \notin \{2l+1, l^2, l^2(2l+1)\}$. Si P est un polynôme entier dont une racine engendre K, alors on a $[\mathbb{Z}_K : \mathbb{Z}_P] > 1$.*

Ce résultat est une généralisation au cas des polynômes non unitaires d'un résultat de [Gras 1986]. Grâce à la méthode que j'introduis, je peux même montrer dans les mêmes conditions, si le degré l est fixé ainsi qu'un entier non nul m, il n'existe qu'un nombre fini d'extensions cycliques L/K pour lesquelles $[\mathbb{Z}_K : \mathbb{Z}_P] = m$ est possible.

2 La classe invariante

Pour étudier les polynômes entiers modulo l'action de $SL_2(\mathbb{Z})$, il est préférable d'utiliser le langage des formes binaires homogènes de degré n. Nous avons à notre disposition deux invariants : le discriminant Disc$P$ et l'anneau invariant $\mathbb{Z}_P$. Dans le cas des formes quadratiques, la théorie de Gauss montre que ces deux invariants ne suffisent pas à distinguer les classes, à cause des fameux groupes de classes de formes quadratiques, que l'on relie aujourd'hui à la théorie plus moderne des groupes de classes d'idéaux des corps de nombres quadratiques. Dans [T6], je propose de relier les classes de formes binaires de degré quelconque à certaines classes dans les groupes de classes des corps de nombres. Contrairement au cas quadratique, cette correspondance n'est en général ni surjective, ni injective, mais elle permet de préciser encore un peu la liste des invariants algébriques associés à une classe de formes binaires.

La construction est la suivante : on montre d'abord que le $\mathbb{Z}$–module $\mathfrak{B}$ engendré par $P_0, P_1(\theta), P_2(\theta), \ldots, P_{n-1}(\theta)$ est un idéal entier inversible de $\mathbb{Z}_P$, de norme exactement a_0. De même, le $\mathbb{Z}$–module $\mathfrak{A}$ engendré par $\theta P_0, \theta P_1(\theta), \theta P_2(\theta), \ldots, \theta P_{n-1}(\theta)$ est un idéal entier inversible de $\mathbb{Z}_P$, de norme a_n. Ces idéaux sont premiers entre eux et la relation $\mathfrak{A} = \theta\mathfrak{B}$ montre que $\mathfrak{A}$ est l'idéal numérateur de θ et $\mathfrak{B}$ son dénominateur. Dans le groupe de classes $Cl(\mathbb{Z}_P)$, on a clairement $[\mathfrak{A}] = [\mathfrak{B}]$. Pour tout $M \in SL_2(\mathbb{Z})$, on a $\mathbb{Z}_P = \mathbb{Z}_{P_M}$, ce qui permet de comparer les classes de $\mathfrak{A}$ et $\mathfrak{A}_M$ dans $Cl(\mathbb{Z}_P)$. Dans [T6], je montre que l'on a toujours $[\mathfrak{A}] = [\mathfrak{A}_M]$. Nous avons ainsi un nouvel invariant ($[\mathfrak{A}]$, *la classe invariante*), qui permet dans certains cas de montrer que deux formes binaires de même discriminant et même anneau invariant ne sont pas équivalentes par $SL_2(\mathbb{Z})$.

3 Décomposition des idéaux

Dans un travail commun avec I. Delcorso et R. Dvornicich de Pise [T9], nous montrons comment utiliser les outils décrits dans les parties §1 et §2 pour travailler dans l'anneau $\mathbb{Z}_P$ avec un polynôme P non unitaire. En particulier, nous étendons le résultat de Kummer donnant la décomposition des nombres premiers p en produit d'idéaux premiers, à partir de la factorisation modulo p de la forme homogène $P(x, y)$.

Si la factorisation de $P(x, y)$ modulo p est donnée par

$$P(x, y) \equiv \prod_i P_i(x, y)^{e_i} \mod p \ ,$$

les formes P_i étant irréductibles modulo p, on définit les idéaux

$$\mathfrak{p}_i = p\mathbb{Z}_P + \mathfrak{B}^{f_i} P_i(\theta, 1)$$

et

$$\mathfrak{q}_i = p\mathbb{Z}_P + \mathfrak{B}^{e_i f_i} P_i^{e_i}(\theta, 1) \ .$$

Les $\mathfrak{p}_i$ sont des idéaux entiers premiers entre eux deux à deux, mais ils ne sont pas nécessairement inversibles. Les $\mathfrak{q}_i$ sont des idéaux entiers inversibles premiers entre eux deux à deux, qui satisfont $\mathfrak{p}_i^{e_i} \subset q_i \subset \mathfrak{p}_i$.

Théorème II *La décomposition de $p\mathbb{Z}_P$ en idéaux primaires est donnée par*

$$p\mathbb{Z}_P = \prod_i \mathfrak{q}_i \ .$$

Si p ne divise pas l'indice $[\mathbb{Z}_K : \mathbb{Z}_P]$, alors on a $\mathfrak{p}_i^{e_i} = q_i$ et la décomposition de $p\mathbb{Z}_P$ en idéaux premiers est donnée par

$$p\mathbb{Z}_P = \prod_i \mathfrak{p}_i^{e_i} \ .$$

L'originalité de ce théorème est qu'il considère les diviseurs premiers du coefficient dominant a_0 comme des premiers ordinaires. À partir de la factorisation du discriminant Disc$P$, il faut être capable de décider si un facteur premier divise $[\mathbb{Z}_K : \mathbb{Z}_P]$ et si c'est le cas, d'agrandir $\mathbb{Z}_P$ d'un facteur au moins p. En utilisant le théorème de Zassenhaus ([Cohen 2000, Prop. 2.4.4]), nous montrons aussi dans [T9] une généralisation du critère de Dedekind ([Cohen 1993, Th. 6.1.4]) pour les polynômes non unitaires.

Comme application de ces résultats, nous considérons dans [T9] la notion d'indice généralisé d'un corps de nombres K, défini comme le pgcd des indices $[\mathbb{Z}_K : \mathbb{Z}_P]$. Nous donnons une description précise des facteurs premiers de cet indice. Nous montrons en particulier que si l'indice généralisé est divisible par un nombre premier p, alors $p \leqslant [K : \mathbb{Q}] - 2$. Pour la notion classique d'indice d'un corps de nombres (celle qui ne considère que les polynômes unitaires, voir [Narkiewicz 1990, Ch. 4, Th. 4.13]), on a seulement $p \leqslant [K : \mathbb{Q}] - 1$.

Chapitre IV

Équations quadratiques

Dans ce chapitre, on considère une forme quadratique Q en n variables $x_1, \ldots, x_n$, à coefficients dans un corps K (Q est un polynôme homogène de degré 2 de $K[x_1, \ldots, x_n]$). Les corps considérés seront toujours des corps de nombres, mais presque toujours $\mathbb{Q}$. L'objectif est de trouver une solution non triviale de l'équation $Q(x_1, \ldots, x_n) = 0$ dans K^n. Bien sûr, pour résoudre cette équation diophantienne, on pourra être amené à localiser, c'est–à–dire à travailler dans $\mathbb{R}$ ou $\mathbb{C}$, ou dans un corps p–adique $\mathbb{Q}_p$, ou plus simplement dans un corps résiduel (ici un corps fini $\mathbb{F}_p$ ou $\mathbb{F}_q$).

Le principal résultat théorique lié à ce problème est le théorème de Hasse–Minkowski, aussi appelé principe local–global.

Théorème (Hasse–Minkowski) *Soit K un corps de nombres. L'équation $Q(x_1, \ldots, x_n) = 0$ admet une solution dans $K^n \setminus (0, \ldots, 0)$ si et seulement si elle admet une solution non triviale localement partout.*

Pour le cas $K = \mathbb{Q}$, on trouve des preuves classiques, qui sont effectives, par exemple dans [Serre 1988] ou dans [Cassels 1978]. Pour le cas d'un corps de nombres quelconque K, la preuve est beaucoup plus abstraite et fait appel à la théorie du corps de classes (voir [Gras 2003]). Ainsi, pour connaître l'existence de solutions globales (c'est–à–dire de solutions dans K^n), il suffit de tester l'existence de solutions locales, ce qui se fait par des symboles locaux (voir par exemple [Serre 1968]). La théorie des symboles locaux donne des critères particulièrement simples. En effet, un nombre fini de tests est suffisant, et chaque test peut être rapidement effectué à l'aide des symboles de Hilbert et des symboles de Legendre (voir aussi [Cohen 1993]).

Pour la plupart des applications, il n'est toutefois pas suffisant de connaître l'existence d'une solution, on veut être capable de construire explicitement une solution ou plusieurs solutions, et même parfois toutes les solutions. Pour cela, le théorème de Hasse–Minkowski est insuffisant. Cet aspect explicite (algorithmique) des équations quadratiques a motivé une partie de mes travaux et c'est l'objectif de ce chapitre. Commençons par la question de la construction d'une solution particulière.

Lorsque $n = 1$, la question est sans intérêt. Lorsque $n = 2$, le problème est équivalent à celui de trouver des racines carrées dans un corps. Dans le cas des corps de nombres, il

est très facile de résoudre ce problème, par exemple en calculant des approximations réelles ou complexes ou en utilisant des algorithmes plus élaborés (mais aussi plus efficaces) de factorisation des polynômes dans les corps de nombres (voir [Belabas 2004]).

Pour les autres cas, on notera Δ le déterminant de la matrice de Gram de Q. Lorsque $\Delta = 0$, on résout facilement l'équation par algèbre linéaire, et donc on supposera dorénavant que $\Delta \neq 0$. Quitte à multiplier Q par un entier non nul, on supposera aussi que les coefficients de Q sont des entiers (algébriques).

1 Points rationnels sur les coniques

Le cas le plus étudié, à la fois sur le plan théorique et sur le plan pratique, est le cas $n = 3$ qui correspond géométriquement à la question de trouver des points rationnels sur des coniques. Ce point de vue est le plus naturel, mais nous ne l'utiliserons pas immédiatement, au profit de deux autres : celui de la résolution des équations aux normes dans les extensions quadratiques et celui de la recherche de vecteurs courts dans les réseaux définis par des formes quadratiques (définies ou indéfinies).

La réduction de Gauss montre que l'on peut toujours se ramener au cas où l'équation est diagonale, c'est–à–dire de la forme $ax^2 + by^2 + cz^2 = 0$: il s'agit alors de l'équation de Legendre. Cette équation très classique (au moins sur $\mathbb{Q}$) a déjà été étudiée par Lagrange et Legendre, dont on reproduit aujourd'hui encore les méthodes de résolution : [Serre 1988, Ch IV §3] ou [Smart 1998, Ch. IV §3.3]. Pour comprendre cette méthode, il faut remarquer que l'équation est équivalente à une équation de la forme $x^2 - Ay^2 = Bz^2$, c'est–à–dire à une équation aux normes dans une extension quadratique. Plus précisément, dans l'extension $K(\sqrt{A})/K$, on cherche un élément de norme B.

Sur $\mathbb{Q}$, l'algorithme est alors le suivant : on calcule une racine carrée de A modulo B, et on en déduit (x_0, y_0) tels que $x_0^2 - Ay_0^2$ soit de la forme BB' où B' est plus petit que B. En utilisant la multiplicativité de la norme, on se ramène à l'équation $x^2 - Ay^2 = B'z^2$. Dès que B devient plus petit que A, on échange le rôle de A et B (l'équation est symétrique en A et B). À la fin, il ne reste plus qu'à résoudre $x^2 - y^2 = -z^2$ ou $x^2 - y^2 = z^2$, ce qui est immédiat.

Cet algorithme a l'avantage d'être simple à décrire et à comprendre. Il ne donne en général pas une petite solution (au sens de [Holzer 1950]), mais on peut utiliser la réduction de Mordell ([Mordell 1969]) pour trouver une petite solution à partir d'une grande. Dans ma thèse ([T1]), j'ai proposé des formules pour que des simplifications se produisent dans la construction de la solution, et ainsi éviter que la solution ne soit démesurément grande. J'ai aussi essayé de généraliser l'algorithme au cas des corps de nombres. Bien que je ne sache pas le démontrer, en pratique, cela m'a permis de résoudre de nombreuses équations. En combinant cette méthode avec la méthode des corps de nombres que j'ai décrite au chapitre II et dans [T3], on obtient une efficacité plus raisonnable que dans [Pohst 2000] (voir aussi [Fieker 1997] et [Fieker, Jurk et Pohst 1997]).

Dans la suite, je ne considérerai plus le cas général des corps de nombres, mais seulement celui de $\mathbb{Q}$, où l'on peut utiliser les outils de la géométrie des nombres.

Si l'on ne dispose d'aucun indice, le calcul d'une racine carrée de A modulo B se fait en factorisant B, puis en calculant des racines carrées de A suivant des modules premiers et en reconstruisant la solution avec le théorème Chinois. Pour le calcul des racines carrées modulo un nombre premier, on peut utiliser l'algorithme probabiliste de Shanks (voir [Cohen 1993]) ou les algorithmes déterministes décrits dans [Woestijne 2005]. Mais la factorisation prend la plus grande part du temps d'exécution, et il est indispensable de réduire le nombre de factorisations. Il semble impossible d'éviter de factoriser A et B, pour les valeurs initiales de A et B, car ce sont ces facteurs premiers qui donnent l'existence de solutions locales. De plus, si on savait résoudre l'équation de Legendre, sans factoriser son déterminant AB, alors on saurait calculer des racines carrées suivant un module composé, et en utilisant un algorithme comme le crible quadratique (voir [Pomerance 1982]), on saurait factoriser AB. Il faut donc chercher à éviter les autres factorisations, celles pour lesquelles les facteurs premiers du coefficient B' ainsi construit sont sans rapport avec le problème initial. En particulier, il n'est pas rare dans les applications que l'on connaisse à l'avance la factorisation de A et B, mais certainement pas celle de B'. Dans [Cochrane et Mitchell 1998] et [Cremona et Rusin 2003], on trouve des algorithmes qui permettent de supprimer toutes ces factorisations inutiles et d'obtenir une complexité polynômiale dès que la factorisation du déterminant initial est connue. En pratique, ces algorithmes sont vraiment efficaces.

Dans [Cochrane et Mitchell 1998], il est remarqué que les solutions de l'équation de Legendre $ax^2 + by^2 + cz^2 = 0$ se trouvent dans un réseau de co–volume $2|abc|$ (défini par des congruences modulo a, b and c) et qu'un plus court vecteur dans ce réseau donne une solution. En utilisant un algorithme pour trouver des petits vecteurs dans un réseau de dimension 3, (comme [Vallée 1987] ou LLL dans [Lenstra, Lenstra et Lovász 1982], [Cohen 1993, §2.6]), on trouve rapidement une solution. Bien que cela ne soit pas formulé en ces termes, l'idée principale de l'algorithme de [Cochrane et Mitchell 1998] est de réduire une forme quadratique définie positive unimodulaire. Cette stratégie est proche d'une autre méthode bien plus ancienne, que nous n'avons pas encore mentionnée : celle de Gauss ([Gauss 1953, §272, 274, 294]). En effet, Gauss attache à la forme quadratique $ax^2 + by^2 + cz^2$ une autre forme quadratique h de déterminant -1, à laquelle il applique également un algorithme de réduction, pour déduire une solution de l'équation initiale. La principale différence est que dans ce cas, la forme quadratique à réduire n'est pas définie positive. Bien que l'algorithme de Gauss soit relativement efficace (et incomparablement plus rapide que la méthode de Legendre), cet algorithme reste peu connu. Dans [Cassels 1978, p.98], Cassels écrit à propos de cet algorithme : «Gauss's proof of the existence of h is explicit but not very transparent, which perhaps explains why it is not often reproduced in the literature ».

Pour réduire une forme quadratique indéfinie Q, Gauss a proposé un algorithme : celui-ci est très spécifique à la dimension 3. Pour les dimensions supérieures, on peut utiliser la transformation d'Hermite (voir [Cassels 1971, II.2.2]) qui consiste à diagonaliser Q, à prendre les valeurs absolues des coefficients pour obtenir une forme définie positive et à réduire la nouvelle forme ainsi obtenue en appliquant au choix l'un des algorithmes de réduction des formes définies positives. Par exemple, en appliquant la transformation d'Hermite (suivie de LLL) à la forme h de déterminant -1 construite par Gauss, on trouve exactement l'algorithme de [Cochrane et Mitchell 1998]. Dans [T7], je propose un algorithme de réduction des formes

indéfinies. Cet algorithme imite l'algorithme LLL ([Lenstra, Lenstra et Lovász 1982]) et travaille directement sur la forme indéfinie, sans utiliser la transformation d'Hermite.

Théorème I *Soit Q une forme quadratique entière (de dimension n), de déterminant $\Delta \neq 0$. En appliquant l'algorithme LLL indéfini, avec un paramètre $\frac{1}{4} < c < 1$, on obtient*

– soit une solution non triviale de $Q(X) = 0$,

– soit une base de $(\mathbf{b}_1, \dots, \mathbf{b}_n)$ de $\mathbb{Z}^n$ qui est réduite au sens de LLL, avec en particulier

$$1 \leqslant |Q(\mathbf{b}_1)|^n \leqslant \gamma^{n(n-1)/2}|\Delta| \ ,$$

où $\gamma = \left(c - \frac{1}{4}\right)^{-1} > \frac{4}{3}$.

Cet algorithme termine après un nombre polynômial d'étapes.

De plus, si Q est indéfinie, on a

$$1 \leqslant |Q(\mathbf{b}_1)|^n \leqslant \frac{3}{4}\gamma^{n(n-1)/2}|\Delta| \ .$$

Cela donne un algorithme naturellement adapté aux formes indéfinies et au moins aussi efficace que LLL. On voit en particulier, que les formes indéfinies se réduisent mieux que les formes définies. En pratique, les résultats sont très satisfaisants, mais pour des questions de facilité de programmation, il peut être préférable de ne pas reprogrammer complètement LLL dans sa version indéfinie, mais seulement la transformation d'Hermite, puis d'utiliser une des très bonnes versions du LLL classique qui existent déjà, comme dans `gp`, `NTL` ou [Nguyễn et Stehlé 2005]. Il est possible que la qualité de la réduction soit moindre, mais peut-être toutefois suffisante.

Si l'on veut résoudre une équation quadratique non diagonale $Q(x, y, z) = 0$, on peut vouloir utiliser les méthodes précédentes en se ramenant à une équation diagonale. Il faut alors être capable de factoriser le nouveau déterminant, ce qui revient à factoriser l'ancien déterminant, ainsi que des facteurs parasites faisant intervenir les coefficients de Q. Comme ces facteurs parasites sont souvent trop grands pour être factorisés, la méthode est impraticable. Il faut donc être capable de résoudre directement les équations non diagonales. Dans [T7], je propose un algorithme en deux étapes : minimisation et réduction.

1– Minimisation : en utilisant la connaissance des facteurs premiers p du déterminant Δ de Q, je suis capable soit de montrer qu'il n'existe pas de solution locale pour un certain p, soit de trouver des solutions locales en chaque p, à partir desquelles je peux construire une nouvelle forme quadratique Q', équivalente (sur $\mathbb{Q}$) à un multiple de Q et de déterminant $\Delta' = -1$:

Théorème II *Soit $Q(x, y, z)$ une forme quadratique entière de déterminant $\Delta \neq 0$ et telle que l'équation $Q = 0$ admette une solution non triviale dans $\mathbb{Q}_p$, pour chaque nombre premier $p \mid \Delta$. Alors, il existe une matrice V à coefficients entiers telle que*

$$\begin{aligned} & \det(V) = \Delta \\ & Q' = \frac{1}{\Delta} V^t Q V \text{ a des coefficients entiers} \\ \text{et} \quad & \det(Q') = \pm 1 \ . \end{aligned}$$

De plus, si la factorisation de Δ est connue, il existe un algorithme pour construire V en au plus $O(\ln^4(|\Delta|))$ opérations. Il existe une constante $\kappa > 0$ telle que les coefficients de V soient de l'ordre de $O(|\Delta|^\kappa)$.

2– Réduction : en utilisant l'algorithme LLL indéfini de [T7] ou une transformation d'Hermite suivie de l'algorithme LLL classique, on trouve une solution de $Q' = 0$.

En combinant les théorèmes I et II, je montre que mon algorithme pour résoudre les équations quadratiques (non diagonales), donne une solution en temps polynômial. Comme me l'a fait remarquer Cremona, un algorithme très proche a été proposé par [Ivanyos et Szántó 1996]. Cet algorithme, dont je n'avais pas la connaissance lorsque j'ai proposé le mien, a un traitement particulier pour les vecteurs isotropes. La conséquence est que la borne donnée par [Ivanyos et Szántó 1996] pour une forme indéfinie est bien moins bonne : ils montrent $|Q(\mathbf{b}_1)|^n < 2^{n(n-1)}|\Delta|$ alors que LLL donne $|Q(\mathbf{b}_1)|^n < 2^{n(n-1)/2}|\Delta|$ (avec le choix de la constante $c = \frac{3}{4}$). Avec le théorème I, j'obtiens une borne meilleure encore $|Q(\mathbf{b}_1)|^n < \frac{3}{4}2^{n(n-1)/2}|\Delta|$.

2 Paramétrisation des coniques et groupes de classes

Quand on a un point rationnel A sur une conique $\mathcal{C}$, c'est–à–dire une solution non triviale de $Q(x, y, z) = 0$, on peut vouloir paramétrer toutes les solutions. On obtient une telle paramétrisation en utilisant la méthode classique de la sécante, comme le montre la figure IV.1 (voir aussi [Smart 1998, Ch IV]) : on fait passer par A une droite D_s de pente rationnelle $s \in \mathbb{P}^1$ et cette droite rencontre la conique en un deuxième point P_s. Il est bien connu que ces points paramétrisent quadratiquement l'ensemble des points rationnels de la conique.

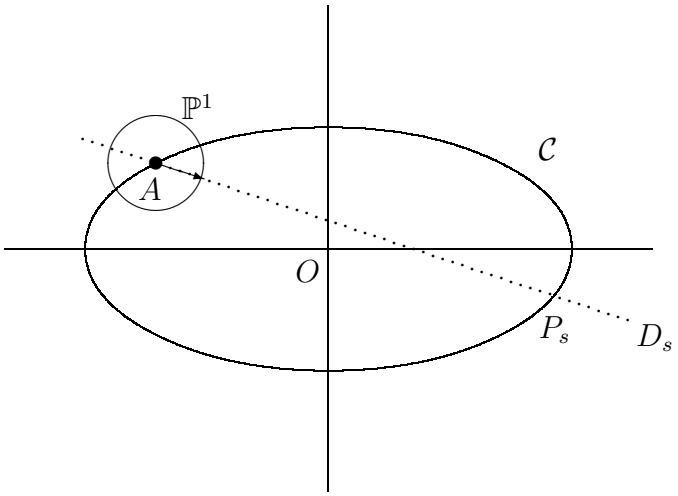

Fig. IV.1 – méthode de la sécante.

Autrement dit, si l'on a une solution particulière (x_0, y_0, z_0) d'une équation quadratique $Q(x, y, z) = 0$, on peut construire trois formes quadratiques $X(s)$, $Y(s)$ et $Z(s)$ (il est

souvent préférable de les écrire sous une forme homogène $X(s,t)$, $Y(s,t)$ et $Z(s,t)$) telles que $Q(X(s),Y(s),Z(s))=0$ et telles que toute solution (x,y,z) soit proportionnelle à une solution de la forme $(X(s),Y(s),Z(s))$. Pour écrire les formules de X,Y et Z en fonction de s, il faut faire un aller–retour entre le modèle projectif et le modèle affine. Cet aller–retour brise la symétrie entre x_0, y_0 et z_0 et quand on calcule les discriminants des trois formes quadratiques X,Y et Z (ce calcul est fait par exemple dans [Cremona et Rusin 2003] et [T8]), on trouve qu'ils sont tous égaux à une constante (qui ne dépend que de Q) multipliée par z_0^2. Ce facteur z_0^2 n'est pas naturel dans ce problème et il faut chercher à le supprimer. En factorisant z_0, on peut éliminer un à un chaque facteur premier de z_0, avec des arguments de même nature que la minimisation définie dans la partie précédente 1. Une méthode plus efficace, n'utilisant que l'algèbre linéaire modulo z_0^2, est décrite dans [Cremona et Rusin 2003], mais elle est restreinte au cas diagonal ou semi-diagonal. Dans [T8], j'exprime la relation polynômiale $Q(X,Y,Z)=0$ sous forme matricielle, ce qui me permet de proposer la construction d'une paramétrisation ayant directement les bons invariants dans le cas général, que l'on peut exprimer en fonction des coefficients de Q exclusivement :

Théorème III *Soit $Q(x,y,z)$ une forme quadratique entière, de déterminant $\Delta\neq 0$. Soit (x_0,y_0,z_0) une solution particulière non triviale de $Q=0$. On peut construire une paramétrisation des solutions de la forme $x=\lambda X(s,t)$, $y=\lambda Y(s,t)$, $z=\lambda Z(s,t)$, où $\lambda\in\mathbb{Q}^*$ et $(s,t)\in\mathbb{Q}^2\setminus(0,0)$ et où X,Y,Z sont trois formes quadratiques entières, ayant pour discriminants*

$$\begin{aligned}\mathrm{Disc}X&=-4(Q_{2,2}Q_{3,3}-Q_{2,3}^2)\\ \mathrm{Disc}Y&=-4(Q_{1,1}Q_{3,3}-Q_{1,3}^2)\\ \mathrm{Disc}Z&=-4(Q_{1,1}Q_{2,2}-Q_{1,2}^2)\end{aligned}$$

Les résultats de [T8] donnent non seulement les valeurs de ces discriminants, mais aussi des relations entre les formes quadratiques X,Y et Z, dont en particulier les valeurs exactes des résultants deux à deux. Le point clé de la construction liée à ce théorème est la construction d'une matrice entière 3×3, dont la première colonne est (x_0,y_0,z_0) et dont le déterminant vaut 1. Plus généralement, si la matrice que l'on construit est de déterminant $d\neq 0$, alors il suffit de multiplier les valeurs des discriminants par d^2 pour que le théorème III reste vrai. En particulier, pour un corps de nombres, on voit que les discriminants des formes X,Y et Z ne dépendent que de Q et du groupe de classes du corps, mais pas de la solution particulière (x_0,y_0,z_0). Si l'on utilise la notion de forme quadratique relative définie dans [Cohen 2000, §2.6], les discriminants annoncés dans le théorème III restent vrais, sans facteur d supplémentaire.

Le cas particulier de l'équation semi-diagonale $Ax^2+Bxy+Cy^2=z^2$ sur $\mathbb{Q}$ est spécialement intéressant. Posons ici $\delta=B^2-4AC\neq 0$ (on suppose aussi que δ est non nul et sans sans facteur carré). D'après le théorème III, si l'équation admet une solution rationnelle non triviale, alors on peut trouver une paramétrisation avec $z=\lambda Z(s,t)$ où $\mathrm{Disc}Z=\delta$. Autrement dit, à partir d'une forme quadratique binaire de discriminant δ, on en fabrique une autre de même discriminant. Nous reviendrons un peu plus loin sur l'interprétation de cette construction.

L'équation $Ax^2 + Bxy + Cy^2 = z^2$ a été étudiée par de nombreux auteurs, dont [Cremona et Rusin 2003] et même [Gauss 1953]. On a déjà vu qu'elle pouvait s'interpréter comme une équation aux normes dans l'extension $\mathbb{Q}(\sqrt{\delta})/\mathbb{Q}$. Dans le chapitre II, nous avons montré que la connaissance du groupe de classes de ce corps permettait de résoudre cette équation. Inversement, d'après la théorie des genres (voir [Gras 2003]), on peut aussi utiliser la résolution de cette équation pour en déduire des informations sur la 2–partie du groupe de classes de $\mathbb{Q}(\sqrt{\delta})$ (notons ce groupe $Cl_2(\delta)$). Plus concrètement, on peut construire complètement $Cl_2(\delta)$, en résolvant successivement plusieurs équations de la forme $Ax^2 + Bxy + Cy^2 = z^2$ avec $B^2 - 4AC = \delta$. Ce calcul a été initié par [Gauss 1953, Art. 286], puis développé dans [Shanks 1971], [Lagarias 1989] et [Bosma et Stevenhagen 1996]. La stratégie est la suivante : on connaît un système de générateurs de $Cl_2(\delta)$ (il s'agit des formes ambiges), ensuite il faut construire, quand cela est possible, les racines carrées des générateurs. En procédant ainsi, on construit de proche en proche $Cl_2(\delta)[2]$, $Cl_2(\delta)[4]$, $Cl_2(\delta)[8]$, ..., jusqu'à obtenir $Cl_2(\delta)$ tout entier. Le point crucial est donc de calculer la racine carrée d'une forme $Ax^2+Bxy+Cy^2$ de discriminant δ. Les auteurs cités précédemment, ainsi que [Hardy et Williams 1993], montrent que l'on peut construire cette racine carrée à partir d'une solution particulière de $Ax^2 + Bxy + Cy^2 = z^2$. En combinant ces résultats avec le théorème III, j'ai pu montrer dans [T8] le lien extrêmement fort qu'il y a entre ces deux aspects des mêmes équations :

Théorème IV *Soient $Q = Ax^2 + Bxy + Cy^2$ et Z deux formes quadratiques entières primitives de discriminant δ (non carré). Les propositions suivantes sont équivalentes :*

(i) on a $[Z]^2 = [Q]^{\pm 1}$ dans $Cl_2(\delta)$,

(ii) on peut trouver deux formes quadratiques entières $X(s,t) = x_1s^2 + 2x_2st + x_4t^2$ et $Y(s,t) = y_1s^2 + 2y_2st + y_4t^2$ (avec x_2 et $y_2 \in \mathbb{Z}$), telles que les solutions de $Q(x,y) = 1$ soient paramétrées par $x = \dfrac{X(s,t)}{Z(s,t)}$ et $y = \dfrac{Y(s,t)}{Z(s,t)}$.

(iii) on peut trouver deux formes quadratiques entières $X(s,t) = x_1s^2 + 2x_2st + x_4t^2$ et $Y(s,t) = y_1s^2+2y_2st+y_4t^2$ (avec x_2 et $y_2 \in \mathbb{Z}$), non proportionnelles, telles que $Q(X,Y) = Z(s,t)^2$.

Autrement dit, le problème de calculer un racine carrée dans $Cl_2(\delta)$ et celui de paramétrer les solutions de $Q(x,y) = 1$ ne sont pas seulement proches, ils sont identiques : la forme quadratique construite pour résoudre un problème résout aussi l'autre. L'algorithme que l'on déduit pour la construction de groupe $Cl_2(\delta)$ n'est donc pas nouveau, mais on en a une nouvelle interprétation. Dans [Lagarias 1989], il est montré que cet algorithme finit en temps polynômial : il nous sera très utile au paragraphe suivant.

3 Équations quadratiques en dimension supérieure

Jusqu'à présent, je n'ai utilisé le théorème de Hasse–Minkowski qu'en dimension $n \leqslant 3$. Je vais maintenant envisager le cas $n \geqslant 4$, pour le corps des rationnels $K = \mathbb{Q}$. D'après ce théorème, un petit nombre de tests locaux suffit à déduire l'existence d'une solution non

triviale. Pour les grandes dimensions $n \geqslant 5$, il suffit même de déterminer la signature réelle de la forme quadratique, et il n'y a aucune condition p–adique ! Une fois de plus, si l'on veut construire explicitement une solution non triviale, ce théorème d'existence n'est pas la fin du problème. À ma connaissance, aucune étude algorithmique n'a été faite pour résoudre ces équations. La preuve classique du théorème de Hasse–Minkowski (voir [Serre 1988] ou [Cassels 1978]) distingue généralement trois cas, suivant la valeur de n : $n = 3$, $n = 4$, puis $n \geqslant 5$, le cas $n = 4$ étant généralement le plus difficile. Pour l'aspect algorithmique, nous allons voir que le passage du cas $n = 3$ au cas $n = 4$ requiert un effort supplémentaire particulièrement important. Une astuce permet de passer de $n = 4$ à $n \geqslant 5$, à moindre coût. Commençons par le cas $n = 4$.

La preuve classique du théorème de Hasse–Minkowski dans le cas $n = 4$ consiste à se ramener à résoudre deux équations quadratiques en dimension 3. En effet, on peut diagonaliser la forme quadratique, c'est–à–dire se ramener au cas $ax_1^2 + bx_2^2 = cx_3^2 + dx_4^2$, puis, à l'aide du théorème de Dirichlet sur les nombres premiers dans les suites arithmétiques, trouver un nombre m représenté simultanément par les deux formes binaires $ax_1^2 + bx_2^2$ et $cx_3^2 + dx_4^2$ et enfin résoudre les deux équations $ax_1^2 + bx_2^2 = m = cx_3^2 + dx_4^2$. D'un point de vue algorithmique, cette preuve permet effectivement de résoudre une équation quadratique en dimension 4. Mais il y a deux inconvénients majeurs. Comme dans le cas de la dimension 3, la diagonalisation entraîne la nécessité de factoriser d'autres entiers que le seul déterminant de Q. Ce premier inconvénient réduit considérablement le nombre d'équations que l'on peut effectivement résoudre par cette méthode. Le deuxième inconvénient est lié au théorème de Dirichlet. En effet, ce théorème assure l'existence de nombres premiers dans certaines suites arithmétiques, mais il n'est pas effectif et il peut être nécessaire de tester un grand nombre de candidats avant de trouver un nombre premier convenable. De plus, les tests de primalité, bien que nettement plus efficaces que les algorithmes de factorisation, sont encore limités à des nombres de quelques centaines de chiffres (voir par exemple [Crandall et Pomerance 2002] ou [Granville 2005]).

Dans [T11], je montre qu'il est possible de généraliser au cas $n = 4$ l'algorithme donné dans [T7] pour $n = 3$, mais seulememt lorsque le déterminant Δ de la forme quadratique Q est égal, au signe près, à un carré. L'algorithme se fait encore en trois étapes :

- factorisation du déterminant de Q,
- minimisation (on se ramène au cas d'une forme quadratique entière Q' de déterminant ± 1),
- réduction (on applique l'algorithme de réduction LLL indéfini pour trouver un zéro de Q').

Lorsque $|\Delta|$ n'est pas un carré, l'étape de minimisation est impossible car on ne peut supprimer que les facteurs carrés du déterminant et donc l'algorithme ne peut pas s'appliquer en général. Dans [Cassels 1959] et [Cassels 1978, §14.7], Cassels donne une nouvelle preuve du théorème de Hasse–Minkowski dans le cas $n = 4$, sans utiliser le théorème de Dirichlet. L'idée principale de Cassels est d'utiliser la connaissance du groupe de classes $Cl_2(\delta)$ et de passer en dimension 6. Dans [T11], je montre comment utiliser cette idée pour donner un algorithme de résolution des équations quadratiques en dimension 4. L'algorithme se

fait en plusieurs étapes :

1– Factoriser le déterminant Δ de Q.

2– Minimiser Q, et se ramener au cas où Δ est sans facteur carré (si on ne peut pas, cela signifie que l'équation n'a pas de solution).

3– Calculer les invariants locaux de Q.

4– Construire le groupe $Cl_2(4\Delta)$, et en extraire une forme binaire Q_2 d'invariants donnés (la valeur exacte de ces invariants est reliée par une formule explicite à ceux de Q).

5– Construire la forme $Q_6 = Q \oplus -Q_2$ de dimension 6, et la minimiser (jusquà ce que son déterminant soit égal à -1).

6– Réduire Q_6 en utilisant l'algorithme LLL indéfini, et en déduire un sous-espace totalement isotrope de dimension 3 pour Q_6.

7– Utiliser l'algèbre linéaire pour en déduire une solution non triviale pour Q.

Dans [T11], nous voyons que la description de cet algorithme requiert beaucoup plus de technique que celui pour la dimension 3. Sa programmation nécessite aussi le recours à de nombreux sous–algorithmes, dont en particulier un pour la construction du groupe de classes $Cl_2(4\Delta)$. Malgré ces difficultés techniques, l'algorithme qui en résulte termine en temps polynômial (sauf pour la factorisation initiale) et s'avère particulièrement efficace. Ainsi, si l'on connaît la factorisation de Δ, on peut sans difficulté résoudre des équations dont les coefficients ont plusieurs centaines de chiffres, et peut–être même plusieurs milliers. Sur la figure IV.2, j'ai représenté le temps d'exécution du programme [T17] pour une forme quadratique de dimension 4, ayant des coefficients aléatoires de l'ordre de 2^t (pour plus de lisibilité du graphique, j'ai séparé le temps utilisé pour la factorisation, `fact`, de celui du reste du programme, `sol`).

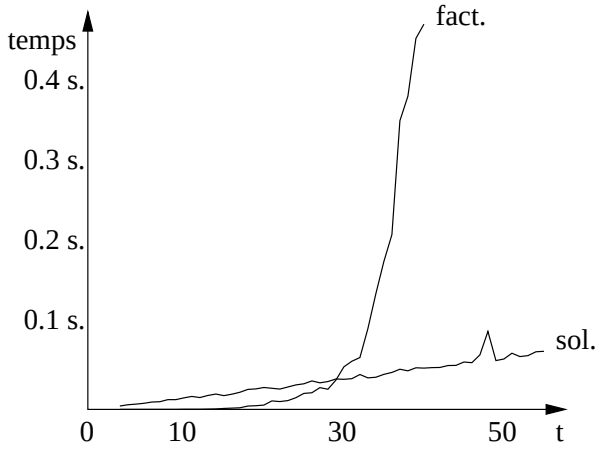

Fig. IV.2 – Performance en dimension 4

Considérons maintenant les équations quadratiques en dimension $n \geqslant 5$. D'après le théroème de Hasse–Minkowski et le théorème de Meyer (voir [Serre 1988]), on sait qu'il suffit que la forme Q soit indéfinie pour que l'équation $Q(x_1, \ldots, x_n) = 0$ admette une solution non triviale. Malheureusement, une telle simplification dans l'énoncé du théorème

sur l'existence d'une solution ne se traduit pas par une simplification de l'algorithme de construction d'une solution particulière. Une légère modification de l'algorithme pour $n = 4$ me permet dans [T11] de traiter le cas $n \geqslant 5$, à condition de distinguer suivant la parité de n :

1– Factoriser le déterminant Δ de Q.

2– Minimiser Q. Si n est impair, alors Δ est sans facteur carré. Si n est pair, il se peut que Δ soit divisible par d^2, auquel cas, il faut continuer avec la forme $Q + dx_{n+1}^2$.

À la fin de cette étape 2, le déterminant de la forme quadratique est sans facteur carré et la suite de l'algorithme est identique à celui pour $n = 4$. On voit en particulier qu'il faut trouver un vecteur isotrope pour une forme quadratique unimodulaire en dimension $n+2$ si n est impair, et $n+3$ si n est pair. On trouve ce vecteur grâce à la réduction par l'algorithme LLL indéfini. Bien que dans la pratique cet algorithme trouve toujours un vecteur isotrope pour les formes unimodulaires jusqu'en en dimension 9, les bornes données par le théorème I sont insuffisantes pour le démontrer. Dans [T10], j'affine l'analyse de l'algorithme LLL indéfini pour montrer que l'on trouve toujours un vecteur isotrope dans ces cas. J'ai ainsi démontré que l'algorithme que je propose peut résoudre toutes les équations quadratiques en dimension $n \leqslant 7$. La complexité est très probablement polynômiale pour n fixé.

Pour les formes quadratiques Q_n en dimension $n \geqslant 8$, on peut toujours appliquer le même algorithme. Avec mon programme [T17], j'ai expérimenté cela sur des millions d'exemples aléatoires jusqu'en dimension 20 : la réduction avec LLL indéfini de la forme unimodulaire Q_{n+2} ou Q_{n+3} a toujours donné un vecteur isotrope et donc l'algorithme a toujours trouvé une solution de $Q_n(x_1, \ldots, x_n) = 0$ en un temps polynômial (pour n fixé). Sur la figure IV.3, je montre le temps de résolution en fonction de n et de la taille des coefficients, dans lequel je n'ai pas compté le temps de la factorisation du déterminant.

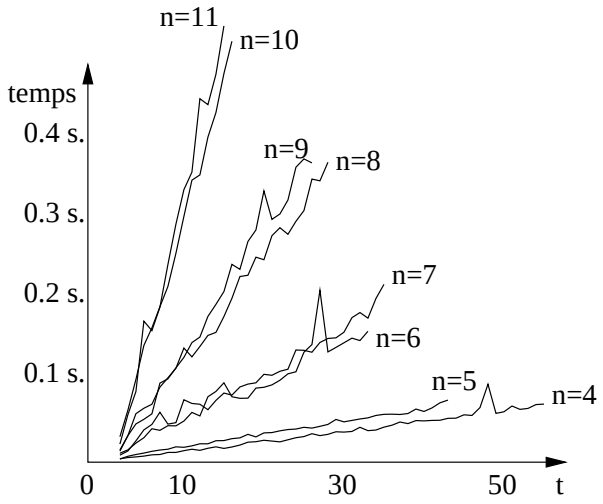

FIG. IV.3 – Performance en grande dimension

Mais il se pourrait que la réduction des formes unimodulaires soit insuffisante et dans ce cas je propose dans [T11] une autre possibilité. La réduction de la forme unimodulaire

Q_{n+2} ou Q_{n+3} donne une nouvelle forme quadratique, dont les coefficients sont majorés uniquement en fonction de n. On peut alors en extraire une forme quadratique indéfinie Q_5, dont les coefficients (et le déterminant) sont bornés uniquement en fonction de n, et qui représente certainement 0 d'après les théorèmes de Hasse–Minkowski et de Meyer. Après avoir factorisé le déterminant de Q_5, on peut résoudre $Q_5 = 0$, et en déduire une solution de $Q_n(x_1, \ldots, x_n) = 0$. La complexité de cet algorithme en fonction de Q ne change pas, mais elle devient assez mauvaise par rapport à n.

Chapitre V

Courbes Elliptiques

À l'occasion de calculs de rang de courbes ellitiques et de leur fameux article [BSD 1963], Birch et Swinnerton–Dyer remarquent que l'une des étapes les plus longues pour la recherche de points sur les courbes elliptiques est la résolution des équations quadratiques. Ayant moi-même expérimenté cela au cours de ma thèse, j'ai cherché à améliorer cette résolution, ce qui a été à l'origine de tous mes travaux décrits dans le chapitre IV. Quoi de plus naturel d'ailleurs que d'avoir besoin de bons algorithmes sur les courbes de genre 0 avant d'en proposer pour les courbes de genre 1 ? En particulier, pour faire de la 2–descente, il faut pouvoir résoudre des équations quadratiques en dimension 3. De même, pour faire de la 4–descente, on doit résoudre des équations quadratiques en dimension 4 (voir [Cremona 1997 b]), et pour la 3–descente des équations quadratiques en dimension 8 (voir [T18]). Une autre étape de la 3–descente consiste à résoudre une équation aux normes cubique, ce qui peut être résolu en utilisant l'arithmétique des corps de nombres (voir [T3] et [T13]) et je suis actuellement en train de mettre au point un nouvel algorithme pour résoudre ces équations, faisant appel à la géométrie des nombres et à des réductions du genre LLL (voir [T19]).

Dans ma thèse [T1], j'ai proposé une version de l'algorithme de la 2–descente pour les courbes elliptiques définies sur les corps de nombres (le programme `gp` complet est publiquement disponible, voir [T14]). Je n'utilise pas pour cela la même approche que le programme `mwrank` de Cremona (voir [Cremona 1997 a]). En effet, celui–ci construit des quartiques à partir de la valeur de leurs invariants et de bornes sur les coefficients : cette métode ne se généralise qu'à des corps de nombres très particuliers (voir [Serf 1995] et [Cremona et Serf 1999]). J'utilise plutôt l'approche qui passe par les corps de nombres (voir [Cremona 2001]). Pour une comparaison entre les deux méthodes, on peut consulter [Djabri et Smart 1998] ou [Smart 1998]. Entre ma thèse [T1] et mon article [T4], puis les résultats énoncés dans [T8], je simplifie largement les formules, ce qui correspond non seulement à une simplification notoire de l'algorithme, mais aussi à la nouvelle possibilité de considérer des familles de tordues quadratiques. Je vais maintenant décrire les principales étapes de la 2–descente, en utilisant la description classique de [Cassels 1991], ainsi bien sûr que celle que je propose dans [T4], mais aussi en tenant compte des améliorations que j'ai apportées grâce à [T7] et [T8]. J'arrêterai ma description après la construction

des quartiques représentant les élements du groupe de Selmer, car je n'ai pas contribué à développer la suite de l'algorithme.

1 2–descente

Soit K un corps de nombres et E une courbe elliptique définie sur K, donnée par une équation de la forme

$$ky^2 = P(x) \ ,$$

où $P(x) = x^3 + Ax^2 + Bx + C$, avec $k \neq 0$, A, B et C sont des entiers de K (on note $\mathbb{Z}_K$ l'anneau des entiers de K). On suppose de plus que le polynôme P est irréductible dans K, c'est–à–dire que $E(K)$ est sans 2–torsion. Dans le corps cubique $L = K[X]/P(X)$, X est une racine de P. Lorsque P n'est pas irréductible, on peut encore travailler dans l'algèbre étale $K[X]/P(X)$ qui est un produit de corps, où la plupart des formules données par la suite se généralisent sans peine. L'application

$$\begin{array}{rlll} \phi : & E(K) & \to L^*/L^{*2} \\ & 0 & \mapsto 1 \\ & (x,y) & \mapsto k(x-X) \end{array}$$

est un morphisme de groupes, dont le noyau est exactement $2E(K)$ (voir [Cassels 1991]). La relation $\mathcal{N}_{L/K}(k(x-X)) = k^3P(x) = (ky)^2$ montre que l'image de ϕ est un incluse dans le noyau de l'application norme $\mathcal{N}_{L/K}$ de L^*/L^{*2} dans K^*/K^{*2}.

Soit S un ensemble fini de places de L, contenant les places infinies. On note

$$L(S,2) = \{\delta \in L^*/L^{*2},\ \forall \mathfrak{P} \notin S, v_{\mathfrak{P}}(\delta) \equiv 0 \pmod 2\} \ .$$

Ce groupe est un groupe fini, que l'on peut déterminer si l'on connaît le S–groupe de classes $Cl_S(L)$ et les S–unités $\mathbb{U}_{L,S}$ de L. En particulier, si S engendre $Cl_2(L)$ (le 2–sous–groupe de Sylow de $Cl(L)$), on a $Cl_{2,S}(L) = 1$ et

$$L(S,2) \simeq \frac{\mathbb{U}_{L,S}}{\mathbb{U}_{L,S}^2}.$$

Dans [T4], je montre le résultat suivant :

Proposition I *Soit S un ensemble fini de places de L, contenant les places inifinies et les idéaux premiers $\mathfrak{P}$ de L au dessus de $\mathfrak{p}$ dans K tels que $\mathfrak{P}|P'(X)$ et $\mathfrak{p}^2|\mathrm{Disc}P$. On suppose aussi que S contient les diviseurs premiers de k. On a*

$$\mathrm{Im}\,\phi \subset L(S,2) \cap \mathrm{Ker}\,\mathcal{N}_{L/K} \ .$$

Cette proposition est une version du théorème faible de Mordell–Weil, qui affirme que $E(K)/2E(K)$ est un groupe fini. Elle montre que $\mathrm{Im}\,\phi$ est inclus dans un autre groupe fini que l'on peut facilement déterminer si l'on connaît bien l'arithmétique de L. Contrairement

aux preuves classiques (voir [Cassels 1991]), on voit qu'il n'est pas nécessaire de prendre tous les diviseurs premiers de 2Disc$P$, mais seulement ceux dont le carré divise Disc$P$. On peut aussi voir [Schaefer 1996] et [Schaefer et Stoll 2004] pour une description de ces premiers en termes de nombres de Tamagawa.

Fixons maintenant un élément $\delta \in L(S,2) \cap \operatorname{Ker} \mathcal{N}_{L/K}$, où S satisfait les hypothèses de la proposition I. On cherche à savoir si $\delta \in \operatorname{Im} \phi$, c'est–à–dire si l'on peut trouver un élément $z \in L^*$ tel que δz^2 soit de la forme $k(x-X)$. En écrivant $\delta = a - bX + cX^2$, avec $\mathcal{N}_{L/K}(\delta) = r^2$ et $z = u + vX + wX^2$, on obtient $\delta z^2 = q_0 - q_1 X + q_2 X^2$, où q_0, q_1 et q_2 sont trois formes quadratiques en (u,v,w), ce qui fait que le problème est équivalent à résoudre simultanément $q_2 = 0$ et $q_1 = k$.

L'idée de la fin de l'algorithme est simple : on résout $q_2(u,v,w) = 0$, on paramétrise quadratiquement ses solutions sous la forme $u = \frac{1}{y}U(\lambda,\mu)$, $v = \frac{1}{y}V(\lambda,\mu)$, $w = \frac{1}{y}W(\lambda,\mu)$, puis on les substitue dans l'équation $q_1(u,v,w) = k$, ce qui donne une seule équation

$$ky^2 = Q(\lambda,\mu)$$

où Q est un polynôme homogène de degré 4.

Pour résoudre $q_2 = 0$, on utilise les algorithmes décrits au chapitre IV. Remarquons que le déterminant de q_2 vaut $-\mathcal{N}_{L/K}(\delta) = -r^2$ et que r est une S–unité, donc on connaît bien la factorisation du déterminant de q_2, ce qui accélère la résolution de cette équation. Si l'on travaille sur un corps de nombres quelconque, il se peut que les discriminants des formes quadratiques U, V, W contiennent des facteurs parasites et je propose dans [T4] d'en enlever une partie. On peut le faire bien plus simplement en utilisant [T8]. Lorsque l'on est sur $\mathbb{Q}$, les formules de [T8] donnent une paramétrisation optimale et l'on voit en particulier que le polynôme quartique Q est à coefficients entiers et de discriminant Disc$Q = 2^{12} r^{12}$Disc$P$. On obtient ainsi un discriminant indépendant de la solution particulière trouvée pour $q_2 = 0$. Lorsque $k = 1$, on sait en théorie que l'on peut trouver des quartiques ayant un discriminant égal à Disc$Q = 2^{12}$Disc$P$ (voir [BSD 1963] et [Cremona 1997 a]), donc on doit pouvoir minimiser celle que l'on a obtenue. Comme le facteur restant est r^{12}, qui est une S–unité, il n'y a aucune difficulté à en connaître la factorisation et donc la minimisation se fait très rapidement.

Un avantage tout à fait remarquable de la description de l'algorithme de la 2–descente tel que je viens de le décrire, est qu'il permet de traiter des familles de tordues quadratiques, $E_k : ky^2 = P(x)$, où P est fixé et k peut varier. En effet, une des parties les plus difficiles de l'algorithme consiste à déterminer les unités et le groupe de classes du corps L. Comme ici ce corps est constant lorsque k varie, il suffit de faire ce travail une seule fois pour toutes les valeurs de k. Ensuite, la complexité en fonction de k est vraiment négligeable et il est tout à fait raisonnable de considérer des valeurs de k ayant des milliers de chiffres, construits de telle sorte que la factorisation soit connue (par exemple lorsque k est un très grand nombre premier, ou lorsque k est le produit d'un grand nombre de petits facteurs premiers). Ces courbes elliptiques sont inaccessibles au programme `mwrank` de Cremona.

J'ai complètement implanté en `gp` l'algorithme de la 2-descente. Le programme [T14] pour les courbes elliptiques définies sur un corps de nombres utilise l'algorithme [T13] pour

résoudre les équations quadratiques comme des équations aux normes dans une extension relative quadratique de corps de nombres. Le programme [T15] pour les courbes elliptiques définies sur $\mathbb{Q}$ utilise l'algorithme [T16] décrit au chapitre IV pour résoudre les équations quadratiques.

2 4–descente et 3–descente

La 4–descente sur une courbe elliptique consiste à faire une 2–descente à partir d'une équation de la forme

$$y^2 = P(x)$$

où P est un polynôme de degré 4 construit comme dans la partie précédente ([Cremona 1997 b] et [Merriman, Siksek et Smart 1996]). Si le polynôme P est unitaire, il y a une solution évidente à l'équation $y^2 = P(x)$. S'il n'est pas unitaire, on peut peut–être utiliser les informations obtenues au chapitre III, mais je n'ai pas encore exploré cette piste. Une idée, maintenant classique, consiste à faire une 2–descente similaire à celle décrite dans la partie 1 : on construit encore une extension $L = K[X]/P(X)$ puis un groupe $L(S, 2)$ pour un ensemble fini S ; pour chaque élément $\delta \in L(S, 2)$, on cherche un élément $z \in L^*$ tel que δz^2 soit de la forme $\delta z^2 = q_0 + q_1 X + q_2 X^2 + q_3 X^3$, avec $q_2 = q_3 = 0$. On voit donc que dans cet algorithme, on est amené à résoudre simultanément deux équations quadratiques en dimension 4. Pour cela, on peut par exemple résoudre $q_3 = 0$ avec les méthodes du chapitre IV et substituer les solutions dans $q_2 = 0$.

Cette stratégie est encore applicable lorsque l'on veut faire une 2–descente sur la jacobienne d'une courbe hyperelliptique de la forme $y^2 = P(x)$, où P est un polynôme de degré d quelconque (voir [Stoll 2001]) : on doit alors considérer des systèmes de plusieurs équations quadratiques en dimension d.

Pour la 3–descente (voir [T18]), une des étapes consiste à trivialiser une algèbre centrale simple de dimension 9. Pour cela, il suffit de trouver un élément nilpotent. En utilisant la notion de trace réduite et de norme réduite, on voit que cela peut se faire en résolvant successivement $Tr_{red}(X) = 0$, $Tr_{red}(X^2) = 0$, puis $Norm_{red}(X) = 0$, où X est dans un espace de dimension 9. En résolvant $Tr_{red}(X) = 0$, on se ramène à résoudre l'équation quadratique $Tr_{red}(X^2) = 0$ dans un espace de dimension 8, d'où l'étude du chapitre IV. La dernière équation $Norm_{red}(X) = 0$ est alors équivalente à une équation aux normes dans une extension cubique cyclique sur $\mathbb{Q}(\zeta_3)$, qui peut se résoudre avec [T3] si l'on sait calculer les unités et le groupe de classes du corps correspondant, ou peut–être en utilisant uniquement la géométrie des nombres dans le corps de base $\mathbb{Q}(\zeta_3)$ avec [T19].

Bibliographie

[Bartels 1980] H.J. Bartels : *Über Normen algebraischer Zahlen*, Math. Ann., **251** (1980), 191–212.

[Belabas 2004] K. Belabas : *A relative van Hoeij algorithm over number fields*, J. Symbolic Computation, **37** (2004), no. 5, 641–668.

[Birch et Merriman 1972] B.J. Birch et R. Merriman : *Finiteness theorems for binary forms with given discriminant*, Proc. London Math. Soc. (3) **24** (1972), 385–394.

[BSD 1963] B.J. Birch et H.P.F. Swinnerton–Dyer : *Notes on Elliptic Curves* J. Reine Angew. Math. **212** (1963), 7–25.

[Bosma et Stevenhagen 1996] W. Bosma et P. Stevenhagen : *On the computation of quadratic* 2*-class groups*, J. Théor. Nombres Bordeaux **8** (1996), no. 2, 283–313.

[Cassels 1959] J.W.S. Cassels : *Note on quadratic forms over the rational field* , Proc. Cambridge Philos. Soc. **55** (1959), 267–270.

[Cassels 1971] J.W.S. Cassels : *An introduction to the geometry of numbers*, Grund. der math. Wiss. in Einzel., Band **99**, seconde éd. corrigée, Springer Verlag (1971).

[Cassels 1978] J.W.S. Cassels : *Rational Quadratic Forms*, L.M.S. Monographs, No. **13**, London, New York, San Francisco : Academic Press (1978).

[Cassels 1991] J.W.S. Cassels : *Lectures on Elliptic Curves*, LMS Student Texts **24**, Cambridge University Press (1991). J. Fac. Sci Tokyo, **2** (1933), 365–475.

[Cochrane et Mitchell 1998] T. Cochrane et P. Mitchell : *Small solutions of the Legendre equation*, Journal of Number Theory **70** (1998), 62–66.

[Cohen 1993] H. Cohen : *A Course in Computational Algebraic Number Theory*, Graduate Texts in Math., Vol. **138**, Springer–Verlag (1993).

[Cohen 2000] H. Cohen : *Advanced Topics in Computational Algebraic Number Theory*, Graduate Texts in Math. **193**, Springer–Verlag (2000).

[Cox 1989] D.A. Cox : *Primes of the form* $x^2 + ny^2$, John Wiley & Sons, New York (1989).

[Crandall et Pomerance 2002] R. Crandall et C. Pomerance : *Prime numbers, a computational perspective*, Springer–Verlag, Berlin (2002).

[Cremona 1997 a] J.E. Cremona : *Algorithms For Modular Elliptic Curves*, Cambridge University Press (1997), seconde édition.

[Cremona 1997 b] J.E. Cremona : *Higher Descents on Elliptic Curves*, actes des "Huitièmes Rencontres Arithmétiques de Caen" J. Boxall ed., (1997), préprint.

[Cremona 2001] J.E. Cremona : *Classical Invariants and 2-descent on Elliptic Curves*, J. Symb. Comput., **31**, No 1-2 (2001), 71–87.

[Cremona et Rusin 2003] J.E. Cremona et D. Rusin : *Efficient solution of rational conics*, Math. Comp. **72** (2003), 1417–1441.

[Cremona et Serf 1999] J.E. Cremona et P. Serf : *Computing the Rank of Elliptic Curves over Real Quadratic Fields of Class Number* 1, Math. Comp. **68** (1999), 1187–1200.

[Delone et Feddeev 1940] B.N. Delone et D.K. Faddeev : *Theory of Irrationalities of Third Degree*, Acad. Sci. URSS. Trav. Inst. Math. Stekloff, **11** (1940).

[Djabri et Smart 1998] Z. Djabri et N.P. Smart : *A Comparison of Direct and Indirect Methods for Computing Selmer Groups of an Elliptic Curve*, in ANTS-III, J. Buhler ed., Springer Verlag, LNCS **1423** (1998), 502–513.

[Fieker 1997] C. Fieker : *Über Relative Normgleichungen in Algebraischen Zahlkörpern*, Dissertation, Technische Univertität Berlin (1997).

[Fieker, Jurk et Pohst 1997] C. Fieker, A. Jurk et M. Pohst : *On solving relative norm equations in algebraic number fields*, Math. Comp., 217 vol. **66** (1997), 399–410.

[Fincke et Pohst 1983] U. Fincke et M. Pohst : *A Procedure for Determining Algebraic Integers of Given Norm*, Proceedings EUROCAL 83, Springer LN in Computer Science, **162** (1983), 194–202.

[Garbanati 1980] D. Garbanati : *An algorithm for finding an algebraic number whose norm is a given rational number*, J. Reine Angew. Math., **316** (1980), 1–13

[Gauss 1953] K.F. Gauss : *Recherches Arithmétiques*, Poullet-Delisle, A.C.M. (trad.), A. Blanchard, (1953).

[Granville 2005] A. Granville : *It is easy to determine whether a given integer is prime*, Bull. Am. Math. Soc., New Ser. **42**, No.1 (2005), 3–38.

[Gras 1986] M.N. Gras : *Non monogénéité de l'anneau des entiers des extensions cycliques de $\mathbb{Q}$ de degré premier $l \geqslant 5$*, J. of Number Theory, vol. **23** No 3 (1986), 347–353.

[Gras 2003] G. Gras : *Class field theory. From theory to practice*, Springer Monographs in Mathematics, Berlin (2003).

[Győry 1998] K. Győry : *Discriminant form and index form equations*, Algebraic number theory and Diophantine analysis (Graz, 1998), de Gruyter, Berlin (2000), 191–214.

[Hancock 1964] H. Hancock : *Foundations of the Theory of Algebraic Numbers*, vol. 2, Dover (1964).

[Hardy et Williams 1993] K. Hardy et K. Williams : *The squareroot of an ambiguous form in the principal genus*, Proc. Edinburgh Math. Soc. (2) **36** (1993), no. 1, 145–150.

[Holzer 1950] L. Holzer : *Minimal Solutions of Diophantine Equations*, Canad. J. Math, **2** (1950), 238–244.

[Hurwitz 1895] A. Hurwitz : *Mathematische Werke*, vol. II, art. LVIII (1895), Birkhäuser Verlag (1963), 198–207.

[Ivanyos et Szántó 1996] G. Ivanyos et A. Szántó : *Lattice basis reduction for indefinite forms and application*, Discrete Math. **153** (1996), 177–188.

[Lagarias 1989] J.C. Lagarias : *Worst-case complexity bounds for algorithms in the theory of integral quadratic forms*, J. American Math. Soc. **2** (1989), no 4, 143–186.

[Lenstra, Lenstra et Lovász 1982] A.K. Lenstra, H.W. Lenstra et L. Lovász : *Factoring polynomials with rational coefficients*, Math. Ann. **261** (1982), 515–534.

[Merriman, Siksek et Smart 1996] J. R. Merriman, S. Siksek et N. P. Smart : *Explicit* 4*–descent on an elliptic curve*, Acta Arithmetica **77** (1996), 385–404.

[Mordell 1969] L.J. Mordell : *Diophantine Equations*, Pure and Applied Mathematics **30**, Academic Press (1969).

[Narkiewicz 1990] W. Narkiewicz : *Elementary and Analytic Theory of Algebraic Numbers*, seconde édition, Springer Verlag (1990).

[Nguyễn et Stehlé 2005] P. Nguyen et D. Stehlé : *Floating–point LLL revisited*, proceedings of Eurocrypt '05, Springer LNCS **3494** (2005), 215–233.

[Pohst 2000] M. Pohst : *On Legendre's equation over number fields*, Publ. Math. **56**, No.3–4 (2000), 535–546.

[Pomerance 1982] C. Pomerance : *Analysis and comparison of some integer factoring algorithms*, in H. Lenstra et R. Tijdeman, éd, *Computational methods in number theory*, Part I, vol **154** of Math. Centre Tracts, Math. centrum (1982), 89–139.

[Schaefer 1996] E.F. Schaefer : *Class groups and Selmer groups*, J. of Number theory **56** (1996), 79–114.

[Schaefer et Stoll 2004] E. F. Schaefer et M. Stoll : *How to do a p-descent on an elliptic curve*, Trans. Am. Math. Soc. **356**, No 3 (2004), 1209–1231.

[Serf 1995] P. Serf : *The Rank of Elliptic Curves Over Real Quadratic Number Fields of Class Number* 1, Doctoral Thesis, Universität des Saarlandes (1995).

[Serre 1968] J.P. Serre : *Corps Locaux*, Hermann, 3^{e}édition (1968).

[Serre 1988] J.P. Serre : *Cours d'arithmétique*, P.U.F. 3^{e}édition (1988).

[Shanks 1971] D. Shanks : *Gauss's ternary form reduction and the* 2*-Sylow subgroup*, Math. Comp. **25**, no 116 (1971), 837–853. Erratum : Math. Comp. **32** (1978), 1328–1329.

[Siegel 1973] C.L. Siegel : *Normen algebraischer Zahlen*, Nachr. Akad. Wiss. Göttingen (1973), 197–215.

[Smart 1998] N.P. Smart : *The algorithmic resolution of diophantine equations*, LMS Student Texts **41**, Cambridge University Press (1998).

[Stoll 2001] M. Stoll : *Implementing* 2*–descent for Jacobians of hyperelliptic curves*, Acta Arith. **98** (2001), no 3, 245–277. Cours Spécialisés, Coll. SMF, no 1 (1995).

[Vallée 1987] B. Vallée : *An affine point of view on minima finding in integer lattices of lower dimensions*, Proc. of EUROCAL '87 (Leipzig, 1987), Lecture Notes in Comput. Sci. **378**, Springer, Berlin (1989), 376–378.

[Woestijne 2005] C. van de Woestijne : *Deterministic equation solving over finite fields*, Ph.D. thesis, Leiden University (2005).