Université Sorbonne Paris Cité

Thèse de doctorat

de l'Université Sorbonne Paris Cité

préparée à l'université Paris Diderot

École Doctorale de Sciences Mathématiques de Paris Centre (ED 386)

Institut de mathématique de Jussieu-Paris Rive Gauche (UMR 7586)

Densité des points rationnels sur les surfaces elliptiques et les surfaces de Del Pezzo de degré 1

---

présentée par

Julie Desjardins

Thèse de Mathématiques

dirigée par Marc Hindry

Soutenue le 18 novembre 2016 devant le jury composé de :

M. Jean-Marc Couveignes	Université de Bordeaux	rapporteur
M. David Harari	Université d'Orsay Paris 11	président du jury
M. Harald Helfgott	Universität Göttingen	examinateur
M. Marc Hindry	Université Paris 7	directeur
M^{me} Ariane Mézard	Université Paris 6	examinatrice

Institut de Mathématiques de Jussieu -
Paris Rive Gauche
Bâtiment Sophie Germain
8, place Aurélie Nemours
75 013 Paris

Cette thèse est dédiée à Héloïse, Fanny et Sarah,
les meilleures soeurs du monde.

"Of course it is happening inside your head, Harry, but why on earth should that mean that it is not real?"

– J.K. Rowling, *Harry Potter and the Deathly Hallows*

Remerciements

Je remercie chaleureusement Marc Hindry qui a aussitôt accepté d'être mon directeur de thèse lorsque je lui ai dit (à peine quelques jours avant la date limite pour candidater à un contrat doctoral) qu'à bien y penser, j'aimerais étudier les surfaces elliptiques après le master. Il m'a appris beaucoup, notamment à être précise dans mes énoncés de théorème ou dans mes démonstrations et à éviter les phrases de quatre lignes ou les titres dans le style des romans du 19e siècle. Je le remercie également pour sa confiance immuable en mon potentiel, même lorsque j'allais perdre espoir, pour sa patience et sa grande pédagogie, et pour son soutien dans les aspects mathématiques et non mathématiques de mon doctorat.

Je remercie les rapporteurs de ma thèse, Jean-Marc Couveignes et David Rohrlich. Je suis très honorée qu'ils aient accepté de rapporter ce manuscrit. Je remercie Jean-Marc Couveignes d'avoir accepté de faire partie de mon jury et pour son rapport détaillé et très encourageant. Je remercie David Rohrlich, dont les travaux ont été très importants pour moi, pour ses suggestions qui ont grandement amélioré le manuscrit.

Je remercie également Ariane Mézard, David Harari et Harald Helfgott d'avoir accepté de faire partie de mon jury. Ariane Mézard m'a enseigné les représentations galoisiennes pendant ma première année de doctorat. Les travaux de Harald Helfgott ont bien sûr été très influents dans cette thèse, puisque le chapitre 2 est dédié à l'un de ses préprints.

Pendant ces années de thèse, j'ai eu l'occasion de fréquenter de nombreux mathématiciens et mathématiciennes dont les discussions sur les mathématiques ou autre m'ont été profitables. Je remercie Tim Dokchitser, Andrew Granville, Claude Levesque, Alexey Zykin, Daniel Fiorilli, Alice Garbagnati, René Pannekoek et Marta Pieropan. De l'Université Paris Diderot, je voudrais remercier Loïc Merel, Régis de la Bretèche, Jean-François Mestre, Pascal Molin, Mireille Fouquet, Séverine Leidwanger et Gentiana Danila. Merci à René Cori, mon partenaire dans la Traviata, et à Gérard Bourdaud, mon chef de choeur. Je remercie en particulier Mathilde Herblot pour son écoute attentive, sa plume accérée et son humour mordant (et certains marques-pages).

Je remercie aussi Francesca Balestrieri, Céline Maistret et Isabel Vogt, que j'ai rencontrées à Leiden il y a peu de temps au cours d'une chouette semaine de recherche.

Je remercie mes « frères et soeurs » de thèse. Cecília Salgado pour m'avoir invitée à WIN-E2 dans son projet sur les surfaces K3, et aussi pour les conversations sur la vie après la thèse. Fabien Pazuki pour ses conseils et sa bienveillance. Richard mon jumeau et co-bureau pour les conférences, le tricot, les chocolats, les insultes et les « je suis prem's pour voir Marc ». Je le remercie aussi d'avoir enduré ma mauvaise humeur (euphémisme). Benjamin pour les conversations intéressantes. Victoria, ma chère petite soeur, pour son dynamisme et sa gentillesse.

Merci aux co-organisateurs du Séminaire des thésards : Anne Giralt, Andres Jaramillo-Puentes, Catherine Gilles et Éric Balandreau. Un merci spécial à Catherine, partenaire de chorale, pour son support à la fin de ma thèse. Merci aussi à Anne d'être une très bonne amie depuis le master.

Je remercie l'Université Grenoble Alpes de m'offrir un ATER « postdoctoral » cette année, et ainsi de me permettre de réaliser un rêve d'enfance : habiter dans les Alpes ! Merci aux théoriciens des nombres de l'Institut Fourier d'avoir soutenu ma candidature.

I thank University of California, Berkeley for employing me as a Lecturer during Fall 2012.

Merci à Bernhard Keller, Christian Lerustre, Thierry de Pauw, Huayi Chen, Christian Blanchet, Marie-France Vigneras et Ivan Marin pour de très bons cours de master ou de licence. Merci aussi à mes professeurs de l'Université Laval : Hugo Chapdeleine, pour le super projet sur l'icosaèdre, Jean-Marie De Koninck, pour le stage d'été, et Frédéric Gourdeau de m'avoir laissé faire un échange à Paris plutôt qu'à Tours. Je suis reconnaissante au camp de l'AMQ 2007 à Sherbrooke qui a marqué le début de mes études de mathématiques, et je souhaite aussi exprimer ma gratitude à Jordi Nadal et Philippe Etchecopar du Cégep de Rimouski pour m'avoir soutenue et partagé leur passion pour les maths. Enfin, je remercie Céline Laflamme qui m'a aidée à prendre mon envol.

Mes étudiants ont aussi été formidables et m'ont appris autant que mes enseignants. Merci à ceux de Paris ! Thanks to my Berkeley students !

Grâce aux activités non mathématiques, je suis resté saine d'esprit... (ou presque : merci à Marilène Callegari, psychologue de la médecine préventive de Paris Diderot.)

D'abord, je dois mentionner les Ateliers du PJE à Muret et l'Université d'été en création littéraire de l'UQAR, où j'ai rencontré de jeunes (et moins jeunes) passionnés de l'écriture qu'il est toujours agréable de revoir.

Je remercie le club d'aïkibudo Mitsurukaï : merci à Christian-sensei, Éric, Guillaume, Arnaud, Boun et tous les autres pour les joyeuses bagarres des mardis et jeudis. Merci aussi à l'ASPP et à Maître Floquet, ainsi qu'à Maître Sugino et son dojo. Je n'oublie pas mes anciens clubs d'aïkido : le Dojo de Beauport avec Maitre Tabouret, et le Dojo de Rimouski avec Ben.

Ich danke Ophélie Sitbon, die mir für fast zwei Jahre Deutsch gelehrt hat. Sie ist eine tolle Lehrerin. I dank o Michaels Familie, dia mir für fasch zwo Johr Gsibergerisch glernt hond !

Les surfaces elliptiques auraient été fades sans Camille, Rémi, Jampe et leur bestiole, et les exposés auraient été ennuyeux sans Oriane, Mélian, Salia et le fléau. Merci à Joanne et Harry, Phillip et Lyra, George et Irene. Merci surtout à ceux qui comprennent ce paragraphe !

Je suis aussi reconnaissante envers les thésards et les thésardes de Paris 6 et de Paris 7 (et d'ailleurs) que j'ai pu côtoyer au cours de mes études. J'ai fréquenté plusieurs générations, aussi qu'on me pardonne d'en oublier. Dans les plus ancestraux, je mentionne Lukas, Loulou, Hoel, Sarah, Paloma, Alfredo, Daniel, Victoria, Roro, Élodie et Isidore. Parmi les petits nourrissons, je mentionne Antoine, Reda, Elie et Véronique. Merci bien sûr aux contemporain : Sammy pour les discussions sur l'écriture et les mangas, Fathi pour la partie de cartes magiques (que j'ai inexplicablement gagnée !) et les autres geekeries, Nicolas pour les soirées Disney et les délicieux gâteaux, Marco pour sa bonne humeur constante et les cours d'allemand, Baptiste le syndicaliste d'être parfois plus crevé que moi (ça fait relativiser), Kévin d'avoir supporté mes invasions de son bureau pour lui expliquer mes problèmes ou mes réussites, Charlotte au sourire contagieux, Annalaura la squatteuse de bureau, Martin le pianiste prodige, Charles pour les suggestions de restos végétariens et notre passion commune pour Kyari. Je remercie toutes ces formidables personnes de m'avoir soutenue quand ma thèse répandait dans mon esprit de sombres bouillards. J'allais oublier : Zoé, Assia, Tony, Jesus, Martin, David, Florian, Jean, Olivier et François et aussi Samuel, Étienne et Bruno ! Je remercie aussi ceux que j'ai oublié de nommer... Désolée !

Je remercie des amis rencontrés pendant le master. Maÿlis, mon extraordinaire coloc' pour quatre mois, qui ne sait pas à quel point elle m'a sauvé. C'est une jeune femme généreuse et brillante qui mérite le meilleur. Eirini, pour les spectacles de ballet et les visites à Amiens. Claire pour les voyages en Savoie ou dans le Tarn. Lorick, qui ne m'a jamais convertie à l'escrime coréenne (katori forever). Sandrine pour les thés et le réconfort.

Je remercie Manon d'être si chouette, pour nos conversations sur l'écriture, le féminisme ou les mangas gays, et pour les barbecues coréens et la patinoire. Ah oui, et je la remercie aussi pour le coup du diamant (comme ça c'est fait).

Merci à de précieuses amies du Québec. Christine et Jacynthe qu'il est si dommage de voir moins souvent. Zoé, à qui je peux parler de math. Pier, inlassable réceptrice de mes cartes postales. Kim, dont l'amitié fidèle résiste à notre correspondance sporadique. Véro, toujours avide d'être ma première lectrice, que ce soit PeF, une nouvelle nouvelle ou (surtout !) ma vie sentimentale. (Bisou à Lilianne et Mandoline. Coucou à Xavier.)

Merci à Anne, ma « soeur » allemande, et à Véné et Fatou, mes « soeurs » africaines.

Merci à la famille de papa : Michel, Barbara, Mario, Francine, Diane, Claude, Gaetane, Berthier, France, Francine et les cousins et cousines Desjardins pour les feux de camp, les baignades et le kayak à la rivière Trois-Pistoles, et merci à grand-papa Bi.

Merci à la famille de maman : Michel que j'étais fière d'avoir pour voisin de bureau et collègue à Paris 7. Isabelle pour tous ses conseils et son aide quand je n'avais nulle part où aller. (Des bisous à Quentin et Lilou.) Françoise, ma maman de remplacement et ma tantounette adorée. Martine, mon autre tantounette qui a traqué les fautes de français dans cette thèse. Piou et Claire pour leurs encouragements. Antoine (à qui je n'ai pas réussi à faire changer d'idée au sujet d'Eragon...) de m'avoir sauvée à l'un de mes déménagements. Alice, Hélène, Emma et Maéline pour les parties de cache-cache !

Il y a aussi des gens pour lesquels de simples remerciements ne suffisent pas.

Shanti, ma belle-maman, a toujours des recommandations et des avis dignes de ceux d'une grande soeur.

Le meilleur, le plus fort, le plus beau, c'est Gaston ! C'est aussi mon papa, j'ai beaucoup de chance. Il est venu plusieurs fois en France pendant ma thèse et nous avons fait de beaux voyages qui m'ont remonté le moral.

J'aimerais être comme ma maman Catherine : courageuse, bienveillante et déterminée. Elle me conseille toujours au mieux, et même lorsque je ne suis pas convaincue, il s'avère qu'elle a raison ! Une pensée pour son cher Hennepin l'explorateur qui lui donnait des excuses pour me rendre visite.

Ma thèse m'a permis de rencontrer Michael, mon fiancé et précieux compagnon. En Angleterre, en France, en Autriche, au Québec, en Allemagne, c'était toujours un bonheur d'aller à l'escalade, de se promener, d'aller dans des musées ou de manger de délicieuses choses - et ce en anglais, en français ou en allemand ! J'ai hâte de voir ce que l'avenir nous réserve, certainement beaucoup de bien !

À mes soeurs, les meilleures de l'univers entier, je dédie cette thèse. À Héloïse, qui n'avait que cinq ans lorsque je suis partie. Elle est maintenant meilleure que moi en piano (et en jeu vidéo mais ce n'est pas difficile), et va bientôt avoir lu plus de romans ! (Câlin à Merlot.) À Fanny, ma petite soeur mathématicienne. Elle est courageuse, dégourdie, et bien plus douée qu'elle ne le croit. Je n'oublierais jamais le voyage à Poudlard en voiture volante, ni le combat contre le monstre du Loch Ness. À Sarah, ma compagne de toujours. C'est un modèle d'indépendance, de force et de sagesse. Peut-être était-elle Gandalf dans une autre vie ? C'est mon mentor et mon Dumbledore. À vous trois, mes soeurs que j'aime. Dongsaeng saranghae.

Résumé

Résumé

Soit $\mathscr{E} \to \mathbb{P}^1_{\mathbb{Q}}$ une surface elliptique sur $\mathbb{Q}$ de base $\mathbb{P}^1$ non triviale. On s'intéresse à la Zariski-densité des points rationnels de $\mathscr{E}$. Il est conjecturé que le signe de l'équation fonctionnelle d'une courbe elliptique est relié à la parité du rang de celle-ci. Modulo cette conjecture, il est suffisant de démontrer que le signe des fibres de $\mathscr{E}$ varie pour démontrer la Zariski-densité de $\mathscr{E}(\mathbb{Q})$. Un théorème conditionnel de Helfgott garantit que le signe moyen d'une surface non isotriviale est strictement compris entre -1 et 1. Dans le cas où $\mathscr{E}$ possède une place générique de réduction multiplicative, le signe moyen serait nul. Ce travail est conditionnel à deux conjectures de théorie analytique des nombres : la conjecture sans facteur carré et la conjecture de Chowla. L'objectif principal de cette thèse est d'éviter les conjectures utilisées par Helfgott pour démontrer la variation du signe sur les surfaces elliptiques non triviales. On réussit à se passer de la conjecture sans facteur carré sous certaines hypothèses techniques. On démontre ainsi (sous l'hypothèse de la conjecture de parité) la densité des points rationnels sur certaines surfaces elliptiques dont les coefficients sont des polynômes de degré arbitraire. Une surface de Del Pezzo de degré 1 est reliée par l'éclatement d'un point canonique à une surface elliptique rationnelle. On démontre inconditionnellement la densité des points rationnels dans plusieurs cas par des arguments géométriques. On étudie aussi la variation du signe de l'équation fonctionnelle pour des surfaces elliptiques rationnelles isotriviales et on cerne des conditions pour que le signe soit fixé. Dans le cas où le signe est $+1$, on en déduit des exemples de surfaces elliptiques non triviales dont les points rationnels pourraient ne pas être denses.

Mots-clefs

courbes elliptiques, surfaces elliptiques, surfaces isotriviales, surfaces de Del Pezzo, signe de l'équation fonctionnelle, densité des points rationnels.

Density of rational points on elliptic surfaces and degree 1 del Pezzo surfaces

Abstract

Let $\mathscr{E} \to \mathbb{P}^1_{\mathbb{Q}}$ be an non-trivial elliptic surface over $\mathbb{Q}$ with base $\mathbb{P}^1$. We are interested in the Zariski density of the rational points of $\mathscr{E}$. It is conjectured that the root number of an elliptic curve E has the same parity as its rank. Assuming this conjecture, it is enough to show that the root number of the fibre of $\mathscr{E}$ varies to prove the Zariski density of $\mathscr{E}(\mathbb{Q})$. A conditional theorem of Helfgott garanties that the average root number of a non-isotrivial elliptic surface is strictly between -1 et 1. In the case where $\mathscr{E}$ has a generic place of multiplicative reduction, the average root number should be zero. This work is conditional to two analytic number theory conjectures : the squarefree conjecture and the Chowla conjecture. The main aim of this Ph.D thesis is to avoid the conjectures used by Helfgott when proving the variation of the root number on non-trivial elliptic surfaces. We manage to drop the squarefree conjecture assumption under some technical hypothesis. We show thus (under the parity conjecture) the density of the rational points on some elliptic surfaces whose coefficients have arbitrary large degree. Blowing up the anticanonical point on a del Pezzo surface of degree 1, one obtains a rational elliptic surface. We show unconditionally the density of the rational points in many cases by means of geometric arguments. We also study the variation of the root number on some isotrivial rational elliptic surfaces and we state the conditions under which it is constant. When it is +1, we deduce examples of non trivial elliptic surfaces whose rational points might not be dense.

Keywords

elliptic curves, elliptic surfaces, isotrivial surfaces, Del Pezzo surfaces, root number, density of rational points.

Table des matières

Introduction

Cette thèse est consacrée à des questions diophantiennes et de théorie analytique des nombres. Le principal problème abordé concerne la densité au sens de Zariski des points rationnels sur une surface elliptique sur $\mathbb{Q}$. Pour ce faire, on étudie la variation du signe de l'équation fonctionnelle sur ses fibres. On s'intéressera également à la densité des points rationnels d'une surface de Del Pezzo de degré 1 en utilisant le lien entre une telle surface et une surface elliptique rationnelle. L'objectif de cette thèse est de démontrer la densité des points rationnels sur ces surfaces en utilisant moins de conjectures de théorie analytique des nombres que le font les résultats antérieurs à ce sujet. Nous y réussissons dans plusieurs cas.

0.1 Contexte et résultats connus

Pour de plus amples explications sur la théorie des surfaces elliptiques, on se réfère au livre de Miranda [33].

Définition 1. Une *surface elliptique* sur $\mathbb{Q}$ est une surface algébrique projective $\mathscr{E}$ définie sur $\mathbb{Q}$ telle que

i) Il existe un morphisme (une *fibration*) $\pi : \mathscr{E} \to \mathbb{P}^1$ tel que la fibre $\mathscr{E}_t := \pi^{-1}(t)$ est une courbe projective lisse de genre 1 pour tout t sauf un nombre fini.

ii) Il existe une section $\sigma : \mathbb{P}^1 \to \mathscr{E}$ pour π définie sur $\mathbb{Q}$.

Certains auteurs ne requièrent pas l'existence d'une section. Cependant, nous désirons étudier une surface elliptique en tant que famille de courbes elliptiques, d'où l'importance de la munir d'une section.

Dans ce cas, une surface elliptique $\mathscr{E}$ peut s'écrire comme l'ensemble des solutions dans $\mathbb{P}^2 \times \mathbb{P}^1$ d'une équation de la forme

$$\mathscr{E} : y^2 = x^3 + A(T)x + B(T),$$

avec $A(T), B(T) \in \mathbb{Z}[T]$. On appellera *fibre générique* de $\mathscr{E}$ la courbe elliptique sur $\mathbb{Q}(T)$ notée $\mathscr{E}_T$ dont un modèle affine est l'équation précédente.

Pour presque tout $t \in \mathbb{P}^1$, la fibre de π au dessus de t donnée par $\mathscr{E}_t = \pi^{-1}(t)$ est une courbe elliptique sur $\mathbb{Q}$ et l'ensemble $E_t(\mathbb{Q})$ a une structure de groupe, appelé le groupe de Mordell-Weil de E sur $\mathbb{Q}$. Par le théorème de Mordell-Weil, ce groupe se décompose comme la somme d'un groupe libre de type fini $\mathbb{Z}^r$ et du groupe fini des éléments de torsion. L'entier r est appelé le *rang de Mordell-Weil* (ou simplement le *rang*) de E sur $\mathbb{Q}$.

On s'intéresse dans cette thèse à la densité des points rationnels sur une surface elliptique. La densité peut avoir deux sens : pour la topologie réelle usuelle ou la topologie de Zariski.

Mazur fait la conjecture suivante au sujet de la topologie réelle.

Conjecture 0.1. *[32, Conjecture 4] Soit $\mathscr{E} \to \mathbb{P}^1$ une surface elliptique. On définit*

$$\mathfrak{P} = \{t \in \mathbb{P}^1_{\mathbb{Q}} \mid \mathscr{E}_t \text{ est une courbe elliptique sur } \mathbb{Q} \text{ et } \mathrm{rang}\mathscr{E}_t(\mathbb{Q}) > 0\}.$$

Alors,

(1) ou bien $\mathfrak{P}$ est fini,

(2) ou bien $\mathfrak{P}$ est dense dans $\mathbb{P}^1(\mathbb{R})$.

Cette thèse s'inscrit dans la continuité des travaux précédemment réalisés pour tenter de démontrer cette conjecture, en remplaçant toutefois « densité pour la topologie réelle » par « densité pour la topologie de Zariski ». Nous étudierons ainsi plutôt la question suivante :

Conjecture 0.2. *Soit $\mathscr{E} \to \mathbb{P}^1_{\mathbb{Q}}$ une surface elliptique sur $\mathbb{Q}$. Alors on a une des deux propositions suivantes :*

1. *$\mathscr{E}$ est triviale, c'est-à-dire qu'il existe une courbe E_0 telle que $\mathscr{E} \simeq E_0 \times \mathbb{P}^1$. Dans ce cas, on a $\mathscr{E}(\mathbb{Q}) = E_0(\mathbb{Q}) \times \mathbb{P}^1(\mathbb{Q})$, où $E_0(\mathbb{Q})$ peut être fini ou infini.*
2. *$\mathscr{E}(\mathbb{Q})$ est dense dans $\mathscr{E}$ pour la topologie de Zariski.*

Remarque 1. Cette conjecture est implicite dans la littérature, en particulier dans [4].

Une formulation plus prudente excluerait dans le point 2 le cas où $\mathscr{E}$ est isotriviale. On a une intuition assez précise de la densité des points rationnels sur les surfaces non isotriviales grâce aux travaux de Helfgott [15] (que nous présentons plus loin) conditionnels à la conjecture de Chowla, des valeurs sans facteur carré et de parité. Cependant, dans le cas isotrivial, il existe des surfaces elliptiques pour lesquelles aucune conjecture ne prédit la densité des points rationnels : il s'agit de celles dont la fonction signe est constante. Nous définissons la fonction signe et la conjecture de parité dans la section 0.1.3 et les autres conjectures mentionnées dans cette remarque dans la section 0.1.6.

Remarque 2. La même question a un sens si l'on remplace $\mathbb{Q}$ par un corps de nombres k, ou encore en prenant une fibration en courbes elliptiques $\mathscr{E} \to C$, où C est une courbe sur un corps k telle que $C(k)$ est infini, mais nous nous contenterons d'étudier les surfaces elliptiques sur $\mathbb{Q}$ de base $\mathbb{P}^1$.

Remarque 3. Pour répondre à la conjecture précédente, on utilise le théorème élémentaire suivant démontré en section 1.2.2.

Théorème 0.1.1. *Supposons que*

$$\#\{t \in \mathbb{P}^1(\mathbb{Q}) \mid \mathrm{rang}\mathscr{E}_t(\mathbb{Q}) > 0\} = \infty.$$

Alors $\mathscr{E}$ a un ensemble dense de points rationnels.

Comme il n'existe pas de méthode générale pour calculer le rang d'une courbe elliptique, on passera parfois par l'étude de son signe, notion que l'on définira dans les sections 0.1.3 et 1.1.5. Celui-ci est conjecturellement relié à la parité du rang.

On étudiera plus en détails les surfaces elliptiques rationnelles, c'est-à-dire que $\mathscr{E}$ est $\bar{\mathbb{Q}}$-birationnel à $\mathbb{P}^2$. Elles nous intéressent particulièrement à cause du théorème suivant, dû à Iskovskih.

Théorème 0.1.2. *[19, Théorème 1]*
Soit une surface elliptique rationnelle $\mathscr{E}$.
Alors, elle possède un modèle minimal $X/\mathbb{Q}$ qui est :

1. *soit un fibré en coniques de degré 1,*
2. *soit une surface de Del Pezzo.*

Pour de plus amples explications sur les surfaces de Del Pezzo et les fibrés en coniques, on pourra se référer au livre de Manin [28].

Définition 2. Une *surface de Del Pezzo* X est une surface algébrique projective non singulière dont le diviseur anticanonique est ample.

Le *degré* d'une surface de Del Pezzo est l'entier d correspondant au nombre d'auto-intersection (K_X, K_X) du diviseur canonique de X noté K_X. Remarquons que le degré est compris entre $1 \leq d \leq 9$.

Nous nous intéressons aux questions suivantes. Étant donnée X une surface de Del Pezzo sur $\mathbb{Q}$ de degré d ou un fibré en conique de degré ≥ 1.

1. Existe-t-il un point rationnel sur X ?
2. L'ensemble des points rationnels est-il dense pour la topologie de Zariski ?

Lorsque X est un fibré en conique, les travaux de Kollar et Mella [23] garantissent que la surface est $\mathbb{Q}$-*unirationnelle*, c'est-à-dire qu'il existe une application dominante $\mathbb{P}^2 \dashrightarrow X$. Par conséquent l'ensemble des points rationnels est dense.

Lorsque $d \geq 3$, on sait par les travaux de Segre et Manin [28] que l'existence d'un point rationnel sur X implique que la surface est unirationnelle.

Lorsque $d = 2$, Salgado, Testa et Várilly-Alvarado [41], en se basant sur un travail de Manin [28, Thm 29.4], ont montré que si X contient un point rationnel qui ne se trouve pas sur une courbe exceptionnelle ni sur une certaine quartique, alors $X(\mathbb{Q})$ est dense pour la topologie de Zariski.

Si $d = 1$, la surface X est automatiquement pourvue d'un point rationnel : le point de base du système linéaire anticanonique. Cependant, les résultats concernant la densité des points rationnels restent partiels (par exemple [42] et [51]).

Si on éclate le point anticanonique sur X une surface de Del Pezzo de degré 1, on obtient une surface elliptique rationnelle $\mathscr{E}$ dont l'image de la section neutre est le diviseur exceptionnel. Par conséquent, il y a densité des points rationnels sur X si et seulement si il y a densité des points rationnels sur $\mathscr{E}$.

En étudiant les points singuliers sur les surfaces elliptiques rationnelles, on détermine lesquelles dont la contraction de la section à l'infini est une surface de Del Pezzo de degré 1 (pour plus de détails, voir le calcul rédigé en section 1.2.10).

On déduit de cette étude le lemme suivant.

Lemme 0.1.3. *Soit $\mathscr{E}$ une surface elliptique rationnelle et un modèle minimal de Weierstrass*

$$y^2 = x^3 + A(t)x + B(t),$$

où $A, B \in \mathbb{Z}[t]$ sont des polynômes de degré respectivement 4 et 6. On note X la surface obtenue de $\mathscr{E}$ par contraction de sa section à l'infini.

Alors X est une surface de Del Pezzo de degré 1 si et seulement si les seules fibres singulières de $\mathscr{E}$ sont de type II ou I_1.

Listons maintenant quelques méthodes permettant d'étudier la densité sur ces surfaces.

0.1.1 Arguments géométriques

Divers arguments géométriques présents dans la littérature permettent de démontrer inconditionnellement la densité des points rationnels sur une surface elliptique ou une surface de Del Pezzo de degré 1. Citons en quelques uns pour exemple.

Ulas a obtenu des résultats de densité sur des familles de surfaces elliptiques rationnelles non isotriviales en étudiant des changements de base explicites.

Théorème 0.1.4. *[50, Thm 2.1] Soit $f(T) = T^5+aT^3+bT^2+cT+d \in \mathbb{Z}[T]$ et considérons la surface $\mathscr{E}$ donnée par l'équation $\mathscr{E} : x^2 - y^3 - f(T) = 0$. Alors*

1. *ou bien f a des racines multiples sur $\overline{\mathbb{Q}}$, auquel cas l'ensemble des points rationnels de $\mathscr{E}_f$ est dense au sens de Zariski.*
2. *ou bien f n'a pas de racine multiple. Si l'ensemble des points rationnels sur la courbe $\mathscr{E}_{a,b} : Y^2 = X^3 + 135(2a-15)X - 1350(5a+2b-26)$ est infini, alors l'ensemble des points rationnels sur la surface $\mathscr{E}_f$ est Zariski-dense.*

D'autre part, Salgado compare le rang de la fibre générique de $\mathscr{E}$ sur $\mathbb{Q}[T]$ avec celui d'une surface elliptique $\mathscr{E}'$ obtenue à partir de $\mathscr{E}$ par changement de variables. Elle démontre le résultat suivant.

Théorème 0.1.5. *[40, Thm. 1.1.] Soit $\pi : \mathscr{E} \to B \simeq \mathbb{P}^1$ une surface elliptique $\mathbb{Q}$-unirationnelle. Il existe une courbe $C \to B$ telle que $C \simeq_{\mathbb{Q}} \mathbb{P}^1$ et*

$$\mathrm{rang}\mathscr{E}_C(\mathbb{Q}(C)) \geq \mathrm{rang}\mathscr{E}(\mathbb{Q}(B)) + 1,$$

où $\mathscr{E}_C = \mathscr{E} \times_B C$.

De plus, un article de Salgado et Van Luijk [42] donne des conditions pour que l'ensemble des points rationnels d'une surface de Del Pezzo de degré 1 soit Zariski-dense. Par exemple :

— Il suffit de supposer que la surface elliptique obtenue par éclatement du point anticanonique a une fibre de type I_m au dessus d'un certain point k-rationnel de $\mathbb{P}^1$.

— Il suffit de supposer l'existence d'un point rationnel qui ne se trouve pas sur six courbes exceptionnelles de S et qui est d'ordre 3 sur sa fibre.

0.1.2 Fibres singulières d'une surface elliptique

Soit $\mathscr{E}_T$ une courbe elliptique sur $\mathbb{Q}(T)$. On s'intéresse à la réduction de $\mathscr{E}$ en les places génériques de $Q(T)$, c'est-à-dire celles qui sont associées à des polynômes irréductibles non constants ou à $\frac{1}{T}$.

Soit une équation de Weierstrass

$$\mathscr{E}_T : y^2 = x^3 + F(T)x + G(T).$$

et soit $\Delta(T)$ son discriminant. Ce dernier se factorise sous la forme : $\Delta(T) = d\prod_{i=0}^{n} P_i(T)^{e_i}$, où les $P_i \in \mathbb{Q}[T]$ sont des polynômes irréductibles unitaires deux à deux distincts et $d \in \mathbb{Q}$ et $e_i \in \mathbb{N}^*$.

Ceux-ci correspondent aux places de mauvaise réduction de $\mathscr{E}_T/\mathbb{Q}(T)$, qu'on appellera *places génériques*.

La caractérisation « usuelle » des types de réduction n'est pas assez précise pour nos besoins. Nous allons décrire la réduction de $\mathscr{E}$ en w_P une place de $\mathbb{Q}[T]$ associée à un

polynôme $P(T) \in \mathbb{Z}[T]$ par un symbole de Kodaira. Ceci est décrit plus en détail dans [47] Appendice C, Tableau 15.1.

La réduction de $\mathscr{E}$ en $P(T)$ est dite de type I_m si et seulement si $\mathscr{E}$ est de réduction multiplicative en P, de type I_m^* si et seulement si $\mathscr{E}$ est de réduction additive potentiellement multiplicative. Si $\mathscr{E}$ est de réduction additive potentiellement bonne alors en fonction de la valeur de $\mathrm{ord}_{w_P}\Delta(T)$, la fibre sera de type II, II^*, III, III^*, IV, IV^* ou I_0^*. Enfin, une fibre est de type I_0 si et seulement si elle est de bonne réduction.

0.1.3 Variation du signe de l'équation fonctionnelle

Soit E une courbe elliptique sur $\mathbb{Q}$. On appelle le *signe de E* (en anglais *root number of E*) l'entier

$$W(E) = \prod_p W_p(E),$$

où le produit est pris sur toutes les places de $\mathbb{Q}$ ($\{p \text{ premiers}\} \cup \infty$) et le signe local $W_p(E) \in \{\pm 1\}$ ne dépend que de $\tilde{E}/\mathbb{Q}_p$. Les formules pour les $W_p(E)$ sont donnée par [13] si $p = 2, 3$. Sinon, [38] donne une formule pour le signe local en p qui sera rappelée dans la section 1.1.5 de cette thèse.

Dans le cas où le corps de définition est $\mathbb{Q}$, le signe est égal au *signe de l'équation fonctionnelle* de E ; c'est-à-dire le signe $W(E) \in \{\pm 1\}$ tel que la fonction L de la courbe elliptique respecte l'équation fonctionnelle

$$\mathscr{N}_E^{(2-s)/2}(2\pi)^{s-2}\Gamma(2-s)L(E,2-s) = W(E)\mathscr{N}_E^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s),$$

pour tout $s \in \mathbb{C}$ où $\mathscr{N}_E$ est le conducteur de E.

Soit $r_{an}(E/\mathbb{Q})$ l'ordre d'annulation en $s = 1$ de $L(E,s)$ la fonction L associée à E. La conjecture de Birch et Swinnerton-Dyer prédit que $\mathrm{rang}(E/\mathbb{Q}) = r_{an}(E/\mathbb{Q})$ et en particulier l'égalité suivante, appelée la *conjecture de parité* :

$$W(E) = (-1)^{\mathrm{rang}(E(\mathbb{Q}))}.$$

Remarque 4. Les travaux de Nekovář [34], Dokchitser et Dokchitser [7] montrent que la finitude du groupe de Tate-Shafarevitch de E implique la conjecture de parité pour E.

Remarque 5. La raison principale pour laquelle on se cantonne au cas $k = \mathbb{Q}$ est que la conjecture est beaucoup plus près d'être démontrée que sur les autres corps de nombres. En effet, l'équation fonctionnelle admet un prolongement analytique adéquat à tout le plan complexe. De plus, le signe de $\mathscr{E}$ est bien égal au signe de l'équation fonctionnelle sur $\mathbb{Q}$.

Soit une surface elliptique $\mathscr{E} \xrightarrow{\pi} \mathbb{P}$ dont la fibre en $t \in \mathbb{Q}$ est notée $\mathscr{E}_t$. On étudiera les ensembles

$$W_\pm(\mathscr{E}) = \{t \in \mathbb{Q} : E_t \text{ est une courbe elliptique et } W(E_t) = \pm 1\}.$$

Une conséquence de la conjecture de parité et du théorème 0.1.1 est qu'il suffit que $\#W_-(\mathscr{E}) = \infty$ pour qu'on ait la densité des points rationnels sur $\mathscr{E}$.

0.1.4 Surfaces isotriviales

On dit qu'une surface elliptique est *isotriviale* si $t \mapsto j(\mathscr{E}_t)$, la fonction du j-invariant des fibres, est constante. On note $j(\mathscr{E})$ cette valeur commune. On a donc $j(\mathscr{E}) \in \mathbb{Q}$.

Une telle surface admet une courbe elliptique E_o sur $\mathbb{Q}$ telle que $\mathscr{E}$ est une famille de tordues de E_o. Elle peut être décrite par un des trois types suivants :

1. $y^2 = x^3 + af(T)^2x + bf(T)^3$, où $f(T)$ est un polynôme sans facteur carré et $ab \neq 0$, (on a $j(T) \in \mathbb{Q}\backslash\{0, 1728\}$.)
2. $y^2 = x^3 + f(T)x$, $f(T)$ est sans facteur de puissance 4, (on a $j(T) = 1728$.)
3. $y^2 = x^3 + f(T)$, $f(T)$ est sans facteur de puissance 6 (on a $j(T) = 0$).

Remarque 6. La raison pour laquelle on fait la distinction entre les cas 1, 2 et 3 est que les tordues d'une courbe elliptique sont paramétrées par $H^1(G_{\mathbb{Q}}, Aut(E))$.

1. Lorsque $j \in \mathbb{Q} \setminus \{0, 1728\}$, on a $Aut(E) = \mathbb{Z}/2\mathbb{Z}$,
2. lorsque $j = 0$, on a $Aut(E) = \mathbb{Z}/6\mathbb{Z}$ et
3. lorsque $j = 1728$, on a $Aut(E) = \mathbb{Z}/4\mathbb{Z}$.

Soit $W := t \mapsto W(\mathscr{E}_t)$ la fonction du signe des fibres de $\mathscr{E}$. Si $\mathscr{E}$ est isotriviale, il est possible que W soit constante. Si W est constant égale à $+1$, on ne peut rien conclure quant à la densité des points rationnels de ces surfaces à partir de l'étude du signe. Dans [3], Cassels et Schinzel trouvent une famille de courbes elliptiques dont le signe est constant, égal à -1. Cet exemple, d'invariant $j = 1728$, est

$$\mathscr{E}_T : y^2 = x^3 - (7 + 7T^4)^2x.$$

Varilly-Alvarado donne dans [51] davantage d'exemples, parmi lesquels la surface elliptique d'invariant $j = 0$ donnée par l'équation de Weierstrass

$$y^2 = x^3 + 27T^6 + 16,$$

dont les fibres sont de signe $+1$.

Dans beaucoup de cas, cependant, on sait que l'application W n'est pas constante. On a notamment le théorème suivant dû à Rohrlich.

Théorème 0.1.6. *[38, Théorème 2] Soit $a, b \in \mathbb{Z}$ tel que $ab \neq 0$. On considère la courbe elliptique définie par l'équation $E : y^2 = x^3 + ax + b$ si $\Delta \neq 0$. Soit $f(t) \in \mathbb{Z}[t]$ et la famille de tordues quadratiques définie par l'équation*

$$E_{f(t)} : f(t)y^2 = x^3 + ax + b$$

Alors, l'une des deux propositions suivantes est vraie :

1. *Les ensembles W_+ et W_- sont denses dans $\mathbb{R}$.*
2. *Les ensembles W_+ ou de W_- sont $\{t \in \mathbb{Q} | f(t) < 0\}$ et $\{t \in \mathbb{Q} | f(t) > 0\}$.*

De plus, pour E donnée,

1. *il existe f tel qu'on est dans le cas 2 et tel que le nombre de changements de signe de f sur $\mathbb{R}$ dépasse n'importe quelle valeur préassignée.*
2. *si en outre E a bonne réduction sur une extension abélienne de $\mathbb{Q}$, on est dans le cas 2.*

Remarque 7. Plus explicitement, si E a bonne réduction sur $\mathbb{Q}^{ab}$ alors $\forall d \in \mathbb{Q}^*$ on a

$$W(E_d) = sgn(d)W(E).$$

Dans le cas d'une surface de Del Pezzo de degré 1 dont la surface elliptique rationnelle associée est isotriviale, Varilly-Alvarado [51] démontre le théorème suivant.

Notation 0.3. Pour tout $n \in \mathbb{Z}$, on désignera par μ_n l'ensemble des racines n-ième de l'unité.

Théorème 0.1.7. *[51, Thm 2.1] Soit $F(x,y) \in \mathbb{Z}[x,y]$ un polynôme homogène de degré 6 dont on suppose que les coefficients en x^6 et en y^6 sont non nuls. Soit X la surface de Del Pezzo de degré 1 sur $\mathbb{Q}$ donnée par*

$$w^2 = z^3 + F(x,y)$$

dans $\mathbb{P}_{\mathbb{Q}}(1,1,2,3)$, l'espace projectif à poids de variables (x,y,z,w). Soit c le contenu de F : on écrit $F(x,y) = cF_1(x,y)$, avec $F_1(x,y) \in \mathbb{Z}[x,y]$. On suppose qu'il existe $f_i \in \mathbb{Z}[x,y]$ un facteur homogène irréductible de F_1 tel que

$$\mu_3 \not\subseteq \mathbb{Q}[t]/f_i(t,1), \tag{1}$$

où μ_3 est le groupe des racines troisième de l'unité dans $\overline{\mathbb{Q}}$. Enfin, on suppose que la conjecture de parité est vérifiée pour les courbes elliptiques sur $\mathbb{Q}$ de j-invariant 0.

Alors les points rationnels de X sont denses pour la topologie de Zariski.

Remarque 8. Dans le même article, on a un résultat similaire [51, Thm 2.3] pour les surfaces représentées dans $\mathbb{P}(1,1,2,3)$ par une équation de la forme

$$w^2 = z^3 + G(x,y)z,$$

où $G(x,y) \in \mathbb{Z}[x,y]$ est un polynôme homogène de degré 4. Ce ne sont pas tout à fait des surfaces de Del Pezzo de degré 1 : elles ont un point qui n'est pas lisse. L'hypothèse remplaçant (1) est celle qu'il existe $g_i \in \mathbb{Z}[x,y]$, un facteur irréductible de G tel que

$$\mu_4 \not\subseteq \mathbb{Q}[t]/g_i(t,1).$$

0.1.5 Surfaces non isotriviales

Rizzo [37] exhibe $E_T : y^2 + Tx^2 - (T+3)x + 1$ une surface elliptique rationnelle non isotriviale dont la fonction du signe restreinte à $\mathbb{Z}$ est constante, c'est-à-dire que $W(E_t) = -1$ pour toute fibre associée à $t \in \mathbb{Z}$. Cependant, le signe de E_t n'est pas constant sur les fibres en $t \in \mathbb{Q}$.

Il est conjecturé que si la surface n'est pas isotriviale, il y a toujours variation du signe des fibres sur $\mathbb{Q}$. Les résultats de Manduchi vont dans ce sens.

Théorème 0.1.8. *[27, Thm 1] Soit $\mathscr{E} \xrightarrow{\pi} \mathbb{P}^1$ une surface elliptique non isotriviale telle que*

1. *les polynômes associés aux places de mauvaise réduction sont de degré ≤ 6,*
2. *$\mathscr{E}$ n'a pas de place générique de type I_m,*

Alors, W_+ et W_- sont denses dans $\mathbb{R}$.

Dans le même article, Manduchi démontre un second théorème, avec des hypothèses légèrement différentes.

Théorème 0.1.9. *[27, Thm 2] Soit $\mathscr{E} \to \mathbb{P}^1$ une surface elliptique non isotriviale telle que*

1. *les polynômes associés aux places de mauvaise réduction sont de degré inférieur ou égal à 3,*
2. *$\mathscr{E}$ a au plus une fibre générique de type I_m et celle-ci est associée à un polynôme linéaire.*

Alors W_+ et W_- sont tous deux infinis.

La technique utilisée par Manduchi consiste à trouver $\mathscr{F}, \mathscr{F} \subseteq \mathbb{Z}^2$, deux ensembles infinis de paires d'entiers premiers entre eux tels que pour tout $(x, y) \in \mathscr{F}_1$ et $(x', y') \in \mathscr{F}$ on ait

$$W\left(E_{\frac{x}{y}}\right) = -W\left(E_{\frac{x'}{y'}}\right).$$

Pour cela, on fait un crible sur les paires (x, y) d'entiers premiers entre eux qui définissent $t = x/y \in \mathbb{Q}$, afin de contrôler les facteurs carrés des polynômes impliqués.

0.1.6 Conjectures de théorie analytique des nombres

L'utilisation des méthodes de crible mentionnées ci-dessus justifie que l'on s'intéresse à deux conjectures, présentées dans cette section. Nous traiterons simultanément le cas d'un polynôme f de degré d à coefficients entiers, ou bien en une variable, ou bien homogène en deux variables ; ainsi ou bien $f(T) = a_0 + \cdots + a_d T^d \in \mathbb{Z}[T]$ ou bien $f(T, U) = a_0 U^d + \cdots + a_d T^d \in \mathbb{Z}[T, U]$. On notera $h = 1$ ou 2 le nombre de variables et v un vecteur à coordonnées entières dans $\mathbb{Z}^h$, c'est-à-dire $\mathrm{v} \in \mathbb{Z}$ ou $\mathrm{v} \in \mathbb{Z}^2$. On étudie deux propriétés décrivant la factorisation de $f(\mathrm{v})$: la première décrit la proportion de valeurs sans facteurs carrés, la deuxième la parité du nombre de facteurs premiers.
Notations. Soit $\delta_f := \mathrm{pgcd}\left\{f(\mathrm{v}) \mid \mathrm{v} \in \mathbb{Z}^h\right\}$, alors d_f désigne le plus petit entier tel que δ_f/d_f soit sans facteur carré. Écrivons $d_f = \prod_p p^{\nu_p}$ On note $t_f(p)$ le nombre de solutions modulo $p^{2+\nu_p}$ de $f(\mathrm{v}) d_f^{-1} \equiv 0 \mod p^2$, ou encore $f(\mathrm{v}) \equiv 0 \mod p^{2+\nu_p}$ et on pose

$$C_f := \prod_p \left(1 - \frac{t_f(p)}{p^{2(2+\nu_p)}}\right)$$

Conjecture 0.1.10. *(Conjecture du crible des facteurs carrés)*
Soit f un polynôme à coefficients entiers sans facteur carré, en h variables ($h = 1$ ou 2).
Alors

$$\#\{\mathrm{v} \in \mathbb{Z}^h \mid |\mathrm{v}| \leq X,\ f(\mathrm{v})/d_f \text{ est sans facteur carré }\} = C_f (2X)^h + o(X^h) \quad (X \to +\infty).$$

Si l'on veut étudier les valeurs (presque) sans facteurs carrés sur une progression arithmétique ou un réseau $\mathcal{A} = \phi(\mathbb{Z}^h)$ (avec $\phi(n) = a + bn$ pour $b \neq 0$ si $h = 1$, et $\phi(m, n) = (am + bn, cm + dn)$), on posera $g := f \circ \phi$, $d_{f,\mathcal{A}} := d_g$, $\tilde{C}_{f,\mathcal{A}} := \tilde{C}_g$ et on peut écrire la conjecture du crible des facteurs carrés sous la forme apparemment plus générale :

$$\sharp\left\{\mathrm{v} \in \mathcal{A}(X) \mid f(\mathrm{v}) d_{f,\mathcal{A}}^{-1} \text{ est sans facteur carré}\right\} = \tilde{C}_{f,\mathcal{A}} A(X) + o(A(X)), \tag{2}$$

où $\mathcal{A}(X) = \{\mathrm{v} \in \mathcal{A} \mid |\mathrm{v}| \leq X\}$ et $A(X) = \sharp\mathcal{A}(X)$.

La conjecture est démontrée pour les polynômes irréductibles de degré ≤ 3 (resp. ≤ 6) en 1 variable (resp. en 2 variables), ce que nous résumons dans l'énoncé suivant. La preuve est relativement simple (résultant en fait essentiellement des considérations qui suivent) lorsque $h = 1$ et $d \leq 2$ ou $h = 2$ et $d \leq 4$. Les cas suivants sont plus délicats, le cas $h = 1$ et $d = 3$ est prouvé par Hooley [18], le cas $h = 2$ et $d = 5, 6$ est prouvé par Greaves [9].

Théorème 0.1.11. *(Hooley [18], Greaves [9]) Soit f un polynôme à coefficients entiers, sans facteurs carrés, en h variables ($h = 1$ ou 2). Supposons que tous les facteurs irréductibles de f soient de degré inférieur ou égal à $3h$, alors f vérifie la conjecture du crible des facteurs carrés.*

La seconde conjecture, dite de Chowla, concerne l'étude de la fonction de Liouville définie comme suit :

Pour $n = p_i^{e_1} \dots p_r^{e_r}$,

$$\lambda(n) = (-1)^{\Omega(n)},$$

où $\Omega(n)$ est le nombre de facteurs premiers de n, comptés avec multiplicité, en d'autres termes, $\Omega(n) = \sum_{i=1}^{r} e_i$.

Conjecture 0.4. *(Conjecture de Chowla)*

Soit f un polynôme à coefficients entiers, sans facteurs carrés. Pour toute progression arithmétique $\mathcal{A}$, on a l'estimation suivante

$$\sum_{v \in \mathcal{A}(X)} \lambda(f(v)) = o(A(X)).$$

Les résultats connus à l'heure actuelle sont les suivants.

Théorème 0.1.12. *Soit f un polynôme de degré d à coefficients entiers, sans facteurs carrés, en h variables ($h = 1$ ou 2). La conjecture de Chowla vaut dans les cas suivants :*

1. *(Hadamard – de la Vallée Poussin) $h = 1$ et $d = 1$.*
2. *(Helfgott, Lachand) $h = 2$ et $d \leq 3$.*
3. *(Green-Tao) $h = 2$ et f est un produit de formes linéaires.*

Le premier item ($h = \deg(f) = 1$) équivaut en fait au théorème des nombres premiers sous la forme $\sum_{m \leq X} \mu(m) = o(X)$. Le deuxième, pour f homogène en deux variables et $\deg(f) \leq 2$ est essentiellement dû à de la Vallée Poussin. Le cas de degré 3 est dû à Helfgott [17] (noter cependant que l'article cité traite d'un polynôme cubique non irréductible ; le cas d'un polynôme cubique irréductible [16] est non publié), puis récemment en 2014 par une autre technique par Lachand dans sa thèse de doctorat [24] et dans un article à paraître [25]. Enfin, Green et Tao [10] prouve Chowla pour un produit de formes linéaires.

0.1.7 Signe moyen

Dans un article à ce jour non publié [15], Helfgott calcule le signe moyen d'une surface elliptique sur tous les $t \in \mathbb{Q}$, où les $t = x/y$ sont représentés par un couple d'entiers premiers entre eux

$$\mathrm{av}_{\mathbb{Q}} W(\mathscr{E}) = \lim_{N \longrightarrow \infty} \frac{\sum_{(x,y) \in [-N,N]^2 : \mathrm{pgcd}(x,y)=1, y \neq 0} W(\mathscr{E}_{x/y})}{|\{(x,y) \in [-N,N]^2 : \mathrm{pgcd}(x,y) = 1\}|}.$$

On peut aussi faire la moyenne seulement sur $n \in \mathbb{Z}$:

$$\mathrm{av}_{\mathbb{Z}} W(\mathscr{E}) = \lim_{N \longrightarrow \infty} \frac{\sum_{n \in [-N,N]} W(\mathscr{E}_n)}{2N}.$$

On note $B_{\mathscr{E}}$ le produit des polynômes associés aux places en lesquelles la réduction de $\mathscr{E}$ n'est pas I_0 ni I_0^*. Quant à $M_{\mathscr{E}}$, c'est le produit des places de réduction multiplicative. Le résultat principal est le théorème suivant.

Théorème 0.1.13. *[15] Soit $\mathscr{E}$ une surface elliptique non isotriviale sur $\mathbb{Q}$. On admet les hypothèses suivantes :*

a. la conjecture du crible des facteurs carrés (dans sa version homogène) est vérifiée par $B_{\mathscr{E}}$,

b. la conjecture de Chowla est vérifiée (dans sa version homogène) par $M_{\mathscr{E}}$.

Alors,

1. *si $\mathscr{E}$ n'a pas de place de réduction multiplicative, on a*

$$av_{\mathbb{Q}}(W(\mathscr{E}_t)) \in]-1,1[;$$

2. *s'il existe une place de réduction multiplicative, on a*

$$av_{\mathbb{Q}}(W(\mathscr{E}_t)) = 0.$$

En particulier, dans les deux cas, W_+ et W_- sont infinis.

0.2 Résultats nouveaux

0.2.1 Revue des résultats de Helfgott sur le signe moyen d'une surface elliptique

Je structure la démonstration du théorème suivant, dû à Helfgott (voir [15], un article à ce jour non publié) :

Théorème 0.2.1. *[15, Thm. 6.6]*
Soit $\mathscr{E}$ une courbe elliptique sur $\mathbb{Q}(T)$. Pour $t \in \mathbb{Q}$, on note $t = \frac{x}{y}$ pour x, y des entiers premiers entre eux. Alors il existe :

1. *S un ensemble fini de places de $\mathbb{Q}$ qui contient la place à l'infini ;*
2. *pour chaque $v \in S$, des fonctions $g_v : \mathbb{Q}_v \times \mathbb{Q}_v \longrightarrow \{-1, 1\}$ localement constantes pour la topologie v-adique en dehors d'un ensemble fini de droites passant par l'origine ; et*
3. *pour chaque $p \notin S$, des fonctions $h_p : \mathbb{Q}_p \times \mathbb{Q}_p \to \{-1, 1\}$ localement constantes en dehors d'un ensemble fini de droites passant par l'origine telles que $h_p(x, y) = 1$ lorsque $p^2 \nmid B_{\mathscr{E}}(x, y)$;*

tels que le signe s'écrit

$$W(\mathscr{E}_t) = \lambda(M_{\mathscr{E}}(x, y)) \cdot \prod_{v \in S} g_v(x, y) \prod_{p \notin S} h_p(x, y),$$

Ce théorème est crucial pour le calcul du signe moyen. En particulier, j'explicite quelles sont l'ensemble S et les fonctions g_v et h_p en fonction de l'équation de la surface elliptique considérée.

De plus, je complète la démonstration du lemme suivant, qui n'avait pas été rédigée entièrement par Helfgott.

Lemme 0.2.2. *Soit $\mathscr{E}$ une surface elliptique non isotriviale sans place de réduction de type I_m. On suppose que $B_{\mathscr{E}}$ respecte la conjecture du crible des facteurs carrés. Alors*

$$-1 < av_{\mathbb{Q}} W(\mathscr{E}_t) < +1.$$

Je donne également, dans la proposition 4.3.1, les conditions sur une surface elliptique rationnelle $\mathscr{E}$ pour que le théorème 0.1.13 s'applique inconditionnellement. Si on suppose vérifiée la conjecture de parité, cela implique la densité des points rationnels sur $\mathscr{E}$.

0.2.2 Surfaces elliptiques non isotriviales

J'étends les résultats de variation du signe de [27] et de [15] à davantage de surfaces elliptiques non isotriviales. C'est le théorème principal de cette thèse (voir le théorème 5.0.8) :

Théorème 0.2.3. *Soit $\mathscr{E} \xrightarrow{\pi} \mathbb{P}^1$ une surface elliptique non isotriviale. Soit $\Delta = d \cdot P_1^{\mathrm{ord}_{P_1}\Delta} \dots P_r^{\mathrm{ord}_{P_r}\Delta}$ la factorisation en facteurs irréductibles sur $\mathbb{Q}(T)$ du discriminant de $\mathscr{E}_T$. On suppose que*

1. *pour tout P_i de réduction de type II, II^*, IV ou IV^*, on a*
$$\mu_3 \subseteq \mathbb{Q}[t]/P_i(t);$$
2. *pour tout P_i de type III ou III^* on a*
$$\mu_4 \subseteq \mathbb{Q}[t]/P_i(t),$$
3. *$\deg M_{\mathscr{E}} \leq 3$, ou $M_{\mathscr{E}}$, de degré arbitraire, est un produit de formes linéaires,*
4. *et tout P_i de réduction I_m^* vérifie $\deg P_i \leq 6$;*

Alors les ensembles
$$W_{\pm}(\mathscr{E}) = \{t \in \mathbb{Q} | W(\mathscr{E}_t) = \pm 1\}$$
sont tous deux de cardinalité infinie.

Ce résultat permet d'obtenir un corollaire direct.

Corollaire 0.2.4. *Soit $\mathscr{E}$ une surface respectant les hypothèses 1 à 4 du théorème 0.2.3. On suppose vraie la conjecture de parité. Alors l'ensemble des points rationnels de $\mathscr{E}$ est Zariski-dense.*

Remarque 9. La condition sur le degré des polynômes dont la réduction est de type I_m^* est là pour assurer qu'il soit possible de contrôler les facteurs carrés de ces polynômes. Toutefois, contrairement aux résultats antérieurs précités, on ne met pas de telle restriction sur les autres places. Leurs polynômes associés peuvent être de degré arbitrairement grand tel que l'illustre l'exemple suivant :

Théorème 0.2.5. *Soit $Q(T) \in \mathbb{Z}[T]$ un produit de facteurs irréductibles distincts Q_i de degré inférieur ou égal à 6, et tel que $Q(0) \neq 0$. On fixe $N \in \mathbb{N}$ et on définit*
$$P(T) = 3\alpha^2 Q(T)^2 + \beta^2 T^{2N},$$
où $\alpha, b \in \mathbb{Z}\backslash\{0\}$ sont premiers entre eux. Soit la surface elliptique décrite par l'équation
$$\mathscr{E} : y^2 = x^3 - 27P(T)Q(T)^2 x - 54\beta P(T)Q(T)^3 T^N.$$

On suppose vraie la conjecture de parité.
Alors les points rationnels de $\mathscr{E}$ sont denses pour la topologie de Zariski.

Remarque 10. Cette surface respecte les hypothèses du théorème 0.2.3. Par conséquent, le corollaire 0.2.4 implique la Zariski-densité des points rationnels sur $\mathscr{E}$, si l'on admet la conjecture de parité.

Remarque 11. Dans cet exemple, on a $\deg P = 2\max(\deg Q, N)$. Par conséquent, dès que $N \geq 4$, on ne sait pas en général si P respecte la conjecture du crible des facteurs carrés. La surface $\mathscr{E}$ définie ci-dessus ne vérifie donc pas les hypothèses du théorème 0.1.13 de Helfgott.

0.2.3 Combinaison des conjectures SFC et Chowla

Notation 1. Un réseau est un ensemble de la forme

$$\mathcal{A} = \{(ax + by, cx + dy) \in \mathbb{Z}^2 |\ (x, y) \in \mathbb{Z}^2\}$$

où $a, b, c, d \in \mathbb{Z}$ et $ad - bc \neq 0$.

On note $\mathcal{A}(X) := \{(m, n) \in \mathcal{A} \mid |(m, n)| \leq X\}$ et $A(X) := \sharp\mathcal{A}(X)$.

La démonstration du théorème 0.2.3 utilise le théorème suivant, dont la démonstration ne semble pas se trouver dans la littérature :

Théorème 0.2.6. *Soit $f \in \mathbb{Z}[X, Y]$ polynôme homogène à coefficients entiers, sans facteurs carrés. Supposons la conjecture du crible des facteurs carrés et la conjecture de Chowla vraies pour f, alors l'estimation suivante vaut pour tout réseau $\mathcal{A}'$, où $\epsilon = \pm 1$:*

$$\sharp\left\{(m, n) \in \mathcal{A}'(X) \mid \frac{f(m, n)}{d_{f,\mathcal{A}'}} \text{ est sans facteur carré et } \lambda(f(m, n)) = \epsilon\right\} = \frac{c_{f,\mathcal{A}'}}{2}\mathrm{A}'(X) + o(A'(X)). \tag{3}$$

Remarque 12. L'énonce indique une sorte d'indépendance des deux propriétés relatives aux valeurs d'un polynôme

1. « sans facteur carré »
2. « parité » du nombre de facteurs.

0.2.4 Surfaces elliptiques rationnelles non isotriviales

Je démontre dans plusieurs cas la densité des points rationnels de certaines surfaces elliptiques rationnelles non isotriviales par des arguments géométriques, en particulier sans étudier la variation du signe sur les fibres de $\mathscr{E}$ et donc sans recours à la conjecture de parité.

Les résultats suivants traitent davantage de surfaces elliptiques rationnelles que l'article de Helfgott et ce d'une manière qui ne dépende d'aucune conjecture.

Lemme 0.2.7. *Soit $\mathscr{E}$ une surface elliptique rationnelle. Si $\mathscr{E}$ possède une place rationnelle de type I_0^*, II^*, III^*, IV^* ou I_m^*, alors les points rationnels de X sont denses pour la topologie de Zariski.*

En particulier, si $\mathscr{E}$ est une surface elliptique non isotriviale sans place de réduction multiplicative, alors les points rationnels de X sont denses.

Lemme 0.2.8. *Soit $\mathscr{E}$, une surface elliptique d'équation de Weierstrass de la forme*

$$y^2 = x^3 + L_1^2 L_2 L_3 x + L_1^3 L_2^2 L_3,$$

où $L_1, L_2, L_3 \in \mathbb{Z}[T]$ sont des polynômes linéaires. Alors les points rationnels de X sont Zariski-denses.

Remarque 13. Cette dernière proposition est contenue dans la précédente. Toutefois, la démonstration utilise des arguments nouveaux et plus simples.

0.2.5 Surfaces elliptiques rationnelles isotriviales

Les surfaces elliptiques rationnelles isotriviales sont de l'une des formes suivantes

1. $y^2 = x^3 + aH(u,v)^2x + bH(u,v)^3$, avec $4a^3 + 27b^2 \neq 0$ (telles que $j(T) \in \mathbb{Q}\backslash\{0, 1728\}$),
   Remarque 14. Une surface de cette forme est birationnelle à
   $$H(u,v)y^2 = x^3 + ax + b.$$
2. $y^2 = x^3 + A(u,v)x$ (telles que $j(T) = 1728$),
3. $y^2 = x^3 + B(u,v)$ (telles que $j(T) = 0$)

où A, B, et H sont des polynômes homogènes de degré respectivement 4, 6 et 2.

On peut supposer également dans les équations précédentes que H n'est pas un carré, A n'est pas un bicarré et que B n'est pas une puissance sixième. En effet, cela équivaut à éviter le cas trivial où il existe une courbe E_0 telle que

$$\mathscr{E} = E_0 \times \mathbb{P}^1,$$

car alors

1. le signe est automatiquement constant,
2. si $E_0(\mathbb{Q})$ est fini, alors $\mathscr{E}(\mathbb{Q})$ n'est pas dense.

Dans chaque cas, j'obtiens des résultats intéressants sur la densité des points rationnels ou sur la variation du signe. Dans un premier temps, je démontre la densité sur certaines de ces surfaces par des arguments géométriques :

Théorème 0.2.9. *Soit X une surface elliptique rationnelle d'équation*

$$X : H(u,v)w^2 = z^3 + az + b,$$

où $H(u,v)$ est un polynôme homogène de degré 2 qui n'est pas un carré et $a, b \in \mathbb{Z}\backslash\{0\}$.

Alors la surface est unirationnelle sur $\mathbb{Q}$. En particulier, ses points rationnels sont denses pour la densité de Zariski.

Remarque 15. Ce résultat est démontré par Rohrlich [38, Theorème 3] sous l'hypothèse *a priori* restrictive qu'il existe une fibre de rang non nul. Cette hypothèse est enlevée ici.

On démontre grâce à divers arguments le théorème suivant. Pour ce faire, on exhibe une section sur $\mathscr{E}$ qui est d'ordre infini pour une infinité de fibres dans certains cas et d'ordre 2 dans les autres.

Théorème 0.2.10. *Soit X une surface elliptique rationnelle d'équation de Weierstrass*

$$X : w^2 = z^3 + A(T,1)z,$$

où $A(u,v) \in \mathbb{Z}[u,v]$ est un polynôme homogène de degré 4 à coefficients entiers.

Alors, les points rationnels de $\mathscr{E}$ sont denses pour la topologie de Zariski.

Le cas le plus délicat est donc le type 3, c'est-à-dire $y^2 = x^3 + B(u,v)$ que l'on ne sais pas traiter en général. Remarquons que, contrairement aux deux cas précédents où il y a des points singuliers, la contraction de la section neutre d'une surface de cette forme donne lieu à une surface de Del Pezzo de degré 1. Poursuivant les travaux de Varilly-Alvarado mentionnés plus tôt (théorème 3.2.4), j'étudie la variation du signe de surfaces elliptiques rationnelles d'équation de la forme :

$$y^2 = x^3 + C(3A^2t^6 + B^2) \tag{4}$$

Ceci me donne des conditions, données par le théorème 4.2.9, pour les coefficients des surfaces pour que le signe de leurs fibres soit constant. (Je trouve des exemples de signe $+1$ et de signe -1.) Pour les surfaces ne respectant pas ces conditions, le signe varie. La conjecture de parité implique donc la densité de leur points rationnels.

On étudie aussi la variation du signe sur les surfaces de la forme

$$y^2 = x^3 + C(A^2t^4 + B^2)x, \tag{5}$$

où $A, B, C \in \mathbb{Z}$ sont tels que $pgcd(A, B) = 1$. Cette forme correspond à un des cas où le théorème 0.2.10 ne permet pas de construire explicitement une infinité de fibre de rang ≥ 1. Pour les surfaces de la forme (4), les conditions pour que le signe des fibres soit constant sur tout $t \in \mathbb{Q}$ sont données par le théorème 4.2.6.

0.2.6 Variation du signe sur les surfaces elliptiques isotriviales

J'étudie plus généralement la variation du signe sur les surfaces elliptiques isotriviales. Pour celles-ci on n'impose pas de restriction sur le degré des coefficients de l'équation de Weierstrass de la surface.

Rappelons que les surfaces elliptiques isotriviales sont celles dont le j-invariant des fibres est constant. J'obtiens les résultats suivants :

Théorème 0.2.11. *Soit $\mathscr{E} \to \mathbb{P}^1$ une surface elliptique isotriviale dont on note $\mathscr{E}_t$ la fibre en t.*

1. *Supposons que la surface est d'équation $\mathscr{E} : Ty^2 = x^3 + ax + b$ pour $a, b \in \mathbb{Z} - \{0\}$. Alors*
   (a) *Il existe M entier tel que, pour $t \in \mathbb{Z} - \{0\}$ sans facteur carré, le signe $W(E_t)$ ne dépend que de la classe de congruence de t modulo M.*
   (b) *Le signe $W(E_t)$ n'est pas constant quand t varie dans $\mathbb{Q}^\times$.*
2. *Supposons que la surface est d'équation $\mathscr{E} : y^2 = x^3 + T$.*
   Soit $t = 2^\alpha 3^\beta t_1^1 t_2^2 t_3^3 t_4^4 t_5^5$, où $\alpha, \beta \in \mathbb{Z}$ et $t_i \in \mathbb{N}$ $i = 1, \cdots, 5$ sont premiers entre eux, non divisibles par 2 et 3, et sans facteur carré. Posons $\tau_1 = t_1t_3t_5$ et $\tau_2 = t_2t_4$.
   Alors on a les conclusions suivantes
   (a) *Le signe peut s'exprimer sous la forme*
   $$W(E_t) = -W_2(E_t)W_3(E_t)(\frac{-1}{\tau_1})(\frac{\tau_2}{3}).$$
   (b) *Il existe des entiers M_1 et M_2 tels que $W(E_t)$ est constant pour les t sans puissance sixième dont la partie τ_1 varie dans une classe de congruence modulo M_1 et dont la partie τ_2 varie dans une classe de congruence modulo M_2.*
   (c) *Il existe des (doubles) classes de t pour lesquelles $W(E_t) = +1$, et d'autres classes pour lesquelles $W(E_t) = -1$.*
3. *Supposons que la surface est d'équation $\mathscr{E} : y^2 = x^3 + Tx$.*
   Soit $t = 2^\alpha 3^\beta t_1^1 t_2^2 t_3^3$, avec $\alpha, \beta \in \mathbb{Z}$ et les t_i premiers entre eux, non divisibles par 2 et 3, et sans facteur carré. On pose $\tau_1 = t_1t_3$.

(a) *Alors le signe peut s'écrire*

$$W(E_t) = -W_2(E_t)W_3(E_t)(\frac{-2}{\tau_1})(\frac{-1}{t_2}).$$

(b) *Il existe des entiers M_1 et M_2 tels que $W(E_t)$ est constant, pour t sans puissance quatrième dont la partie τ_1 varie dans une classe de congruence modulo M_1 et dont la partie t_2 varie dans une classe de congruence modulo M_2.*

(c) *Il existe des (doubles) classes de t pour lesquelles $W(E_t) = +1$, et d'autres classes pour lesquelles $W(E_t) = -1$.*

Remarque 16. Ce résultat complète le théorème de Rohrlich cité précédemment (Théorème 0.1.6). En effet, ce dernier ne permet pas de conclusion directe sur la constance du signe dans le cas où E_1 n'est pas de bonne réduction sur $\mathbb{Q}^{ab}$ et $f(t) < 0$ (ou > 0). De plus, il ne dit rien sur les cas où la surface elliptique considérée a pour fonction du j-invariant $j(T) = 0$ ou 1728.

Remarque 17. Birch et Stephens [**?**] démontrent des formules pour le signe de $y^2 = x^3 - Dx$, et pour celui de $z^3 = x^3 + A$ (qui peut être ramené à l'équation $y^2 = x^3 - 432A^2$). Liverance [26] complète ces résultats en donnant une formule pour le signe de $y^2 = x^3 + D$ en général.

Les formules données en 2a et en 3a sont d'une nature légèrement différente de celles de ces deux articles, notamment parce qu'elles séparent les nombres premiers $p \geq 5$ selon si leur carré divise ou ne divise pas t. En ce sens, nos formules se rapproche plutôt de celles de Várilly-Alvarado [51, Prop. 4.4 et 4.8].

0.2.7 Organisation du texte

Dans le premier chapitre, nous rappellerons les notions qui seront utilisées dans cette thèse : les courbes elliptiques (type de réduction en une place de $\mathbb{Q}$, point de torsion, signe de l'équation fonctionnelle et conjecture de parité), les surfaces elliptiques (correspondance entre les surfaces elliptiques rationnelles lisses et les surfaces de Del Pezzo de degré 1, utilisation de la conjecture de parité sur les fibres de la surface pour démontrer la densité des points rationnels) et finalement les conjectures de théorie analytique des nombres (conjecture du crible des facteurs carrés, conjecture de Chowla, la liste des cas où elles sont démontrées et la démonstration du théorème 0.2.6).

Dans le second chapitre, nous reprendrons l'article non publié de Helfgott [15] dont nous structurons et complétons le théorème 0.1.13.

Le troisième chapitre sera consacré à la variation du signe sur les familles de tordues de courbes elliptiques. Nous démontrerons le théorème 0.2.11.

Nous étudierons les surfaces elliptiques rationnelles dans le quatrième chapitre, qui sera divisé en trois parties. La première est un rappel sur les surfaces de Del Pezzo de degré 1. Dans la second partie, nous traiterons de la densité des points rationnels sur les surfaces elliptiques rationnelles isotriviales. Nous présenterons des arguments géométriques démontrant la densité des points rationnels sur celles dont la surface elliptique associée est telle que $j(T) = 1728$ (le théorème 0.2.10) ou l'unirationnalité si $j(T) \in \mathbb{Q}/\{0, 1728\}$ (le théorème 0.2.9). Nous déterminerons sous quelles conditions le signe des fibres de la surface elliptique associée est constant, dans les cas où une démonstration plus directe n'est pas connue. On déterminera ainsi des conditions sur les coefficients d'une surface de Del Pezzo d'équations dans $\mathbb{P}(1, 1, 2, 3)$: $w^2 = z^3 + Au^6 + Bv^6$, (théorème 4.2.6) et $w^2 = z^3 + C(A^2u^4 + B^2v^4)z$ (théorème 4.2.9) pour que le signe de celle-ci soit constant. La troisième partie s'intéressera aux surfaces elliptiques rationnelles non isotriviales. Dans

un premier temps, on démontrera les lemmes 0.2.7 et 0.2.8 qui donnent la densité des points rationnels sur certaines de ces surfaces avec des arguments géométriques inédits. Nous ferons ensuite dans la proposition 4.3.1 une classification des surfaces elliptiques rationnelles non isotriviales et cerneront lesquelles sont traitées inconditionnellement par les résultats de Helfgott.

Dans le cinquième chapitre, nous démontrons le théorème 0.2.3. Ce théorème s'applique à des surfaces elliptiques qui ne sont pas incluses dans des travaux de nos prédécesseurs, par exemple celles construites dans le théorème 0.2.5.

1

Notions préliminaires

1.1 Courbes elliptiques

Définition 3. Une *courbe elliptique* E sur un corps k est une courbe projective lisse de genre 1 munie d'un point marqué $\mathscr{O}$.

Chacune de ces courbes peut être représentée comme le lieu dans $\mathbb{P}^2$ d'une équation cubique avec un point sur la ligne à l'infini, le point marqué. Une courbe elliptique admet une équation dite *de Weierstrass* de la forme

$$E : y^2 + a_1xy + a_3y = x^3a_2x^2 + a_4x + a_6, \tag{1.1}$$

où $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}$. Celle-ci est écrite sous forme affine pour alléger la notation, il faut donc se rappeler d'ajouter le point $[0, 1, 0]$ à l'infini.

Remarque 18. Lorsque la caractéristique du corps n'est pas 2 ou 3, on peut simplifier l'équation de Weierstrass.

D'abord, on fait la substitution $y \mapsto \frac{1}{2}(y - a_1x - a_3)$ pour obtenir une équation de la forme

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

où $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$ et $b_6 = a_3^2 + 4a_6$.

Avec le second changement de variable $(x, y) \mapsto (\frac{x-3b_2}{36}, \frac{y}{108})$, on obtient une équation de la forme

$$E : y^2 = x^3 - 27c_4x - 54c_6, \tag{1.2}$$

où $c_4 = b_2^2 - 4b_4$, et $c_6 = -b_2^3 + 36b_2b_4 - 216$.

Définition 4. Le discriminant d'une équation de Weierstrass est l'entier

$$\Delta = \frac{c_4^3 - c_6^2}{1728},$$

et son j-invariant est

$$j = \frac{c_4^3}{\Delta}.$$

L'homogénéisée d'une équation de la forme (1.1) définit une courbe C dans $\mathbb{P}^2$ avec un point à l'infini $\mathscr{O} = [0; 1; 0]$.

Cette courbe définit une courbe lisse si et seulement si le discriminant est non nul. Dans ce cas, on dit que C est *non singulière*.

Si $\Delta = 0$ et $c_4 \neq 0$, on dit que C a une *node*.

Si $\Delta = 0$ et $c_4 = 0$, on dit que C a une *pointe*

Notation 2. Soit E une courbe elliptique sur k et $k \subset K$ une extention de corps.

On note $E(K) = \{[x;y;1]\ (x,y)$ solution de E dans $\mathbb{A}_{\mathbb{K}}{}^2\} \cup [0;1;0]$ et on l'appelle *l'ensemble des points K-rationnels de E* ou encore le *groupe de Mordell-Weil* (on verra dans la suite qu'il s'agit bien d'un groupe).

Cette définition a aussi un sens pour les courbes de genre 1 qui sont singulières.

Définition 5. On appellera *tordue* (ou *twist*) d'une courbe elliptique, une courbe qui lui est isomorphe sur $\overline{\mathbb{Q}}$.

Proposition 1.1.1. *Deux courbes elliptiques sont isomorphes sur $\overline{\mathbb{Q}}$ si et seulement si elles ont le même $j-$invariant. De plus, soit $j_0 \in \overline{\mathbb{Q}}$, il existe une courbe elliptique définie sur $\overline{\mathbb{Q}}$ dont le j-invariant est égal à j_0.*

Définition 6. Soit E une courbe elliptique sur k. Une équation de Weierstrass pour E de la forme (1.1) est minimal si les coefficients a_1, a_2, a_3, a_4, a_6 sont k-entiers et si Δ le discriminant est minimal parmi les discriminants des équations de Weierstrass associés à cette courbe.

Remarque 19. Soit p, un nombre premier. Si $k = \mathbb{Q}$, une équation de Weierstrass est p-minimale si le discriminant est de valuation p-adique minimale. Par conséquent, l'équation est *minimale* si elle est p-minimale pour tout p.

De plus, pour tout courbe elliptique, on peut trouver un représentant *minimal* de l'équation de Weierstrass, c'est-à-dire que pour tout p, on a $p^4 \nmid c_4$ ou $p^6 \nmid c_6$.

1.1.1 Loi de groupe

Soit E une courbe elliptique sur $\mathbb{Q}$ donnée par une équation de Weierstrass. Soit L une droite dans $\mathbb{P}^2$. Étant donné que E est définie par une équation de degré 3, par le théorème de Bezout [14, I.7.8], la droite L coupe E en exactement 3 points ; nommons les P, Q, R. Ceux-ci peuvent ne pas être distincts, par exemple si L est tangente à E.

On définit la loi de composition $\oplus$ entre deux points $P, Q \in E$ de la manière usuelle, que l'on peut retrouver dans [47, III.2].

Définition 7. Soient $P, Q \in E$ et soit L, la droite reliant P et Q (ou si $P = Q$, la droite tangente à E en ce point). Soit aussi R, le troisième point d'intersection de L avec E. Soit L' la droite reliant R et $\mathscr{O}$, le point marqué de E. Alors L' coupe E en $R, \mathscr{O}$, et un troisième point. On note ce troisième point $P \oplus Q$.

Cette loi se visualise comme sur la figure 1.1.

Théorème 1.1.2. *(Mordell-Weil)*

Soit E, une courbe elliptique sur un corps de nombres k.

Alors $E(k)$ muni de $\oplus$ la loi de composition définie précédemment est un groupe abélien de type fini :

$$E(k) \simeq E(k)_{tor} \oplus \mathbb{Z}^r,$$

où $E(k)_{tor}$ est le groupe fini des points de torsion (appelé sous-groupe de torsion*) et $r \in \mathbb{N}$ est un entier positif ou nul appelé le* rang de E.

Dans la section suivante, on verra quelques résultats permettant de calculer le sous-groupe de torsion de E. Toutefois, si on sait comment calculer ce dernier, il n'en est pas de même pour le rang de E. Il n'existe pas de méthode générale pour le calculer.

Pour cette raison, nous utilisons en remplacement, dans cette thèse, le signe de l'équation fonctionnelle (présenté en section 1.1.5), une valeur parmi $\{-1, 1\}$ conjecturellement reliée à la parité du rang.

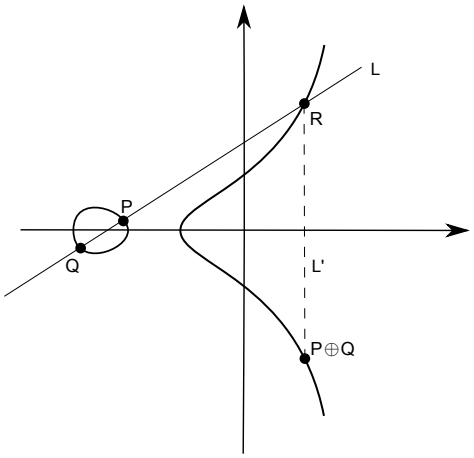


FIGURE 1.1 – Loi de groupe sur une courbe elliptique

1.1.2 Points de torsion

Soit E une courbe elliptique sur $\mathbb{Q}$.

Le théorème de Mordell-Weil implique que le groupe des points de torsion rationnels sur E est fini. Le théorème suivant donne des conditions pour qu'un point sur E soit de torsion. Ce résultat a été démontré de façon indépendante par Lutz et Nagell, et on le retrouve dans [47, p.240].

Proposition 1.1.3. *Soit $E/\mathbb{Q}$ une courbe elliptique d'équation de Weierstrass $y^2 = x^3 + Ax + B$, où $A, B \in \mathbb{Z}$.*

Supposons que $P \in E(\mathbb{Q})$ est un point de torsion différent du point à l'infini.

1. *$x(P), y(P) \in \mathbb{Z}$.*
2. *On a ou bien $[2]P = O$ ou bien $x([2]P) \in \mathbb{Z}$ et $y(P)^2$ divise $\Delta = 4A^3 - 27B^2$.*

Si l'on souhaite borner la torsion de E, la façon la plus rapide est de choisir un certain nombre de places v en lesquelles E est de bonne réduction et d'utiliser l'injection de la proposition suivante que l'on retrouve dans [47, VII.3] :

Proposition 1.1.4. *Soit E une courbe elliptique sur $\mathbb{Q}$ et soit p un nombre premier et $m \geq 1$ un entier premier à p. Si la courbe réduite $\tilde{E}/\mathbb{Q}_p$ est non singulière, alors l'application réduction*

$$E(\mathbb{Q})[m] \to \tilde{E}(\mathbb{Q}_p)$$

est injective, où $E(\mathbb{Q})[m]$ dénote l'ensemble des points d'ordre m dans $E(K)$.

De plus, on a le théorème suivant, qui caractérise pour de bon les formes que peuvent avoir le groupe $E(\mathbb{Q})_{\text{tor}}$:

Théorème 1.1.5. *[30],[31] Soit E une courbe elliptique sur $\mathbb{Q}$. Alors le sous-groupe de torsion $E(\mathbb{Q})_{tor}$ de $E(\mathbb{Q})$ est isomorphe à l'un des quinze groupes suivants :*

$$\begin{array}{ll} \mathbb{Z}/N\mathbb{Z} & \text{où } 1 \leq N \leq 10 \text{ ou } N = 12, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z} & \text{où } 1 \leq N \leq 4. \end{array}$$

1.1.3 Changement de modèle : le cas d'une quartique

On rappelle ici ce qui est expliqué dans le livre de Cassels [2].

Soit la courbe D représentée par l'équation

$$Y^2 = f(X)$$

où $f(X)$ est un polynôme de degré 4 munie d'un point rationnel. Comme D est une courbe de genre 1, c'est une courbe elliptique si elle possède un point rationnel. Soit (a, b), le point rationnel de D et supposons que $(a, b) \in D(\mathbb{Q})$.

Nous verrons dans cette section le changement de variable permettant de passer d'une telle équation à une équation de Weierstrass.

Quitte à effectuer le changement de variables

$$X \mapsto \frac{1}{X-a},\ Y \mapsto \frac{Y}{(X-a)^2},$$

on peut supposer que le point rationnel est à l'infini :

$$Y^2 = f_0 + f_1T + f_2T^2 + f_3T^3 + f_4T^4,$$

où f_4 est un carré.

Quitte à diviser par f_4 et à imposer le changement de variable $Y \mapsto \frac{Y}{\sqrt{f_4}}$, on peut supposer que $f_4 = 1$.

Par conséquent, on peut écrire le côté droit de l'équation sous la forme suivante :

$$G(T)^2 + H(T),$$

où

$$G(T) = T^2 + g_1T + g_0$$
$$H(T) = h_1T + h_0,$$

et où les g_j et les h_j sont donnés en termes des f_j. Explicitement, on a

$$g_0 = \frac{4f_2 - f_3^2}{8},\ g_1 = \frac{f_3}{2},\ h_0 = f_0 - (\frac{4f_2 - f_3^2}{8})^2,\ h_1 = f_1 - \frac{f_3}{2}(f_2 - \frac{f_3^2}{4}).$$

L'équation de la courbe s'écrit

$$(Y + G(T))(Y - G(T)) = H(T). \tag{1.3}$$

On pose $Y + G(T) = R'$, de façon à ce que

$$Y - G(T) = \frac{H(T)}{R'}$$

et que

$$2G(T) = R' - \frac{H(T)}{R'}.$$

On pose de plus $T = \frac{S'}{R'}$.

$$2(\frac{S'^2}{R'^2} + g_1\frac{S'}{R'} + g_0) = R' - h_1\frac{S'}{R'^2} - \frac{h_0}{R'}. \tag{1.4}$$

En multipliant l'équation (1.3) par R', on obtient

$$2S'^2 + 2g_1R'S' + 2g_0R'^2 = R'^3 - h_1S' - h_0R'. \tag{1.5}$$

Finalement, on procède au changement de variable $(R', S') = (2R, 2S)$ pour obtenir l'équation de Weierstrass générale suivante pour C_x.

$$C_x : S^2 + g_1RS + \frac{h_1}{4}S = R^3 - g_0R^2 - \frac{h_0}{4}R, \tag{1.6}$$

1.1.4 Types de réduction, symbole de Kodaira

Soit E une courbe elliptique sur un corps $\mathbb{Q}$ et v une place de $\mathbb{Q}$. On classifie E selon les possibilités suivantes.

Définition 8. Soit $E/\mathbb{Q}$ une courbe elliptique et une équation de Weierstrass minimale dont les coefficients c_4 et c_6 sont entiers, et soit $\tilde{E}$ la réduction de cette équation modulo une place de $\mathbb{Q}$. On dira que :

(a) E est de bonne réduction si $\tilde{E}$ est non singulière ($p \nmid \Delta$).

(b) E est de réduction multiplicative si $\tilde{E}$ a une node ($p \mid \Delta$ et $p \nmid c_4$). On dit qu'elle est :

i) déployée (*split*) si $-c_6$ est un carré modulo p,

ii) non déployé (*non-split*) sinon.

(c) E est de réduction additive si $\tilde{E}$ a une pointe ($p \mid \Delta$ et $p \mid c_4$).

Dans les cas (b) et (c), on dit que E a mauvaise réduction.

Ces notions ne sont pas assez précises pour ce qui suivra. Aussi introduit-on les symboles de Kodaira associés aux réductions de courbes elliptiques. (voir [47] Appendice C, Tableau 15.1)

Soit p un nombre premier différent de 2 ou 3. Nous avons les correspondances suivantes :
Réduction multiplicative

— la réduction de E en p est de type I_m si et seulement si $p \nmid c_4$, $p \mid \Delta$ et $m = \mathrm{ord}\Delta = -\mathrm{ord}j$;

Réduction additive potentiellement multiplicative

— de type I_m^* si et seulement si $p \mid c_4$, $p \mid \Delta$, $-ord\mathrm{j} = m$ et $\mathrm{ord}\Delta = m + 6$;

Réduction additive potentiellement bonne

— de type II si et seulement si $p \mid c_4$, $\mathrm{ord}_p\Delta = 2$;
— de type III si et seulement si $p \mid c_4$, $\mathrm{ord}_p\Delta = 3$;
— de type IV si et seulement si $p \mid c_4$, $\mathrm{ord}_p\Delta = 4$;
— de type I_o^* si et seulement si $p \mid c_4$, $\mathrm{ord}_p\Delta = 6$;
— de type IV^* si et seulement si $p \mid c_4$, $\mathrm{ord}_p\Delta = 8$;
— de type III^* si et seulement si $p \mid c_4$, $\mathrm{ord}_p\Delta = 9$;
— de type II^* si et seulement si $p \mid c_4$, $\mathrm{ord}_p\Delta = 10$;

Bonne réduction

— de type I_o si $p \nmid \Delta$.

Les tables de Halberstadt [13] et de Rizzo [37] décrivent les comportement des réductions locales en 2 et en 3.

1.1.5 Signe de l'équation fonctionnelle de la fonction L

La fonction-L d'une courbe elliptique est une fonction qui recense des informations sur le type de réduction de la courbe modulo chaque nombre premier.

Soit $E/\mathbb{Q}$ une courbe elliptique et soit v une place de $\mathbb{Q}$ pour laquelle on note $q_v = \sharp k_v$, la norme de l'idéal premier correspondant à v, et $a_v = q_v + 1 - \sharp\tilde{E}_v(k_v)$. On définit

$$L_v(T) = \begin{cases} 1 - a_v T + q_v T^2 & \text{si } E \text{ a bonne réduction en } v, \\ 1 - T & \text{si } E \text{ est de réduction } I_m \text{ déployée en } v, \\ 1 + T & \text{si } E \text{ est de réduction } I_m \text{ non déployée en } v, \\ 1 & \text{si } E \text{ est de réduction additive en } v. \end{cases}$$

Définition 9. La fonction-L associée à $E/\mathbb{Q}$ est définie par le produit eulérien

$$L(E,s) = \prod_p L_p(q_p^{-s})^{-1}.$$

Le produit définissant $L(E,s)$ converge et donne une fonction analytique pour tout $\Re(s) > \frac{3}{2}$.

Soit E une courbe elliptique sur $\mathbb{Q}$. Grâce aux travaux de Wiles [52], on sait que la fonction $L(E,s)$ associée à cette courbe elliptique admet un prolongement analytique et une équation fonctionnelle de la forme

$$\mathscr{N}_E^{(2-s)/2}(2\pi)^{s-2}\Gamma(2-s)L(E,2-s) = W(E)\mathscr{N}_E^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s),$$

où $\mathscr{N}_E$ est le conducteur de E et la constante $W(E) \in \{\pm 1\}$ est appelée le *signe* de cette équation fonctionnelle.

Le comportement du signe d'une courbe elliptique a été beaucoup étudié, principalement dans les articles [38] et [39] de Rohrlich.

Le signe peut s'exprimer comme un produit de facteurs locaux

$$W(E) = \prod_{p \leq \infty} W_p(E), \tag{1.7}$$

où p parcourt les nombres premiers rationnels et l'infini, $W_p(E) \in \{\pm 1\}$ et $W_p(E) = +1$ pour tout p sauf un nombre fini. Le signe local $W_p(E)$ en p de E est défini en terme des facteurs epsilon de représentations de Weil-Deligne de $\mathbb{Q}_p$ (voir [6] et [49] pour une définition de ces facteurs locaux). Si p est un premier de bonne réduction pour E, alors $W_p(E) = +1$ et de plus, $W_\infty(E) = -1$ (selon [38]).

L'étude du signe de l'équation fonctionnelle est reliée à l'étude du rang de la courbe elliptique par la *conjecture de parité*.

Conjecture 1.1.6. *(Conjecture de parité)*
Soit E une courbe elliptique. On a

$$W(E) = (-1)^{rang(E)}. \tag{1.8}$$

Cet énoncé est une version affaiblie de la conjecture de Birch et Swinnerton-Dyer. En effet, si $r_{an} = ord_{s-1}L(E,s)$ et $r = rang(E(K))$ alors la conjecture de BSD prédit, entre autre, que $r_{an} = r$. Or, sur $\mathbb{Q}$, on a $W(E) = (-1)^{r_{an}}$. La conjecture de parité équivaut donc à

$$r_{an} \equiv r \mod 2$$

En particulier, une courbe de signe négatif serait de rang impair (et donc non-nul).

1.1.6 Cas connus où la conjecture de parité est vérifiée

Dans le survol de Darmon [5] sur la conjecture de Birch et Swinnerton-Dyer, les théorème 4.1 et 4.4 consistuent les cas connus où la conjecture de parité sont vérifiés. Ceux-ci découlent des travaux de Kolyvagin, Rubin, Gross, Zagier et plusieurs autres.

Théorème 1.1.7. *Soit une courbe elliptique E telle que le rang analytique de E est ≤ 1 (c'est à dire que $L(E,1)$ ou $L'(E,1) \neq 0$). On a les résultats suivants :*

1. *Si $L(E,1) \neq 0$, alors* $\mathrm{rg}E(\mathbb{Q}) = 0$ *(et $W(E) = +1$).*
2. *Si $L(E,1) = 0$ et $L'(E,1) \neq 0$, alors* $\mathrm{rg}E(\mathbb{Q}) = +1$ *(et $W(E) = -1$).*

Soit E une courbe elliptique sur k. L'étude de son groupe de Mordell-Weil est souvent ramenée à celle des suites exactes

$$0 \to E(k)/mE(k) \to S^{(m)}(E/k) \to Ш(E/k)[m] \to 0,$$

où $S^{(m)}(E/k)$ sont les *m-groupes de Selmer* associés à E/k et $Ш(E/k)$ est le *groupe de Tate-Shafarevich* de E/k. Pour plus d'explications sur ces groupes, consulter [47, pp.331-341]. Nous donnons la définition formelle de ce dernier.

Définition 10. Soit E une courbe elliptique sur k. Le groupe de Tate-Shafarevitch de E est le groupe

$$Ш(E) := \bigcap_v \ker\{H^1(G_k, A(\overline{k})) \to H^1(G_v, A(\overline{k}_v))\},$$

où v parcourt toutes les places de k.

Les travaux de Nekovář [34], Dokchitser et Dokchitser [7] montrent que

Théorème 1.1.8. *Soit une courbe elliptique E sur k. On suppose que* Ш *le groupe de Tate-Shafarevitch de E est fini.*

Alors la conjecture de parité est vérifiée sur E, c'est-à-dire que

$$W(E) = (-1)^{\mathrm{rang}(E)}.$$

1.1.7 Le signe local selon le type de réduction

Nous présentons dans cette section les principales propriétés connues pour les signes locaux d'une courbe elliptique.

Proposition 1.1.9. *[38, Prop. 2 v)]*

Soit p un nombre premier de $\mathbb{Q}$ différent de 2 et 3. Soit E une courbe elliptique sur $\mathbb{Q}$ que l'on écrit sous forme de Weierstrass

$$E : y^2 = x^3 - 27c_4x - 54c_6.$$

Alors le signe local en p est

$$W_p(E) = \begin{cases} 1 & \text{si la réduction de } E \text{ en } p \text{ est de type } I_0; \\ (-1/p) & \text{si la réduction est de type } II,\ II^*,\ I_m^* \text{ ou } I_0^*; \\ (-2/p) & \text{si la réduction est de type } III \text{ ou } III^*; \\ (-3/p) & \text{si la réduction est de type } IV \text{ ou } IV^*; \\ -(-c_6/p) & \text{si la réduction est de type } I_m; \end{cases}$$

Pour $p = 2, 3$, on se réfère aux tableaux d'Halberstadt [13] ou de Rizzo [37].

Proposition 1.1.10. *[38, Prop. 1]*

Soit K un corps de nombres et E une courbe elliptique sur K. Soit v une place à l'infini de K. Alors

$$W_v(E) = -1.$$

1.2 Surfaces algébriques

1.2.1 Surfaces elliptiques

Définition 11. Soit C une courbe projective non-singulière sur un corps k. Une *surface elliptique sur C* est la donnée :

i) d'une surface $\mathscr{E}$, c'est-à-dire une variété projective de dimension 2 ;

ii) d'un morphisme $\pi : \mathscr{E} \to C$ tel pour que toutes les fibres $\mathscr{E}_t = \pi^{-1}(t)$ sauf un nombre fini sont les courbes non singulières de genre 1 ;

iii) d'une section à π, $\sigma : C \to \mathscr{E}$.

Remarque 20. Dorénavant, sauf précision, une surface elliptique sera de base $\mathbb{P}^1$ et définie sur $\mathbb{Q}$.

La plupart des auteurs définissent une surface elliptique comme satisfaisant les propriétés i) et ii), sans imposer l'existence d'une section. Toutefois, l'existence d'une section est très pratique car chaque fibre non singulière sauf un nombre fini est une courbe elliptique.

Une surface elliptique $\mathscr{E}$ peut donc être vue comme une famille de courbes elliptiques. Quitte à remanier cette famille, nous pouvons décrire $\mathscr{E}$ sous forme de Weierstrass, c'est-à-dire que $\mathscr{E}$ est décrite par l'équation

$$y^2 = x^3 + A(T)x + B(T), \tag{1.9}$$

où $A(T), B(T) \in \mathbb{Q}(T)$ sont des fonctions rationnelles.

Pour presque tout $t \in \mathbb{P}^1$, la fibre de $\mathscr{E}$ en t est la courbe elliptique définie par l'équation (1.9) évaluée en t :

$$E_t : y^2 = x^3 + A(t)x + B(t).$$

On peut définir $\mathscr{E}$ par le sous-ensemble de $\mathbb{P}^2 \times \mathbb{P}^1$ suivant :

$$\left\{([X, Y, Z], t) \in \mathbb{P}^2 \times \mathbb{P}^1 : \ A \text{ ou } B \text{ a un pôle en } t, \text{ ou } \ Y^2Z = X^3 + A(t)XZ^2 + B(t)Z^3\right\}$$

Définition 12. Soit $\mathscr{E}$ une surface elliptique et une forme de Weierstrass

$$y^2 = x^3 + A(T)x + B(T).$$

On appelle *la fibre générique de $\mathscr{E}$* la courbe elliptique sur $\mathbb{Q}(T)$, notée E_T qui est le lieu des solutions de l'homogénéisée de cette équation.

Nous exclurons de notre étude les surfaces elliptiques *triviales*, c'est-à-dire celles qui sont isomorphes à un produit $E \times C$ d'une courbe elliptique E avec une courbe projective lisse C.

1.2.2 Densité des points rationnels sur une surface elliptique

Proposition 1.2.1. *Soit $\mathscr{E}$ une surface elliptique dotée de la section π. Si, pour une infinité de $t \in \mathbb{P}(\mathbb{Q})$, la fibre $\mathscr{E}_t$ de π est une courbe elliptique de rang de Mordell-Weil positif, $\mathscr{E}$ aura un ensemble dense de points rationnels.*

Démonstration. Supposons que

$$\#\{t \in \mathbb{P}^1(\mathbb{Q}) \mid rg\mathscr{E}_t(\mathbb{Q}) > 0\} = \infty.$$

Nommons E l'adhérence de $\mathscr{E}(\mathbb{Q})$. E est le plus petit fermé contenant tous les points rationnels de la surface $\mathscr{E}$. Pour la topologie de Zariski, les fermés d'une variété projective sont les ensembles algébriques projectifs, c'est-à-dire l'ensemble des zéros dans $\mathbb{P}^n$

d'un idéal homogène de $\overline{k}[x_0, ..., x_n]$. Notons également que les fibres $\mathscr{E}_t$, en tant qu'image réciproque de fermés ($\{t\}$ est bien un fermé de $\mathbb{P}^1$) par des applications continues, sont également des fermés de $\mathscr{E}$.

Remarquons que l'adhérence des points rationnels sur une fibre $\mathscr{E}_t$ dont le rang de Mordell-Weil est positif est la fibre en entier. En effet, les fermés d'une variété algébrique de dimension 1 sont les ensembles finis de points ou la fibre entière. L'ensemble des points rationnels étant de cardinalité infinie, le seul fermé assez grand pour le contenir est la fibre en entier.

On sait donc que l'adhérence de $\mathscr{E}(\mathbb{Q})$ contient une infinité de courbes elliptiques, qui correspondent à l'infinité de fibres de rang positif. Le seul fermé capable de contenir toutes ces courbes est la surface elliptique entière.

Puisque son adhérence est $\mathscr{E}$, $\mathscr{E}(\mathbb{Q})$ est dense pour la topologie de Zariski. □

Remarque 21. La réciproque de ce théorème est vraie. On ne l'utilisera cependant pas dans ce travail.

On considère les ensembles

$$W_+(\mathscr{E}) = \{t \in \mathbb{Q} | W(\mathscr{E}(t)) = +1\},$$

$$W_-(\mathscr{E}) = \{t \in \mathbb{Q} | W(\mathscr{E}(t)) = -1\}.$$

Corollaire 1.2.2. *On suppose vraie la conjecture de parité.*

Si l'ensemble W_- est de cardinalité infinie alors les points rationnels de $\mathscr{E}$ sont denses pour la topologie de Zariski.

1.2.3 Modèle de Weierstrass minimal d'une surface elliptique

Soit une surface elliptique d'équation de Weierstrass $y^2 = x^3 + c_4(T)x + c_6(T)$ telle que $v(c_4) \geq 4$ et $v(c_6) \geq 6$ en une certaine place v associée à $s \in \mathbb{Q}(T)$.

On peut appliquer le changement de variables

$$x \mapsto s^{-2}x, \ y \mapsto s^{-3}y$$

pour obtenir une équation isomorphe à coefficients entiers et dont la valuation du discriminant est diminuée de 12.

Ce procédé, appelé *minimalisation*, peut se faire uniquement un nombre fini de fois et l'équation résultante est appelée *l'équation de Weierstrass minimale en v*.

À toute surface elliptique, on pourra associer un *modèle de Weierstrass minimal*, c'est-à-dire une équation de Weierstrass minimale en toute place. En terme de coefficients, un modèle de Weierstrass minimal est caractérisé par

$$v(c_4(T)) < 4 \text{ ou } v(c_6(T)) < 6 \text{ en toute place finie de } \mathbb{P}^1.$$

Dans le cas de la place à l'infini, on introduit le paramètre $u = \frac{1}{t}$ et l'équation minimale en $u = 0$

$$y^2 = x^3 + u^{4n}A(\frac{1}{u})x + u^{6n}B(\frac{1}{u}),$$

dont le discriminant est $\tilde{\Delta}_o(u) = u^{12n}\Delta_o(\frac{1}{u})$, où n est le plus petit entier tel que $4n \geq \deg A$ et $6n \geq \deg B$.

Pour résumer cela, on introduit $\Delta_{\mathscr{E}}(T, U)$ tel que $\Delta_{\mathscr{E}}(t, 1) = \Delta_o(t)$ et $\Delta_{\mathscr{E}}(1, u) = \tilde{\Delta}_o(u)$. Cette fonction est un polynôme homogène de degré $12n$ pour un certain n et telle que pour

tout P polynôme irréductible, $P^4 \nmid c_4$ ou $P^6 \nmid c_6$. L'entier κ indiqué ci-dessous sera appelé la dimension de Kodaira de $\mathscr{E}$.

$n = 0$	surface triviale ($\mathscr{E} = E_0 \times \mathbb{P}^1$)	
$n = 1$	surface elliptique rationnelle ($\Leftrightarrow \deg A \leq 4$ et $\deg B \leq 6$)	$\kappa = -\infty$
$n = 2$	surface K3,	$\kappa = 0$,
$n > 2$	surface elliptique « de type général »	$\kappa = 1$.

Nous nous intéresserons en particulier aux surface elliptiques rationnelles aux quelles nous reviendrons en section 1.2.7. Auparavant, nous présenterons des notions importantes de l'étude des surfaces elliptiques : la classification des fibres singulières en section 1.2.4, la relation du rang de Shioda-Tate en 1.2.5 et l'isotrivialité en 1.2.6.

1.2.4 Classification des fibres singulières

Dans cette section, nous discutons de la classification des fibres singulières d'une surface elliptique. Celle-ci a été donnée pour la première fois par Kodaira [20] dans le cadre des surfaces elliptiques complexes, puis étudié par Néron [35] qui a trouvé une façon canonique de déterminer les fibres singulières, et Tate [48] qui donne un algorithme simplifié qui est valide sur les corps parfaits.

Théorème 1.2.3. *([20], [35]) Soit E_T une courbe elliptique sur $\mathbb{Q}(T)$ et soit $\mathscr{C} : y^2 = z^3 + c_4(T)x + c_6(T)$ un modèle de Weierstrass minimal pour E_T. Alors $\mathscr{C}_P$ l'équation obtenue de $\mathscr{C}$ par la réduction de $c_4(T)$ et $c_6(T)$en P associée à une place de $Q(T)$ a une des formes suivantes :*

	$ord_{w_p} j(T)$	$ord_{w_p} \Delta(T)$	$P(T) \mid c_4(T)$?
Type I_0	0	0	
Type I_m	$-m$	m	*non*
Type I_m^*	$-m$	$m+6$	*oui*
Type II	0	2	*oui*
Type III	0	3	*oui*
Type IV	0	4	*oui*
Type I_0^*	0	6	*oui*
Type IV^*	0	8	*oui*
Type III^*	0	9	*oui*
Type II^*	0	10	*oui*

1.2.5 Relation fondamentale du rang de Shioda-Tate

Soit $\mathscr{E} \to C$ une surface elliptique minimale de base C sur $\overline{\mathbb{Q}}$, et soit $E/\overline{\mathbb{Q}}(T)$ sa fibre générique.

Le groupe de Néron-Séveri de $\mathscr{E}$, que l'on note $NS(\mathscr{E})$ est le quotient du groupe de ses diviseurs par une certaine relation d'équivalence. On renvoie à [14, Exercice V.A.7] pour la définition de cette relation d'équivalence.

On peut démontrer que $\mathrm{NS}(\mathscr{E})$ est un groupe finiment engendré et que le couplage de l'intersection sur $\mathrm{Div}(\mathscr{E})$ donne un couplage bien défini sur $\mathrm{NS}(\mathscr{E})$.

Shioda [44] a montré comment trouver des générateurs pour $\mathrm{NS}(\mathscr{E})$ en utilisant les générateurs de $E(K)$ et des fibres de $\mathscr{E}$. En particulier, il démontre la *relation fondamentale du rang* [44, Corollaire 1.5] :

$$\mathrm{rgNS}(\mathscr{E}_{\overline{\mathbb{Q}}}) = \mathrm{rg}E(\overline{\mathbb{Q}}(T)) + 2 + \sum_{v \in C} (m_v - 1),$$

où m_v est le nombre de composantes irréductibles de la fibre $\mathscr{E}_v$

Explicitement, ce nombre est

$$m_v = \begin{cases} 1 & \text{si la réduction en } v \text{ est } I_0 \\ n & \text{si la réduction en } v \text{ est } I_n \ (n \geq 1) \\ 5+n & \text{si la réduction en } v \text{ est } I_n^* \ (n \geq 0) \\ 1 & \text{si la réduction en } v \text{ est } II \\ 2 & \text{si la réduction en } v \text{ est } III \\ 3 & \text{si la réduction en } v \text{ est } IV \\ 7 & \text{si la réduction en } v \text{ est } IV^* \\ 8 & \text{si la réduction en } v \text{ est } III^* \\ 9 & \text{si la réduction en } v \text{ est } II^* \end{cases}$$

Notons que $\mathrm{rg}NS(\mathscr{E}_{\overline{\mathbb{Q}}}) = 10$ lorsque $\mathscr{E}$ est rationnelle. Par conséquent, on obtient l'inégalité :

$$\mathrm{rg}\mathscr{E}(\mathbb{Q}(T)) \leq \mathrm{rg}\mathscr{E}(\overline{\mathbb{Q}}(T)) = 8 - \sum_{v \in \mathbb{P}^1} (m_v - 1).$$

1.2.6 Surfaces isotriviales

Définition 13. Une surface elliptique *triviale* est une surface qui est birationnelle à un produit de la forme $\mathbb{P}^1 \times E_0$ où E_0 est une courbe elliptique.

Une surface elliptique *isotriviale* est $\mathscr{E}$, une surface elliptique de base B, telle qu'il existe une courbe C telle que $\mathscr{E} \times_B C$ est une surface elliptique triviale de base C.

$$\begin{array}{ccc} \mathscr{E} & \longleftarrow & \mathscr{E} \times_B C \\ \pi \downarrow & & \downarrow \\ B & \xleftarrow{\pi'} & C \end{array}$$

L'isotrivialité équivaut à une condition très importante sur le j-invariant, une quantité associée à une courbe elliptique présentée dans la définition 4

Théorème 1.2.4. *Une surface elliptique $\mathscr{E} \to B$ est isotriviale si et seulement si sa fonction $j : B \to \mathbb{P}^1$ qui à $t \in B$ associe le j-invariant de la fibre $\mathscr{E}_t$ est constante.*

Par conséquent, une surface elliptique isotriviale de base $\mathbb{P}^1$ admet une courbe elliptique E_o sur $\mathbb{Q}$ telle que $\mathscr{E}$ est une famille de tordues de E_o. Elle peut être décrite par une des trois formes suivantes :

1. $y^2 = x^3 + af(T)^2x + bf(T)^3$, où $f(T)$ est un polynôme sans facteur carré et $ab \neq 0$, (si $j(T) \in \mathbb{Q}\backslash\{0, 1728\}$)
2. $y^2 = x^3 + f(T)x$, $f(T)$ est sans facteur de degré 4, (si $j(T) = 1728$.)
3. $y^2 = x^3 + f(T)$, $f(T)$ est sans facteur de degré 6. (si $j(T) = 0$.)

Remarque 22. La restriction sur les facteurs de $f(T)$ sert à garantir que le modèle de Weierstrass de $\mathscr{E}$ est minimal.

Remarque 23. En effectuant le changement de variable $y' = \frac{y}{f(t)^2}$ $x' = \frac{x}{f(t)}$, on obtient la représentation du cas 1 sous la forme

$$f(t)y'^2 = x'^3 + ax' + b.$$

Remarque 24. La raison pour laquelle on fait la distinction entre les cas 1, 3 et 2 est que les tordues d'une courbe elliptique sont paramétrées par $H^1(G_{\mathbb{Q}}, Aut(E))$.

1. Lorsque $j \in \mathbb{Q} \setminus \{0, 1728\}$, on a $Aut(E) = \mathbb{Z}/2\mathbb{Z}$,
2. lorsque $j = 0$, on a $Aut(E) = \mathbb{Z}/6\mathbb{Z}$ et
3. lorsque $j = 1728$, on a $Aut(E) = \mathbb{Z}/4\mathbb{Z}$.

Remarque 25. Dans chaque cas, les fibres singulières ont la configuration suivante :

1. Toute fibre singulière est de type I_0^*.
2. Toute fibre singulière est de type III ou III^*.
3. Toute fibre singulière est de type II, II^*, IV ou IV^*

1.2.7 Surfaces elliptiques rationnelles

Soit $\mathscr{E} \to \mathbb{P}^1$ une surface elliptique sur $\mathbb{Q}$ qui s'écrit avec l'équation de Weierstrass

$$\mathscr{E} : y^2 = x^3 + A(T)x + B(T),$$

où $A, B \in \mathbb{Z}[T]$. Le discriminant est noté $\Delta(T) = 4A(T)^3 + 27B(T)^2$.

Proposition 1.2.5. *(Critère de rationnalité [33]) Une surface elliptique est rationnelle, c'est à dire qu'elle est birationnelle à $\mathbb{P}^2$ sur $\overline{\mathbb{Q}}$, si et seulement si*

$$0 < \max\{3 \deg A, 2 \deg B\} \leq 12$$

Une conséquence du critère de rationnalité est qu'une surface rationnelle s'écrit :

$$y^2 = x^3 + A(u, v)x + B(u, v),$$

où $A(u, v) = v^4 A\left(\frac{u}{v}\right)$ et $B(u, v) = v^6\left(\frac{u}{v}\right)$ sont des polynômes homogènes de degré respectivement 4 et 6.

On peut voir (1.2.7) comme l'équation d'une hypersurface dans $\mathbb{P}(1, 1, 2, 3)$.

Théorème 1.2.6. *[19, Théorème 1]*

Soit $E \to B$, une surface elliptique rationnelle, c'est-à-dire que $\mathscr{E}$ est $\bar{\mathbb{Q}}$-birationnel à $\mathbb{P}^2$.

Alors

1. *$B \simeq \mathbb{P}^1$,*
2. *elle possède un modèle minimal $X/\mathbb{Q}$ qui est :*
   (a) *soit un fibré en coniques de degré ≥ 1,*
   (b) *soit une surface de Del Pezzo de degré $d \in [1, 9]$.*

De plus, si on regarde la surface définie par $y^2 = x^3 + A(u, v)x + B(u, v)$ avec $A, B \in \mathbb{Z}[u, v]$ des polynômes homogènes de degré respectivement 4 et 6, l'équation est lisse si et seulement si elle définit une surface de Del Pezzo de degré 1.

Remarque 26. Le dernier point de ce théorème est un corollaire de [19] en remarquant que l'on doit avoir que le nombre d'autointersection du diviseur anticanonique de X est tel que $K_X \cdot K_X \geq 1$.

On verra le lien explicite entre les surfaces elliptiques rationnelles lisses et les surfaces de Del Pezzo dans la section 1.2.9. Auparavant, nous verrons en section 1.2.8 la définition d'une surface de Del Pezzo.

1.2.8 Surfaces de Del Pezzo

Définition 14. Une *surface de Del Pezzo*, ou *surface de Fano*, est une surface algébrique projective non singulière X dont le diviseur *anticanonique* est ample, c'est-à-dire que, si K_X est le diviseur canonique de X, le diviseur $-K_X$ est ample. C'est une variété de Fano de dimension 2. Le *degré* d d'une surface de Del Pezzo X est le nombre d'autointersection (K, K) de sa classe de diviseur canonique K.

Une surface de Del Pezzo a un degré d au plus 9 (voir [28, p.118]). Si la surface est sur un corps algébriquement clos, chaque surface de del Pezzo est ou bien un produit de deux droites projectives (alors $d = 8$), ou encore l'éclatement de $9 - d$ points sur le plan projectif (il n'y a pas trois points colinéaires, pas 6 sur la même conique et pas 8 sur une cubique qui a une node en l'un d'eux).

On aimerait pouvoir voir les surfaces de Del Pezzo comme des surfaces lisses dans un certain espace projectif. Un résultat décrit dans le livre de Kollár le permet pour les surfaces de Del Pezzo de degré 1, 2, 3 et 4.

Théorème 1.2.7. *(**Kollár**, [21, p.174]) Soit X, une surface de Del Pezzo sur un corps k de degré inférieur ou égal à 4. Alors X peut être décrite de la manière suivante :*

- *si $d = 1$, alors X est isomorphe à une hypersurface de degré 6 de $\mathbb{P}(1, 1, 2, 3)$;*
- *si $d = 2$, alors X est isomorphe à une hypersurface de degré 4 dans $\mathbb{P}(1, 1, 1, 2)$;*
- *si $d = 3$, alors X est isomorphe à une hypersurface de degré 3 dans $\mathbb{P}^3$;*
- *et $d = 4$, alors X est isomorphe à l'intersection de deux quadriques dans $\mathbb{P}^4$.*

1.2.9 Lien entre surface Del Pezzo de degré 1 et surface elliptique rationnelle

Soit k un corps de nombres, et soit $(\mathscr{E}, \rho, \sigma)$ une surface elliptique sur $\mathbb{P}^1_k$. On suppose que $\mathscr{E}$ est rationnelle, c'est-à-dire que $\mathscr{E} \times_k \overline{k}$ est birationelle à $\mathbb{P}^2_{\overline{k}}$. Alors la fibre générique de $\mathscr{E}$ est une courbe elliptique E_T sur $k(T)$ qui est représentée par une équation de Weierstrass de la forme

$$Y^2 = X^3 + A(T)X + B(T),$$

où $A(T), B(T) \in k[T]$ sont tels que

$$\deg A(T) \leq 4, \deg B(T) \leq 6 \text{ et } \Delta := 4A(T)^3 + 27B(T)^2 \notin k.$$

Réciproquement, à toute courbe elliptique sur $\mathbb{Q}[T]$ de cette forme correspond à une surface elliptique rationnelle de base $\mathbb{P}^1$.

On associe à $\mathscr{E}$ une hypersurface X de degré 6 dans l'espace projectif $\mathbb{P}(1, 1, 2, 3)$ de coordonnées $[x, y, z, w]$. Pour ce faire, on définit X comme suit

$$w^2 = z^3 + G(x, y)z + F(x, y),$$

où $G(x, y) = y^4 A(x/y)$ et $F(x, y) = y^6 B(x/y)$.

Ces deux schémas sont birationnels. En effet, X peut-être obtenue de $\mathscr{E}$ par contraction de l'image de la section σ et des composantes des fibres sigulières de ρ qui ne rencontrent pas $\sigma(\mathbb{P}^1)$. En général, X sera une hypersurface singulière.

Si toutefois X est lisse, alors c'est une surface de Del Pezzo de degré 1.

D'une façon similaire, pour toute surface de Del Pezzo de degré 1 X on obtient une surface elliptique rationnelle qui lui est birationnelle. En effet, on remarque que la correspondance définie précédemment correspond dans ce cas à l'éclatement du point de base anticanonique sur X.

1.2.10 Surfaces de Del Pezzo de degré 1

Dans cette section, nous déterminons les surfaces elliptiques rationnelles dont la surface X obtenue par la contraction de la section à l'infini est une surface de Del Pezzo de degré 1.

Si on écrit la surface elliptique rationnelle sous forme de modèle minimal de Weierstrass on a

$$y^2 = x^3 + A(t)x + B(t),$$

où

On notera par la suite $\tilde{A}(u,v) = v^4 A(\frac{u}{v})$ et $\tilde{B}(u,v) = v^6 B(\frac{u}{v})$.

Lemme 1.2.8. *Soit $\mathscr{E}$ une surface elliptique rationnelle d'équation de Weierstrass*

$$y^2 = x^3 + A(T)x + B(T),$$

où $A, B \in \mathbb{Z}[T]$. On note $Sing_{\mathscr{E}}$ l'ensemble des points singuliers de $\mathscr{E}$. Alors $Sing_{\mathscr{E}}$ est formé des points suivants :

1. *les points $(0,0,t_0)$ où $t_0 \in \mathbb{Q}$ est racine de A et double de B.*
2. *les points $(\frac{-3B(t_0)}{2A(t_0)}, 0, t_0)$ où $t_0 \in \mathbb{Q}$ est racine double de $\Delta_{\mathscr{E}}$ telle que $A(t_0) \neq 0$.*

On en déduit le corolaire suivant :

Corollaire 1.2.9. *Soit $\mathscr{E}$ une surface elliptique rationnelle et soit X son modèle minimal. Alors X est lisse (et est donc une surface de Del Pezzo de degré 1) si et seulement si les places de $\mathscr{E}$ sont de type II ou I_1.*

Démonstration. (de la proposition 1.2.8)

Soit une équation de Weierstrass définissant $\mathscr{E}$

$$y^2 = x^3 + A(T)x + B(T).$$

L'étude du gradient de l'équation définissant $\mathscr{E}$ mène à l'obtention des relations suivantes que doivent respecter un point singulier (x_0, y_0, t_0) :

$$\begin{cases} y_0 = 0 = x_0^3 + A(t_0)x_0 + B(t_0) \\ 3x_0^2 + A(t) = 0 \\ A'(t)x + B'(t) = 0 \end{cases}$$

Remarquons que si $A'(t_0) = 0$, la troisième relation implique que $B'(t_0) = 0$. Si $A'(t_0) = 0$, alors on a plutôt $x = -\frac{B'}{A'}(t)$. Les deux premières relations sont possibles uniquement si x_0 est racine double de $x^3 + A(t_0)x + B(t_0)$. Voyons dans quels cas cela est possible.

Si $A(t_0) = B(t_0) = 0$ alors pour $x_0 = y_0 = 0$, le point est bien singulier.

Si un de $A(t_0)$ ou de $B(t_0)$ n'est pas 0, alors x_0 doit être racine double de $x^3 + A(t_0)x + B(t_0)$ et par conséquent,

$$x_0 = -\frac{3B(t_0)}{2A(t_0)}.$$

À noter que dans ce cas, si $A(t_0) = 0$, alors il n'y a pas de racine double.

Comme $3x^2 + A(t_0) = 0$, on a $\frac{9B(t_0)^2}{4A(t_0)^2} + A(t) = 0$, alors le discriminant

$$\Delta(t_0) = 4A(t_0)^3 + 27B(t_0)^2 = 0.$$

De plus la troisième relation implique que $\frac{-3A'(t_0)}{A(t_0)} + \frac{B'(t_0)}{B(t_0)} = 0$ et par conséquent

$$\Delta'(t_0) = 12A^2A' + 54BB' = 27B^2\left(-3\frac{A'}{A} + 2\frac{B'}{B}\right) = 0$$

Par conséquent, t_0 est une racine double de $\Delta_{\mathscr{E}}(t)$.

De plus, un calcul similaire permet de traiter en la fibre à l'infini. En ce point, le modèle s'écrit

$$y^2 = x^3 + \tilde{A}(1,v)x + \tilde{B}(1,v),$$

où on note $\tilde{\Delta}(u,v) = v^{12}\Delta(\frac{u}{v})$.

La fibre en ∞ est singulière si et seulement si

1. $\tilde(1,0) = 0 = \tilde{B}(1,0) = \tilde{B}'(1,0)$, ce qui arrive lorsque $\deg A \leq 3$ et $\deg B \leq 4$
2. $\deg A = 4$, $\deg B = 6$ et 0 est une racine double de $\tilde{\Delta}$, c'est-à-dire $\deg \Delta \leq 10$.

□

On déduit de cette étude le lemme suivant qui caractérise les surfaces de Del Pezzo de degré 1.

Lemme 1.2.10. *Soit X l'hypersurface de degré 6 dans $\mathbb{P}(1,1,2,3)$ décrite par l'équation*

$$y^2 = x^3 + A(u,v)x + B(u,v),$$

où $A, B \in \mathbb{Z}[u,v]$ sont des polynômes homogènes de degré respectif 4 et 6.

Les affirmations suivantes sont équivalentes :

1. *X est une surface de Del Pezzo de degré 1.*
2. *La surface X est lisse.*
3. *L'éclatement du point de base anticanonique sur X est une surface elliptique rationnelle $\mathscr{E}$ dont les fibres singulières sont de type II ou I_1.*
4. *Les polynômes en une variable $A(T,1)$ et $B(T,1)$ respectent les propriétés suivantes*
   (a) *Une racine commune à A et B n'est pas double pour B.*
   (b) *Les racines de Δ non commune à A sont simples.*
   (c) *Si $\deg A \leq 3$, alors $\deg B \leq 5$.*
   (d) *Si $\deg A = 4$ et $\deg B = 6$, alors $\deg \Delta \geq 11$.*

Remarque 27. En particulier, les surfaces elliptiques rationnelles isotriviales des formes $y^2 = x^3 + H(t)^2x + H(t)^3$ et $y^2 = x^3 + A(t)x$ ne vérifient pas ces propriétés. La contraction de la section neutre ne donne en aucun de ces cas une surface de Del Pezzo de degré 1.

Cependant, une surface elliptique rationnelle isotriviale de la forme $y^2 = x^3 + B(t)$ avec $\deg B \geq 5$ et sans racine double respecte les critères. Par conséquent, la contraction de sa section neutre est une surface de Del Pezzo de degré 1.

1.2.11 Densité des points rationnels sur une surface de Del Pezzo ou un fibré en conique

Rappelons que le théorème d'Iskovskih présenté en section 1.2.7 dit qu'une surface elliptique rationnelle possède un modèle minimal $X/\mathbb{Q}$ qui est :

1. soit un fibré en coniques de degré 1,
2. soit une surface de Del Pezzo.

En effet, l'application $\mathscr{E} \to X$ est une suite de contractions de r courbes exceptionnelles. L'autointersection du diviseur canonique est

$$K_X \cdot K_X = K_{\mathscr{E}} \cdot K_{\mathscr{E}} + r = r.$$

Les points rationnels d'une surface elliptique rationnelle sont denses si et seulement si on a aussi ceux de son modèle minimal le sont aussi.

Dans le cas où X est un fibré en conique de degré ≥ 1, Kollár et Mella [23] démontrent l'unirationnalité de X, propriété qui implique la densité des points rationnels.

On a explicitement le théorème suivant.

Théorème 1.2.11. *[23, Thm. 1] Soit K un corps de caractéristique différente de 2 et $a_0(t)$, $a_1(t)$, $a_2(t)$, $a_3(t) \in K[t]$, des polynômes de degré 2 définissant une famille non triviale de courbes elliptiques. Alors, la surface*

$$S : y^2 = a_3(t)x^3 + a_2(t)x^2 + a_1(t)x + a_0(t) \subset \mathbb{A}^3_{xyt}$$

est unirationelle sur K.

Lorsque X est une surface de Del Pezzo de degré $d \geq 3$, l'unirationnalité est démontrée par Segre et Manin [28] sous la condition qu'il ne soit pas vide. Lorsque $d = 2$, Salgado, Testa et Várilly-Alvarado [41], basés sur un travail de Manin, ont montré que si X contient un point rationnel qui ne se trouve pas sur une courbe exceptionnelle ni sur la quartique distinguée, alors X est unirationnelle.

Les surfaces de Del Pezzo de degré 1 sont automatiquement pourvues d'un point rationnel qui n'est pas sur une courbe exceptionnelle : le point de base du système linéaire anticanonique. Cependant, la densité des points rationnels n'est connue que dans certains cas. Par exemple :

Théorème 1.2.12. *[50, Thm 2.1] Soit $f(T) = t^5 + at^3 + bt^2 + ct + d \in \mathbb{Z}[T]$ et considérons la surface donnée par l'équation $\mathscr{E} : x^2 - y^3 - f(t) = 0$. Alors*

1. *si f a des racines multiples sur $\mathbb{C}$, alors l'ensemble des points rationnels de $\mathscr{E}_f$ est dense au sens de Zariski.*
2. *si f n'a pas de racine multiple et que l'ensemble des points rationnels sur la courbe $\mathscr{E}_{a,b} : Y^2 = X^3 + 135(2a-15)X - 1350(5a+2b-26)$ est infini, alors l'ensemble des points rationnels sur la surface $\mathscr{E}_f$ est Zariski-dense.*

Remarque 28. Remarquons que dans le premier cas, où f a des racines multiples sur $\mathbb{C}$, le modèle minimal de la surface $\mathscr{E}$ n'est pas une surface de Del Pezzo de degré 1.

De plus, un article de Salgado et Van Luijk [42] donne des conditions sous lesquelles l'ensemble des points rationnels d'une surface de Del Pezzo de degré 1 sont denses au sens de Zariski.

Théorème 1.2.13. *[42, Théorème 1.2] Soit $S \subset \mathbb{P}(1,1,2,3)$ une surface de Del Pezzo donnée par une équation de la forme*

$$w^2 = z^3 + f(x,y)z + g(x,y),$$

où $f, g \in \mathbb{Z}[x,y]$, et soit $\mathscr{E} \xrightarrow{\pi} \mathbb{P}^1$ la surface elliptique obtenue par l'éclatement du point de base anticanonique de S.

Soit $Q \in S(\mathbb{Q})$, un point qui n'est pas fixé par les automorphismes de S qui changent le signe de w. Soit $\mathscr{C}_Q(5)$ la courbe formée des sections locales qui rencontrent S en Q avec une multiplicité au moins 5.

On pose $t = \pi(Q)$. On suppose que les propositions suivantes sont vérifiées :

1. *L'ordre de Q sur $\mathscr{E}_t^{ns}(\mathbb{Q})$ est au moins 3.*
2. *Si l'ordre de Q dans $\mathscr{E}_t^{ns}(\mathbb{Q})$ est au moins 4, alors $\mathscr{C}_Q(5)$ a une infinité de points rationnels.*
3. *Si l'ordre de Q dans $\mathscr{E}_t^{ns}$ est 3 ou 5, alors Q ne se trouve pas sur six courbes exceptionnelle de S.*

Alors l'ensemble des points rationnels de S est Zariski-dense.

On a plusieurs corollaires à ce théorème. Par exemple, il suffit de supposer que la surface elliptique obtenue par éclatement du point anticanonique ait une fibre nodale au dessus d'un certain point k-rationnel de $\mathbb{P}^1$. Il suffit aussi de supposer l'existence d'un point rationnel qui ne se trouve pas sur six courbes exceptionnelles de S et qui est d'ordre 3 sur sa fibre générique.

Várilly-Alvarado a travaillé sur les surfaces de Del Pezzo de degré 1 dont la surface elliptique associée est isotriviale, démontrant le théorème suivant :

Théorème 1.2.14. *[51, Thm 2.1] Soit $F(x,y) \in \mathbb{Z}[x,y]$ un polynôme homogène de degré 6 dont on suppose que les coefficients en x^6 et en y^6 sont non nuls. Soit X la surface de del Pezzo de degré 1 sur $\mathbb{Q}$ donnée par*

$$w^2 = z^3 + F(x,y)$$

dans $\mathbb{P}_{\mathbb{Q}}(1,1,2,3)$, l'espace projectif à poids de variable (x,y,z,w). Soit c le contenu de F : on écrit $F(x,y) = cF_1(x,y)$, avec $F_1(x,y) \in \mathbb{Z}[x,y]$. On suppose que F_1 est unitaire et que $F_1 = \prod_i f_i$, où les $f_i \in \mathbb{Z}[x,y]$ sont des polynômes homogènes irréductibles. On suppose de plus qu'il existe f_i tel que

$$\mu_3 \not\subseteq \mathbb{Q}[t]/f_i(t,1) \text{ pour un certain } i,$$

où μ_3 est le groupe des racines troisième de l'unité dans $\overline{\mathbb{Q}}$. Enfin, on suppose que la conjecture de parité est vérifiée pour les courbes elliptiques sur $\mathbb{Q}$ de j-invariant 0.

Alors les points rationnels de X sont denses pour la topologie de Zariski.

Várilly-Alvarado démontre également un énoncé équivalent, en remplaçant μ_3 par μ_4 (racines quatrièmes de l'unité dans $\mathbb{Q}$) pour les surfaces définies par l'hypersurface dans $\mathbb{P}(1,1,2,3)$ de coordonnée (u,v,z,w) d'équation

$$w^2 = z^3 + F(u,v)z,$$

où $F(u,v)$ est un polynôme homogène de degré 4. Ces surfaces ne sont pas tout à fait des surfaces de Del Pezzo de degré 1 : elles ont des points non lisses.

1.3 Conjectures de théorie analytique des nombres

Nous traiterons simultanément le cas d'un polynôme f de degré d à coefficients entiers, ou bien en une variable, ou bien homogène en deux variables ; ainsi ou bien $f(T) = a_0 + \cdots + a_d T^d \in \mathbb{Z}[T]$ ou bien $f(T,U) = a_0 U^d + \cdots + a_d T^d \in \mathbb{Z}[T,U]$. On notera $h = 1$ ou 2 le nombre de variables et v un vecteur à coordonnées entières dans $\mathbb{Z}^h$, c'est-à-dire $\mathrm{v} \in \mathbb{Z}$ ou $\mathrm{v} \in \mathbb{Z}^2$. On étudie deux propriétés décrivant la factorisation de $f(\mathrm{v})$: la première décrit la proportion de valeurs sans facteurs carrés, la deuxième la parité du nombre de facteurs premiers.

Dans l'étude de la factorisation de $f(\mathrm{v})$, il est naturel de supposer f *primitif*, c'est-à-dire que son contenu – le pgcd de ces coefficients – est égal à 1. Cela n'entraîne pas l'absence de facteur commun aux valeurs $f(\mathrm{v})$ mais limite ce phénomène comme l'illustre le lemme élémentaire suivant.

Lemme 1.3.1. *Soit f de degré d, à coefficients entiers, en h variables (ou bien $h = 1$, ou bien $h = 2$ et f homogène). Supposons que Δ divise $f(\mathrm{v})$ pour tout $\mathrm{v} \in \mathbb{Z}^h$, alors il existe un polynôme $g(\mathrm{v})$ à coefficients entiers tel que $d!f(\mathrm{v}) = \Delta g(\mathrm{v})$. En particulier, si f est primitif, on a que Δ divise $d!$.*

Démonstration. Lorsque $h = 1$, il est bien connu qu'un polynôme à coefficients rationnels et prenant des valeurs entières sur $\mathbb{Z}$ est combinaison linéaire à coefficients entiers des polynômes $C_k(T) = T(T-1)\dots(T-k+1)/k!$. L'application de ce principe à $g_1(T) = \Delta^{-1}f(T)$ montre que $d!g_1(T)$ est un polynôme à coefficients entiers. Lorsque $h = 2$, on applique ce qui précède à $f(T, 1)$. □

Nous noterons $\mathcal{A}$ une "progression arithmétique" de la forme [1]

$$\mathcal{A} := \{a + bn \mid n \in \mathbb{Z}\} \quad \text{ou} \quad \mathcal{A} := \{(ax + by, cx + dz) \mid (x, y) \in \mathbb{Z}^2\},$$

où l'on suppose $b \neq 0$ dans le premier cas et $ad - bc \neq 0$ dans le second. On peut aussi écrire $\mathcal{A} = \phi(\mathbb{Z})$ avec $\phi(n) = a + bn$ ou $\mathcal{A} = \phi(\mathbb{Z}^2)$ avec $\phi(m, n) = (am + bn, cm + dn)$. On notera $d(\mathcal{A}) := |b|^{-1}$, resp. $|ad - bc|^{-1}$ la densité de $\mathcal{A}$ dans $\mathbb{Z}^h$.

On désigne par $|\cdot|$ la valeur absolue usuelle sur $\mathbb{R}$ ou la norme max sur $\mathbb{R}^2$. On introduit également les notations

$$\mathbb{Z}^h(X) = \left\{\mathrm{v} \in \mathbb{Z}^h \mid |\mathrm{v}| \leq X\right\}, \quad \mathcal{A}(X) := \{\mathrm{v} \in \mathcal{A} \mid |\mathrm{v}| \leq X\} \quad \text{et} \quad \mathrm{A}(X) := \sharp\mathcal{A}(X),$$

de sorte que $\mathrm{A}(X)$ est proportionnel à X^h, où $h = 1$ dans le cas d'une variable (resp. $h = 2$ dans le cas de deux variables). Plus précisément, on voit aisément que, en fait $A(X) \sim d(\mathcal{A})(2X)^h$.

1.3.1 Conjecture du crible des facteurs carrés

On souhaite estimer la proportion de valeurs sans facteurs carrés sur une progression arithmétique, il est alors naturel de supposer f *sans facteurs carrés*, ce qui équivaut à supposer que son discriminant D_f est non nul. Sous cette hypothèse, la conjecture du crible des facteurs carrés s'énonce comme suit.

Conjecture 1.1. *(Conjecture du crible des facteurs carrés, 1ère forme) Soit f un polynôme à coefficients entiers, sans facteurs carrés,*

$$\sharp\left\{\mathrm{v} \in \mathbb{Z}^h(X) \mid \textit{il existe } p > X^{h/2}, \textit{ tel que } p^2 \textit{ divise } f(\mathrm{v})\right\} = o(X^h). \tag{1.10}$$

La conjecture est démontrée pour les polynômes irréductibles de degré ≤ 3 (resp. ≤ 6) en 1 variable (resp. en 2 variables), ce que nous résumons dans l'énoncé suivant. La preuve est relativement simple (résultant en fait essentiellement des considérations qui suivent) lorsque $h = 1$ et $d \leq 2$ ou $h = 2$ et $d \leq 4$. Les cas suivants sont plus délicats, le cas $h = 1$ et $d = 3$ est prouvé par Hooley [18], le cas $h = 2$ et $d = 5, 6$ est prouvé par Greaves [9].

Théorème 1.3.2. *(Hooley [18], Greaves [9]) Soit f un polynôme à coefficients entiers, sans facteurs carrés, en h variables ($h = 1$ ou 2). Supposons que tous les facteurs irréductibles de f soient de degré inférieur ou égal à $3h$, alors f vérifie la conjecture du crible des facteurs carrés.*

1. Le mot "progression arithmétique" est d'habitude réservé à ce qui correspond ici au cas $h = 1$, dans le cas $h = 2$ on parle d'habitude de "réseau".

Pour mieux comprendre l'énoncé de la conjecture et voir qu'elle permet de déterminer la proportion de valeurs sans facteurs carrés, on peut la reformuler à l'aide des considérations suivantes, où, pour simplifier, on supposera d'abord que le polynôme f a la propriété suivante (on indiquera plus tard comment modifier le calcul dans le cas général).

Hypothèse (SFC) : *On dira que f vérifie (SFC) si, pour tout p premier, il existe* $\mathrm{v} \in \mathbb{Z}^h$ *tel que p^2 ne divise pas $f(\mathrm{v})$.*

Définition 15. On note $t_f(p)$ le nombre de solutions modulo p^2 de $f(\mathrm{v}) \equiv 0 \mod p^2$. La constante du crible des facteurs carrés d'un polynôme f est définie par

$$C_f := \prod_p \left(1 - \frac{t_f(p)}{p^{2h}}\right) \tag{1.11}$$

Remarque 29. Il est élémentaire de voir que $t_f(p)$ est $O(1)$ (resp. $O(p^2)$) si $h = 1$ (resp. $h = 2$), ainsi le produit définissant C_f est absolument convergent. Ceci est déduit du lemme suivant. La constante C_f n'est intéressante que si le polynôme f vérifie la propriété (SFC), car sinon on a évidemment $C_f = 0$.

Soit I un intervalle entier de longueur p^2, c'est-à-dire $I = [M+1, M+p^2]$ ou un produit de deux tels intervalles, c'est-à-dire $I = [M+1, M+p^2] \times [M'+1, M'+p^2]$. On a naturellement

$$\sharp\left\{\mathrm{v} \in I \mid p^2 \text{ divise } f(\mathrm{v})\right\} = t_f(p)$$

puis

$$\sharp\left\{\mathrm{v} \in \mathbb{Z}^h(Np^2) \mid p^2 \text{ divise } f(\mathrm{v})\right\} = t_f(p)(2N)^h$$

et enfin

$$\sharp\left\{\mathrm{v} \in \mathbb{Z}^h(X) \mid p^2 \text{ divise } f(\mathrm{v})\right\} = t_f(p)\left(2\frac{X}{p^2} + O(1)\right)^h \tag{1.12}$$

Pour $h = 1$, l'estimation est satisfaisante, lorsque $h = 2$ on peut introduire le raffinement élémentaire suivant (Cf. Lemma 1 de [9]).

Si on note Z_p l'ensemble des solutions ω modulo p^2 de $f(\omega, 1) \equiv 0 \mod p^2$, alors l'ensemble des solutions de $f(a,b) \equiv 0 \mod p^2$ peut être réparti en l'ensemble $L_0 = p\mathbb{Z}^h$ et les progressions arithmétiques $L_\omega = \{\mathrm{v} = (a,b) \in \mathbb{Z}^h \mid a \equiv \omega b \mod p^2\}$. Le cardinal des éléments de L_0 de norme $\leq X$ est trivialement $O(X^2/p^2)$ et, comme le réseau L_ω est d'indice p^2 dans $\mathbb{Z}^h$, le cardinal des éléments de L_ω de norme $\leq X$ est $O(X^2/p^2 + X)$. On peut même écrire une borne en $X^2/p^2 + X/M_\omega$ où M_ω est la plus petite norme d'un élément non nul de L_ω. On résume cela dans l'estimation simplifiée :

$$\sharp\left\{\mathrm{v} \in \mathbb{Z}^h(X) \mid p^2 \text{ divise } f(\mathrm{v})\right\} \ll \frac{X^h}{p^2} + X^{h-1} \tag{1.13}$$

On peut aisément généraliser ce calcul élémentaire en criblant, pour Z donné, les facteurs p^2 pour $p \leq Z$. On pose $N_Z := \prod_{p \leq Z} p^2$, alors, pour $I \subset\in \mathbb{Z}^h$ un intervalle ou produit de deux intervalles de longueur N_Z on a

$$\sharp\left\{\mathrm{v} \in I \mid \text{si } p \leq Z \text{ on a } p^2 \text{ ne divise pas } f(\mathrm{v})\right\} = \prod_{p \leq Z}\left(1 - \frac{t_f(p)}{p^{2h}}\right) N_Z^h$$

puis

$$\sharp\left\{\mathrm{v} \in \mathbb{Z}^h(MN_Z) \mid \text{si } p \leq Z \text{ on a } p^2 \text{ ne divise pas } f(\mathrm{v})\right\} = \prod_{p \leq Z}\left(1 - \frac{t_f(p)}{p^{2h}}\right)(2MN_Z)^h$$

et enfin

$$\sharp\Big\{\mathrm{v}\in\mathbb{Z}^h(X)\mid \text{si } p\le Z \text{ on a } p^2 \text{ ne divise pas } f(\mathrm{v})\Big\}=\prod_{p\le Z}\left(1-\frac{t_f(p)}{p^{2h}}\right)(2X+O(N_Z))^h \tag{1.14}$$

Pour le choix de $Z=\log X/3$ on obtient, par le théorème des nombres premiers :

$$N_Z=\prod_{p\le Z}p^2=\exp(2\sum_{p\le Z}\log p)=\exp(\frac{2}{3}\log X+o(\log X))=X^{\frac{2}{3}+o(1)}$$

Par ailleurs, lorsque Z tend vers l'infini

$$\prod_{p\le Z}\left(1-\frac{t_f(p)}{p^{2h}}\right)=C_f(1+o(1)),$$

donc on obtient un premier résultat inconditionnel

$$\sharp\left\{\mathrm{v}\in\mathbb{Z}^h(X)\mid \text{si } p\le\frac{\log X}{3} \text{ on a } p^2 \text{ ne divise pas } f(\mathrm{v})\right\}=C_f(2X)^h+o(X^h) \tag{1.15}$$

En combinant ceci avec l'estimation (1.13), on obtient pour $Z_1<Z_2$

$$\sharp\Big\{\mathrm{v}\in\mathbb{Z}^h(X)\mid \text{il existe } p\in[Z_1,Z_2] \text{ tel que } p^2 \text{ divise } f(\mathrm{v})\Big\}\ll\sum_{p\in[Z_1,Z_2]}\left(\frac{X^h}{p^2}+X^{h-1}\right)$$

$$\ll\frac{X^h}{Z_1}+X^{h-1}\pi(Z_2).$$

Mentionnons au passage une conséquence de ceci lorsqu'on prend $Z_1=M$ (pour $M\in\mathbb{Z}$ fixé, inférieur à X) et $Z_2=\sqrt{X}$. Cette proposition inconditionnelle est utilisée par Helfgott , dans les démonstrations des formules pour le signe moyen d'une surface elliptique (revues dans nos propositions 2.4.2, 2.4.3, 2.5.2 et 2.5.6) :

Proposition 1.3.3. *Soit f un polynôme vérifiant la condition (SFC) :*

$$\sharp\Big\{\mathrm{v}\in\mathbb{Z}^h(X)\mid \textit{il existe } p\in[M,\sqrt{X}] \textit{ tel que } p^2 \textit{ divise } f(\mathrm{v})\Big\}\ll\frac{X^h}{M}+o(X^h)$$

En choisissant plutôt $Z_1=\frac{1}{3}\log X$ et $Z_2=X^h$, on en déduit le résultat inconditionnel, suivant :

Proposition 1.3.4. *Soit f un polynôme vérifiant la condition (SFC) :*

$$\sharp\Big\{\mathrm{v}\in\mathbb{Z}^h(X)\mid \textit{si } p\le X^h, \textit{ on a } p^2 \textit{ ne divise pas } f(\mathrm{v})\Big\}=C_f(2X)^h+o(X^h) \tag{1.16}$$

D'après cette proposition, il est clair que la conjecture 1.1 est équivalente à l'énoncé suivant, au moins pour les polynômes vérifiant la condition (SFC).

Conjecture 1.2. *(Conjecture du crible des facteurs carrés, 2ème forme) Soit f un polynôme à coefficients entiers, sans facteurs carrés :*

$$\sharp\Big\{\mathrm{v}\in\mathbb{Z}^h(X)\mid f(\mathrm{v}) \textit{ est sans facteur carré}\Big\}=C_f(2X)^h+o(X^h) \tag{1.17}$$

Si le polynôme ne vérifie pas (SFC) le membre de gauche est nul et la constante C_f est nulle donc l'équation (1.17) est trivialement vérifiée mais ne donne pas l'information cherchée. Il convient en fait de modifier les considérations précédentes, lorsque le polynôme possède un facteur p^2 divisant toute ses valeurs.

Notations. Soit $\delta_f := \text{pgcd}\left\{f(\mathrm{v}) \mid \mathrm{v} \in \mathbb{Z}^h\right\}$, alors d_f désigne le plus petit entier tel que $\delta(f)/d_f$ soit sans facteur carré. Écrivons $d_f = \prod_p p^{\nu_p}$ On note $\tilde{t}_f(p)$ le nombre de solutions modulo $p^{2+\nu_p}$ de $f(\mathrm{v})d_f^{-1} \equiv 0 \mod p^2$, ou encore $f(\mathrm{v}) \equiv 0 \mod p^{2+\nu_p}$ et on pose

$$\tilde{C}_f := \prod_p \left(1 - \frac{\tilde{t}_f(p)}{p^{2+\nu_p}}\right)$$

Remarquons que, d'après le lemme 1.3.1, si le polynôme est primitif, on a $\tilde{t}_f(p) = t_f(p)$ pour $p > d := \deg f$, donc le produit définissant $\tilde{C}_f$ est absloument convergent comme le produit définissant C_f.

La conjecture du crible des facteurs carrés s'énonce alors sous la forme suivante

Conjecture 1.3. *(Conjecture du crible des facteurs carrés, 3ème forme) Soit f un polynôme à coefficients entiers, sans facteurs carrés,*

$$\sharp\left\{\mathrm{v} \in \mathbb{Z}^h(X) \mid f(\mathrm{v})d_f^{-1} \text{ est sans facteur carré}\right\} = \tilde{C}_f(2X)^h + o(X^h) \tag{1.18}$$

Si l'on veut étudier les valeurs (presque) sans facteurs carrés sur une progression arithmétique $\mathcal{A} = \phi(\mathbb{Z}^h)$, on posera $g := f \circ \phi$, $d_{f,\mathcal{A}} := d_g$, $\tilde{C}_{f,\mathcal{A}} := \tilde{C}_g$ et on peut écrire la conjecture du crible des facteurs carrés sous la forme apparemment plus générale :

$$\sharp\left\{\mathrm{v} \in \mathcal{A}(X) \mid f(\mathrm{v})d_{f,\mathcal{A}}^{-1} \text{ est sans facteur carré}\right\} = \tilde{C}_{f,\mathcal{A}}A(X) + o(A(X)) \tag{1.19}$$

Comme son nom l'indique, la conjecture du crible des facteurs carrés mène à un crible. Celui-ci permet de trouver une infinité de valeur d'un polynôme dont la partie carré est une constante donnée. Nous utiliserons le suivant, développé par Várilly-Alvarado dans [51], qui utilise des polynômes homogènes en deux variables, dans la démonstration du théorème 5.0.8.

Corollaire 1.3.5. *[51, Corollaire 5.8] Soit $F(m,n) \in \mathbb{Z}[m,n]$ un polynôme homogène en deux variables de degré d. On suppose $F(m,n)$ sans facteur carré dans $\mathbb{Z}[m,n]$, et qu'aucun facteur irréductible de F est de degré plus grand que 6. On fixe les ensembles*

- *$S = (p_1, \ldots, p_r)$ de premiers distincts et*
- *$T = (t_1, \ldots, t_r)$ d'entier positifs.*

Soit M un entier tel que $p^2 \mid M$ pour tout premier $p < \deg F$ et $p_1^{t_1+1} \ldots p_r^{t_r+1} \mid M$. Supposons qu'il existe des entiers tels que

$$F(a,b) \not\equiv 0 \mod p^2, \text{ quand } p \mid M \text{ et } p \neq p_i \text{ pour tout } i,$$

et tels que

$$v_{p_i}(F(a,b)) = t_i \text{ pour tout } i = 1, \ldots, r.$$

Alors il existe une infinité de paires (m,n) d'entiers tels que

$$m \equiv a \mod M, n \equiv b \mod M,$$

et

$$F(m,n) = p_1^{t_1} \ldots p_r^{t_r} \cdot l,$$

où l est sans facteur carré et $v_{p_i}(l) = 0$ pour tout i.

Pour conclure cette section sur la conjecture du crible sans facteur carré, mentionnons la conjecture *abc*, dûe à Oesterlé, Masser et Szpiro.

Conjecture 1.4. *(Conjecture abc) On fixe $\epsilon > 0$. Si a, b, c sont des entiers positifs premiers entre eux qui satisfaisant $a + b = c$, alors*

$$c \ll_\epsilon N(a, b, c)^{1+\epsilon},$$

où $N(a, b, c)$ est le produit des facteurs premiers distincts de abc.

Une conséquence de cette conjecture est que la conjecture sans facteur carré serait vérifiée pour tout polynôme en une variable, ou homogène en deux variables (voir [1] et [8])

1.3.2 Conjecture de Chowla

La deuxième conjecture concerne la parité du nombre de facteurs premiers des valeurs $f(\mathrm{v})$. Pour l'énoncer, nous rappelons la définition de la fonction de Liouville.

Définition 16. Pour un entier non nul $n = \prod_p p^{v_p(n)}$, on note $\Omega(n) = \sum_p v_p(n)$ le nombre de facteurs premiers de sa décomposition et on définit la *fonction de Liouville* par la formule.

$$\lambda(n) = (-1)^{\Omega(n)}$$

Remarque 30. La fonction de Liouville ressemble à la fonction de Moebius mais diffère en présence justement d'un facteur carré. Plus précisément la relation est la suivante : $\mu(n) = \lambda(n)$ si n est sans facteur carré et $\mu(n) = 0$ s'il existe p^2 divisant n.

Conjecture 1.5. *(Conjecture de Chowla) Soit f un polynôme à coefficients entiers, sans facteurs carrés, l'estimation suivante vaut pour toute progression arithmétique $\mathcal{A}$:*

$$\sum_{\mathrm{v} \in \mathcal{A}(X)} \lambda(f(\mathrm{v})) = o(A(X)) \tag{1.20}$$

Remarque 31. On peut chercher à raffiner cet énoncé en introduisant une uniformité par rapport à la progression arithmétique. Nous n'aurons pas besoin de ce raffinement et omettons donc ce point.

Le théorème des nombres premiers et de la progression arithmétique permet de démontrer cette conjecture pour les polynômes de degré 1 et, en adaptant les arguments de de la Vallée Poussin, pour les polynômes homogènes de degré 2. Les résultats connus à l'heure actuelle sont les suivants.

Théorème 1.3.6. *Soit f un polynôme de degré d à coefficients entiers, sans facteurs carrés, en h variables ($h = 1$ ou 2). La conjecture de Chowla vaut dans les cas suivants :*

1. *(Hadamard – de la Vallée Poussin) $h = 1$ et $d = 1$.*
2. *(Helfgott, Lachand) $h = 2$ et $d \leq 3$.*
3. *(Green-Tao) $h = 2$ et f est un produit de formes linéaires.*

Le premier item ($h = \deg(f) = 1$) équivaut en fait au théorème des nombres premiers sous la forme $\sum_{m \leq X} \mu(m) = o(X)$. Le deuxième, pour f homogène en deux variables et $\deg(f) \leq 2$ est essentiellement dû à de la Vallée Poussin. Le cas de degré 3 a été démontré par Helfgott [17] (noter cependant que l'article cité traite d'un polynôme cubique non

irréductible ; le cas d'un polynôme cubique irréductible [16] est non publié), puis récemment en 2014 par une autre technique par Lachand dans sa thèse de doctorat [24] et dans un article à paraître [25].

Enfin Helfgott indique page 48 de [15] que Green et Tao [10] (article qui était un preprint à ce moment-là) prouve Chowla pour un produit de 4 formes linéaires. En fait l'article [10] prouve l'énoncé plus général suivant.

Proposition 1.3.7. *(Green-Tao [10], Proposition 9.1) Soit $\psi_i(x,y) = a_i x + b_i y$ $(1 \leq t)$ des formes linéaires non colinéaires deux à deux ; soit K un corps convexe inclus dans $[-X,X]^2$, alors*

$$\sum_{(x,y)\in K\cap\mathbb{Z}^2} \prod_{i=1}^{t} \lambda(\psi_i(x,y)) = o(X^2) \tag{1.21}$$

De plus la même estimation vaut en remplaçant λ par μ la fonction de Moebius.

Il s'agit bien de la conjecture de Chowla pour un polynôme sans facteurs carrés et produit de formes linéaires. Green et Tao montre même que le petit "o" est uniforme en la complexité s du système linéaire, le nombre de formes t et une borne pour leur taille. Notons que l'énoncé est prouvé, dans [10], conditionnellement à deux conjectures de nature technique poétiquement baptisées $GI(s)$ et $MN(s)$; cependant ces deux conjectures ont été ensuite établies par les mêmes auteurs et Ziegler, respectivement dans [12] et [11].

Enfin dans un autre registre, il y a une preuve de la conjecture de Chowla *en moyenne* [29] pour les produits de facteurs linéaires en 1 variable. C'est-à-dire que, à défaut de prouver que

$$\sum_{n\leq X} \lambda((n+h_1)\dots(n+h_k)) = o(X)?$$

les auteurs prouvent que

$$\sum_{h_1,\dots,h_k\leq H} \left| \sum_{n\leq X} \lambda((n+h_1)\dots(n+h_k)) \right| = o(H^k X),$$

pourvu que H tende vers l'infini (en fonction de X) et $H \leq X$.

1.3.3 Un résultat combinant les deux conjectures

La conjecture du crible des facteurs carrés décrit, au moins statistiquement, les facteurs carrés des valeurs $f(\mathrm{v})$, tandis que la conjecture de Chowla décrit, au moins statistiquement, la parité du nombre de facteurs premiers des valeurs $f(\mathrm{v})$. Nous établissons dans cette partie un résultat affirmant une sorte d'indépendance des deux propriétés "valeur sans facteur carré" et "parité donnée du nombre de facteurs premiers".

Ce résultat analytique semble être nouveau ; nous l'utiliserons au chapitre 5 pour la preuve du théorème 5.0.8.

Théorème 1.3.8. *Soit f polynôme à coefficients entiers, sans facteurs carrés. Supposons la conjecture du crible des facteurs carrés et la conjecture de Chowla vraies pour f, alors l'estimation suivante vaut pour toute progression arithmétique $\mathcal{A}$, où $\epsilon = \pm 1$:*

$$\sharp\left\{ \mathrm{v}\in\mathcal{A}(X) \mid \frac{f(\mathrm{v})}{d_{f,\mathcal{A}}} \text{ est sans facteur carré et } \lambda(f(\mathrm{v})) = \epsilon \right\} = \frac{C_{f,\mathcal{A}}}{2}\mathrm{A}(X) + o(A(X)). \tag{1.22}$$

En combinant cet énoncé avec les résultats cités précédemment (Théorèmes 1.3.2 et 1.3.6), on obtient :

Corollaire 1.3.9. *Soit f un polynôme homogène en deux variables, à coefficients entiers, sans facteurs carrés. Supposons, ou bien que* $\deg f \leq 3$*, ou bien que f est produit de formes linéaires, alors l'estimation suivante vaut pour toute progression arithmétique $\mathcal{A}$, où $\epsilon = \pm 1$:*

$$\sharp\left\{\mathrm{v} \in \mathcal{A}(X) \mid \frac{f(\mathrm{v})}{d_{f,\mathcal{A}}} \text{ est sans facteur carré et } \lambda(f(\mathrm{v})) = \epsilon\right\} = \frac{C_{f,\mathcal{A}}}{2}\mathrm{A}(X) + o(A(X)). \tag{1.23}$$

Démonstration. (du théorème 1.3.8) Notons $T(X)$ la fonction de comptage que l'on veut estimer. Observons, d'une part, que $\mu^2(n)$ vaut 1 si n est sans facteur carré et vaut 0 sinon, d'autre part, que $1 + \epsilon\lambda(n)$ vaut 2 si $\lambda(n) = \epsilon$ et vaut 0 sinon. Notons aussi la relation $\mu^2(n)\lambda(n) = \mu(n)$. On en tire

$$2T(X) = \sum_{\mathrm{v}\in\mathcal{A}(X)} \mu^2\left(\frac{f(\mathrm{v})}{d_{f,\mathcal{A}}}\right)\left(1 + \epsilon\lambda\left(\frac{f(\mathrm{v})}{d_{f,\mathcal{A}}}\right)\right) = \sum_{\mathrm{v}\in\mathcal{A}(X)} \mu^2\left(\frac{f(\mathrm{v})}{d_{f,\mathcal{A}}}\right) + \epsilon \sum_{\mathrm{v}\in\mathcal{A}(X)} \mu\left(\frac{f(\mathrm{v})}{d_{f,\mathcal{A}}}\right)$$

Appelons $S_1(X)$ et $S_2(X)$ ces deux dernières sommes. La conjecture du crible des facteurs carrés dit précisément que $S_1(X) = C_{f,\mathcal{A}}A(X) + o(A(X))$, tandis que la conjecture de Chowla affirme que, en remplaçant dans la deuxième somme μ par λ on obtient une somme $o(A(X))$; il suffit donc de démontrer le lemme suivant pour conclure la preuve du théorème.

Lemme 1.3.10. *Sous les hypothèses du théorème, on a l'estimation*

$$\sum_{\mathrm{v}\in\mathcal{A}(X)} \left\{\lambda\left(\frac{f(\mathrm{v})}{d_{f,\mathcal{A}}}\right) - \mu\left(\frac{f(\mathrm{v})}{d_{f,\mathcal{A}}}\right)\right\} = o(A(X))$$

Comme le terme de la somme est nul si $f(\mathrm{v})d_{f,\mathcal{A}}^{-1}$ est sans facteur carré, la somme à évaluer est la somme des $\lambda(f(\mathrm{v})d_{f,\mathcal{A}}^{-1}) = \epsilon_0\lambda(f(\mathrm{v}))$ quand v parcourt $\mathcal{A}(X)$ et $f(\mathrm{v})d_{f,\mathcal{A}}^{-1}$est divisible par p^2 pour au moins un p (où $\epsilon_0 = \lambda(d_{f,\mathcal{A}})$).

Pour alléger la notation, posons

$$F(X) = \sum_{\mathrm{v}\in\mathcal{A}(X)} \left\{\lambda\left(\frac{f(\mathrm{v})}{d_{f,\mathcal{A}}}\right) - \mu\left(\frac{f(\mathrm{v})}{d_{f,\mathcal{A}}}\right)\right\}.$$

Rappelons, que l'on veut démontrer qu'il existe une constante c_1 telle que pour $Z > 0$ donné, on a $\forall\epsilon > 0$, $\exists X_o = X_o(\epsilon, Z)$ tel que pour $X \geq X_o$ on a

$$|F(X)| \leq (\frac{c_1}{Z} + \epsilon)X^h.$$

Ceci signifierait que

$$\limsup \frac{|F(x)|}{X^h} \leq \frac{c_1}{Z} + \epsilon.$$

Donc que

$$|F(X)| = o(X^h).$$

Pour ce faire, on sépare la somme $F(X)$ en trois parties. La première s'occupe des nombres premiers tels que $p \geq X$, la seconde de $p \in [Z, X]$ et la dernière des $p < Z$. Ici, Z est une constante fixée, qui peut être très grande (et qui ne dépend pas de X).

Pour la première somme, la conjecture des facteurs carrés prédit que

$$\left|\sum_{\substack{\mathrm{v}\in\mathcal{A}(X),\\ \exists p>X, p^2|f(\mathrm{v})}}\lambda(f(\mathrm{v}))\right| \leq \sum_{\substack{\mathrm{v}\in\mathcal{A}(X),\\ \exists p>X, p^2|f(\mathrm{v})}} 1 = o(X^h).$$

Pour la seconde somme, l'estimation (1.13) donne

$$\left|\sum_{\substack{\mathrm{v}\in\mathcal{A}(X),\\ \exists p\in[Z,X], p^2|f(\mathrm{v})}}\lambda(f(\mathrm{v}))\right| \leq \frac{c_1}{Z}X^h,$$

où c_1 est une constante.

Pour la dernière somme, on veut traiter les "petits" p (c'est-à dire les $p \leq Z$) tels que p^2 divise $f(\mathrm{v})d_{f,\mathcal{A}}^{-1}$, on remarque qu'ils sont en nombre fini (on prendra $p < Z$, avec Z "grand" mais fixé) on utilise un argument différent en regroupant les $\mathrm{v} = (x, y)$ selon des sous-réseaux de congruence $L_{p,i}$ définis par $x \equiv \omega_i y \mod p^2$ (où $f(\omega_i, 1) \equiv 0 \mod p^2$) et en écrivant sur ce sous-réseau $\mathrm{v} = \phi_i \mathrm{w}$ (pour $\mathrm{w} \in \mathbb{Z}^2$) et $d!f(\phi_i(\mathrm{w})) = p^2 g_{p,i}(\mathrm{w})$. En écrivant la conjecture de Chowla pour $g_{p,i}$ on obtient

$$\sum_{\mathrm{v}\in L_{p,i}(X),}\lambda(f(\mathrm{v})) = \lambda(d!)\sum_{\mathrm{w}\in L_{p,i}(X)}\lambda(g_{p,i}(\mathrm{w})) = o(X^h)$$

et, en sommant sur le nombre fini de sous-réseaux :

$$\sum_{\substack{\mathrm{v}\in\mathcal{A}(X),\\ p^2|\,f(\mathrm{v})}}\lambda(f(\mathrm{v})) = o(X^h).$$

On peut préciser cela en disant que, pour ϵ donné, on a, pour $X > X_0(p, \epsilon)$

$$\left|\sum_{\substack{\mathrm{v}\in\mathcal{A}(X),\\ p^2|\,f(\mathrm{v})}}\lambda(f(\mathrm{v}))\right| \leq \epsilon X^h.$$

On peut généraliser l'argument à $q = p_1 \dots p_r$ produit de premiers et obtenir que pour $X > X_0(q, \epsilon)$

$$\left|\sum_{\substack{\mathrm{v}\in\mathcal{A}(X),\\ q^2|\,f(\mathrm{v})}}\lambda(f(\mathrm{v}))\right| \leq \epsilon X^h.$$

On applique cela de la façon suivante : on note $p_1 < p_2 < \dots < p_r$ les nombres premiers $< Z$ et, pour chaque $J \subset [1, r]$ on pose $q_J := \prod_{j\in J} p_j$.

En appliquant le principe d'inclusion-exclusion on voit que

$$\sum_{\substack{\mathrm{v}\in\mathcal{A}(X),\\ \exists p<Z, p^2|\,f(\mathrm{v})}}\lambda(f(\mathrm{v})) = -\sum_{J\neq\emptyset}(-1)^{|J|}\sum_{\substack{\mathrm{v}\in\mathcal{A}(X),\\ q_J^2|\,f(\mathrm{v})}}\lambda(f(\mathrm{v})).$$

La somme extérieure comporte environ $2^{\frac{Z}{\log Z}}$ termes. Quant aux termes de la somme intérieure, on vient de démontrer qu'ils sont tels que

$$\sum_{\substack{\mathrm{v}\in\mathcal{A}(X),\\ q_J^2|\,f(\mathrm{v})}}\lambda(f(\mathrm{v})) \leq \epsilon X^h,$$

pour $X \geq X_0(p, \epsilon)$.

Cela permet de conclure que la somme est bornée par $\left(2^{\frac{Z}{\log Z}}\epsilon\right) X^h$, (ou plus simplement par $\epsilon' X^h$, où $\epsilon' = 2^{\frac{Z}{\log Z}}\epsilon$), dès que X est assez grand (c'est-à-dire pour X supérieur à un certain $X_o(\epsilon, Z)$).

Rappelons la notation

$$F(X) = \sum_{\mathrm{v} \in \mathcal{A}(X)} \left\{ \lambda\left(\frac{f(\mathrm{v})}{d_{f,\mathcal{A}}}\right) - \mu\left(\frac{f(\mathrm{v})}{d_{f,\mathcal{A}}}\right) \right\}.$$

On a démontré qu'il existe une constante c_1 telle que pour $Z > 0$ donné, on a $\forall \epsilon > 0, \exists X_o = X_o(\epsilon, Z)$ tel que pour $X \geq X_o$ on a

$$|F(X)| \leq \left(\frac{c_1}{Z} + \epsilon\right) X^h.$$

Ceci signifie que

$$\limsup \frac{|F(x)|}{X^h} \leq \frac{c_1}{Z} + \epsilon.$$

Donc

$$\left| \sum_{\mathrm{v} \in \mathcal{A}(X)} \left\{ \lambda\left(\frac{f(\mathrm{v})}{d_{f,\mathcal{A}}}\right) - \mu\left(\frac{f(\mathrm{v})}{d_{f,\mathcal{A}}}\right) \right\} \right| = o(X^h).$$

Ceci achève la preuve du lemme.

□

2

Moyenne du signe (d'après Helfgott)

En 2003, Helfgott met en ligne un article dont le résultat principal est le théorème suivant.

On rappelle que $B_{\mathscr{E}}$ est le produit des polynômes (homogènes) associés aux places en lesquelles la réduction de $\mathscr{E}$ n'est pas I_0 ni I_0^*. Quant à $M_{\mathscr{E}}$, c'est le produit des polynômes (homogènes) associés aux places de réduction multiplicative.

Théorème 2.0.11. *[15] Soit $\mathscr{E}$ une surface elliptique non isotriviale sur $\mathbb{Q}$. On admet les hypothèses suivantes :*

a. la conjecture du crible des facteurs carrés en version homogène est vérifiée par $B_{\mathscr{E}}$,

b. la conjecture de Chowla est vérifiée en version homogène par $M_{\mathscr{E}}$.

On a,

1. *si $M_{\mathscr{E}} = 1$, alors*
$$av_{\mathbb{Q}}(W(\mathscr{E}_t)) \in]-1, 1[;$$
2. *si $M_{\mathscr{E}} \neq 1$, alors*
$$av_{\mathbb{Q}}(W(\mathscr{E}_t)) = 0.$$

En particulier, dans les deux cas, W_+ et W_- sont infinis.

Remarque 32. La démonstration du point 1 de ce théorème n'est pas donnée dans l'article. Elle nécessite l'utilisation d'un lemme de Manduchi. Nous complétons la démonstration par le corollaire 2.5.4.

Remarque 33. Pour les surfaces qui admettent une place de réduction multiplicative, on a également (sous les conjectures du crible des facteurs carrés et de Chowla à une variable)

$$av_{\mathbb{Z}}(W(\mathscr{E}_t)) = 0.$$

Cependant, ce n'est pas vrai pour les surfaces sans réduction multiplicative. En effet, on a un exemple de Rizzo [37] d'une surface non isotriviale sur laquelle le signe est constant égal à -1 sur $\mathbb{Z}$.

On déduit du théorème 2.0.11 le corollaire suivant qui est inconditionnel. Il découle des cas connus des conjectures de Chowla et du crible des facteurs carrés.

Corollaire 2.0.12. *Soit $\mathscr{E}$ une surface elliptique sur $\mathbb{Q}$. On admet les hypothèses suivantes.*

1. *Toute place w_P qui n'est pas de réduction I_0 ou I_0^* est telle que* $\deg P \leq 6$.
2. $\deg M_{\mathscr{E}} \leq 3$ *ou bien M un produit de degré arbitraire de facteurs linéaires.*

Alors $W_+(\mathbb{Q})$ et $W_-(\mathbb{Q})$ sont infinis.

2.1 Introduction

2.1.1 Motivations et idées générales

Soit E une courbe elliptique sur $\mathbb{Q}$. Grâce aux travaux de Wiles [52], on sait que la fonction $L(E,s)$ associée à cette courbe elliptique admet un prolongement analytique et une équation fonctionnelle de la forme

$$\mathscr{N}_E^{(2-s)/2}(2\pi)^{s-2}\Gamma(2-s)L(E,2-s) = W(E)\mathscr{N}_E^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s),$$

où $\mathscr{N}_E$ est le conducteur de E et la constante $W(E) \in \{\pm 1\}$ est appelée le *signe* de cette équation fonctionnelle.

Soit $r_{an}(E/\mathbb{Q})$ l'ordre d'annulation de $L(E,s)$ en $s=1$. La conjecture de Birch et Swinnerton-Dyer prédit que $\text{rang } E/\mathbb{Q} = r_{an}(E/\mathbb{Q})$ et, en particulier, l'égalité suivante, appelée la *conjecture de parité* :

$$W(E) = (-1)^{\text{rang } E(\mathbb{Q})}.$$

Une conséquence de cette égalité est qu'il est suffisant que $W(E) = -1$ pour que rang $E(\mathbb{Q})$ soit non nul et en particulier que $E(\mathbb{Q})$ soit infini.

Soit une surface elliptique $\mathscr{E}$ sur $\mathbb{Q}$ dont les fibres en $t \in \mathbb{Q}$ sont notées $\mathscr{E}_t$. On peut s'intéresser à la variation de $W(\mathscr{E}_t)$ quand $t \in \mathbb{Q}$ varie.

On étudiera les ensembles W_+ et W_- donnés par

$$W_\pm(\mathscr{E}) = \{t \in \mathbb{Q} : \mathscr{E}_t \text{ est une courbe elliptique et } W(\mathscr{E}_t) = \pm 1\}$$

Remarque 34. Une conséquence de la conjecture de parité (combinée avec la proposition 1.2.1) est qu'il suffit que W_- soit infini pour que la densité des points rationnels de $\mathscr{E}$ soit démontrée. Si le signe varie, c'est-à-dire que ces deux ensembles soient tels que $\#W_\pm = \infty$, alors on a aussi cette conclusion.

Si le signe est équidistribué, c'est à dire si la moyenne du signe sur un sous ensemble infini de $\mathbb{Z}$ ou de $\mathbb{Q}$ est $av(W(\mathscr{E}_t)) = 0$, alors $W_\pm$ sont infinis. De même si $-1 < av(W(\mathscr{E}_t)) < 1$.

2.1.2 Résumé des résultats

Soit $\mathscr{E}$, une surface elliptique, et $f : \mathbb{Q} \to \{-1,+1\}$ une fonction (nous nous intéresserons plus particulièrement à celle définie par $t \mapsto W(\mathscr{E}_t)$).

On étudiera la moyenne du signe des fibres sur $\mathbb{Q}$, une valeur qui nous renseignera sur les cardinalités des ensembles $W_\pm(\mathscr{E})$. Celle-ci sera calculée en ordonnant les fibres en $t \in \mathbb{Q}$ (ou $t \in \mathbb{Z}$) selon la hauteur de t (voir 2.2.1 pour plus de détails) :

$$av_{\mathbb{Q}} f = \lim_{N\to\infty} \frac{\sum_{(x,y)\in[-N,N]^2,\text{pgcd}(x,y)=1,y\neq 0} f(x/y)}{\sum_{(x,y)\in[-N,N]^2,\text{pgcd}(x,y)=1} 1}.$$

Dans un premier temps, on obtiendra la décomposition pour le signe d'une fibre de $\mathscr{E}$ donnée par le théorème suivant :

Théorème 2.1.1. *[15, Thm. 6.6].*

Soit $\mathscr{E}$ une courbe elliptique sur $\mathbb{Q}(T)$. Pour $t \in \mathbb{Q}$, on note $t = \frac{x}{y}$ pour x, y des entiers premiers entre eux.

Alors il existe

1. *S un ensemble fini de places de $\mathbb{Q}$ contenant ∞ ;*
2. *pour chaque $v \in S$, des fonctions $g_v : \mathbb{Q}_v \times \mathbb{Q}_v \longrightarrow \{-1, 1\}$ localement constantes en dehors d'un ensemble fini de droites passant par l'origine ; et*
3. *pour chaque $p \notin S$, des fonctions $h_p : \mathbb{Q}_p \times \mathbb{Q}_p \to \{-1, 1\}$ localement constantes en dehors d'un ensemble fini de droites passant par l'origine telles que $h_p(x, y) = 1$ lorsque $p^2 \nmid B_{\mathscr{E}}(x, y)$;*

tels que le signe s'écrit

$$W(\mathscr{E}_t) = \lambda(M_{\mathscr{E}}(x, y)) \cdot \prod_{v \in S} g_v(x, y) \prod_{v \notin S} h_v(x, y),$$

Dans le cas où la surface considérée est isotriviale, il est possible que la moyenne du signe soit -1 ou $+1$. Dans ces cas, toute fibre sauf un ensemble non dense est de signe $+1$ ou -1. Si la moyenne est $+1$, on ne peut rien conclure sur la densité des points rationnels à partir de l'étude de la moyenne du signe. On obtient toutefois pour toute surface isotriviale une formule pour la moyenne du signe (Proposition 2.5.1).

Proposition 2.1. *Soit $\mathscr{E}$ une surface elliptique isotriviale dont le j-invariant est différent de 0 et 1728. Soient S l'ensemble et pour chaque $v \in S$ la fonction g_v donnée par le théorème 2.3.3.*

Alors le signe moyen sur $\mathbb{Q}$ s'écrit

$$av_{\mathbb{Q}}\left(W(\mathscr{E}_t)\right) = -\prod_{p \in S} \frac{1}{1 - p^{-2}} \int_{\mathscr{Z}_p} g_p(x, y) dx dy,$$

où $\mathscr{Z}_p = (\mathbb{Z}_p \times \mathbb{Z}_p) \backslash (p\mathbb{Z}_p \times p\mathbb{Z}_p)$.

Dans le cas non isotrivial où $\mathscr{E}$ n'admet pas de place de réduction I_m, on utilise la conjecture du crible des facteurs carrés (1.1) pour démontrer la formule suivante pour la moyenne du signe (Proposition 2.5.2) :

Proposition 2.2. *Soit une surface elliptique qui est soit isotriviale avec $j = 0$ ou $j = 1728$ ou non isotriviale sans place de réduction I_m. Alors, sous l'hypothèse que la conjecture du crible des facteurs carrés soit vérifiée pour $B_{\mathscr{E}}$, la moyenne du signe sur $\mathbb{Q}$ s'écrit*

$$av_{\mathbb{Q}} W(\mathscr{E}_t) = -\prod_{p \in S} \frac{1}{1 - p^{-2}} \int_{\mathscr{Z}_p} g_p(x, y) dx dy \cdot \prod_{p \notin S} \frac{1}{1 - p^{-2}} \int_{\mathscr{Z}_p} h_p(x, y) dx dy,$$

où S, g_p et h_p sont l'ensemble et les fonctions données par le théorème 2.3.3.

De cette formule, on déduit le corollaire suivant :

Corollaire 2.1.2. *Soit $\mathscr{E}$ une surface elliptique non isotriviale sans place de réduction de type I_m. On suppose que $B_{\mathscr{E}}$ respecte la conjecture du crible des facteurs carrés. Alors*

$$-1 < av_{\mathbb{Q}} W(\mathscr{E}_t) < +1.$$

La démonstration n'est pas explicitement donnée par Helfgott. Le résultat est tout simplement mentionné dans un article postérieur de Conrad, Conrad et Helfgott [4]. Nous donnons la démonstration ici.

Dans le cas où $\mathscr{E}$ admet une place de réduction I_m, la conjecture du crible des facteurs carrés et la conjecture de Chowla permettent de démontrer que le comportement du signe vérifie une propriété plus forte : que le signe moyen est nul sur tout sous-ensemble de $\mathbb{Q}$ provenant d'un réseau de $\mathbb{Z}^2$ (Proposition 2.4.3). On énonce ici plus simplement le résultat sur $\mathbb{Q}$:

Corollaire 2.1.3. *Soit $\mathscr{E}$ une surface elliptique qui admet au moins une place de réduction multiplicative. On fait les hypothèses suivantes :*

1. *$B_{\mathscr{E}}$ vérifie la conjecture du crible des facteurs carrés, et*
2. *$M_{\mathscr{E}}$ vérifie la conjecture de Chowla.*

Alors la moyenne du signe des fibres sur $\mathbb{Q}$ est

$$av_{\mathbb{Q}} W(\mathscr{E}_t) = 0.$$

La plupart des résultats de [15] dépendent de conjectures de théorie analytique des nombres : la conjecture du crible des facteurs carrés et la conjecture de Chowla. Dans la section 1.3, nous les présentons et donnons les énoncés inconditionnels selon ce que nous connaissons actuellement.

De plus, nous nous intéressons aux surfaces elliptiques rationnelles pour lesquelles les résultats sont inconditionnels dans la section 4.3.1 de cette thèse.

Un article antérieur de Manduchi [27] étudie de même le signe de l'équation fonctionnelle des fibres d'une surface elliptique (sans toutefois calculer leur moyenne). Dans la section 2.7, nous expliquons les avancées de Helfgott par rapport à ce travail.

2.2 Notions préliminaires

2.2.1 Moyennes d'une fonction

Nous allons calculer la moyenne de fonctions sur les entiers, les progressions arithmétiques, les sous-ensembles de $\mathbb{Z}^2$ et les rationnels. Pour ce faire, nous allons ordonner $\mathbb{Z}^2$ et $\mathbb{Q}$ en terme de hauteur. Plus précisément, nous procéderons de la façon suivante.

Soit $f : \mathbb{Z} \to \mathbb{C}$ et une progression arithmétique $a + m\mathbb{Z}$. On définit la moyenne de f sur $a + m\mathbb{Z}$ par

$$av_{a+m\mathbb{Z}} f = \lim_{N\to\infty} \frac{1}{N/m} \sum_{1\leq n\leq N; n\equiv a \mod m} f(n).$$

En particulier, la moyenne de f sur $\mathbb{Z}$ est définie ainsi

$$av_{\mathbb{Z}}(f) = \lim_{N\to\infty} \frac{\sum_{n\in[-N,N]} f(n)}{\sum_{n\in[-N,N]} 1}.$$

Soit une fonction $f : \mathbb{Z}^2 \to \mathbb{C}$, un réseau $a + L \subset \mathbb{Z}^2$ et un secteur $S \subset \mathbb{R}^2$, c'est-à-dire une composante connexe d'un ensemble de la forme $\mathbb{R}^2 \backslash \mathscr{L}$ où $\mathscr{L}$ est un ensemble fini de droites passant par l'origine. On définit

$$av_{S\cap(a+L)} f = \lim_{N\to\infty} \frac{\sum_{(x,y)\in S\cap(a+L)\cap[-N,N]^2} f(x,y)}{\sum_{(x,y)\in S\cap(a+L)\cap[-N,N]^2} 1}$$

On peut voir $\mathbb{Q}$ comme le sous-ensemble des paires $(x, y) \in \mathbb{Z}^2$ pour lesquelles x et $y \geq 0$ sont premiers entre eux. Aussi, pour une fonction $f : \mathbb{Q} \to \mathbb{Z}$, un réseau $a + L \subset \mathbb{Z}^2$ et un secteur $S \subset \mathbb{R}^2$, on définit

$$av_{\mathbb{Q},S\cap(a+L)}f = \lim_{N\to\infty} \frac{\sum_{(x,y)\in S\cap(a+L)\cap[-N,N]^2,\mathrm{pgcd}(x,y)=1,y\neq 0} f(x,y)}{\sum_{(x,y)\in S\cap(a+L)\cap[-N,N]^2;\mathrm{pgcd}(x,y)=1} 1}.$$

En particulier, on a

$$av_{\mathbb{Q}}f = \lim_{N\to\infty} \frac{\sum_{(x,y)\in[-N,N]^2,\mathrm{pgcd}(x,y)=1,y\neq 0} f(x,y)}{\sum_{(x,y)\in[-N,N]^2,\mathrm{pgcd}(x,y)=1} 1}.$$

Remarque 35. Comme on prend x et y parmi $[-N, N]$, chaque valeur de $t \in \mathbb{Q}$ est obtenue exactement deux fois. Toutefois, cela n'a pas d'importance car le diviseur comptabilise également deux fois chaque t. La moyenne est donc inchangée.

Remarque 36. Dans le cas où ces limites n'existent pas, on les remplace par lim inf ou lim sup.

Remarque 37. Dans les moyennes précédentes, les fonctions f peuvent ne pas être définies pour un nombre fini de valeurs. La moyenne n'en sera pas changée.

2.2.2 Signe local d'une fibre selon le type de réduction

Soit E une courbe elliptique. Le signe de E peut s'exprimer comme un produit de facteurs locaux

$$W(E) = \prod_{p\leq\infty} W_p(E), \tag{2.1}$$

où p parcourt les nombres premiers rationnels et l'infini, $W_p(E) \in \{\pm 1\}$ et $W_p(E) = +1$ pour tout p sauf un nombre fini. Le signe local $W_p(E)$ en p de E est défini en terme des facteurs epsilon de représentations de Weil-Deligne de $\mathbb{Q}_p$ (voir [6] et [49] pour une définition de ces facteurs locaux). Les travaux de Rohrlich donnent une formule pour le signe local en $p \neq 2, 3$ en terme du type de réduction en p d'une courbe elliptique.

Proposition 2.2.1. *[38] Soit p un nombre premier de $\mathbb{Q}$ différent de 2 et 3. Soit E une courbe elliptique sur $\mathbb{Q}$ que l'on écrit sous forme de Weierstrass*

$$E : y^2 = x^3 - 27c_4x - 54c_6.$$

Alors le signe local en p est

$$W_p(E) = \begin{cases} 1 & \text{si la réduction de } E \text{ en } p \text{ est de type } I_0; \\ (-1/p) & \text{si la réduction est de type } II,\ II^*,\ I_m^* \text{ ou } I_0^*; \\ (-2/p) & \text{si la réduction est de type } III \text{ ou } III^*; \\ (-3/p) & \text{si la réduction est de type } IV \text{ ou } IV^*; \\ -(-c_6/p) & \text{si la réduction est de type } I_m; \end{cases}$$

Pour $p = 2, 3$, on se réfère aux tableaux d'Halberstadt [13] ou de Rizzo [37]. De plus, on a toujours $W_\infty(E) = -1$.

2.2.3 Places de réduction génériques d'une surface elliptique

Soit une surface elliptique $\mathscr{E}$ sur $\mathbb{Q}$ et soit $\Delta(T) \in \mathbb{Z}[T]$ son discriminant. Nous allons décrire la réduction de $\mathscr{E}$ en w_P une place de $\mathbb{Q}[T]$ associée à un polynôme irréductible unitaire $P(T) \in \mathbb{Z}[T]$ par un symbole de Kodaira.

Soit $(m,n) \in \mathbb{Z} \times \mathbb{Z}^*$ des entiers premiers entre eux pour lesquels on pose $t = \frac{m}{n}$. Soit k le plus petit entier tel que $12k \geq \deg \Delta(T)$, comme dans la section 1.2.1. Une fibre $\mathscr{E}_t$ en t non singulière est isomorphe à la courbe

$$\mathscr{E}_{m,n} : y^2 = x^3 - 27n^{4k}c_4(m/n)x - 54n^{6k}c_6(m/n),$$

de discriminant $\Delta_{m,n} = n^{12k}\Delta(m/n)$. On note $P(m,n) = n^{\deg P}P(m/n)$, et $P(X,Y) \in \mathbb{Z}[X,Y]$ le polynôme homogène obtenu de cette façon.

On a que
- la réduction de $\mathscr{E}$ en $P(X,Y)$ est de type I_m si et seulement si $P(X,Y) \mid \Delta(X,Y)$, $P(X,Y) \nmid c_4(X,Y)$ et $m = \mathrm{ord}_{w_P}\Delta(X,Y) = -\mathrm{ord}_{w_P}j(X,Y)$;
- de type I_m^* si et seulement si $P(X,Y) \mid \Delta(X,Y)$, $P(X,Y) \mid c_4(X,Y)$, $-\mathrm{ord}_{w_P}j = m$ et $\mathrm{ord}_{w_P}\Delta(X,Y) = m+6$;
- de type II si et seulement si $P(X,Y) \mid c_4(X,Y)$, $\mathrm{ord}_{w_P}\Delta(X,Y) = 2$;
- de type III si et seulement si $P(X,Y) \mid c_4(X,Y)$, $\mathrm{ord}_{w_P}\Delta(X,Y) = 3$;
- de type IV si et seulement si $P(X,Y) \mid c_4(X,Y)$, $\mathrm{ord}_{w_P}\Delta(X,Y) = 4$;
- de type I_0^* si et seulement si $P(X,Y) \mid c_4(X,Y)$, $\mathrm{ord}_{w_P}\Delta(X,Y) = 6$;
- de type IV^* si et seulement si $P(X,Y) \mid c_4(X,Y)$, $\mathrm{ord}_{w_P}\Delta(X,Y) = 8$;
- de type III^* si et seulement si $P(X,Y) \mid c_4(X,Y)$, $\mathrm{ord}_{w_P}\Delta(X,Y) = 9$;
- de type II^* si et seulement si $P(X,Y) \mid c_4(X,Y)$, $\mathrm{ord}_{w_P}\Delta(X,Y) = 10$;
- de type I_0 si $P(X,Y) \nmid \Delta(X,Y)$.

Pour alléger les notations, on utilisera la convention suivante.

On note $\mathscr{A}_2(\mathscr{E})$ l'ensemble des places de réduction de type II et II^*, $\mathscr{A}_3(\mathscr{E})$ l'ensemble des places de type III et III^*, $\mathscr{A}_4(\mathscr{E})$ celui des places de type IV et IV^*, $\mathscr{M}^*$ celui des places de type I_m^*. L'ensemble de toutes les places additives sera noté $\mathscr{A}(\mathscr{E})$.

On définit $\mathscr{M}(\mathscr{E})$, comme l'ensemble des places v de $\mathbb{Q}(T)$ pour lesquelles la réduction de $\mathscr{E}$ en v est de type I_m.

On définira aussi $\mathscr{B}(\mathscr{E})$, l'ensemble des places v de $\mathbb{Q}(T)$ pour lesquelles la réduction de $\mathscr{E}$ en v n'est ni de type I_0, ni de type I_0^*. Finalement, on définit $\mathscr{B}'(\mathscr{E})$, l'ensemble des places qui ne sont pas de type I_0, autrement dit les places de mauvaise réduction.

Remarquons que

$$\mathscr{M}(\mathscr{E}) \subseteq \mathscr{B}(\mathscr{E}) \subseteq \mathscr{B}'(\mathscr{E}).$$

On définit les polynômes homogènes

$$M_{\mathscr{E}}(x,y) = \prod_{v \in \mathscr{M}_{\mathscr{E}}} P_v(x,y)$$

et

$$B_{\mathscr{E}}(x,y) = \prod_{v \in \mathscr{B}_{\mathscr{E}}} P_v(x,y).$$

Avec ces définitions, on a que $M_{\mathscr{E}}(x,y)$ divise $B_{\mathscr{E}}(x,y)$ (qui divise $\Delta(x,y)$).

On fera souvent un abus de notation en omettant de préciser la surface si celle-ci est évidente.

2.2.4 Surfaces elliptiques

On peut classifier les surfaces elliptiques en quatre catégories, pour lesquelles le comportement de la fonction signe sera sensiblement différent.

A. La surface $\mathscr{E}$ considérée est une surface isotriviale dont la fonction du j-invariant est constante, égale à un rationnel qui n'est ni 0 ni 1728. Autrement dit, la surface est une famille de twists d'une courbe elliptique de forme générale, c'est-à-dire qu'il existe une fonction $f(T) \in \mathbb{Z}[T]$ et $a, b \in \mathbb{Z}^\times$ tels que $\mathscr{E}$ est décrite par l'équation de Weierstrass

$$f(T)y^2 = x^3 + ax + b.$$

Dans ce cas, les places génériques sont uniquement de réduction I_0 ou I_0^*.

La variation du signe de ces surfaces est plus amplement étudié dans la section 3.1.

B. La surface $\mathscr{E}$ est isotriviale d'invariant $j = 0$ ou 1728.

(a) Si la fonction j-invariant est 1728, il existe $f(T) \in \mathbb{Z}[T]$ telle que E est décrite par l'équation

$$y^2 = x^3 + f(T)x.$$

Une place générique sur une surface de cette forme peut être de type I_0, I_0^*, II, II^*, IV ou IV^*.

(b) Si la fonction j-invariant égale 0, il existe $f(T) \in \mathbb{Z}[T]$ tel que $\mathscr{E}$ est décrite par l'équation

$$y^2 = x^3 + f(T).$$

Une place générique sur une surface de cette forme peut être de type I_0, I_0^*, III ou III^*.

Nous étudierons ces surfaces dans la section 3.2, et dans les sections 4.2.4 et 4.2.3 lorsque la surface considérée est rationnelle et $F(T)$ est d'une certaine forme.

C. La surface n'est pas isotriviale et n'admet pas de réduction de type I_m.

Dans ce cas, par le fait que la fonction j-invariant a un pôle (car elle est non constante), la surface admet une place de réduction I_m^*. Cette place est éventuellement à l'infini.

D. La surface admet au moins une place de type I_m.

2.2.5 Symboles quadratiques

Soit $p \neq 2$ un nombre premier. On se rappelle que le symbole de Legendre, noté $\left(\frac{\cdot}{p}\right)$, est tel que

$$\left(\frac{n}{p}\right) = 1 \Leftrightarrow n = \text{ carré } \mod p.$$

Soit N un nombre impair et $N = p_1^{k_1} \dots p_r^{k_r}$ sa décomposition en facteurs irréductibles. Le symbole de Jacobi, également noté $\left(\frac{\cdot}{N}\right)$, est défini par :

$$\left(\frac{\cdot}{N}\right) = \prod_i \left(\frac{\cdot}{p_i}\right)^{k_i}.$$

Dans cette section, on considère une variante du symbole de Jacobi.

Notation 3. Pour un polynôme $a \in \mathbb{Q}(T)^*$, nous noterons $a(x,y) := y^{deg(a)}a(t)$ où $t = \frac{x}{y}$, représenté par $x, y \in \mathbb{Z}$ premiers entre eux.

De plus, pour un entier N et un nombre premier p, on notera $N_{(p)}$ l'entier tel que $N = p^{v_p(N)}N_{(p)}$.

Pour δ entier et $a, b \in \mathbb{Q}(T)^*$, la fonction $(a|b)_\delta : \mathbb{Q} \to \{-1, 1\}$ est définie par

$$(a|b)_\delta(t) = \prod_{p \nmid 2\delta} \Big(\frac{a(x,y)_{(p)}}{p}\Big)^{v_p(b(x,y))},$$

pour $x, y \in \mathbb{Z}$ premiers entre eux tels que $t = \frac{x}{y}$, où $(\frac{\cdot}{p})$ est le symbole de Legendre.

Cette fonction respecte les propriétés suivantes.

(a) $(ab|c)_\delta(t) = (a|c)_\delta(t) \cdot (b|c)_\delta(t)$, car le symbole $\left(\frac{\cdot}{p}\right)$ est multiplicatif ;

(b) $(a|bc)_\delta(t) = (a|b)_\delta(t) \cdot (a|c)_\delta(t)$, par définition.

(c) $(a|b)_\delta(t) = (a + bc|b)_\delta(t)$, car $(\frac{a}{p}) = (\frac{a+px}{p})$ pour tout $a \neq p$, $x \in \mathbb{Z}$.

(d) Pour b fixé, $a \mapsto (a|b)_\delta(t)$ est un produit fini de fonctions localement constantes pour la topologie p-adique.

(e) Si $\delta_1|\delta_2$ (resp. $\delta_2|\delta_1$) et $a, b \neq 0$, on a

$$\frac{(a|b)_{\delta_1}(t)}{(a|b)_{\delta_2}(t)} = \prod_{\substack{p \text{ premier,} \\ p|2\delta_2, p\nmid 2\delta_1}} \Big(\frac{a(x,y)_{(p)}}{p}\Big)^{v_p(b(x,y))},$$

pour (x, y) tels que $\mathrm{pgcd}(x, y)|\delta_1$ (resp. $\mathrm{pgcd}(x, y)|\delta_2$). De plus, cette fonction est un produit fini de fonctions localement constantes pour la topologie p-adique.

(f) Pour $a, b \in \mathbb{Q}$ constants, on a

$$\frac{(a|b)_\delta}{(b|a)_\delta} = \prod_{p|2\delta} \Big(\frac{a_{(p)}, b_{(p)}}{p}\Big)^{-1},$$

où $(\frac{a,b}{p})$ est le symbole de Hilbert quadratique. C'est un produit fini de fonctions localement constantes car les symboles de Hilbert ne dépendent que de a et b modulo $\mathbb{Q}_p^2$. Une introduction aux symboles de Hilbert est donnée dans [43, Chap. III].

2.2.6 Réseaux

Définition 17. On définit un réseau $\mathcal{A}$ comme le sous-ensemble de $\mathbb{Z}^2$

$$\mathcal{A} := \{(ax + by, cx + dz) \mid (x, y) \in \mathbb{Z}^2\},$$

où l'on suppose $ad - bc \neq 0$. On peut aussi écrire $\mathcal{A} = \phi(\mathbb{Z}^2)$ avec $\phi(m, n) = (am + bn, cm + dn)$.

Le translaté par $a \in \mathbb{Z}^2$ d'un réseau $\mathcal{A}$, est l'ensemble

$$T := \{(m, n) \mid ((m, n) - a) \in \mathcal{A})\}.$$

Les lemmes élémentaires suivants, énoncés dans [15], sont utilisés dans la démonstration des propositions 2.5.1, 2.5.2 et 2.5.6.

Lemme 2.2.2. *Soient $a_1 + L_1$, $a_2 + L_2$, $a_3 + L_3$, ..., $a_k + L_k$ des translatés de réseaux de $\mathbb{Z}^2$ d'indices $[\mathbb{Z}^2 : L_1] = p_1^{e_1}$, $[\mathbb{Z}^2, L_2] = p_2^{e_2}$, $[\mathbb{Z}^2 : L_3] = p_3^{e_3}$, ..., $[\mathbb{Z}^2 : L_k] = p_k^{e_k}$ (où p_1, p_2, p_3, ..., p_k sont des nombres premiers distincts), alors l'intersection*

$$\bigcap_{1 \leq j \leq k} (a_j + L_j)$$

est un réseau $a + L$ d'indice $[\mathbb{Z}^2 : L] = \prod_{j \leq k} p_j^{e_j}$.

Lemme 2.2.3. *Soit un réseau $a + L \subset \mathbb{Z}^2$ et un secteur $S \subset \mathbb{R}^2$. On a*

$$\lim_{B \to \infty} \frac{|S \cap (a + L) \cap [-B, B]^2|}{(2B)^2} = \frac{1}{[\mathbb{Z}^2 : L]} \cdot \lim_{B \to \infty} \frac{|S \cap [-B, B]^2|}{(2B)^2}$$

2.3 Une formule pour le signe global

2.3.1 Monodromie des fibres selon le type de réduction des places génériques

Soit $\mathscr{E}_T$ une surface elliptique de discriminant $\Delta(T)$ décrite par l'équation de Weierstrass

$$Y^2 = X^3 - 27c_4(T)X - 54c_6(T).$$

Pour une place générique décrite par un polynôme $P(T) \in \mathbb{Z}[T]$, on se demande quel est le type de réduction de la fibre $\mathscr{E}_t$ de $\mathscr{E}$ en $t = \frac{x}{y} \in \mathbb{Q}$ en un nombre premier $p \mid P(x, y)$.

Pour ce faire, nous analyserons les valuations p-adique du discriminant et des coefficients $c_4(t)$ et $c_6(t)$ de la fibre.

Nous supposerons que p vérifie les propriétés suivantes :

1. $p \neq 2, 3$;
2. les numérateurs et les dénominateurs, (d_0, d_1), (d_2, d_3) et (d_4, d_5), des contenus des polynômes $c_4(T)$, $c_6(T)$ et $\Delta(T)$ ne sont pas divisibles par p ;
3. si $p \mid P(x, y)$, alors pour tout $P' \neq P$ de mauvaise réduction, on a $p \nmid P'(x, y)$. Autrement dit, $p \nmid \prod_{Q, Q' \in \mathscr{B}} Res(Q, Q')$.

Notons que presque tous les nombres premiers vérifie 1, 2 et 3. Il n'y a qu'un nombre fini d'exceptions, et que ce sont les nombres premiers qui divisent l'entier

$$\delta = 2 \cdot 3 \cdot d_1 \ldots d_5 \prod_{Q, Q' \in \mathscr{B}} Res(Q, Q').$$

Le signe local en p dépend des valeurs de $v_p(c_4(x, y))$, $v_p(c_6(x, y))$ et $v_p(\Delta(x, y))$ tel que vu dans la classification des fibres singulières de Néron-Kodaira, en section 1.2.4. Lorsque p respecte les propriétés (1) à (3), ces valuations sont égales à

$$v_p(c_4(x, y)) = w_P(c_4(T)) \cdot v_p(P(x, y)),$$

$$v_p(c_6(x, y)) = w_P(c_6(T)) \cdot v_p(P(x, y))$$

$$v_p(\Delta(x, y)) = w_P(\Delta(T)) \cdot v_p(P(x, y)),$$

où w_P dénote la place générique associée à P. Le type de réduction en p ne dépendra que de la valuation p-adique de $P(x, y)$.

Ce raisonnement permet de déduire le lemme suivant :

Type de $\mathscr{E}_T$ en $P(T)$	$n = v_p(P(x,y))$	Type de $\mathscr{E}_t$ en p	Type de $\mathscr{E}_T$ en $P(T)$	$n = v_p(P(x,y))$	Type de $\mathscr{E}_t$ en p
I_m	$M \geq 1$	I_{Mm}	I_m^*	$0 \mod 2$	I_{mM}
				$1 \mod 2$	I_{mM}^*
II	$0 \mod 6$	I_0	II^*	$0 \mod 6$	I_0
	$1 \mod 6$	II		$1 \mod 6$	II^*
	$2 \mod 6$	IV		$2 \mod 6$	IV^*
	$3 \mod 6$	I_0^*		$3 \mod 6$	I_0^*
	$4 \mod 6$	IV^*		$4 \mod 6$	IV
	$5 \mod 6$	II^*		$5 \mod 6$	II
III	$0 \mod 2$	I_0	III^*	$0 \mod 4$	I_0
	$1 \mod 4$	III		$1 \mod 4$	III^*
	$2 \mod 4$	I_0^*		$2 \mod 4$	I_0^*
	$3 \mod 4$	III^*		$3 \mod 4$	III
IV	$0 \mod 3$	I_0	IV^*	$0 \mod 3$	I_0
	$1 \mod 3$	IV		$1 \mod 3$	IV^*
	$2 \mod 3$	IV^*		$2 \mod 3$	IV
I_0^*	$0 \mod 2$	I_0	I_0	$n \geq 0$	I_0
	$1 \mod 2$	I_0^*			

TABLE 2.1 – Récapitulatif du lemme 2.3.1

Lemme 2.3.1. *Soit $\mathscr{E}_T$, une surface elliptique, et p, un nombre premier qui ne divise pas δ. Soit P le polynôme associé à une place générique de $\mathscr{E}_T$. Soit (x,y) des entiers premiers entre eux tel que $P(x,y)$ soit divisible par p. On pose $t = x/y$ et $n = v_p(P(x,y))$.*

Alors les assertions suivantes sont vérifiées :

1. *Si $\mathscr{E}$ est de type I_m en P, alors $\mathscr{E}_{\frac{x}{y}}$ est de type I_{nm} en p.*
2. *Si $\mathscr{E}$ est de type I_m^* en P, alors $\mathscr{E}_{\frac{x}{y}}$ est de type I_{nm} en p si n est pair, et de type I_{nm}^* si n est impair.*
3. *Si $\mathscr{E}$ est de type II en P, alors $\mathscr{E}_{\frac{x}{y}}$ est de type I_0, II, IV, I_0^*, IV^*, II^* en p si $n \equiv 0,1,2,3,4,5 \mod 6$ respectivement.*
4. *Si $\mathscr{E}$ est de type II^* en P, alors $\mathscr{E}_{\frac{x}{y}}$ est de type I_0, II^*, IV^*, I_0^*, IV, II en p si $n \equiv 0,1,2,3,4,5 \mod 6$ respectivement.*
5. *Si $\mathscr{E}$ est de type III en P, alors $\mathscr{E}_{\frac{x}{y}}$ est de type I_0, III, I_0^*, III^* en p si $n \equiv 0,1,2,3 \mod 4$ respectivement.*
6. *Si $\mathscr{E}$ est de type III^* en P, alors $\mathscr{E}_{\frac{x}{y}}$ est de type I_0, III^*, I_0^*, III en p si $n \equiv 0,1,2,3 \mod 4$ respectivement.*
7. *Si $\mathscr{E}$ est de type IV en P, alors $\mathscr{E}_{\frac{x}{y}}$ est de type I_0, IV, IV^* en p si $n \equiv 0,1,2 \mod 3$ respectivement.*
8. *Si $\mathscr{E}$ est de type IV^* en P, alors $\mathscr{E}_{\frac{x}{y}}$ est de type I_0, IV^*, IV en p si $n \equiv 0,1,2 \mod 3$ respectivement.*

Démonstration. Ceci se déduit directement de l'algorithme de Tate [48] que nous avons présenté dans la section 1.2.4.

□

Type	Forme de $g_{\mathscr{E},\delta,P}(x,y)$	Forme de $h_{\mathscr{E},\delta,P}(x,y)$
I_0	1	1
I_0^*	$(-1\|P(x,y))_\delta$	1
II, II^*	$(-1\|P(x,y))_\delta$	$\prod_{\substack{p\nmid\delta \\ p^2\|P(x,y)}} \begin{cases}(-3/p) & v_p(P(x,y))\equiv 2,4 \mod 6\\ +1 & \text{sinon.}\end{cases}$
III, III^*	$(-2\|P(x,y))_\delta$	$\prod_{\substack{p\nmid\delta \\ p^2\|P(x,y)}} \begin{cases}(-1/p) & v_p(P(x,y))\equiv 2 \mod 4\\ +1 & \text{sinon.}\end{cases}$
IV, IV^*	$(-3\|P(x,y))_\delta$	$\prod_{\substack{p\nmid\delta \\ p^2\|P(x,y)}} \begin{cases}(-3/p) & v_p(P(x,y))\equiv 2,3,4 \mod 6\\ +1 & \text{sinon.}\end{cases}$
I_v^*	$(-1\|P(x,y))_\delta$	$\prod_{\substack{p\nmid\delta \\ p^2\|P(x,y)}} (-\left(\frac{-c_6(x,y)_{(p)}}{p}\right))^{v_p(P(x,y))-1}$
I_v	$\left(\prod_{p\|\delta}(-1)^{v_p(P(x,y))}\right)$ $\cdot(-c_6(x,y)\|P(x,y))$	$\prod_{\substack{p\nmid\delta \\ p^2\|P(x,y)}} (-\left(\frac{-c_6(x,y)_{(p)}}{p}\right))^{v_p(P(x,y))-1}$

TABLE 2.2 – Contribution d'une place au signe selon le type de réduction

2.3.2 Décomposition du signe selon les places génériques

Théorème 2.3.2. *Soit $\mathscr{E}$ une surface elliptique sur $\mathbb{Q}$. Pour $t\in\mathbb{Q}$, on note $t=\frac{x}{y}$ où x,y sont des entiers premiers entre eux.*

Alors, il existe un entier δ et pour chaque P, facteur irréductible primitif de Δ des fonctions $g_{\mathscr{E},\delta,P}$ et $h_{\mathscr{E},\delta,P}$ décrites par le tableau 2.2 telles que le signe s'écrit

$$W(\mathscr{E}_t)=\lambda(M_{\mathscr{E}}(x,y))\cdot\prod_{p|\delta}W_p(\mathscr{E}_t)\cdot\prod_{P|\Delta}g_{\mathscr{E},\delta,P}(x,y)\cdot\prod_{P|\Delta}h_{\mathscr{E},\delta,P}(x,y).$$

Démonstration. Soit $\mathscr{E}$ une surface elliptique d'équation

$$\mathscr{E}: y^2=x^3-27c_4(T)x-54c_6(T),$$

et soit $\Delta(T)$ son discriminant.

Soit $(m,n)\in\mathbb{Z}\times\mathbb{Z}^{\geq 0}$ des entiers premiers entre eux tels que $t=\frac{m}{n}$. Soit k le plus petit entier tel que $12k\geq\deg\Delta(T)$. Une fibre $\mathscr{E}_t$ en t qui est non singulière est isomorphe à la courbe

$$\mathscr{E}_{m,n}: y^2=x^3-27n^{4k}c_4(m/n)x-54n^{6k}c_6(m/n),$$

qui est de discriminant $\Delta_{m,n}=n^{12k}\Delta(m/n)$.

On a donc

$$\begin{aligned} W(\mathscr{E}_t) &= W(\mathscr{E}_{m,n}) \\ &= \prod_{\{p\}\cup\{\infty\}} W_p(\mathscr{E}_{m,n}) \\ &= -\prod_{p|\Delta_{\mathscr{E}_{m,n}}} W_p(\mathscr{E}_{m,n}) \end{aligned}$$

On écrit

$$c_4(m/n) = \frac{d_0}{d_1} \prod_{P_w|c_4} P_w(m/n)^{\mathrm{ord}_w c_4},$$

$$c_6(m/n) = \frac{d_2}{d_3} \prod_{P_w|c_6} P_w(m/n)^{\mathrm{ord}_w(c_6)},$$

$$\Delta(m/n) = \frac{d_4}{d_5} \prod_{P_w|\Delta} P_w(m/n)^{\mathrm{ord}_w(\Delta)},$$

avec $d_0, ..., d_5 \in \mathbb{Z}$ et où w est la place associée au polynôme P_w.

Comme on l'a vu en section 2.3.1, il faut traiter différemment les signes locaux en 2, en 3, en d_i pour $i = 0, \ldots, 5$ et en p qui peuvent diviser P_w et $P_{w'}$ en même temps, en d'autres termes les p qui divisent

$$\prod_{w,w'\in\mathscr{B}'|w\neq w'} Res(P_w, P_{w'}).$$

Pour les autres p, le comportement du type de réduction des fibres est décrit par le lemme 2.3.1.

On pose

$$\delta = 2 \cdot 3 \cdot d_0 \cdot d_1 \cdot d_2 \cdot d_3 \cdot d_4 \cdot d_5 \prod_{w_1,w_2|\Delta} Res(P_{w_1}, P_{w_2}).$$

Le signe s'écrit

$$W(\mathscr{E}_t) = -\prod_{p|\delta} W_p(t) \prod_{P_w|\Delta} W_{\mathscr{E}_{T,\delta,P_w}}(x,y),$$

où

$$W_{\mathscr{E},\delta,P_w}(x,y) = \prod_{p\nmid\delta:p|P_w(x,y)} W_p(\mathscr{E}(x/y)).$$

Pour chaque P_w, on cherchera par la suite à établir la séparation suivante

$$W_{\mathscr{E},\delta,P_w}(x,y) = \begin{cases} g_{\mathscr{E},\delta,P_w}(x,y)h_{\mathscr{E},\delta,P_w}(x,y) & \text{si la réduction de } P_w \text{ n'est pas de type } I_m, \\ \lambda(P_w(x,y))g_{\mathscr{E},\delta,P_w}(x,y)h_{\mathscr{E},\delta,P_w}(x,y) & \text{si la réduction de } P_w \text{ est de type } I_m \end{cases}$$

où $g_{\mathscr{E},\delta,P_w}$ et $h_{\mathscr{E},\delta,P_w}$ sont les fonctions décrites par le tableau 2.2.

Selon la réduction de $\mathscr{E}(x/y)$ en p tel que $p \nmid \delta$ et $p|P_w(x,y)$, on aura une formule pour $W_{\mathscr{E},\delta,P_w}(\mathscr{E}(x,y))$ qui nous permettra de trouver $g_{\mathscr{E},\delta,P_w}$ et $h_{\mathscr{E},\delta,P_w}$.

Cas 1 : Supposons que la réduction est de type I_0 en P_w. Alors, comme on l'a vu dans la section 2.3.1, la réduction est également de type I_0.

Dans ce cas,

$$W_{\mathscr{E},\delta,w}(x,y) = \prod_{p\nmid\delta;p|P_w(x,y)} W_p(\mathscr{E}(x/y)) = 1,$$

pour tout $t = x/y \in \mathbb{Q}$ où $x, y \in \mathbb{Z}$ premier entre eux.

Cas 2 : Supposons que la réduction est de type I_0^* . Alors le type de réduction en p dépendra de la parité de $v_p(P_w(x,y))$.

Nous avons la formule

$$W_{\mathscr{E},\delta,w}(x,y) = \prod_{p\nmid\delta,p|P_w(x,y)} \begin{cases} 1 & v_p(P_w(x,y)) \text{ pair (et non nul) (type } I_o), \\ (-1/p) & v_p(P_w(x,y)) \text{ impair (type } I_o^*)\,; \end{cases}$$

$$= \prod_{p\nmid\delta,p|P_w(x,y)} (-1/p)^{v_p(P_w(x,y))}$$

$$= (-1|P_w(x,y))_\delta,$$

pour tout $x, y \in \mathbb{Z}$ premier entre eux.

Cas 3 : Supposons que la réduction est de type II ou II^*, alors le type de réduction en p dépendra de $v_p(P_w(x,y)) \mod 6$.

Nous avons la formule

$$W_{\mathscr{E},\delta,w}(x,y) = \prod_{p|\delta,p|P_w(x,y)} \begin{cases} (-1/p) & v_p(P_w(x,y)) \equiv 1,5 \mod 6 \text{ (type } II \text{ ou } II^*), \\ (-3/p) & v_p(P_w(x,y)) \equiv 2,4 \mod 6 \text{ (type } IV \text{ ou } IV^*), \\ (-1/p) & v_p(P_w(x,y)) \equiv 3 \mod 6 \text{ (type } I_0^*) \\ 1 & v_p(P_w(x,y)) \equiv 0 \mod 6 \text{ (type } I_0)\,; \end{cases}$$

$$= (-1|P_w(x,y))_\delta \prod_{p\nmid\delta;v_p(P_w(x,y))\equiv 2,4 \mod 6} (-3/p).$$

Cas 4 : Supposons que la réduction est de type III ou III^*, alors le type de réduction en p dépendra de $v_p(P_w(x,y)) \mod 4$.

En terme de formule, on a

$$W_{\mathscr{E},\delta,w}(x,y) = \prod_{p|\delta,p|P_w(x,y)} \begin{cases} (-2/p) & v_p(P_w(x,y)) \equiv 1,3 \mod 4 \text{ (type } III \text{ ou } III^*), \\ (-1/p) & v_p(P_w(x,y)) \equiv 2 \mod 4 \text{ (type } I_0^*), \\ 1 & v_p(P_w(x,y)) \equiv 0 \mod 6 \text{ (type } I_0) \end{cases}$$

$$= (-2|P_w(x,y))_\delta \prod_{p\nmid\delta;v_p(P_w(x,y))\equiv 2 \mod 4} (-1/p).$$

Cas 5 : Supposons que la réduction est de type IV ou IV^*, alors le type de réduction en p dépendra de $v_p(P_w(x,y)) \mod 3$.

En terme de formule, on a

$$W_{\mathscr{E},\delta,w}(x,y) = \prod_{p|\delta,p|P_w(x,y)} \begin{cases} (-3/p) & v_p(P_w(x,y)) \equiv 1,2 \mod 3 \text{ (type } IV \text{ ou } IV^*), \\ 1 & v_p(P_w(x,y)) \equiv 0 \mod 3 \text{ (type } I_0) \end{cases}$$

$$= (-3|P_w(x,y)) \prod_{p|\delta,v_p(P_w(x,y))\equiv 2,3,4 \mod 6} (-1/p)$$

Cas 6 : Supposons que la réduction est de type I_v^*. Alors le type de réduction en p dépendra de la parité de λ.

En terme de formule, on a

$$W_{\mathscr{E},\delta,w}(x,y) = \prod_{p|\delta, p|P_w(x,y)} \begin{cases} -\left(\frac{-c_6(x,y)_{(p)}}{p}\right) & v_p(P_w(x,y)) \text{ pair (type } I_m), \\ (-1/p) & v_p(P_w(x,y)) \text{ impair (type } I_m^*)\,; \end{cases}$$

$$= (-1|P_w(x,y))_\delta \cdot \prod_{p\nmid\delta; p^2|P_w(x,y)} (-\left(\frac{-c_6(x,y)_{(p)}}{p}\right)^{v_p(P_w(x,y))-1}.$$

Cas 7 : Supposons que la réduction est multiplicative, alors par un argument similaire, la réduction en p sera également de type multiplicatif.

En terme de formule, nous avons

$$\begin{aligned} W_{\mathscr{E},\delta,w}(x,y) &= \prod_{p\nmid\delta, p|P_w(x,y)} (-\left(\frac{-c_6(x,y)_{(p)}}{p}\right)) \\ &= \prod_{p\nmid\delta, p|P_w(x,y)} -\left(\frac{-c_6(x,y)_{(p)}}{p}\right)^{v_p(P_w(x,y))} \cdot \prod_{p\nmid\delta, p^2|P_w(x,y)} -\left(\frac{-c_6(x,y)_{(p)}}{p}\right)^{v_p(P_w(x,y))-1} \\ &= \prod_{p\nmid\delta, p|P_w(x,y)} (-1)^{v_p(P_w(x,y))} \cdot (-c_6(x,y)|P_w(x,y))_\delta \\ &\quad \cdot \prod_{p\nmid\delta, p^2|P_w(x,y)} -\left(\frac{-c_6(x,y)_{(p)}}{p}\right)^{v_p(P_w(x,y))-1} \\ &= \lambda(P_w(x,y))\Big(\prod_{p|\delta} (-1)^{v_p(P_w(x,y))}\Big) \cdot (-c_6(x,y)|P_w(x,y))_\delta \\ &\quad \cdot \prod_{p\nmid\delta, p^2|P_w(x,y)} -\left(\frac{-c_6(x,y)_{(p)}}{p}\right)^{v_p(P_w(x,y))-1}, \end{aligned}$$

pour tout $x, y \in \mathbb{Z}$ premier entre eux.

Cela nous donne donc bien la décomposition prédite par le théorème.

□

2.3.3 Propriétés des fonctions apparaissant dans le théorème 2.3.2

Théorème 2.3.3. *(Thm. 6.6 [15]).*

Soit $\mathscr{E}$ une courbe elliptique sur $\mathbb{Q}(T)$. Pour $t \in \mathbb{Q}$, on note $t = \frac{x}{y}$ pour x, y des entiers premiers entre eux.

Alors il existe

1. *S un ensemble fini de places de $\mathbb{Q}$;*
2. *pour chaque $v \in S$, des fonctions $g_v : \mathbb{Q}_v \times \mathbb{Q}_v \longrightarrow \{-1, 1\}$ localement constantes en dehors d'un ensemble fini de droites passant par l'origine ; et*
3. *pour chaque $p \notin S$, des fonctions $h_p : \mathbb{Q}_p \times \mathbb{Q}_p \to \{-1, 1\}$ localement constantes en dehors d'un ensemble fini de droites passant par l'origine telles que $h_p(x, y) = 1$ lorsque $p^2 \nmid B_{\mathscr{E}}(x, y)$;*

tels que le signe s'écrit

$$W(\mathscr{E}_t) = \lambda(M_{\mathscr{E}}(x,y)) \cdot \prod_{v\in S} g_v(x,y) \prod_{p\notin S} h_p(x,y),$$

Remarque 38. Plus précisément, on a

$$W(\mathscr{E}_t) = \lambda(M_{\mathscr{E}}(x,y)) \cdot \prod_{v\in S} g_v(x,y) \prod_{p^2|B_{\mathscr{E}}(x,y);p\notin S} h_p(x,y).$$

Remarque 39. Il faut faire attention à ne pas confondre les fonctions g_v et h_p de ce théorème avec les fonctions $g_{\mathscr{E},\delta,P}$ et $h_{\mathscr{E},\delta,P}$ du théorème 2.3.2. En effet, bien que les premières soient définies à partir des autres, ces fonctions ne sont pas du tout les mêmes comme on le verra dans la démonstration qui suit.

Remarque 40. On écrira dorénavant « fonction presque partout localement constante » plutôt que « fonction presque partout localement constante en dehors d'un ensemble fini de droites passant par l'origine ».

Démonstration. Pour démontrer le théorème, on va décomposer les fonctions $g_{\mathscr{E},\delta,P}$ et $h_{\mathscr{E},\delta,P}$ du tableau 2.2 en produit de fonctions presque partout localement constantes, et les réordonner d'une façon adéquate.

G) Étudions $g_{\mathscr{E},\delta,P}(x,y)$.

1. Si $P \in \mathscr{A}$, alors on a $g_{\mathscr{E},\delta,P}(x,y) = \left(\frac{\varepsilon_P}{P(x,y)}\right)_\delta$ avec

$$\varepsilon_P = \begin{cases} -1 & P \text{ est de type } II,\ II^*,\ I_m^* \text{ ou } I_0^* \\ -2 & P \text{ est de type } III \text{ ou } III^* \\ -3 & P \text{ est de type } IV \text{ ou } IV^*. \end{cases}$$

   Donc, chaque $g_{\mathscr{E},\delta,P}(x,y)$ dépend uniquement du reste de $P(x,y)$ modulo (respectivement) 4, 8 ou 3.

2. Si $P \in \mathscr{M}$, alors on a $g_{\mathscr{E},\delta,P}(x,y) = \left(\frac{-c_6(x,y)}{P(x,y)}\right)_\delta$, qui comme on le verra dans la section 2.3.4 est un produit fini de fonctions localement constantes. Autrement dit, il existe S_P un ensemble fini de nombres premiers tel que $g_{\mathscr{E},\delta,P}(x,y) = \prod_{v\in S_P} g_{P,v}(x,y)$, pour des fonctions $g_{P,v}(x,y)$ presque partout localement constantes.

H) Étudions $h_{\mathscr{E},\delta,P}(x,y)$. Soit p un nombre premier qui ne divise pas δ. Par choix de δ, on a que p ne peut diviser qu'un seul $P \in \mathscr{B}$ à la fois.

Si P est de type I_0 ou I_0^*, on a $h_{\mathscr{E},\delta,P} = +1$ une fonction constante.

On pose pour $P \in \mathscr{A}_2$,

$$h_{P,p}(x,y) = \begin{cases} (-3/p) & v_p(P(x,y) \equiv 2,4 \mod 6 \\ +1 & \text{sinon,} \end{cases}$$

pour $P \in \mathscr{A}_3$,

$$h_{P,p}(x,y) = \begin{cases} (-1/p) & v_p(x,y) \equiv 2 \mod 4 \\ +1 & \text{sinon,} \end{cases}$$

pour $P \in \mathscr{A}_4$,

$$h_{P,p}(x,y) = \begin{cases} (-3/p) & v_p(x,y) \equiv 2,3,4 \mod 6 \\ +1 & \text{sinon,} \end{cases}$$

et pour P de type I_m^* ou I_m,

$$h_{P,p}(x,y) = (-\left(\frac{-c_6(x,y)_{(p)}}{p}\right)^{v_p(P(x,y))-1}.$$

On pose $S = \cup_{P\in\mathscr{M}} S_P$.

Pour tout $v \in S$ une fonction $g_v(x,y)$ qui sera telle que

$$g_v(x,y) = \begin{cases} W_2(x,y)\prod_{P\in\mathscr{A}_2\cup\mathscr{M}'\cup\mathscr{A}_6}(\frac{-1}{P(x,y)})\prod_{P\in\mathscr{A}_3}(\frac{-2}{P(x,y)})\prod_{P\in\mathscr{M}} g_{P,2}(x,y) & \text{si } v=2;\\ W_3(x,y)\prod_{P\in\mathscr{A}_3}(\frac{-3}{P(x,y)})\prod_{P\in\mathscr{M}} g_{P,3}(x,y) & \text{si } v=3\,;\\ W_p(x,y)\prod_{P\in\mathscr{M}} g_{P,v}(x,y) & \text{si } v\mid\delta\,;\\ \prod_{P\in\mathscr{M}} g_{P,v}(x,y)\prod_{P\in\mathscr{B}} h_{P,v} & \text{sinon.}\end{cases}$$

Chacune de ces fonctions sont des produits de fonction presque partout localement constantes.

Pour $p\notin S$, on pose $h_p(x,y) = \prod_{P\in\mathscr{B}} h_{P,p}(x,y)$. Pour chaque (x,y), il y a au plus un seul des $h_{P,p}(x,y)$ qui est différent de $+1$. De plus, ces $h_{P,p}$ sont des fonctions presque partout localement constantes pour la topologie p-adique. De plus, on a bien l'égalité $h_p(x,y) = +1$ lorsque $p^2 \nmid B_{\mathscr{E}}(x,y)$.

□

2.3.4 Constance locale

Cette section sert à justifier que les fonctions $g_{\mathscr{E},\delta,P}$ du tableau 2.2 sont des produits finis de fonctions presque partout localement constantes.

Proposition 2.3.4. *Soit w une place de $\mathbb{Q}(T)$ et P_w son polynôme associé. Soit $f\in\mathbb{Q}(T)$ non nul qui n'est pas divisible par P_w. Soit δ_0 un entier non nul.*

Alors, pour tout $x,y\in\mathbb{Z}$ tels que $pgcd(x,y)|\delta_0$, on peut écrire $(f|P_w)$ comme un produit fini de fonctions à valeurs dans $\{-1,1\}$ presque partout localement constantes.

Démonstration. On écrit f en produit de facteurs irréductibles

$$f = c\cdot\prod_{w'(f)\neq 0} P_{w'}^{w(f)},$$

où $c\in\mathbb{Q}^*$. On écrit $c=\frac{c_0}{c_1}$ pour des entiers c_0,c_1. Posons

$$\delta = c_0\cdot c_1\cdot\delta_0\cdot\prod_{w'(f)\neq 0} Res(P_w,P_{w'}).$$

Par les propriétés du symbole $(\cdot|\cdot)$, on a

$$(f|P_w)_\delta = (c_0|P_w)_\delta\cdot(c_1|P_w)_\delta^{-1}\prod_{w'(f)\text{ impair}}(P'_w|P_w)_\delta.$$

Par hypothèse sur f, on a bien que chaque P'_w est différent de P_w.

On utilise le lemme 2.3.5 (qui suivra) pour démontrer que $(c_0|P_w)$ et $(c_1|P_w)$ sont des produits finis de fonctions presque partout localement constantes. Par ce même lemme, on sait que chaque facteur $(P_{w'}|P_w)_\delta$ est de la forme

$$(P_{w'}|P_w)_\delta = \begin{cases} h_{w'}(x,y)(x|y)_{\delta_0} & \text{si } deg(w') \text{ et } deg(w) \text{ sont tous deux impairs;}\\ h_{w'}(x,y) & \text{sinon,}\end{cases}$$

où $h_{w'}$ est un produit de fonctions presque partout localement constantes à valeurs dans $\{-1,1\}$.

Pour démontrer que $(f|P_w)$ est un produit fini de fonctions presque partout localement constantes, nous devons démontrer qu'il y a un nombre pair de w' places de $\mathbb{Q}(T)$ telles que $deg(w')$ est impair. Cela est vrai par la formule du produit qui dit que

$$\sum_{w' \in \mathscr{B}_{\mathscr{E}}} w'(f) deg(w') = 0.$$

Il reste à montrer que $\frac{(f|P_w)_{\delta_0}}{(f|P_w)_{\delta}}$ est un produit fini de fonctions presque partout localement constantes. Pour cela on remarque que

$$\frac{(f|P_w)_{\delta_0}}{(f|P_w)_{\delta}} = \prod_{p \text{ premier}, p\nmid 2\delta_0, p|2\delta} \Big(\frac{f(x,y)}{p}\Big)^{v_p(P_w(x,y))},$$

qui est bien un produit fini de fonctions à valeurs dans $\{-1,1\}$, presque partout localement constantes pour une topologie p-adique.

□

Lemme 2.3.5. *Soit $f, g \in \mathbb{Q}[x,y]$ des polynômes homogènes premiers entre eux. Soit δ un entier divisible par $Res(f,g)$, le résultant de f et g, et δ_0 qui divise δ. Alors il existe une fonction $h : \mathbb{Z} \times \mathbb{Z} \to \{-1,1\}$ produit fini de fonctions presque partout localement constantes telle que*

$$(f(x,y)|g(x,y))_{\delta_0} = h(x,y)(x|y)_{\delta_0}^{(\deg f)(\deg g)},$$

pour tout $x, y \in \mathbb{Z}$ dont le pgcd divise δ et x/y en dehors d'un sous ensemble fini de $\mathbb{P}^1(\mathbb{Q})$.

Démonstration. On peut supposer que x, y, $f(x,y)$ et $g(x,y)$ sont non nuls, car ces cas n'arrivent que pour une quantité finie de valeurs de $\frac{x}{y}$.

Étape 0. Si c est un entier non nul, $(f|c)$ est bien un produit fini de fonctions presque partout localement constantes par la propriété d. De même pour $(c|g)$, si on utilise la propriété f pour se ramener au cas précédent.

Étape 1. On suppose que $g = cx$ pour c entier non nul et que f est irréductible. Alors

$$\begin{aligned}
(f(x,y)|g(x,y))_{\delta} &= (a_0x^k + a_1x^{k-1}y + ... + a_ky^k|cx)_{\delta} \\
&= (f|c)_{\delta} \cdot (a_ky^k|x)_{\delta}, && \text{par (b) et (c)} \\
&= (f|c)_{\delta} \cdot (a_k|x)_{\delta} \cdot (y|x)_{\delta_0}^k, && \text{par (a)} \\
&= (f|c)_{\delta} \cdot (a_k|x)_{\delta} \cdot \prod_{p|\delta, p=\infty} \Big(\frac{y,x}{p}\Big) \prod_{p|(\frac{\delta}{\delta_0})} (f/p)^{v_p(g)} (x|y)_{\delta_0}^k. && \text{par (e) et (f)}
\end{aligned}$$

Étape 2. On suppose f et g irréductible, sinon on utilise les propriétés multiplicatives du symbole, a et b, pour se ramener à un produit de termes dont chacun serait un produit fini de fonctions presque partout localement constante. On suppose également que $f, g \neq cx$ pour un c entier et que $\deg(f) \geq \deg(g)$, sinon on se ramène à l'étape 1 ou on utilise la propriété f.

On écrit $f = a_0x^k + ... + a_ky^k$ et $g = b_0x^l + b_1x^{l-1}y + ... + b_{l-1}xy^{l+1} + b_ly^l$. Alors,

$$
\begin{aligned}
&(f(x,y)|g(x,y))_\delta \\
&= \prod_{p|b_0} (f(x,y)/p)^{v_p(g(x,y))} (f(x,y)|g(x,y))_{b_0\delta}, && \text{par (e)} \\
&= \prod_{p|b_0} (f(x,y)/p)^{v_p(g(x,y))} (b_0|g(x,y))_{b_0\delta} (b_0 f(x,y)|g(x,y))_{b_0\delta}, && \text{par (a)} \\
&= \prod_{p|b_0} (f(x,y)/p)^{v_p(g(x,y))} (b_0|g(x,y))_{b_0\delta} (b_0 f(x,y) - a_0 g(x,y) x^{k-l}|g(x,y))_{b_0\delta}, && \text{par (c)}
\end{aligned}
$$

pour tout $(x,y) \in \mathbb{Z}^2$ tel que $pgcd(x,y) \mid \delta$ et $b_0 f(x,y) - a_0 g(x,y) x^{k-l} \neq 0$.

Remarquons que, par construction, le coefficient de x^k dans $b_0 f(x,y) - a_0 g(x,y) x^{k-l}$ est nul. Par conséquent, $b_0 f(x,y) - a_0 g(x,y) x^{k-l}$ est un multiple de y. La combinaison linéaire $b_0 f(x,y) - a_0 g(x,y) x^{k-l}$ ne peut pas être le polynôme constant nul car les polynômes f et g sont premiers entre eux par hypothèse. Il s'agit soit d'un polynôme réductible, soit du produit de y par une constante non nulle.

Dans le premier cas, on utilise les propriétés de multiplicativité pour pouvoir utiliser à nouveau l'étape 2 sur les nouveaux termes obtenus. Dans le second, une application de la propriété (f) nous fait revenir au cas où f est irréductible et $g = cy$, qui est traité par l'étape 1.

Comme le degré de f et de g est fini, on utilise un nombre fini de ces étapes pour obtenir un produit fini de fonctions presque partout localement constantes.

□

2.4 Signe moyen sur une progression arithmétique

2.4.1 Surfaces isotriviales avec $j(T) \neq 0, 1728$

Proposition 2.4.1. *([15, Prop. 7.1.])*
Soit A une progression arithmétique que l'on écrit

$$A = a + m\mathbb{Z},$$

pour $a, m \in \mathbb{Z}$.

Soit S un ensemble fini de places de $\mathbb{Q}$ et pour tout $v \in S$, $g_v : \mathbb{Q}_v \to \mathbb{C}$ des fonctions bornées presque partout localement constantes. Alors la moyenne sur A du produit des g_v s'écrit

$$av_A \prod_{v \in S} g_v(n) = c_\infty \cdot \prod_{p \in S \setminus \{\infty\}} \int_{A_p} g_p(x)dx,$$

où

$$A_p = a + m\mathbb{Z}_p$$

et où, si $\infty \notin S$, alors $c_\infty = 1$, ou si $\infty \in S$, alors c_∞ est la valeur que prend $g_\infty(x)$ pour tout x positif assez grand.

Remarque 41. Soit $\mathscr{E}$ une surface elliptique isotriviale qui est une famille de twists quadratiques. La proposition précédente implique que la moyenne du signe des fibres sur une progression arithmétique A s'écrit

$$av_A \prod_{v \in S} g_v(n) = -\prod_{p \in S} \int_{A_p} g_p(x)dx,$$

où S et g_p sont l'ensemble et les fonctions donnés par le théorème 2.3.3.

Quand $A = \mathbb{Z}$, on aura comme conclusion

$$av_{\mathbb{Z}} \prod_{v \in S} g_v(n) = - \prod_{p \in S} \int_{\mathbb{Z}_p} g_p(x) dx,$$

Démonstration. Par le changement de variable $x = a + mx'$, on peut se ramener au cas $A = \mathbb{Z}$.

Soit $p \in S$ et posons $S_p \subseteq \mathbb{Z}_p$ l'ensemble fini des points où g_p n'est pas localement constante.

On couvre S_p de boules ouvertes arbitrairement petites : pour un $a \in \mathbb{Z}$, point singulier de g_p, on définit $U_p = a + p^k \mathbb{Z}_p$ pour un certain $k \geq 0$. On les prend telles que X_p, leur union, est de mesure inférieure à $\frac{\epsilon}{|S|}$ pour un $\epsilon < 0$ choisi.

On pose $R_p = \mathbb{Z}_p \backslash X_p$.

Pour démontrer l'égalité de la proposition, nous allons nous intéresser à la somme

$$\sum_{\substack{n \in \mathbb{Z} \\ |n| \leq B}} \prod_{p \in S} g_p(E_n).$$

Les deux premiers termes que nous considérerons correspondront à ce qui se passe autour des points où les fonctions g_p ne sont pas localement constantes. On montrera que ces termes sont de moyenne négligeable. Le dernier terme étudiera le comportement de la somme sur les autres points et ce sera lui qui aura la forme du produit d'intégrale dont il est question dans le théorème.

1) Comparons les valeurs de

$$T = \prod_{p \in S} \int_{\mathbb{Z}_p} g_p(x) dx \qquad \text{et de} \qquad P = - \prod_{p \in S} \int_{R_p} g_p(x) dx.$$

Puisque g_p est une fonction bornée, on a

$$|T - P| \leq |S| \frac{\epsilon}{|S|} \max_x \prod_{p \in S} g_p(x) = O(\epsilon). \tag{2.2}$$

Ceci démontre qu'il est équivalent d'étudier $\lim_{\epsilon \to 0} P$ pour obtenir la valeur de T.

2) Pour étudier la moyenne sur l'intersection des R_p, on procède par deux étapes.

a) On étudie la moyenne sur U_p, une des boules qui composent X_p. On a dit précédemment que $U_p = a + p^k \mathbb{Z}_p$ pour $a \in \mathbb{Z}$ et $k \geq 0$. Sur cette boule,

$$\Big| \sum_{\substack{|n| \leq B \\ n \in U_p}} \prod_{v \in S} g_v(n) \Big| = \Big| \sum_{\substack{|n| \leq B \\ n \equiv a \mod p^k}} \prod_{v \in S} g_v(n) \Big| \leq C \Big| \sum_{\substack{|n| \leq B \\ n \equiv a \mod p^k}} 1 \Big|$$

On a de plus

$$\sum_{\substack{|n| B \\ n \in U_p}} 1 \leq \frac{N}{p^k} + 1 = N \cdot \nu_p(U_p) + 1, \tag{2.3}$$

où ν_p est la mesure sur $\mathbb{Z}_p$.

b) Soit ι_p l'inclusion de $\mathbb{Z}$ dans $\mathbb{Z}_p$. Soit de plus l'ensemble $Z = \{n \in \mathbb{Z} : \forall p \in S \ \iota_p(n) \in R_p\}$. Remarquons que $n \notin Z$ si et seulement si il existe $p \in S$ tel que $\iota_p(n) \in X_p$.

Parce que X_p est l'union des ouverts U_p et par l'inégalité (2.3), on a pour une certaine constante C

$$\Big| \sum_{\substack{n\in[-B,B]\\ n\notin Z}} \prod_{p\in S} g_p(n)\Big| \ll \sum_{\substack{n\in[-B,B]\\ n\notin Z}} 1 \tag{2.4}$$

$$\leq (\sum_{p\in S} B\cdot \mu_p(X_p) + O(1)) \leq (\epsilon\cdot B + o(B)).$$

3) On étudie la moyenne du signe sur Z est égale à

$$av_Z \prod_{v\in S} g_v(n)\Bigg(= \lim_{B\to\infty} \frac{\sum_{|n|\leq B:\iota(n)\in Z}\prod_{v\in S} g_v(n)}{\sum_{|n|\leq B:\iota(n)\in Z}\rho(n)}\Bigg) = c_\infty \prod_{p\in S\setminus\{\infty\}} \int_{U_{p,j_p}} g_p(x)dx.$$

Pour tout $p \in S$, on fixe une partition de $R_p = \cup_j U_{p,j}$. On choisit $\vec{j} = \{j_p\}_{p\in S}$ pour que $\{U_{p,j_p}\}_{p\in S}$ soit une famille de représentants des partitions de R_p. De plus, on note $Z_{\vec{j}} = \{n \in \mathbb{Z} : \forall p \in S \ \iota_p(n) \in U_{p,j_p}\}$.

a) Remarquons que

$$\lim_{B\to\infty}\left(\frac{1}{B}\sum_{\substack{|n|\leq B\\ n\in Z_{\vec{j}}}}\prod_{v\in S} g_v(n)\right) = c_\infty\cdot\prod_{p\in S}\int_{U_{p,jp}} g_p(x)dx, \tag{2.5}$$

car g_p est constant sur U_{p,j_p}.

On a

$$\lim_{B\to\infty}\frac{1}{B}\sum_{|n|\leq B}\prod_{p\in S} g_p(n) = \lim_{B\to\infty}\frac{1}{B}\sum_{\substack{\tilde{j} \text{ possibles}\\ \text{représentants}}}\sum_{\substack{|n|\leq B\\ n\in Z_{\vec{j}}}}\prod_{p\in S} g_v(n). \tag{2.6}$$

Par la remarque 2.5 et parce que la somme sur les représentants $\vec{j}$ est finie, on obtient

$$\lim_{B\to\infty}\frac{1}{B}\sum_{\substack{\tilde{j} \text{ possibles}\\ \text{représentants}}}\sum_{\substack{|n|\leq B\\ n\in Z_{\vec{j}}}}\prod_{p\in S} g_v(n) = c_\infty\cdot\sum_{\vec{j}}\prod_{p\in S'}\int_{U_{p,jp}} g_p(x)dx. \tag{2.7}$$

Fixons $\vec{i} = \{i_p\}_{p\in S'}$ l'un de ces représentants. On a, en se rappelant que les termes étudiés précédemment sont négligeables et que $\prod_{p\in S'} g_v(n)$ est constant sur l'intersection des U_{p,j_p}, que

$$\sum_{\vec{j}}\prod_{p\in S'}\int_{U_{p,jp}} g_p(x)dx = c_\infty\cdot\prod_{p\in S}\int_{R_p} g_p(x)dx \tag{2.8}$$

$$= \Big(\prod_{p\in S'}\mu_p(U_{p,i_p})\Big)\cdot c_\infty\cdot\prod_{p\in S'}\int_{R_p} g_p(x)dx. \tag{2.9}$$

b) Il reste à démontrer que

$$\lim_{B\to\infty}\frac{1}{2B}\sum_{\substack{|n|\leq B\\ n\in Z_{\vec{j}}}} 1, = \prod_{p\in S}\mu_p(U_{p,j_p}), \tag{2.10}$$

où μ_p est la mesure usuelle sur $\mathbb{Z}_p$.

On écrit $U_{p,j_p} = a_p + p^{e_p}\mathbb{Z}_p$ pour des $a_p \in \mathbb{Z}$ et $e_p \geq 0$ appropriés. On a alors que $\mu_p(U_{p,jp}) = p^{-e_p}$ et donc

$$\prod_{p\in S} \mu_p(U_{p,j_p}) = \prod_{p\in S} p^{-e_p}.$$

Par le théorème chinois, les entiers n tels que $\iota_p(n) \in U_{p,j_p}$ pour tout $p \in S$ forment une progression arithmétique de module $m = \prod_{p\in S} p^{e_p}$. De ce fait, on a (2.10)$= N/m$ et donc

$$\lim_{B\to\infty} \frac{1}{B} \sum_{\substack{|n|\leq B \\ n\in Z_{\vec{j}}}} 1 = \lim_{B\to\infty} \frac{1}{B}\cdot\frac{B}{m} = \frac{1}{m} = \prod_{p\in S} p^{-e_p}. \tag{2.11}$$

Pour conclure, on rassemble tout ce que nous avons fait jusqu'à présent.

$$\begin{aligned}
av_{\mathbb{Z}} \prod_{v\in S} g_v(n) &= \lim_{\epsilon\to 0}\left(av_Z \prod_{v\in S} g_v(n)\right) && \text{(par 2.4)}\\
&= \lim_{\epsilon\to 0}\left(\lim_{B\to\infty} \frac{\frac{1}{2B}\sum_{n\in[-B,B]\cap Z_{\vec{j}}} \prod_{v\in S} g_v(n)}{\frac{1}{2B}\sum_{n\in[-B,B]\cap Z_{\vec{j}}} 1}\right)\\
&= \lim_{\epsilon\to 0}\left(\lim_{B\to\infty} \sum_{\substack{\vec{j} \text{ possibles} \\ \text{représentants}}} \frac{\frac{1}{B}\sum_{|n|\leq B} \prod\limits_{\substack{v\in S \\ n\in U_{p,j_p}}} g_v(n)}{\frac{1}{B}\sum\limits_{\substack{|n|\leq B \\ n\in U_{p,jp}}} 1}\right) && \text{(par 2.6)}\\
&= \lim_{\epsilon\to 0}\left(\sum_{\vec{j}} \frac{c_\infty \cdot \prod_{p\in S\setminus\{\infty\}} \int_{U_{p,j_p}} g_p(x)dx}{\prod_{p\in S}\mu(U_{p,j_p})}\right) && \text{(par 2.10) et (2.11)}\\
&= c_\infty \cdot \lim_{\epsilon\to 0}\left(\frac{\prod_{p\in S}\mu(U_{p,i_p}) \cdot \prod_{p\in S}\int_{R_p} g_p(x)dx}{\prod_{p\in S}\mu(U_{p,i_p})}\right) && \text{(par 2.7)}\\
&= c_\infty \cdot \lim_{\epsilon\to 0}\left(\prod_{p\in S}\int_{R_p} g_p(x)dx\right)\\
&= c_\infty \cdot \prod_{p\in S}\int_{\mathbb{Z}_p} g_p(x)dx && \text{(par 2.2)}
\end{aligned}$$

□

2.4.2 Surfaces avec $j(T) \in \{0, 1728\}$ ou non isotriviale sans place I_m

Proposition 2.4.2. *([15, Prop. 7.7.])*

Soit A une progression arithmétique que l'on écrit

$$A = a + m\mathbb{Z},$$

pour $a, m \in \mathbb{Z}$.

Soit $B(T) \in \mathbb{Z}[T]$ un polynôme non nul qui vérifie la conjecture du crible des facteurs carrés. Soit S un ensemble fini de places de $\mathbb{Q}$. Pour tout $v \in S$ soit une fonction g_v bornée presque partout localement constantes. Pour tout $p \notin S$ soit h_p une fonction

(a) presque partout localement constante

(b) telle que $|h_p(n)| \leq 1$ *pour tout* $n \in A$

(c) telle que $h_p(n) = +1$ *si* $v_p(B(n))$ *est pair.*

Soit la fonction $W(n) = \prod_{v \in S} g_v(n) \cdot \prod_{p \notin S} h_p(n)$.

Alors

$$av_A W(n) = c_\infty \prod_{p \in S \setminus \{\infty\}} \int_{A_p} g_p(x)dx \cdot \prod_{p \notin S} \int_{A_p} h_p(x)dx.$$

où

$$A_p = a + m\mathbb{Z}_p$$

et où, si $\infty \notin S$, *alors* $c_\infty = 1$, *ou si* $\infty \in S$, *alors* c_∞ *est la valeur que prend* $g_\infty(x)$ *pour tout* x *positif assez grand.*

Remarque 42. Soit une surface elliptique $\mathscr{E}$ qui est une surface elliptique isotriviale dont $j = 0$ ou 1728 ou une surface non isotriviale sans place de type I_m. Alors la proposition 2.4.2 dit, conditionnellement à la conjecture du crible des facteurs carrés sur $B(n)$ que la moyenne du signe sur A est

$$av_A W(n) = -\prod_{p \in S} \int_{\mathbb{A}_p} g_p(x)dx \cdot \prod_{p \notin S} \int_{A_p} h_p(x)dx.$$

où S, g_p et h_p sont les fonctions données par le théorème 2.3.3.

Démonstration. Comme précédemment, on peut se ramener au cas $A = \mathbb{Z}$ par le changement de variable $x = a + mx'$.

Cela repose d'abord sur la formule quand le produit est fini. Posons

$$W_M(n) = \prod_{v \in S} g_v(n) \cdot \prod_{p \notin S} h_p(n).$$

La technique de la proposition 2.4.1 permet de démontrer

$$av_{\mathbb{Z}} W_N(n) = c_\infty \prod_{p \in S} \int_{\mathbb{Z}_p} g_p(x)dx \cdot \prod_{p \notin S, p < M} \int_{\mathbb{Z}_p} h_p(x)dx.$$

Nous démontrerons que chacun des côtés de cette équation tend vers le côté correspondant de la formule à démontrer lorsque $M \to \infty$.

1) On veut démontrer

$$av_{\mathbb{Z}} W(n) = \lim_{M \to \infty} av_{\mathbb{Z}} W_N(n).$$

Pour cela, on combine la conjecture du crible des facteurs carrés

$$\#\{n \leq N \mid p^2 | B(n) \text{ pour } n > \sqrt{N}\} = o(N),$$

et le théorème 1.3.3

$$\#\{n \leq N \mid p^2 | B(n) \text{ pour } p \text{ entre } M \text{ et } \sqrt{N}\} = \frac{N}{M} + o(N),$$

pour obtenir

$$\#\{n \leq N \mid p^2 | B(n) \text{ pour } p > M\} = O(\frac{N}{M}) + o(N).$$

De là et par le fait que $h_p(n) = 1$ pour tout p tel que $p^2 \nmid B(n)$, on obtient que

$$\Big| \sum_{n \leq N} \prod_{v \in S} g_v(n) \cdot \prod_{p \notin S} h_v(n) - \sum_{n \leq N} \prod_{v \in S} g_v(n) \cdot \prod_{p \notin S, p < M} h_v(n) \Big| = O(\frac{N}{M}) + o(N),$$

d'où le résultat. En effet, lorsqu'on fait tendre N vers ∞, on obtient

$$\left| av_{\mathbb{Z}} W(n) - av_Z \left(\prod_{p \in S} g_v(n) \prod_{p \notin S : p < M} h_v(n) \right) \right| = O(\frac{1}{M}),$$

et l'expression $O(\frac{1}{M})$ tend vers 0 quand $M \to \infty$.

2) On veut montrer l'égalité des parties de droite des équations. Pour cela il faut prouver que

$$\prod_{p \notin S} \int_{\mathbb{Z}_p} h_v(n) = \lim_{M \to \infty} \prod_{p \notin S} \int_{\mathbb{Z}_p} h_v(n),$$

et pour ce faire il est suffisant de montrer

$$\lim_{M \to \infty} \prod_{p \notin S, p \geq M} \int_{\mathbb{Z}_p} h_v(n) = 1.$$

Rappelons (voir remarque 29) que le nombre de solutions $t \mod p^2$ à l'équation $B(t) \equiv 0 \mod p^2$ est $O(1)$, c'est-à-dire qu'il est borné. De plus, on a $|h_p(x)| \leq 1$ pour tout $x \in \mathbb{Z}_p$ et $h_p(x) = 1$ quand $v_p(B(x, y)) > 2$. Ces deux faits impliquent qu'on a

$$\int_{\mathbb{Z}_p} h_p(n) = 1 - O(\frac{1}{p^2}).$$

Donc

$$\prod_{p \notin S, p \geq M} \int_{\mathbb{Z}_p} h_p(n) = \prod_{p \geq M} 1 - O(\frac{1}{p^2}) = 1 - O(\sum_{m \geq M} \frac{1}{m^2}) = 1 - O(\frac{1}{M}),$$

ce qui tend vers 1 lorsque $M \to \infty$. □

2.4.3 Surfaces qui admettent des places de réduction I_m

Proposition 2.4.3. *[15, Prop. 7.11.]*

Soit A une progression arithmétique. Soit $P(T) \in \mathbb{Z}[T]$ un polynôme non nul. Soit S un ensemble fini de places de $\mathbb{Q}$.

Pour tout $v \in S$ soit une fonction g_v bornée presque partout localement constantes. Pour tout $p \notin S$ soit h_p une fonction qui est

(a) presque partout localement constante

(b) telle que $|h_p(n)| \leq 1$ pour tout $n \in A$

(c) telle que $h_p(n) = +1$ si $v_p(P(n))$ est pair.

Soit α une fonction $\mathbb{Z} \to \mathbb{C}$ telle que $|\alpha(x)| \leq 1$ pour tout n et telle que

$$av_A \alpha(n) = 0 \tag{2.12}$$

pour toute progression arithmétique A.

Soit la fonction $W(n) = \alpha(n) \prod_{v \in S} g_v(n) \cdot \prod_{p \notin S} h_p(n)$. Alors

$$av_A W(n) = 0. \tag{2.13}$$

On peut déduire le théorème suivant sur la variation du signe de surfaces elliptiques.

Corollaire 2.4.4. *Soit $\mathscr{E}$ une surface elliptique possédant une place sur $\mathbb{Q}(T)$ dont la réduction est de type I_m. En supposant que $M_{\mathscr{E}}$ vérifie la conjecture de Chowla et que $B_{\mathscr{E}}$ vérifie la conjecture du crible des facteurs carrés, alors par le théorème 2.4.3*

$$av_{a+m\mathbb{Z}}W(n) = 0, \tag{2.14}$$

pour toute progression arithmétique $a + m\mathbb{Z}$.

En particulier, les ensembles W_+ et W_- sont tous deux de cardinalité infinie.

Remarque 43. On utilise, dans le cas du signe d'une surface elliptique, la fonction $\alpha(n) = \lambda(M_{\mathscr{E}}(n))$.

Démonstration. On pose pour tout $N \in \mathbb{N}$ la fonction

$$W_N(n) = \lambda(M(n)) \cdot \prod_{v\in S} g_p(x) \cdot \prod_{p\notin S, p<N} h_p(x).$$

Pour simplifier la notation, on réindexe le produit fini comme suit : on pose $S' = S \cup \{p \notin S | p < N\}$ et $g_p = h_p$ pour $p \in S'\backslash S$. On veut alors démontrer pour tout $M \in \mathbb{N}$

$$av_{a+m\mathbb{Z}} \prod_{v\in S'} g_v(n) \cdot \alpha(n) = 0.$$

La démonstration est similaire à celle de la proposition 2.4.1.

De la même façon que pour cette proposition, on a

$$\left| av_{a+m\mathbb{Z}}W(n) - av_{(a+m\mathbb{Z})\cap Z}\left(\alpha(n) \cdot \prod_{v\in S'} g_v(n)\right)\right| = O\left(\frac{1}{M}\right).$$

Pour finir, il est suffisant de démontrer que

$$\lim_{N'\to\infty}\left(\frac{1}{N/m} \sum_{n\in(a+m\mathbb{Z})\cap Z:|n|\leq N'} \alpha(n) \prod_{v\in S'} g_v(n)\right) = 0$$

pour tout choix de $\vec{j} = \{j_p\}_{p\in S'}$, et pour cela, comme $g_p(x)$ est constant sur U_{p,j_p}, on doit simplement montrer que

$$\lim_{N\to\infty}\left(\frac{1}{N/m}\sum \alpha(n)\right) = 0,$$

pour tout choix de $\vec{j}$. Cela est vrai par l'hypothèse 2.12 puisqu'étant donné que $Z_{\vec{j}}$ est une progression arithmétique, alors $(a + m\mathbb{Z}) \cap Z_{\vec{j}}$ est soit une progression arithmétique, soit vide.

On fait ensuite tendre M vers l'infini de chaque côté de l'équation. À droite, cela tend bien entendu vers 0. Reste à montrer que

$$\lim_{M\to\infty} av_{a+m\mathbb{Z}}\Big(\alpha(n) \prod_{v\in S_M} g_v(n)\Big) = av_{a+m\mathbb{Z}}\Big(\alpha(n)\prod_p g_v\Big),$$

où $S_M = S \cup \{p \notin S : p < M\}$ et $g_p = h_p$ pour $p \in S_M\backslash S$. Cela se fait avec le même argument que celui de la proposition 2.4.2.

□

2.5 Signe moyen sur $\mathbb{Q}$

2.5.1 Surface isotriviale telle que $j(T) \neq 0, 1728$

Proposition 2.5.1. *[15, Prop 7.2.] On note $\mathscr{Z}_p = (\mathbb{Z}_p \times \mathbb{Z}_p)\backslash(p\mathbb{Z}_p \times p\mathbb{Z}_p)$.*

Soit S un ensemble fini de places de $\mathbb{Q}$. Pour tout $v \in S$, soit $g_v : \mathbb{Q}_v \times \mathbb{Q}_v \to \mathbb{C}$ une fonction bornée qui est localement constante en dehors d'un ensemble fini de droites passant par l'origine. Alors

$$av_{\mathscr{Z}_p} \prod_{v\in S} g_v(x,y) = c_\infty \prod_{p\in S\backslash\{\infty\}} \frac{1}{1-p^{-2}} \int_{\mathscr{Z}_p} g_p(x,y)dxdy,$$

où $c_\infty = 1$ si $\infty \notin S$ ou

$$c_\infty = \lim_{B\to\infty} \frac{1}{(2B)^2} \int_{-B}^{B}\int_{-B}^{B} g_\infty(x,y)dxdy$$

si $\infty \in S$.

Remarque 44. Soit $\mathscr{E}$ une surface elliptique isotriviale dont le j-invariant est différent de 0 et 1728. Le théorème 2.3.3 donne une formule du signe de fibres de $\mathscr{E}$ qui correspond aux hypothèses de la proposition. On a dans ce cas $g_\infty = -1$ et par conséquent, le terme c_∞ est tout simplement -1.

Quant aux autres $p \in S$, on a $g_2(m,n) = W(\mathscr{E}_{\frac{m}{n}})$ si $p = 2$ et $g_p(m,n) = W_p(\mathscr{E}_{\frac{m}{n}})$ sinon.

Alors le signe moyen sur $t = \frac{m}{n} \in \mathbb{Q}$ s'écrit

$$\mathrm{av}_{\mathbb{Q}} \prod_{v\in S} g_v(x,y) = -\prod_{p\in S} \frac{1}{1-p^{-2}} \int_{\mathscr{Z}_p} g_p(x,y)dxdy,$$

où $\mathscr{Z}_p = (\mathbb{Z}_p \times \mathbb{Z}_p)\backslash(p\mathbb{Z}_p \times p\mathbb{Z}_p)$.

Remarque 45. En faisant cette moyenne, notre objectif est d'étudier les variations du signe des fibres $\mathscr{E}_t$ d'une courbe elliptique quand t varie sur $\mathbb{Q}$. Aussi, nous excluons les (m,n) qui sont premiers entre eux, car ceux-ci représentent un même $t = \frac{m}{n}$. En terme de valuation p-adique, cela correspond aux $(m,n) \in \mathbb{Z}^2$ pour lesquels il existe un p premier tel que le plongement de (m,n) dans $\mathbb{Z}_p \times \mathbb{Z}_p$ est dans $p\mathbb{Z}_p \times p\mathbb{Z}_p$. Voilà pourquoi dans l'intégrale de la proposition, on se limite à $\mathscr{Z}_p = (\mathbb{Z}_p \times \mathbb{Z}_p)\backslash(p\mathbb{Z}_p \times p\mathbb{Z}_p)$.

Remarque 46. Le terme $1 - p^{-2}$ est simplement la mesure de $\mathscr{Z}_p$.

Démonstration. La démonstration se construit sur le modèle de la précédente avec quelques variations.

Cette fois, nous posons S_p comme étant l'ensemble des droites passant par l'origine sur lesquelles g_p est localement constante. On prendra comme voisinage de ces droites des *sections* : pour une droite d'équation $y = ax$, on définit l'ouvert

$$U_p = \{(x,y) \in \mathscr{Z}_p : |y/x - a|_p < \epsilon\},$$

et on note X_p leur union. On pose $R_p = \mathscr{Z}_p - X_p$.

De la même façon que dans la version en une variable,

1. on compare les valeurs de

$$T = \prod_{p\in S} \int_{\mathscr{O}_p} g_p(x,y)dxdy$$

et

$$P = \prod_{p\in S} \int_{R_p} g_p(x,y)dxdy,$$

afin de déduire qu'il est équivalent d'étudier $\lim_{\epsilon\to\epsilon} P$ pour obtenir la valeur de T car leur différence est négligeable ;

2. On démontre que le signe moyen sur les $(m,n) \in U_p$ est négligeable (car $\sum_{(m,n)\in U_p} \prod_{p\in S} g_v(m,n)$ se comporte assymptotiquement comme $\sum_{(m,n)\in U_p} 1$) ;
3. on utilise le point 2 pour étudier le signe moyen sur les (m,n) pour lesquels il existe p tel que le plongement p-adique de (m,n) n'est pas dans R_p. D'une façon très similaire, on démontre qu'il est négligeable.

La suite diffère légèrement. Pour alléger la notation, nous écrirons $\iota_p(m,n)$ à la place de $(\iota_p(m), \iota_p(n))$. De plus, on définit l'ensemble $Z = \{(m,n) \in \mathscr{Z} | \forall p \in S \ \iota_p(m,n) \in R_p\}$.

On s'intéresse à

$$\sum_{\substack{|m|,|n|\leq B \\ \forall p\in S: \iota_p(m,n)\in R_p}} \prod_{p\in S} g_p(m,n). \tag{2.15}$$

On fixe une partition de $R_p = \cup_j U_{p,j}$, que l'on peut supposer finie car R_p est compact, étant un fermé de $\mathbb{Z}_p \times \mathbb{Z}_p$ (car on lui enlève un nombre fini d'ouverts).

Comme précédement, on obtient

$$\lim_{B\to\infty} \frac{1}{(2B)^2} \sum_{\substack{|m|,|n|\leq B \\ (m,n)\in Z}} \prod_{v\in S} g_v(m,n) = \Big(\prod_{p\in S} \mu_p(U_{p,i_p})\Big) \cdot \prod_{p\in S} \int_{R_p} g_p(x,y)dxdy. \tag{2.16}$$

Pour compléter la démonstration, on veut démontrer que

$$\lim_{B\to\infty} \frac{1}{(2B)^2} \sum_{\substack{|n|\leq B \\ (m,n)\in Z}} 1 = \prod_{p\in S} \mu_p(U_{p,i_p}), \tag{2.17}$$

pour tout choix de représentant $\vec{i}$.

On écrit $U_{p,j_p} = (a_p, b_p) + p^{e_p}\mathbb{Z}_p \times p^{f_p}\mathbb{Z}_p$ pour des $a_p, b_p \in \mathbb{Z}$ et $e_p, f_p \geq 0$ appropriés. Ce sont des translatés de réseaux. On pose $\eta_p = e_p + f_p$. L'indice de U_{p,j_p} est $[\mathbb{Z}^2 : p^{e_p}\mathbb{Z} \times p^{f_p}\mathbb{Z}] = p_1^{\eta_p}$.

Par le lemme 2.2.2, $Z := \cap_{1\leq j\leq k} U_{p,j_p}$ est le translaté de réseau $a + L$ d'indice $[\mathbb{Z}^2 : L] = \prod_{j\leq k} p_j^{\eta_j}$. Pour conclure, on utilise le lemme 2.2.3 pour démontrer que

$$\lim_{B\to\infty} \sum_{n\in Z\cap[-B,B]} 1 = \prod_{j\leq k} p_j^{\eta_j}.$$

□

2.5.2 Surface isotriviale avec $j(T) \in \{0, 1728\}$ ou sans place I_m

Proposition 2.5.2. *[15, Prop. 7.10.]*

On note $\mathscr{Z}_p = (\mathbb{Z}_p \times \mathbb{Z}_p)\backslash(p\mathbb{Z}_p \times p\mathbb{Z}_p)$.

Soit $B(m,n) \in \mathbb{Z}[M,N]$ un polynôme homogène non nul qui vérifie la conjecture du crible des facteurs carrés.

Soit S un ensemble fini de places. Pour tout $v \in S$, soit une fonction g_v bornée presque partout localement constantes. Pour tout $p \notin S$, soit h_p une fonction

(a) presque partout localement constante

(b) telle que $|h_p(m,n)| \leq 1$ *pour tout* $(m,n) \in \mathscr{Z}$

(c) telle que $h_p(m,n) = +1$ *si* $v_p(B(m,n))$ *est pair.*

Soit la fonction $W(m,n) = \prod_{v\in S} g_v(m,n) \cdot \prod_{p\notin S} h_p(m,n)$.
Alors la moyenne du produit des g_v *et des* h_v *sur* $\mathbb{Q}$ *s'écrit*

$$av_{\mathbb{Q}}W(x,y) = c_\infty \cdot \prod_{p\in S} \frac{1}{1-p^{-2}} \int_{\mathscr{O}_p} g_p(x,y)dxdy \cdot \prod_{p\notin S} \frac{1}{1-p^{-2}} \int_{\mathscr{O}_p} h_p(x,y)dxdy,$$

où $\mathscr{Z}_p = (\mathbb{Z}_p \times \mathbb{Z}_p)\backslash(p\mathbb{Z}_p \times p\mathbb{Z}_p)$, *et*

$$c_\infty = \begin{cases} 1 & si\ \infty \notin S,\ et \\ \lim_{N\to\infty} \frac{1}{(2N)^2} \int_{-N}^{N}\int_{-N}^{N} g_\infty(x,y)dxdy, & si\ \infty \in S. \end{cases}$$

On en déduit le corollaire suivant :

Corollaire 2.5.3. *Soit une surface elliptique qui est isotriviale avec* $j = 0$ *ou* $j = 1728$ *ou non isotriviale sans place de réduction* I_m. *Alors, sous l'hypothèse que la conjecture du crible des facteurs carrés soit vérifiée sur* $B_{\mathscr{E}}$, *la moyenne du signe sur* $\mathbb{Q}$ *s'écrit*

$$av_{\mathbb{Q}}W(n) = -\prod_{p\in S} \frac{1}{1-p^{-2}} \int_{\mathscr{O}_p} g_p(x,y)dxdy \cdot \prod_{p\notin S} \frac{1}{1-p^{-2}} \int_{\mathbb{Q}_p} h_p(x,y)dxdy,$$

où S, g_p *et* h_p *sont l'ensemble et les fonctions données par le théorème 2.3.3.*

Démonstration. Cela repose d'abord sur la formule quand le produit est fini, c'est-à-dire la proposition 2.5.1. On a

$$av_{\mathbb{Q}} \prod_{p\in S} g_p(x,y) \cdot \prod_{p\notin S, p<M} h_p(x,y)$$

$$= c_\infty \prod_{p\in S} \frac{1}{1-p^{-2}} \int_{\mathscr{Z}_p} g_p(x,y)dxdy \cdot \prod_{p\notin S, p<M} \frac{1}{1-p^{-2}} \int_{\mathscr{Z}_p} h_p(x,y)dxdy.$$

Nous verrons que chaque membre de cette équation tend vers les côtés correspondants de la formule à démontrer lorsque $M \to \infty$.

On s'intéresse d'abord au membre de gauche : on veut démontrer

$$av_{\mathbb{Q}}(W(x,y)) = \lim_{M\to\infty} av_{\mathbb{Q}}(\prod_{v\in S} g_v(x,y) \cdot \prod_{p\notin S, p<M} h_v(x,y)).$$

On étudie la variation de

$$\Big| av_{\mathscr{Z}}W(x,y) - av_{\mathscr{Z}}(\prod_{v\in S} g_v(x,y) \cdot \prod_{p\notin S, p<M} h_v(x,y)) \Big|$$

et on montre qu'elle est $O(\frac{1}{M})$, donc tend vers 0 lorsque $M \to \infty$.

Pour cela, on combine la conjecture du crible des facteurs carrés

$$\#\{n,m \leq N | p^2 | B(m,n) \text{ pour } p > N\} = o(N^2),$$

et le théorème 1.3.3 pour les polynômes homogènes en deux variables :

$$\#\{m,n\leq N|p^2|B(m,n) \text{ pour } p \text{ entre } M \text{ et } \sqrt{N}\} = \frac{N^2}{M} + o(N^2),$$

pour obtenir

$$\#\{m,n\leq N|p^2|B(m,n) \text{ pour } p > M\} = O(\frac{N^2}{M}) + o(N^2).$$

De là et par le fait que $h_p(m,n) = 1$ pour tout p tel que $p^2 \nmid B(m,n)$, on obtient que

$$\left|\sum_{m,n\leq N}\prod_{v\in S} g_v(m,n)\cdot\prod_{p\notin S} h_v(m,n) - \sum_{m,n\leq N}\prod_{v\in S} g_v(m,n)\cdot\prod_{p\notin S,p<M} h_v(m,n)\right| = O(\frac{N^2}{M})+o(N^2),$$

d'où le résultat.

On veut maintenant montrer l'égalité des parties de droites des équations, et pour cela il faut prouver que

$$\prod_{p\notin S}\int_{\mathscr{Z}_p} h_v(m,n) = \lim_{M\to\infty}\prod_{p\notin S}\int_{\mathscr{Z}_p} h_v(m,n),$$

et pour ce faire il est suffisant de montrer

$$\lim_{M\to\infty}\prod_{p\notin S,p\geq M}\int_{\mathscr{Z}_p} h_v(m,n) = 1.$$

On rappelle (voir remarque 29) que le nombre de solutions $m,n \mod p^2$ à l'équation $B(m,n)\equiv 0 \mod p^2$ est $O(p^2)$, c'est-à-dire qu'il est borné. De plus, on a $|h_p(x,y)|\leq 1$ pour tout $x,y\in\mathbb{Z}_p$ et $h_p(x,y) = 1$ quand $v_p(B(x,y)) > 2$. Ces deux faits impliquent qu'on a

$$\int_{\mathscr{Z}_p} h_p(m,n) = 1 - O(\frac{1}{p^2}).$$

Donc

$$\prod_{p\notin S,p\geq M}\int_{\mathscr{Z}_p} h_p(n) = \prod_{p\geq M} 1 - O\left(\frac{1}{p^2}\right) = 1 - o\left(\sum_{m\geq M}\frac{1}{m^2}\right) = 1 - o\left(\frac{1}{M}\right),$$

ce qui tend vers 1 lorsque $M\to\infty$.

□

Corollaire 2.5.4. *Soit $\mathscr{E}$ une surface elliptique non isotriviale sans place de réduction de type I_m. On suppose que $B_{\mathscr{E}}$ respecte la conjecture du crible des facteurs carrés. Alors*

$$-1 < av_Q W(\mathscr{E}_t) < +1.$$

La démonstration de ce corollaire se base sur le lemme suivant dont la démonstration est élémentaire.

Lemme 2.5.5. *([27, Lemme 2.3]) Soit $Q(T)$ et $P(T)\in\mathbb{Z}[T]$ avec $Q(T)$ non constant. Soit $R = Res(P,Q)$ le résultant de P et de Q, et soit Δ_Q, le discriminant de Q. On suppose que R et $\Delta_r \neq 0$. Soit $\mathscr{P}_0$ un ensemble fini de nombres premiers.*

Alors il existe un nombre premier $p_0\notin\mathscr{P}_0$ et n un entier positif tel que $p_0^2 \mid Q(n)$ et $p_0^{-2}P(n)Q(n)\equiv 1 \mod p_0$.

En particulier, $p_0^2 \,||\, Q(n)$ et $p_0\nmid P(n)$.

Démonstration. Par le corollaire 2.5.3, il est suffisant de montrer

$$|\prod_{p\notin S}\int_{\mathscr{Z}_p} h_p(x,y)dxdy| < 1.$$

En se rappelant de la manière dont les fonctions $h_p(x,y)$ sont définies, on sait que $h_p(x,y) = \prod_{P\in\mathscr{B}'} h_{P,v}(x,y)$ où $h_{P,v} = +1$ pour au plus un des $v \notin S$, où les $h_{P,v}$ sont définies dans la démonstration du théorème 2.3.3. Plus précisément, on a

$$\begin{aligned}\prod_{p\notin S} h_p(x,y) &= \prod_{v\notin S}\prod_{P\in\mathscr{B}'} h_{P,v}(x,y)\\ &= \prod_{P\in\mathscr{B}'}\prod_{p\notin S} h_{P,v}(x,y)\\ &= \prod_{P\in\mathscr{B}'} h_{\mathscr{E},\delta,P}(x,y), \qquad \text{où } \delta = \prod_{p\in S\setminus\{\infty\}} p\end{aligned}$$

Soit Q un polynôme irréductible associé à une place de réduction I_m^*.

La conjecture du crible des facteurs carrés permet de sélectionner $\mathscr{F}\subseteq\mathscr{Z}$ un ensemble infini de paires (m,n) telles que pour chaque $P\in\mathscr{B}'\setminus\{Q\}$ la valeur de $P(m,n)$ est sans facteur carré. Sur cet ensemble, on a $h_{\mathscr{E},\delta,P} = +1$ pour tout $P\in\mathscr{B}'\setminus\{Q\}$. Par conséquent, pour $(x,y)\in\mathscr{F}$ on a

$$\prod_{p\notin S} h_p(x,y) = h_{\mathscr{E},\delta,Q}(x,y) \tag{2.18}$$

$$= \prod_{p\notin S} -\left(\frac{-c_6(x,y)}{p}\right)^{v_p(Q(x,y))-1} \tag{2.19}$$

Pour compléter la démonstration, il faut que $\mathscr{F}$ contienne deux ensembles infinis de paires pour lesquels la valeur de $h_{\mathscr{E},\delta,Q}$ est de signe opposé et que de plus ces ensembles soient de proportion positive.

Explicitement, on cherche à construire des ensembles infinis $\mathscr{F}_1,\mathscr{F}_2$ de paires d'entiers premiers entre eux telles que

1. pour tout $(m_1,n_1),(m_2,n_2)\in\mathscr{F}_1\cup\mathscr{F}_2$, on a $(m_1,n_1)\equiv(m_2,n_2) \mod N_{\mathscr{E}}$ une classe de congruence non nulle pour $N_{\mathscr{E}}$ l'entier correspondant à $\mathscr{E}$ donné par le théorème 5.2.3 ;
2. pour tout $(m,n)\in\mathscr{F}_1$, $p_0^{-2}Q(m,n) = c^2 l$ est un entier sans facteur carré premier à $N_{\mathscr{E}}$, pour un nombre premier p_0 tel que $(c_6(x,y)/p_0) = +1$;
3. pour tout $(m,n)\in\mathscr{F}_2$, $Q(m,n) = c^2 l$ est un entier sans facteur carré premier à $N_{\mathscr{E}}$.

Ceci est possible grâce au crible des valeurs dans facteurs carrés 1.3.5 (valable car la conjecture des facteurs carrés est supposée vérifiée) et au lemme 2.5.5. Ce dernier assure l'existence d'un tel p_0. (On pose $P(x,y) = \frac{-c_6(x,y)}{Q(x,y)^3}$ pour obtenir que $p_0^{-2}\frac{-c_6(x,y)}{Q(x,y)^2} \equiv 1 \mod p_0$. Par conséquent, $-p_0^{-6}c_6(x,y)$ est un carré modulo p_0.) De plus, remarquons que les ensembles $\mathscr{F}_1$ et $\mathscr{F}_2$ donnés par le crible sont de proposition positive, car ils sont tirés de l'estimation de la conjecture sans facteur carré.

Par la proposition 5.2.10, on aura pour tout $(m,n),(m',n')\in\mathscr{F}_i$ $(i=1,2)$

$$W(m,n) = W(m',n')$$

et par la proposition 5.2.11, on aura pour tout $(m_1,n_1)\in\mathscr{F}_1$, $(m_2,n_2)\in\mathscr{F}_2$

$$W(m_1,n_1) = -W(m_2,n_2).$$

Sur l'union $\mathscr{F}_1 \cup \mathscr{F}_2$, on aura par conséquent

$$|av_{\mathscr{F}_1 \cup \mathscr{F}_2} W(m,n)| < 1,$$

d'où le résultat pour la moyenne sur $\mathbb{Q}$. □

Remarque 47. On utilise la même idée, c'est-à-dire la construction des ensembles $\mathscr{F}_1$ et $\mathscr{F}_2$, dans les travaux de Manduchi [27], ceux de Várilly-Alvarado [51], ainsi que dans la démonstration du théorème 5.0.8 dans le chapitre 5. Nous invitons le lecteur déçu du manque de précision de la démonstration du corollaire 2.5.4 à consulter le chapitre 5 qui contient davantage de détails.

2.5.3 Surfaces admettant des places de type I_m

Proposition 2.5.6. *[15, Prop. 7.12.]*

On note $\mathscr{Z} = (\mathbb{Z} \times \mathbb{Z}) \backslash \{(x,y) | pgcd(x,y) \neq 1\}$.

Soit $B(m,n) \in \mathbb{Z}[M,N]$ *un polynôme homogène non nul qui vérifie la conjecture du crible des facteurs carrés.*

Soit S *un ensemble fini de places. Pour tout* $v \in S$*, soit une fonction* g_v *bornée presque partout localement constantes. Pour tout* $p \notin S$*, soit* h_p *une fonction*

(a) presque partout localement constante

(b) telle que $|h_p(m,n)| \leq 1$ *pour tout* $(m,n) \in \mathscr{Z}$

(c) telle que $h_p(m,n) = +1$ *si* $v_p(B(m,n))$ *est pair.*

Soit $\alpha : \mathbb{Z} \times \mathbb{Z} \to \mathbb{C}$ *une fonction telle que*

$$av_{\mathscr{S} \cap (a+L) \cap \mathscr{Z}} \alpha(x,y) = 0, \tag{2.20}$$

pour tout secteur $\mathscr{S}$ *et tout réseau* $a + L$ *tel que* $L \cap \mathscr{Z}$ *est non vide.*

On suppose de plus que $|\alpha(x,y)| \leq 1$ *pour tout* $(x,y) \in \mathscr{Z}$.

Soit la fonction $W(m,n) = \prod_{v \in S} g_v(n) \cdot \prod_{p \notin S} h_p(m,n)$.

Alors

$$av_{\mathscr{S} \cap (a+L) \cap \mathscr{Z}} W(x,y) = 0, \tag{2.21}$$

pour tout secteur S *et tout réseau* L.

Remarque 48. Dans cette proposition, on peut prendre $\mathbb{Z}^2$ plutôt que $\mathscr{Z}$ (autrement dit, on ne suppose plus que $\text{pgcd}(x,y) = 1$) sans que la conclusion soit modifiée. Ceci est démontré par [15, Lemme 7.13] et [15, Lemme 7.14].

On en déduit le corollaire suivant :

Corollaire 2.5.7. *Soit* $\mathscr{E}$ *une surface elliptique qui admet au moins une place de réduction multiplicative. On fait les hypothèses suivantes :*

1. $B_{\mathscr{E}}$ *vérifie la conjecture du crible des facteurs carrés, et*
2. $M_{\mathscr{E}}$ *vérifie la conjecture de Chowla.*

Alors la moyenne du signe des fibres sur $\mathbb{Q}$ *est*

$$av_{\mathbb{Q}} W(\mathscr{E}_t) = 0.$$

Remarque 49. On peut aller dans la direction inverse : si le signe moyen des fibres d'une surface elliptique est 0, alors la conjecture de Chowla est vérifiée pour $M_{\mathscr{E}}$. Ces faits sont démontrés par [15, Prop. 7.15] et [15, Prop. 7.16].

Démonstration. On procède comme dans la démonstration de 2.4.3, mais en utilisant les arguments de 2.5.1 plutôt que ceux de 2.4.1.

Il est suffisant de montrer que pour tout N_1 un entier assez grand, on a

$$av_{\mathscr{S}\cap(a+L)\cap\mathscr{Z}}\alpha(x,y)\cdot\prod_{v\in S}g_v(x,y)\cdot\prod_{p\notin S;p\leq N_1}h_p(x,y)=0,$$

car le même argument que dans 2.5.2 permettra de conclure l'égalité 2.21.

Soit un entier N_1. Pour simplifier la notation, on réindexe le produit fini comme suit : on pose $S'=S\cap\{p\notin S\mid p<N_1\}$ et $g_p=h_p$ pour $p\in S'\backslash S$.

1) Chaque fonction g_v est localement constante en dehors d'un nombre fini de droites de $\mathbb{Q}_v\times\mathbb{Q}_v$. On recouvre ces droites par un ensemble X_v défini comme l'union de section suffisament étroit (en terme d'angle) autour de ces droites.

Si $v=\infty$, on construit X_v avec une restriction supplémentaire. Le nombre d'entier $-N\leq x,y\leq N$ contenu dans un secteur d'angle ϵ dans $\mathbb{R}^2=\mathbb{Q}_\infty^2$ est $O(\epsilon)$. Ainsi on prend soin de prendre chaque secteur de X_∞ d'angle $\leq\epsilon$, afin d'avoir

$$|\{-N_2\leq x,y\leq N_2:(x,y)\in X_\infty\}|=O(\epsilon N_2^2).$$

Si v est finie, alors X_v consiste en une union d'ensembles de la forme $\{(x,y)\in\mathbb{Q}_v\times\mathbb{Q}_v : x/y\in B_p\}$ où $B_p\subset\mathbb{Q}_v$ est une boule d'aire $\leq\epsilon$.

a) Donc, la contribution totale des ensembles X_v au signe est $O(\epsilon)$.

On pose $R_v=\mathbb{Q}_v\backslash X_v$ et $\iota_v(m,n)$ l'inclusion de $\mathscr{Z}$ dans $\mathbb{Q}_v$. Soit

$$Z=\{(x,y)\in\mathscr{Z}\mid\iota_v(m,n)\in R_v\text{ pour tout }v\in S'\}.$$

Nous venons de montrer que

$$av_{\mathscr{S}\cap(a+L)\cap\mathscr{Z}}\alpha(x,y)\prod_{v\in S'}g_v(x,y)=av_{\mathscr{S}\cap(a+L)\cap\mathscr{Z}}\alpha(x,y)\prod_{v\in S'}g_v(x,y)+O(\epsilon).$$

b) Pour tout $v\in S$, la fonction g_v est localement constante sur R_v.

L'ensemble $R_\infty\in\mathbb{R}^2$ est l'union de la fermeture d'une quantité finie de secteur disjoints $\{U_{\infty,j}\}$. Les secteurs étant connexes, g_∞ est constant sur chaque secteur.

Pour tout $p\in S'$, l'ensemble R_p est compact. Par conséquent, on peut le recouvrir d'un nombre fini de boule $U_{p,j}$ dans $\mathbb{Q}_p$. Sur chacune de ces boules, g_p est constant.

On montre que la moyenne est 0 sur tout ensemble de la forme Cela est vrai car le produit $\prod_{v\in S'}g_v(x,y)$ est constant sur chaque $F_{\vec{j}}$ et l'hypothèse 2.20 garantie que $\alpha(x,y)$ est de moyenne 0 sur $F_{\vec{j}}$.

□

2.6 Conclusions sur la variation du signe

La valeur de la moyenne du signe sur $\mathbb{Q}$ ou sur un sous-ensemble donne des informations sur la variation du signe de l'équation fonctionnelle.

Une surface dont le signe est constant sur toute fibre est telle que $av_KW(\mathscr{E}_t)$ est de cette même valeur sur tout sous-ensemble de $K\subseteq\mathbb{Q}$. Une conséquence de ceci est que pour toute surface de signe moyen différent de $+1$, les points rationnels sont denses conditionnellement à la conjecture de parité. Par conséquent, pour une surface $\mathscr{E}$ telle que $-1<av_{\mathbb{Q}}W(\mathscr{E}_t)<+1$, les ensembles $W_\pm$ sont tous deux de cardinalité infinie.

2.6.1 Surfaces isotriviales telles que $j(T) \neq 0, 1728$

Soit $\mathscr{E}$ une surface elliptique isotriviale qui est une famille de twists quadratiques. Dans ce cas, la proposition 2.4.1 dit que la moyenne du signe sur $\mathbb{Q}$ est un produit fini d'intégrale.

Pour tout $p \in S$, on a que $g_p : \mathbb{Q}_p \to [-1, 1]$, la fonction associée à $\mathscr{E}$ par le théorème 2.3.3, est telle que

$$\int_{\mathbb{Q}_p} g_p(x)dx \in [-1, 1],$$

et en particulier on a

$$\Big| \int_{\mathbb{Q}_p} g_p(x)dx \Big| \leq 1.$$

Par conséquent, il suffit qu'un seul des g_p varie pour que le signe global varie également. Il est toutefois possible que le signe soit constant. Des exemples de telles surfaces sont donnés dans [51], [3], par les théorèmes 4.2.6 et 4.2.9 de cette thèse ou par la proposition suivante

Proposition 2.6.1. *[15, Corollaire 7.4.] Soit E la courbe elliptique donnée par l'équation de Weierstrass*

$$y^2 = x^3 + ax + b$$

où $a, b \in \mathbb{Q}$ et pour tout $t \in \mathbb{Q}$, soit la courbe

$$E_t : ty^2 = x^3 + ax + b.$$

Alors il existe un polynôme $f \in \mathbb{Q}[T]$ tel que la fonction définie par

$$t \to W(E_{f(t)})$$

est constante sur $\mathbb{Q}\backslash\{$zéros de f dans $\mathbb{Q}\}$.

Remarque 50. Dans la démonstration de cette proposition, Helfgott exhibe la surface définie par les twists quadratiques par une fonction de la forme

$$f(t) = 3^3 t^m + 4^2,$$

où $m = 2^k 5^4 \prod_{p \in S} (p^2 - 1)$, k un entier positif assez grand.

2.6.2 Surfaces non isotriviales sans place de réduction I_m

Théorème 2.6.2. *[15] Soit $\mathscr{E}$ une surface elliptique sur $\mathbb{Q}$. On fait les hypothèses suivantes :*

1. *tout polynôme P associé aux places de mauvaise réduction (sauf type I_0^*) est tel que* $\deg P \leq 6$.
2. *$\mathscr{E}$ n'admet pas de place générique de type I_m,*

Alors, $W_+(\mathbb{Q})$ et $W_-(\mathbb{Q})$ sont infinis.

Démonstration. La démonstration découle directement du corollaire **??**. □

La formule donnée par la proposition 2.4.2 peut être utilisée pour calculer la valeur de la moyenne du signe des fibres. Cependant, ce calcul est fastidieux. Helfgott traite en appendice l'exemple suivant, où la moyenne est $\sim -.15294$.

Exemple 1. On pose $f_1 = -5 - 2T^2$ et $f_2 = 2 + 5T^2$.

Soit $\mathscr{E}$ la surface elliptique isotriviale décrite par l'équation

$$\mathscr{E} : y^2 = x^3 - 27c_4(T)x - 54c_6(T),$$

$c_4 = f_1 f_2 (f_1^3 - f_2^3)^2$ et $c_6 = \frac{1}{2}(f_1^3 + f_2^3)(f_1^3 - f_2^3)^3$.

Alors on a

$$av_{\mathbb{Q}} W(\mathscr{E}(x/y)) = -\frac{19}{112} \cdot \prod_{p \neq 2,3,7,19} \left(1 - a_p \frac{p^{-2}(1-p^{-1})}{(1-p^{-2})}\right),$$

où a_p est le nombre de racines de l'équation

$$(19t^4 + 11t^2 + 19)(t^2 + 1) \equiv 0 \mod p$$

dans $\mathbb{Z}/p\mathbb{Z}$.

2.6.3 Surfaces avec place de réduction I_m

Théorème 2.6.3. *[15] Soit $\mathscr{E}$ une surface elliptique définie sur $\mathbb{Q}$. On fait les hypothèses suivantes :*

1. *tout polynôme P associé aux places de mauvaise réduction (sauf type I_0^*) est tel que* $\deg P \leq 6$,
2. $\deg M_{\mathscr{E}} \leq 3$, *ou encore $M_{\mathscr{E}}$ est un produit de degré arbitraire de formes linéaires.*

Alors, $W_+(\mathbb{Q})$ et $W_-(\mathbb{Q})$ sont infinis.

Démonstration. Ce théorème se déduit directement de la proposition 2.5.6 si $\mathscr{E}$ a des places de réductions I_m et du corollaire 2.4.4 sinon. □

2.7 Comparaison avec les travaux de Manduchi

2.7.1 Surface non isotriviale sans place de type I_m

Théorème 2.7.1. *[27, Théorème 1] Soit $\mathscr{E}$ une surface elliptique non isotriviale On suppose que*

1. *les polynômes associés aux places de mauvaise réduction (sauf de type I_0^*) ont degrés inférieurs ou égaux à 6,*
2. *il n'y a pas de place de réduction I_m.*

Helfgott ne démontre pas la variation du signe sur davantage de surface elliptique sans place de réduction I_m que Manduchi. Il remarque cependant que les travaux de celle-ci peuvent être étendus à toutes surfaces dont le polynôme $B_{\mathscr{E}}(x, y)$ respecte la conjecture du crible des facteurs carrés.

2.7.2 Surface avec place de type I_m

Théorème 2.7.2. *[27, Théorème 2] Soit $\mathscr{E}$ une surface elliptique non isotriviale. On suppose que*

1. *les polynômes associés aux places de mauvaise réduction (sauf de type I_0^*) ont degrés inférieurs ou égaux à 3,*

2. $\deg M = 1$.

Les travaux de Manduchi utilisent les conjectures de Chowla et du crible des facteurs carrés dans leurs versions pour les polynômes en une variable. Une des innovations de Helfgott est que sa preuve utilise les conjectures sous forme homogène. Elle est donc inconditionnelle dans davantage de cas.

3

Variation du signe des fibres sur les surfaces elliptiques isotriviales

Une *surface elliptique isotriviale* est une surface elliptique $\mathscr{E}$ dont la fonction du j-invariant est constante. On observe qu'elle doit avoir la forme d'une famille de twists d'une courbe elliptique donnée. Ces surfaces elliptiques sont de trois types :

1. $y^2 = x^3 + af(T)^2x + bf(T)^3$, où $f(T)$ est sans facteur carré et $ab \neq 0$ (dans ce cas, $j(T) \in \mathbb{Z}\backslash\{0, 1728\}$),
2. $y^2 = x^3 + f(T)x$, où $f(T)$ est sans facteur qui est une puissance quatrième ($j(T) = 1728$),
3. $y^2 = x^3 + f(T)$, où $f(T)$ est sans facteur qui est une puissance sixième ($j(T) = 0$).

Dans ce chapitre, on étudie les variations de la fonction du signe des fibres de ces surfaces $t \to W(\mathscr{E}_t)$. En particulier, on veut vérifier si les ensembles

$$W_{\pm}(\mathscr{E}) = \{t \in \mathbb{Q}^* | W(\mathscr{E}_t) = \pm 1\}$$

sont de cardinalité infinie. Le cas échéant, la conjecture de parité garantit la densité des points rationnels. (Plus précisément, il suffit que $\#W_-(\mathscr{E}) = \infty$.)

La spécificité des surfaces elliptiques isotriviales est que le signe de l'équation fonctionnelle des fibres est parfois constant. Pour les surfaces où le signe prend uniquement des valeurs $+1$, on ne peut rien conclure à partir de l'étude du signe sur la densité des points rationnels de ces surfaces.

3.1 Surfaces de la forme $H(T)y^2 = x^3 + ax + b$

3.1.1 Théorème de variation

Le théorème suivant décrit la variation du signe sur les surfaces elliptiques isotriviales de type général. Remarquons que ces surfaces sont caractérisées par le fait que les places génériques sont uniquement de type I_0 ou I_0^*.

Théorème 3.1.1. *Soit E une courbe elliptique donnée par l'équation de Weierstrass*

$$y^2 = x^3 + ax + b,$$

où $a, b \in \mathbb{Z}$ sont tels que $ab \neq 0$.

Pour $t \in \mathbb{Z} - \{0\}$, on définit $E_t : ty^2 = x^3 + ax + b$.

Alors

1. *Il existe M entier tel que, pour t sans facteur carré, le signe $W(E_t)$ ne dépend que de la classe de congruence de t modulo M.*
2. *Le signe $W(E_t)$ n'est pas constant quand t varie dans $\mathbb{Q}^\times$.*

Remarque 51. On choisit $t_0, \dots, t_m$ des représentants de chaque classe modulo M qui n'ont pas de facteur carré. On pose $S = \{t_0, \dots, t_m\}$. Le deuxième point du théorème 3.1.1 peut être plus explicitement formulé comme suit :

Pour toutes valeurs de $a, b \in \mathbb{Z}^*$ telles que $4a^3 + 27b^2 \neq 0$, il existe une partition non-triviale $S = S_+ \sqcup S_-$ telle que

$$W(E_t) = +1 \Leftrightarrow [t]_M \in S_+$$

$$W(E_t) = -1 \Leftrightarrow [t]_M \in S_-,$$

où $[t]_M$ désigne la classe de t' modulo M, où t' est la partie de t dépourvue de facteur carré.

Soit $t \in \mathbb{Q}^\times$, que l'on écrit $t = \left(\frac{c}{d}\right)^2 \frac{t_1}{t_2}$ avec $c, d \in \mathbb{Z}$, et t_1, t_2 des entiers sans facteur carré, premiers entre eux. On a alors $E_t : ty^2 = x^3 + ax + b$ isomorphe à $E_{t_1 t_2}$ et

$$W(E_t) = \pm 1 \Leftrightarrow (t_1 t_2 \mod M) \in S_\pm.$$

Corollaire 3.1.2. *Soit la surface elliptique $\mathscr{E} : f(T)y^2 = x^3 + ax + b$, où $a, b \in \mathbb{Q}$ et $f(T)$ une fonction rationnelle sur $\mathbb{Q}$.*

S'il est possible de trouver une infinité de paires (t_1, t_2) pour lesquelles les parties libres de carré de $f(t_1)$ et de $f(t_2)$ tombent dans deux classes de congruences de signes opposés, alors la conjecture de parité implique que l'ensemble $\mathscr{E}(\mathbb{Q})$ des points rationnels de $\mathscr{E}$ est dense pour la topologie de Zariski.

Remarque 52. Pour une surface d'équation $\mathscr{E} : f(t)y^2 = x^3 + ax + b$ où $f(t)$ est un polynôme quadratique, on démontre inconditionnellement la densité de $\mathscr{E}$ grâce à un argument géométrique (voir section 4.2.1).

3.1.2 Comparaison avec Rohrlich

Rappelons le théorème de Rohrlich déjà énoncé dans l'introduction (théorème 0.1.6)

Théorème 3.1.3. *[38, Théorème 2] Soit $a, b \in \mathbb{Z}$ tel que $ab \neq 0$. On considère la courbe elliptique définie par l'équation $E : y^2 = x^3 + ax + b$ si $\Delta \neq 0$. Soit $f(t) \in \mathbb{Z}[t]$ et la famille de tordues quadratiques définie par l'équation*

$$E_{f(t)} : f(t)y^2 = x^3 + ax + b$$

Alors, l'une des deux propositions suivantes est vraie :

1. *Les ensembles W_+ et W_- sont denses dans $\mathbb{R}$.*
2. *Les ensembles W_+ et W_- sont $\{t \in \mathbb{Q} | f(t) < 0\}$ et $\{t \in \mathbb{Q} | f(t) > 0\}$.*

De plus, pour E donnée,

1. *il existe f tel qu'on est dans le cas 2 et tel que le nombre de changements de signe de f sur $\mathbb{R}$ dépasse n'importe quelle valeur préassignée.*
2. *si en outre E a bonne réduction sur une extension abélienne de $\mathbb{Q}$, on est dans le cas 2.*

Si l'on cherche à savoir si une famille de tordues d'une courbe elliptique est de signe constant, on obtient de ce théorème les conclusions suivantes :

1. si E a bonne réduction sur $\mathbb{Q}^{ab}$ alors $E^{f(t)}$ est de signe constant si et seulement si $f(t)$ est de signe constant pour tout $t \in \mathbb{Q}$,
2. si E n'a pas bonne réduction sur $\mathbb{Q}^{ab}$, alors
   (a) si $f(t)$ n'est pas de signe constant, alors W_+ et W_- sont de cardinalité infinie.
   (b) si $f(t) > 0$ (ou < 0), alors le théorème de Rohrlich ne permet pas de conclure directement. Pour savoir si le signe est constant ou non, on doit utiliser le théorème 3.1.1. Il faut déterminer les valeurs de la partie sans facteur carré de $f(t)$ modulo M (pour l'entier donné par le théorème, qui dépend des coefficients d'une équation de Weierstrass de E) et vérifier dans quelles classes d'équivalences ces valeurs tombent. Les fibres en des valeurs tombant dans la même classe d'équivalence seront de même signe. On étudiera donc simplement la variation du signe d'un choix de représentants de ces classes.

De plus, Rohrlich ne dit rien sur les cas où $ab = 0$. Nous traitons ces cas dans les théorèmes 3.2.1 et 3.2.2.

3.1.3 Constance locale des signes locaux

Lemme 3.1.4. *Soit la famille isotriviale des formes tordues*

$$E : y^2 = x^3 + at^2x + bt^3,$$

où $a, b \in \mathbb{Z}$ et $t \in \mathbb{Z} - \{0\}$. On pose $\Delta(t) = \Delta_0 t^6$ la fonction des discriminants de cette famille, où $\Delta_0 = 4a^3 + 27b^2$.

Pour chaque $t \in \mathbb{Z} - \{0\}$, soit t' l'entier dépourvu de facteur carré tel que $t = c^2t'$ pour c un entier approprié.

Soit p un nombre premier tel que $p|6\Delta_0$.

Alors il existe α_p un entier tel que, lorsqu'on fait varier t de telle sorte que t' reste dans la même classe de congruence modulo p^{α_p}, le signe local en p de E_t est invariant.

Démonstration. Soit Δ_0 le discriminant de E_1. Soit t un entier, et la décomposition $t = t_0t_1$, où t_0 est un produit de facteurs premiers de Δ_0 et t_1 est un entier premier avec Δ_0.

Si $p \geq 5$ et que $v_p(t) = 2$, on aura $v_p(\Delta_{E_t}) = v_p(\Delta_0) + 12v_p(t_1)$. Puisque $p \nmid t_1$, alors $v_p(\Delta_{E_t}) = v_p(\Delta_0)$. Or, on sait que le signe d'une courbe reste invariant lorsqu'elle est tordue par une puissance douzième. Connaître t modulo p^2 suffit donc pour connaître $W_p(E_t)$.

Soit, pour $p = 2, 3$ et $l = 4, 6$, les entiers $c_{l,p}$ tels que $c_l = p^{v_p(t)}c_{l,p}$. Les formules que l'ont trouve grâce aux tables [13] ne dépendent en effet que de la valuation 2-adique et 3-adique de c_4 et de c_6 ainsi que du reste de $c_{4,2}$, $c_{4,3}$, $c_{6,2}$, $c_{6,3}$ modulo certaines puissances de 2 ou de 3. □

3.1.4 Signes locaux en 2 et 3

Soit $E : y^2 = x^3 - 27c_4(T)x - 54c_6(T)$ une surface elliptique de discriminant $\Delta(T)$. Le signe local en $p = 2, 3$ d'une fibre $\mathscr{E}_t$ en $t \in \mathbb{Z}$ dépend des valeurs du triplets

$$(v_p(c_4(t)), v_p(c_6(t)), v_p(\Delta(t))).$$

Connaissant la valeur de ce triplet, on consulte les tableaux [37, Table II, III] pour obtenir une façon de calculer le signe local.

Dans le cas de $E : y^2 = x^3 + aT^2x + bT^3$, ce triplet est de valeur

$$(v_p(a) + 2v_p(t), v_p(b) + 3v_3(t), v_p(\Delta) + 6v_p(t))$$

pour toute valeur de $t \in \mathbb{Z}$. Ainsi, la valeur du triplet $(v_p(a), v_p(b), v_p(\Delta))$ nous donne toutes les informations nécéssaires pour calculer le signe local en p en toute fibre de la surface. Dans ce qui suit, nous sélectionnons les triplets dont les surfaces $E : y^2 = x^3+ax+b$ tels que leur signe local est décrit par une formule spécifique.

Lemme 3.1.5. *Soit $E : y^2 = x^3+ax+b$ une courbe elliptique et soit $E_t : y^2 = x^3+at^2x+bt^3$ la tordue de E par $t \in \mathbb{Z}$. On pose t_2, b_2 et Δ_2 les entiers tels que $t = 2^{v_2(t)}t_2$, $b = 2^{v_2(b)}b_2$ et $\Delta = 2^{v_2(\Delta)}\Delta_2$.*

Alors $W_2(E_t) = \left(\frac{-1}{t_2}\right)$ pour tout $t \in \mathbb{Z}$ si et seulement si le triplet $(v_2(a), v_2(b), v_2(\Delta))$ fait partie des choix suivants :

1. *$(0, 0, 0)$ ou $(2, 3, 6)$, et que de plus $b_2 \equiv \Delta_2 \equiv 3 \mod 4$; ou*
2. *$(\geq 4, 3, 0)$ ou $(\geq 6, 6, 6)$, et que de plus $b_2 \equiv 1 \mod 4$.*

Démonstration. Soit $E : y^2 = x^3 + ax + b$ une courbe elliptique et soit Δ son discriminant. Pour tout $t \in \mathbb{Z}^*$, on considère la tordue de E par t, $E_t : ty^2 = x^3 + ax + b$.

Nous listerons ici les conditions sur les coefficients a, b et Δ pour que le signe en 2 des fibres E_t soit $W_2(t) = \left(\frac{-1}{t_2}\right)$ pour tout t. On peut classifier les surfaces par le triplet $(v_2(a), v_3(b), v_2(\Delta))$, et trouver la formule de leur signe en 2 grâce au tableau de Rizzo [37, Table III]. Pour commencer, on sélectionne les surfaces telles que $W_2(E_t) = (\frac{-1}{t})$ lorsque $2 \nmid t$. Pour sélectionner ces triplets et déterminer les conditions supplémentaires correspondantes, nous avons procédé de la manière suivante, dont nous donnerons seulement deux exemples, les autres se traitant de manière similaire.

Si $(v_2(a), v_2(b), v_2(\Delta)) = (0, 0, 0)$, alors la table de Rizzo donne la formule suivante pour le signe des fibres en t impair :

$$W_2(\mathscr{E}_t) = \begin{cases} +1 & \text{si } c_6t^3 \equiv 3 \mod 4 \\ -1 & \text{sinon.} \end{cases}$$

On veut $W_2(\mathscr{E}_t) = +1 \Leftrightarrow t \equiv 1 \mod 4$, ce qui est possible si et seulement si $c_6 \equiv 3 \mod 4$.

Si $(v_2(a), v_2(b), v_2(\Delta)) = (2, 4, 0)$, alors la table de Rizzo donne la formule suivante pour le signe des fibres en t impair :

$$W_2(\mathscr{E}_t) = \begin{cases} +1 & \text{si } c_4 \equiv 1 \mod 4 \text{ et si } c_4 + 4c_6t^3 \equiv 9, 13 \mod 16, \\ -1 & \text{sinon.} \end{cases}$$

On veut $W_2(\mathscr{E}_t) = +1 \Leftrightarrow t \equiv 1 \mod 4$, ce qui est possible si et seulement si $c_4 \equiv 1, 13 \mod 16$ et $c_6 \equiv 3 \mod 4$, ou si $c_4 \equiv 5, 9 \mod 16$ et $c_6 \equiv 1 \mod 4$.

En procédant d'une façon similaire pour tous les autres triplets, on obtient la liste suivante dont les surfaces associées vérifient $W_2(E_t) = \left(\frac{-1}{t}\right)$ pour tout $t \in \mathbb{Z}$.

- $(0, 0, 0)$, si de plus $c_6 \equiv 3 \mod 4$,
- $(\geq 4, 3, 0)$, si de plus $c_6 \equiv 1 \mod 4$,
- $(2, 4, 0)$, si l'une des conditions suivantes est respectée :
  - $c_4 \equiv 1, 13 \mod 16$ et $c_6 \equiv 3 \mod 4$;
  - $c_4 \equiv 5, 9 \mod 16$ et $c_6 \equiv 1 \mod 4$,
- $(2, 5, 0)$, si l'une des conditions suivantes est respectée :
  - $c_4 \equiv 1, 5 \mod 16$ et $c_6 \equiv 1 \mod 4$;

— $c_4 \equiv 9, 13 \mod 16$ et $c_6 \equiv 3 \mod 4$,
— $(2, 3, 1)$, si l'une des conditions suivantes est respectée :
— $c_4 \equiv 15 \mod 16$ et $c_6 \equiv 1 \mod 4$;
— $c_4 \equiv 7 \mod 16$ et $c_6 \equiv 3 \mod 4$,
— $(2, 3, 6)$, si $c_6 \equiv \Delta \mod 4$,
— $(\geq 4, 4, 2)$, si $c_6 \equiv 1 \mod 4$,
— $(3, 5, 3)$, si l'une des conditions suivantes est respectée :
— $c_4 \equiv 1, 7 \mod 8$ et $c_6 \equiv 1 \mod 4$;
— $c_4 \equiv 3, 5 \mod 16$ et $c_6 \equiv 3 \mod 4$,
— $(2, 3, \geq 4)$ si $c_6 \equiv 3 \mod 4$,
— $(\geq 6, 5, 4)$ si $c_6 \equiv 3 \mod 4$,
— $(\geq 6, 6, 6)$, si $c_6 \equiv 1 \mod 4$,
— $(4, 6, 7)$ si $c_6 \equiv 1, 5 \mod 8$ et $c_4 \equiv 5 \mod 8$
— $\geq 7, 7, 8$, si $c_6 \equiv 3 \mod 4$
— $(6, 8, 10)$, si $c_4 c_6 \equiv 3 \mod 4$ et
— $(\geq 7, 8, 10)$, si $c_6 \equiv 3 \mod 4$.

La dernière étape est de ne retenir que les triplets (munis de leurs conditions particulières) tels que $W_2(E_{2t}) = W_2(E_t)$. Pour chaque cas listé, on vérifie si le triplet d'une fibre en $2t$, c'est à dire $(v_2(a) + 2, v_2(b) + 3, v_2(\Delta) + 6)$ est également tel que le signe local en 2 est $W_2(\mathscr{E}_{2t}) = \left(\frac{1}{t}\right)$. On trouve ce faisant les cas listés dans l'énoncé. □

Lemme 3.1.6. *Soit $E : y^2 = x^3 + ax + b$ une courbe elliptique non singulière et $E_t := y^2 = x^3 + at^2x + bt^3$ la tordue de E par $t \in \mathbb{Z}$.*

Alors le signe local en 3 est égal à $W_3(E_t) = (-1)^{v_3(t)}$ pour tout $t \in \mathbb{Z}$ si et seulement si le triplet des valeurs $(v_3(a), v_3(b), v_3(\Delta))$ fait partie d'un des suivants :

1. $(0, 0, 0)$,
2. $(1, \geq 3, 0)$ *ou*
3. $(1, 2, 0)$ *et que de plus* $a \equiv 2 \mod 3$.

Démonstration. Soit $t \in \mathbb{Z}$ un entier.

Si t est tel que $3 \nmid t$. Alors le signe local en 3 est donné par la formule du tableau [37, Table II] correspondant à $(v_3(a), v_3(b), v_3(\Delta))$.

Si $v_3(t)$ est impair, alors le triplet associé est $(v_3(a) + 2, v_3(b) + 3, v_3(\Delta) + 6)$

Pour déterminer les conditions sur a, b pour que le signe local en 2 ait la forme voulue, on commence par sélectionner les triplets tels que $W_3(E_t) = +1$ pour tout $t \in \mathbb{Z}$ premier à 3. Ceux-ci font partie de la liste suivante : $(0, 0, 0)$, $(1, \geq 3, 0)$, $(1, 2, 0)$, $(2, \geq 5, 3)$, $(2, 3, 4)$, $(3, 5, 6)$ (si de plus $a \equiv 2 \mod 3$) et $(4, \geq 8, 9)$.

Ensuite, on ne retient que ceux tels que $W_3(E_{3t}) = -W_3(E_t)$, c'est-à-dire $(0, 0, 0)$, $(1, \leq 3, 0)$ et $(1, 2, 0)$ (si de plus $a \equiv 2 \mod 3$).

□

3.1.5 Monodromie des types de réduction des fibres

Soient des entiers a, b. Soit E la courbe elliptique représentée par l'équation de Weierstrass

$$E : y^2 = x^3 + ax + b,$$

et soit Δ_0 son discriminant que l'on suppose minimal.

Pour tout $t \in \mathbb{Z} - \{0\}$, on définit la tordue de E en t

$$E_t : y^2 = x^3 + at^2x + bt^3.$$

Soit t_0 un entier sans facteur carré et premier avec Δ_0. Soit λ un entier sans facteur carré et premier avec t_0. Soit p un nombre premier différent de 2 ou 3. On cherche à comparer $W_p(E_{t_0})$ et $W_p(E_{\lambda t_0})$.

On pose $D_p \in \{-1, +1\}$ l'entier tel que $W_p(E_{t_0}) = D_p W_p(E_{\lambda t_0})$.

1. Supposons que $p \nmid \Delta_0$. Dans ce cas, la courbe E_{t_0} est de réduction de type I_0 en p.
   (a) Si $p \nmid \lambda$, la réduction de $E_{\lambda t_0}$ en p reste de type I_0 et on a $D_p = +1$.
   (b) Si $p \mid \lambda$, la réduction de $E_{\lambda t_0}$ en p est I_0^*. On a donc $D_p = \left(\frac{-1}{p}\right)$.
2. Supposons que $p \mid \Delta_0$. On a que D_p dépend du type de réduction en p de E.
   (a) Si $p \nmid \lambda$ et que la réduction de E n'est pas multiplicative, on a $D_p = +1$. Si la réduction est de type I_m, alors on a

$$D_p = \left(\frac{\lambda}{p}\right),$$

car

$$\begin{aligned} W_p(E_{t_0\lambda}) &= -\left(\frac{-c_6\lambda^3 t_0^3}{p}\right) \\ &= -\left(\frac{-c_6 t_0}{p}\right)\left(\frac{\lambda}{p}\right) \\ &= W_p(E_{t_0})\left(\frac{\lambda}{p}\right). \end{aligned}$$

   (b) Si $p \mid \lambda$, on a une des variations suivantes selon le type de variation de E_t en p.
      i. Si E_t est de type I_0, alors E_{pt} est de type I_0^*. Inversement, si E_t est de type I_0^*, alors E_{pt} est de type I_0. Le signe local en p passe de $(\frac{-1}{p})$ à $+1$. On a $D_p = (\frac{-1}{p})$.
      ii. Si E_t est de type II, alors E_{pt} est de type IV^*. Inversement, si E_t est de type IV^*, alors E_{pt} est de type II. Le signe local en p passe de $(\frac{-1}{p})$ à $(\frac{-3}{p})$. On a $D_p = (\frac{3}{p})$.
      iii. Si E_t est de type III, alors E_{pt} est de type III^*. Le signe local en p passe de $(\frac{-2}{p})$ à $(\frac{-2}{p})$. On a $D_p = +1$.
      iv. Si E_t est de type I_m^*, alors E_{pt} est de type I_m. Le signe local en p passe de $(\frac{-1}{p})$ à $-\left(\frac{-b\lambda_{(p)}t}{p}\right)$. On a $D_p = -\left(\frac{b\lambda_{(p)}t}{p}\right)$.

   En résumé :

$I_0^* \leftrightarrow I_0$	$II \leftrightarrow IV^*$
$(\frac{-1}{p}) \xrightarrow{D_p=(\frac{-1}{p})} +1$	$(\frac{-1}{p}) \xrightarrow{D_p=\left(\frac{3}{p}\right)} (\frac{-3}{p})$
$III \leftrightarrow III^*$	$I_m^* \leftrightarrow I_m$
$(\frac{-2}{p}) \xrightarrow{D_p=+1} (\frac{-1}{p})$	$(\frac{-1}{p}) \xrightarrow{D_p=-\left(\frac{b\lambda_{(p)}t}{p}\right)} -\left(\frac{-b\lambda_{(p)}t}{p}\right).$

Le tableau suivant résume la situation.

	Conditions sur p		Valeur de $D_p(\lambda)$
$p \nmid \Delta_0$	$p \nmid \lambda$		$+1$
	$p \mid \lambda$		$(\frac{-1}{p})$
$p \mid \Delta_0$	$p \nmid \lambda$	réduction I_m	$(\frac{\lambda}{p})$
		réduction additive	$+1$
	$p \mid \lambda$	réduction I_0 ou I_0^*	$(\frac{-1}{p})$
		réduction II, II^*, IV, IV^*	$(\frac{3}{p})$
		réduction III, III^*	$+1$
		réduction I_m, I_m^*	$-\left(\frac{b\lambda_{(p)}t}{p}\right)$

3.1.6 Démonstration du théorème de variation

Notation 4. Nous utilisons une version spéciale du symbole de Jacobi dans cette section. Pour des entiers impairs a, b premiers entre eux, on écrit

$$\left(\frac{a}{b}\right)_c := \left(\frac{a'}{b'}\right)$$

où $a', b' \in \mathbb{Z}$ sont les parties respectives de a et de b premières à c.

Notation 5. Soit $t \in \mathbb{Z}$. Nous utiliserons fréquemment la notation $t_{(p)}$ pour désigner l'entier tel que $t_{(p)} = p^{-v_p(t)}t$.

Attention à ne pas les confondre avec t_1, t_2 qui sont définis autrement.

Soit, comme dans l'énoncé du théorème, E_t la courbe elliptique qui est la tordue par $t \in \mathbb{Z}$ de la courbe elliptique $E : y^2 = x^3 + ax + b$ de coefficients $a, b \in \mathbb{Z}$. On pose $\Delta_0 = 2^\alpha 3^\beta \Delta_1$, où α, β des entiers tels que $2 \nmid \Delta_1$ et $3 \nmid \Delta_1$, le discriminant de E que l'on suppose minimal parmi tous ses twists.

Remarquons que la fonction du signe peut s'écrire

$$W(E_t) = -W_2(E_t)W_3(E_t) \prod_{p|\Delta_1} W_p(E_t) \prod_{p|t; p\nmid\Delta_1} W_p(E_t),$$

et comme les seules places de mauvaise réductions sont de type I_0^*, on a

$$W(E_t) = -W_2(E_t)W_3(E_t) \left(\prod_{p|\Delta_1} W_p(E_t) \right) \left(\frac{-1}{t}\right)_{6\Delta_1}.$$

On peut supposer que t est un entier sans facteur carré. Par conséquent, E_t est minimale et on a alors $\Delta_{E_t} = \Delta_0 t^6$. On écrit $t = 2^\gamma 3^\delta t_1 t_2$ avec $t_2 = pgcd(\Delta_1, t)$ et t_1, t_2 non divisible par 2 et par 3.

On pourra écrire

$$W(E_t) = -W_2(E_t)W_3(E_t) \prod_{p|\Delta_1} W_p(E_t)\Big(\frac{-1}{t_1}\Big). \tag{3.1}$$

Démonstration de la propriété 1.

Le lemme 3.1.4 donne pour tout nombre premier p des entiers α_p pour lesquels $W_p(E_t) = Wp(E_{t'})$ pour tout $t \equiv t' \mod p^{\alpha_p}$. Si on pose $M = 2^{\alpha_2}3^{\alpha_3}\prod_{p|\Delta_1} p^{\alpha_p}$, le signe global est constant pour t et t' des entiers sans facteur carré qui sont dans la même classe de congruence modulo M.

Démonstration de la propriété 2.

Il reste à montrer que cette partition est non triviale, c'est-à-dire qu'il existe au moins une classe t_+ de signe positif et une classe t_- de signe négatif.

On définit l'ensemble $S = \{2, 3, p \text{ tel que } p|\Delta_0\}$. Soit t sans facteur carré qui n'est divisible par aucun $p \in S$. Pour les entiers $s \in \mathbb{Z}$ dont la partie sans facteur carré appartient à la classe de congruence $s' \mod M$, le signe de la fibre E_s sera le même que celui de E_t.

On cherche une classe de congruence $t_1 \mod M$ telle que $W(E_t) = -W(E_{t_1})$.

Soit λ un entier sans facteur carré et premier avec t. On considère $E_{\lambda t}$ la fibre en λt, qui est la tordue de E_t par λ.

Pour comparer $W(E_t)$ et $W(E_{\lambda t})$, nous comparons les signes locaux selon leur type de réduction de E_{t_0}.

Pour chaque nombre premier p, soit l'entier $D_p \in \{+1, -1\}$ tel que $W_p(E_{\lambda t}) = D_p W_p(E_t)$. Nous avons étudié les valeurs possibles de D_p en section 3.1.5.

Alors

$$W(E_{\lambda t}) = D_2 D_3 \Big(\frac{\lambda}{\Delta_M}\Big)\Big(\frac{-1}{\lambda_1}\Big)\Bigg(\prod_{p|\lambda; p|\Delta_0; p\neq 2,3} D_{p_0}\Bigg) W(E_t),$$

où Δ_M est le produit des nombres premiers $p \mid \Delta_0$ en lesquels la réduction de E est de type I_m et λ_1 est un entier premier avec Δ_0 tel que

$$\lambda = 2^{v_2(\lambda)} 3^{v_3(\lambda)} \lambda_0 \lambda_1.$$

où $\lambda_0 = \prod_{p|\Delta_0; p\neq 2,3} p^{v_p(\lambda)}$. On pose également $\lambda_{(2)}$, l'entier tel que $\lambda = 2^{v_2(\lambda)}\lambda_{(2)}$, c'est-à-dire que $\lambda_{(2)} = 3^{v_3(\lambda)}\lambda_0\lambda_1$. On peut réécrire

$$\Big(\frac{-1}{\lambda_1}\Big) = \Big(\frac{-1}{\lambda_{(2)}}\Big)(-1)^{v_3(\lambda)}\Big(\frac{-1}{\lambda_0}\Big).$$

On pose

$$C_2 = D_2\Big(\frac{-1}{\lambda_{(2)}}\Big),\ C_3 = D_3(-1)^{v_3(\lambda)},\ C_M = \Big(\frac{\lambda}{\Delta_M}\Big),\ C_0 = \prod_{p|\lambda; p|\Delta_0; p\neq 2,3} D_{p_0}$$

et

$$C = C_2\Big(\frac{-1}{\lambda_0}\Big) C_3 C_M C_0,$$

qui l'entier tel que $W(E_{\lambda t}) = CW(E_t)$.

1) Supposons que E possède des places de réduction multiplicative, c'est-à-dire que $\Delta_M \neq 1$. Soit p_0 un nombre premier qui ne divise pas Δ_0, qui n'est pas un carré modulo Δ_M et tel que $C_2(p_0) = +1$ et $C_3(p_0) = +1$. Un tel nombre premier existe par le lemme chinois. Pour ce p_0, on a bien $W(E_{p_0 t}) = -W(E_t)$.

2) Supposons qu'il existe un nombre premier p_0 qui ne divise pas Δ_0 tel que $C_2(p_0) = 1$. Alors par le lemme chinois, on peut choisir $p \nmid \Delta_0$ un nombre premier qui est dans la même classe d'équivalence modulo 2^{α_2} que p_0 et tel que $C_3 = C_M = +1$. Pour celui-ci, on aura $C_0 = +1$ et par conséquent,

$$W(E_t) = W(E_{\lambda t}).$$

3) D'un manière similaire au point précédent, on démontre que s'il existe $p_0 \nmid \Delta_0$ tel que $C_3 = -1$, alors on peut choisir $\lambda \nmid \Delta_0$ tel que $C_3 = C_M = C_0 = +1$ et que pour ce λ on a

$$W(E_t) = W(E_{\lambda t}).$$

4) On suppose que pour tout λ qui ne divise pas Δ_0, on a $C_2 = C_3 = C_M = +1$.

Les lemmes 3.1.5 et 3.1.6 permettent de constater que si C_2 est constant égal à $+1$, alors on peut supposer que $2 \nmid \Delta_0$. De même, si C_3 est constant égal à $+1$, on peut supposer que $3 \nmid \Delta_0$. On fait cette supposition, quitte à étudier plutôt une tordue par $\frac{1}{2}$ ou $\frac{1}{3}$. De ceci, on déduit qu'il existe une place de réduction de type I_m ou I_m^* sur la courbe $E : y^2 = x^3 + ax + b$ en un p_0 différent de 2 et 3. Comme on a supposé que $C_M = +1$, cette place en p_0 est de type I_m^*. Le tableau de la section 3.1.5 indique que $D_p = -(\frac{bt}{p_0})$.

Pour faire varier le signe, on étudie la tordue d'une fibre en des t tel que $t \equiv c_6 \mod p$ et qui sont premiers à $6\Delta_0$. Il existe une infinité de tels t. Dans ce cas, on a

$$\begin{aligned} W(E_{p_0 t}) &= D_0 W(E_t), && \text{par hypothèse que } C_2 = C_3 = C_M = +1 \\ &= -\left(\frac{c_6 t}{p_0}\right) W(E_t) = -\left(\frac{c_6^2}{p_0}\right) W(E_t) \\ &= -W(E_t). \end{aligned}$$

Ceci démontre que $\#W_{\pm}(E_t) = \infty$ pour tous les cas de $a, b \in \mathbb{Z}$.

3.2 Surfaces de la forme $y^2 = x^3 + A(T)x$ ou $y^2 = x^3 + B(T)$

Les surfaces elliptiques d'invariant $j = 0$ (respectivement $j = 1728$) ont un comportement différent du cas général, car on retrouve des places génériques dont la réduction est de type II, II^* IV ou IV^* (respectivement III ou III^*).

3.2.1 Théorème de variation pour les surfaces telles que $j = 0$

Pour chaque $t \in \mathbb{Z} - \{0\}$, on pose la courbe $E_t : y^2 = x^3 + t$.

Théorème 3.2.1. *Soit t est un entier sans facteur qui soit une puissance sixième.*

Soit $t = 2^\alpha 3^\beta t_1^1 t_2^2 t_3^3 t_4^4 t_5^5$, où $\alpha = v_2(t)$, $\beta = v_3(t)$ et $t_i \in \mathbb{N}$ $i = 1, \cdots, 5$ sont premiers entre eux et sans facteur carré. Posons $\tau_1 = t_1 t_3 t_5$ et $\tau_2 = t_2 t_4$.

Alors le signe peut s'exprimer sous la forme

$$W(E_t) = -W_2(E_t) W_3(E_t) (\frac{-1}{\tau_1}) (\frac{\tau_2}{3}).$$

De plus, il existe des entiers $M_1 = 2^7 3^7$ et $M_2 = 3$ tels que $W(E_t)$ est constant pour les t sans puissance sixième dont la partie τ_1 varie dans une classe de congruence modulo M_1 et dont la partie τ_2 varie dans une classe de congruence modulo M_2.

Il existe des (doubles) classes de t pour lesquelles $W(E_t) = +1$, et d'autres classes pour lesquelles $W(E_t) = -1$.

Démonstration. Soit la famille de courbe elliptique $E_t : y^2 = x^3 + t$ indexée par la variable t.

Nous supposons t sans puissance sixième, c'est-à-dire que pour tout p, $p^6 \nmid t$. La formule du signe s'écrit

$$W(E_t) = -W_2(E_t) W_3(E_t) \prod_{p|t,\ p \neq 2,3} W_p(E_t).$$

Comme auparavant, nous simplifierons les notations en écrivant $W_p(t)$ plutôt que $W_p(E_t)$. Les formules pour les signes locaux en 2 et en 3 sont rappelées en appendice de ce chapitre.

Le signe local en 2 est constant sur une classe d'équivalence modulo 2^7 et que le signe local en 3 est constant sur une classe d'équivalence modulo 3^7.

Étudions à présent la partie produit de la formule du signe, c'est-à-dire

$$\mathscr{P}(t) = \prod_{p|t,\ p\neq 2,3} W_p(E_t).$$

D'après la proposition [38, Prop. 2], nous avons dans ce cas-ci la formule suivante

$$\mathscr{P}(t) = \prod_{p|t,p\neq 2,3} \begin{cases} +1 & \text{si } v_p(t) \equiv 0 \mod 6; \\ (\frac{-1}{p}) & \text{si } v_p(t) \equiv 1,3,5 \mod 6; \\ (\frac{-3}{p}) & \text{si } v_p(t) \equiv 2,4 \mod 6. \end{cases}$$

Soit, $t = 2^\alpha 3^\beta t_1 t_2^2 t_3^3 t_4^4 t_5^5$ où t_i sont premiers entre eux et divisibles ni par 2 ni par 3. On pose $\tau_1 = t_1 t_3 t_5$ et $\tau_2 = t_2 t_4$.

Alors on sépare $\mathscr{P}$ en deux parties, selon si $p|\tau_1$ ou $p|\tau_2$.

$$\begin{aligned} \mathscr{P} &= \prod_{p|\tau_1} W_p(E_t) \prod_{p|\tau_2} W_p(E_t) \\ &= \prod_{p|\tau_1} (\frac{-1}{p}) \prod_{p|\tau_2} (\frac{-3}{p}) \\ &= (\frac{-1}{\tau_1})(\frac{-3}{\tau_2}) = (\frac{-1}{\tau_1})(\frac{\tau_2}{3}) \end{aligned}$$

Ainsi, on trouve que la formule du signe est

$$W(E_t) = -W_2(E_t)W_3(E_t)(\frac{-1}{\tau_1})(\frac{\tau_2}{3}).$$

Le signe dépend donc des valeurs de t modulo $2^7 3^7$ et de τ_2 modulo 3. Notons qu'il est possible de trouver une infinité de paires de t de signes opposés. En effet, prenant $t \equiv C \mod 2^7 3^7$, on peut, en substituant τ_2 par un entier τ_2' premier à $6\tau_1$ et tel que $\tau_2' \equiv -\tau_2 \mod 3$, définir $t' = 2^\alpha 3^\beta t_1 \tau_2'$ dont le signe est opposé à celui de t.

□

Remarque 53. On peut également déduire cette formule du théorème 2.3.2 en remarquant qu'une place mauvaise sur $\mathscr{E}$ est de type II, II^*, IV, IV^* ou I_0^*.

Remarque 54. L'article [51] de Várilly-Alvarado donne des exemples de surfaces dont le signe demeure constant :

$$y^2 = x^3 + 6(27t^6 + 1) \tag{3.2}$$

et

$$y^2 = x^3 + 27t^6 + 16. \tag{3.3}$$

Pour la surface 3.3, on considère pour toute fibre E_t en $t = \frac{m}{n} \in \mathbb{Q}$ la courbe suivante qui lui est isomorphe sur $\mathbb{Q}$:

$$E_{m,n} : y^2 = x^3 + 27m^6 + 16n^6.$$

On remarque qu'on a $-3 \equiv (4m^3/3n^3)^2 \mod p$ et donc $\left(\frac{-3}{p}\right) = 1$ pour tout $p|f(t)$. La formule devient alors

$$W(E_t) = -W_2(E_t)W_3(E_t)\left(\frac{-1}{(27m^6+16n^6)_2}\right).$$

De plus, pour toute valeur de t, le reste modulo 3 de $27m^6 + 16n^6$ est 1.

Toutefois, il est possible de trouver une valeur de M_1 inférieur à celle donnée par le théorème, c'est à dire $M_1 = 2^7 3^7$. Celle si sera $M_1' = 2^4 3^0 = 16$. La valeur minimale de M_2 reste 3.

Or, on remarque que $27m^6 + 16n^6$ tombe dans les classes d'équivalence $1, 11 \mod 16$. Ces valeurs correspondent à un signe positif.

3.2.2 Théorème de variation pour les surfaces elliptiques telles que $j = 1728$

Pour tout $t \in \mathbb{Z} - \{0\}$, on pose la courbe $E_t : y^2 = x^3 + tx$.

Théorème 3.2.2. *Soit t est un entier sans facteur qui soit une puissance quatrième.*

Soit la décomposition $t = 2^\alpha 3^\beta t_1^1 t_2^2 t_3^3$, avec les t_i premiers entre eux et sans facteur carré. On pose $\tau_1 = t_1 t_3$.

Alors le signe peut s'écrire

$$W(E_t) = -W_2(E_t)W_3(E_t)\left(\frac{-2}{\tau_1}\right)\left(\frac{-1}{t_2}\right).$$

De plus, il existe des entiers $M_1 = 2^5 3^5$ et $M_2 = 4$ tels que $W(E_t)$ est constant, pour t sans puissance quatrième dont la partie τ_1 varie dans une classe de congruence modulo M_1 et dont la partie t_2 varie dans une classe de congruence modulo M_2.

Il existe des classes de t pour lesquelles $W(E_t) = +1$, et d'autres classes pour lesquelles $W(E_t) = -1$.

Démonstration. Soit la famille de courbe elliptique $E_T : y^2 = x^3 + Tx$ indexée par la variable T.

Nous supposons que t est un entier sans facteur de degré 4. La formule du signe s'écrit alors

$$W(E_t) = -W_2(E_t)W_3(E_t) \prod_{p|t,\ p\neq 2,3} W_p(E_t).$$

Dorénavant, pour simplifier les notations, nous écrirons $W_p(t)$ plutôt que $W_p(E_t)$. Les formules pour les signes locaux en 2 et en 3 sont données par le lemme [51, Lemme 4.7].

Nous avons des conditions sur $v_2(t)$ modulo 4 et sur t_2 modulo 16 qui déterminent le signe local en 2.

Par exemple, la classe des $t \equiv 8 \mod 16$, qui représente les t tels que $v_2(t) = 3$, contient tout aussi bien les t tels que $t_2 \equiv 1 \mod 16$ que les $t_2 \equiv 5 \mod 16$ qui n'ont pas le même signe local en 2. Cependant, modulo 2^6, nous faisons la différence entre tous ces cas. Le signe local en 2 sera donc constant sur une classe de congruence modulo 2^6. Le signe local en 3, quant à lui, sera fixé sur une classe de congruence modulo 3^4.

Étudions à présent la partie produit de la formule du signe, c'est-à-dire

$$\prod_{p|t,p\neq 2,3} W_p(E_t). \tag{3.4}$$

D'après la proposition [38, Prop. 2], nous avons dans ce cas-ci la formule suivante

$$\prod_{p|t,p\neq 2,3} W_p(E_t) = \prod_{p|t,p\neq 2,3} \begin{cases} +1 & \text{si } v_p(t) \equiv 0 \mod 4; \\ (\frac{-1}{p}) & \text{si } v_p(t) \equiv 2 \mod 4 \\ (\frac{-2}{p}) & \text{si } v_p(t) \equiv 1, 3 \mod 4. \end{cases}$$

Soit $t = 2^\alpha 3^\beta t_1 t_2^2 t_3^3$, où t_i sont premiers entre eux et divisibles ni par 2 ni par 3. On pose $\tau_1 = t_1 t_3$.

Alors on peut écrire $t = 2^\alpha 3^\beta \tau_1 t_2$ et on sépare (3.4) en deux parties, selon si $p|\tau_1$ ou $p|t_2$.

$$\begin{aligned}(3.4) &= \prod_{p|\tau_1} W_p(E_t) \prod_{p|t_2} W_p(E_t) \\ &= \prod_{p|\tau_1} (\frac{-2}{p}) \prod_{p|t_2} (\frac{-1}{p})) \\ &= \Big(\frac{-2}{\tau_1}\Big)\Big(\frac{-1}{t_2}\Big). \\ &= \Big(\frac{-2}{\tau_1}\Big)\Big(\frac{-1}{t_2}\Big).\end{aligned}$$

Cela implique que le signe s'écrit

$$W(E_t) = -W_2(E_t)W_3(E_t)\Big(\frac{-2}{\tau_1}\Big)\Big(\frac{-1}{t_2}\Big).$$

Sa valeur dépend donc de la valeur de τ_1 modulo $2^6 3^4$ et de t_2 modulo 4.

□

Remarque 55. On peut également déduire cette formule du théorème 2.3.2 en remarquant qu'une place mauvaise sur $\mathscr{E}$ est de type III, III^* ou I_0^*.

Remarque 56. Dans l'article de Cassels et Schinzel [3], on démontre que les surfaces elliptiques définies par

$$y^2 = x(x^2 - (1+t^4)^2) \tag{3.5}$$

et

$$y^2 = x(x^2 - 7^2(1+t^4)^2) \tag{3.6}$$

sont telles que toutes les fibres en $t \in \mathbb{Q}$ sont de même signe. Sur 3.5, le signe toujours positif et sur 3.6, toujours négatif.

Remarquons qu'il est possible de trouver une valeur de M_1 inférieure à celle donné par le théorème. Celle-ci sera $2^4 3^2 = 144$.

Les seules valeurs que peut prendre le reste $-(1+t^4)^2 \mod 16$ sont -1 et -4, et l'unique valeur du reste modulo 9 est -1. Grâce au théorème des restes chinois, on trouve une petite quantité de valeurs possibles modulo 144 possible pour le reste de $-(1+t^4)^2$, et le signe qui leur est associé est $+1$.

Pour la surface 3.5, on ne peut rien conclure sur la densité des points rationnels. Pour 3.6 toutefois, le signe est négatif pour les classes possibles que peuvent prendre $-7^2(1+t^4)^2$. En supposant vraie la conjecture de parité, on peut en déduire que les points rationnels de (3.6) est dense.

3.2.3 Formule des signes locaux en 2 et en 3

Voici les formules des signes locaux en 2 et en 3 pour les cas (A) et (B) de familles de twists telles que décrites dans les lemmes 4.7 et 4.1 de Várilly-Alvarado [51]. Nous en aurons besoin dans le chapitre 4, section 4.2.3, 4.2.4 pour calculer les signes locaux W_2 et W_3.

Lemme 3.2.3. *[51, Lemme 4.7]*

Soit t un entier non nul et la courbe elliptique $E_t : y^2 = x^3 + tx$ dont on note $W_2(t)$ et $W_3(t)$ les signes locaux en 2 et en 3. On pose t_2 et t_3 comme étant les entiers tels que $t = 2^{v_2(t)}t_2 = 3^{v_3(t)}t_3$. Alors

$$W_2(t) = \begin{cases} -1 & \text{si } v_2(t) \equiv 1 \text{ ou } 3 \mod 4 \text{ et } t_2 \equiv 1 \text{ ou } 3 \mod 8; \\ & \text{ou si } v_2(t) \equiv 0 \mod 4 \text{ et } t_2 \equiv 1, 5, 9, 11, 13 \text{ ou } 15 \mod 16; \\ & \text{ou si } v_2(t) \equiv 2 \mod 4 \text{ et } t_2 \equiv 1, 3, 5, 7, 11, \text{ ou } 15 \mod 16; \\ +1 & \text{sinon.} \end{cases}$$

$$W_3(t) = \begin{cases} -1 & \text{si } v_3(t) \equiv 2 \mod 4; \\ +1 & \text{sinon.} \end{cases}$$

Lemme 3.2.4. *[51, Lemme 4.1]*

Soit t, un entier non nul et la courbe elliptique $E_t : y^2 = x^3 + t$ dont on note $W_2(t)$ et $W_3(t)$ les signes locaux en 2 et en 3. On pose t_2 et t_3 comme étant les entiers tels que $t = 2^{v_2(t)}t_2 = 3^{v_3(t)}t_3$. Alors

$$W_2(t) = \begin{cases} -1 & \text{si } v_2(t) \equiv 0 \text{ ou } 2 \mod 6; \\ & \text{ou si } v_2(t) \equiv 1, 3, 4 \text{ ou } 5 \mod 6 \text{ et } t_2 \equiv 3 \mod 4; \\ +1, & \text{sinon.} \end{cases}$$

$$W_3(t) = \begin{cases} -1 & \text{si } v_3(t) \equiv 1 \text{ ou } 2 \mod 6 \text{ et } t_3 \equiv 1 \mod 3; \\ & \text{ou si } v_3(t) \equiv 4 \text{ ou } 5 \mod 6 \text{ et } t_3 \equiv 2 \mod 3; \\ & \text{ou si } v_3(t) \equiv 0 \mod 6 \text{ et } t_3 \equiv 5 \text{ ou } 7 \mod 9; \\ & \text{ou si } v_3(t) \equiv 3 \mod 6 \text{ et } t_3 \equiv 2 \text{ ou } 4 \mod 9; \\ +1, & \text{sinon.} \end{cases}$$

4

Surfaces elliptiques rationnelles

4.1 Rappels sur les surfaces de Del Pezzo de degré 1

Une *surface de Del Pezzo* est une surface algébrique projective lisse X dont le diviseur anticanonique $-K_X$ est ample. Le *degré* de cette surface est le nombre d'autointersection de K_X. C'est un entier $1 \leq d \leq 9$.

Comme on l'a vu dans les sections 1.2.8, chaque surface de Del Pezzo de degré 1 est isomorphe à une hypersurface lisse de degré 6 dans $\mathbb{P}(1,1,2,3)$. Réciproquement, une hypersurface lisse de degré 6 dans cet espace à poids est isomorphe à une surface de Del Pezzo de degré 1.

Ce résultat décrit dans le livre de Kollar [21, p.174] démontre que la surface X peut être représentée par une équation de la forme

$$w^2 = z^3 + F(x,y)z + G(x,y), \tag{4.1}$$

où F et G sont des polynômes homogènes de degrés respectivement 4 et 6 et les coordonnées $[x,y,z,w]$ sont prises dans l'espace projectif à poid $\mathbb{P}(1,1,2,3)$.

En section 1.2.9, on explique qu'il y a un point rationnel canonique sur X, l'unique point base du système linéaire anticanonique $-K_X$. Sur l'équation 4.1, il s'agit du point $[x,y,z,w] = [0,0,1,1]$. En éclatant ce point, on obtient une surface elliptique rationnelle lisse d'équation de Weierstrass

$$y^2 = x^3 + F(t,1)x + G(t,1).$$

Dans la section 1.2.10, on calcule les points singuliers des surfaces elliptiques rationnelles et on en déduit la proposition suivante :

Proposition 4.1.1. *Soit $\mathscr{E}$ une surface elliptique rationnelle et un modèle minimal de Weierstrass $y^2 - x^3 + A(t)x + B(t)$, où $A, B \in \mathbb{Z}[t]$ sont des polynômes de degré respectivement 4 et 6.*

On note X la surface obtenue de $\mathscr{E}$ par la contraction de la section à l'infini.

Alors X est une surface de Del Pezzo de degré 1 si et seulement si les places de $\mathscr{E}$ sont de type II ou I_1.

4.2 Densité des points rationnels sur des surfaces rationnelles isotriviales

Les surfaces elliptiques rationnelles isotriviales sont de l'une des formes suivantes

1. $y^2 = x^3 + aH(T,1)^2x + bH(T,1)^3$, avec $a, b \in \mathbb{Z}$ tels que $4a^3 + 27b^2 \neq 0$ (telles que $j(T) \in \mathbb{Q}/\{0, 1728\}$),
   Remarque 57. Une surface de cette forme est birationnelle à la surface
   $$H(T,1)y^2 = x^3 + ax + b.$$
2. $y^2 = x^3 + A(T,1)x$ (telles que $j(T) = 1728$),
3. $y^2 = x^3 + B(T,1)$ (telles que $j(T) = 0$)

où A, B, et H sont des polynômes homogènes de degré respectivement 2, 4 et 6.

On suppose également dans les équations précédentes que H n'est pas un carré, que A n'est pas un bicarré et que B n'est pas une puissance sixième. En effet, cela équivaut à éviter le cas trivial où il existe une courbe E_0 telle que

$$\mathscr{E} = E_0 \times \mathbb{P}^1,$$

car alors

1. le signe est automatiquement constant,
2. si $E_0(\mathbb{Q})$ est fini, alors $\mathscr{E}(\mathbb{Q})$ n'est pas dense.

Remarque 58. On déduit du lemme 4.1.1 que les surfaces elliptiques rationnelles isotriviales (non triviales) des formes $y^2 = x^3 + H(t)^2x + H(t)^3$ et $y^2 = x^3 + A(t)x$ ne vérifient pas ces propriétés. La contraction de la section neutre ne donne en aucun de ces cas une surface de Del Pezzo de degré 1.

Cependant, une surface elliptique rationnelle isotriviale de la forme $y^2 = x^3 + B(t)$ avec $\deg B \geq 5$ et sans racine double respecte les critères. Par conséquent, la contraction de sa section neutre est une surface de Del Pezzo de degré 1.

4.2.1 Surfaces avec $j(T) \neq 0, 1728$: unirationalité

Théorème 4.2.1. *Soit $\mathscr{E}$ une surface rationnelle isotriviale d'équation*

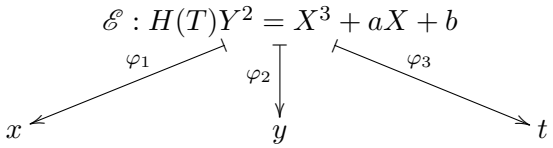
$$\mathscr{E} : Y^2 = X^3 + aH(T)^3X + bH(T)^2,$$

où $a, b \in \mathbb{Z}\backslash\{0\}$ et $H(T)$ est un polynôme de degré ≤ 2 qui n'est pas un carré.

Alors la surface est unirationnelle sur $\mathbb{Q}$. En particulier, ses points rationnels sont denses pour la densité de Zariski.

Remarque 59. Ce résultat est démontré par Rohrlich [38, Theorème 3] sous l'hypothèse *a priori* restrictive qu'il existe une fibre de rang non nul. Cette hypothèse est enlevée ici.

Démonstration. Remarquons qu'on peut munir la surface $\mathscr{E}$ de plusieurs fibrations.



Les deux dernières, φ_2 et φ_3, sont des fibrations en courbes elliptiques. Bien que la fibration définie par φ_3 soit isotriviale, celle définie par φ_2 ne l'est pas.

En effet, si on écrit $H(T) = \alpha_2T^2 + \alpha_1T + \alpha_0$ pour les coefficients α_i appropriés, la fibration φ_2 a pour fibre

$$\mathscr{E}_y := \alpha_2y^2T^2 + \alpha_1y^2T = X^3 + aX + b - \alpha_0y^2$$

qui peut, par changement de variables (d'abord avec $T' = \alpha_2^2 yT$ et $x = \alpha_2 X$, puis $t = T' + \frac{\alpha_1\alpha_2 y}{2}$), s'écrire

$$\mathscr{E}_y : t^2 = x^3 - 27c_4(y)x - 54c_6(y)$$

où $c_4(y) = \alpha_2^2 a$ et $c_6(y) = (\alpha_2^3\alpha_0 + \frac{\alpha_1^2\alpha_2^2}{4})y^2 + \alpha_2^3 b$.

En calculant l'invariant j, on voit que cette courbe n'est pas isotriviale, hormis dans les cas où $a = 0$ ($c_4(y)$ est nul) et $\alpha_0 = \alpha_2^3\alpha_0 + \frac{1}{4}\alpha_1^2\alpha_2^2$, c'est-à-dire lorsque H est le carré d'un polynôme linéaire (dans ce cas, $\mathscr{E}$ est triviale). Ces cas sont exclus par hypothèse.

Par conséquent, on peut appliquer le théorème 1.2.11, dû à Kollár et Mella, qui démontre l'unirationalité de $\mathscr{E}$ muni de la fibration elliptique φ_2.

□

Remarque 60. Dans une première version de l'article de Kollár-Mella [23], le théorème 1.2.11 excluait le cas isotrivial. Le théorème 4.2.1 avait pour motivation de compléter ce résultat. Cependant, le temps du dépôt de cette thèse, le résultat était complété par Kollár et Mella eux-même. Leur méthode diffère toutefois de la notre, qui utilise la fibration non-isotriviale φ_2.

Remarque 61. Une autre approche pour démontrer le théorème 4.2.1 aurait été l'utilisation des travaux de Colliot-Thélène [**?**]. Le théorème 2 de cet article démontre que pour X, une surface fibrée en coniques de degré 4, l'obstruction de Brauer-Manin au principe de Hasse est la seule obstruction. Pour déduire de ceci le théorème 4.2.1, il faudrait vérifier que le groupe de Brauer des surfaces étudiées (d'équation $h(t)y^2 = x^3 - ax$ où $\deg h = 2$) est bien réduit au groupe de Brauer de $\mathbb{Q}$.

4.2.2 Surfaces avec $j(T) = 1728$: point d'ordre infini

Nous étudions à présent les surfaces elliptiques rationnelles isotriviales de la forme $y^2 = x^3 + xA(T)$ où $A \in \mathbb{Z}[T]$ est un polynôme tel que $\deg A \leq 4$.

La densité des points rationnels sur celles-ci est facilement démontrable lorsque $\deg A \leq 3$. Nous nous intéressons donc aux surfaces telles que $\deg A = 4$. On pose $a_4, a_3, a_2, a_1, a_0 \in \mathbb{Z}$ les coefficients tels que

$$A(T) = a_4T^4 + a_3T^3 + a_2T^2 + a_1T + a_0.$$

Dans un premier temps, remarquons que $F(T) = a_4\left((T^2 + g_1T + g_0)^2 + h_1T + h_0\right)$, pour les constantes

$$g_0 = \frac{4a_2a_4 - a_3^2}{8a_4^2},\ g_1 = \frac{a_3}{2a_4},\ h_0 = \frac{2^6a_4^3(a_0 + x^2) - (4a_2a_4 - a_3^2)^2}{2^6a_4^4}$$

et

$$h_1 = \frac{2^3a_1a_4^2 - a_3(4a_2a_4 - a_3^2)}{2^3a_4^3}.$$

Remarquons ce qui se produit lorsqu'on procède au changement de variables $T' = T - g_1/2$.

On a

$$T'^4 = T^4 + \frac{g_1}{2}T^3 + \frac{6g_1^2}{4}T^2 + \frac{g_1^3}{2}T + \frac{g_1^4}{16}$$

Par conséquent on peut écrire

$$F(T) = a_4(T'^4 + (\frac{-g_1^2}{2} + 2g_0)T^2 + (\frac{-g_1^3}{2} + 2g_1g_0)T + (\frac{-g_1^4}{2^4} + g_0^2 + h_0)).$$

En remplaçant T^2 et T par leurs expressions en fonction de T', on obtient l'équation suivante :

$$y^2 = x^3 + a_4x(T'^4 + A_2T'^2 + A_1T' + A_0),$$

où

$$A_2 = (g_0 - \frac{g_1^2}{2}),$$

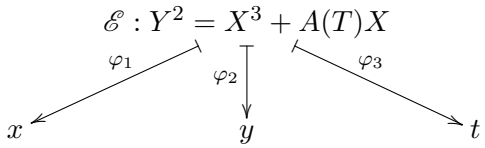
$$A_1 = (\frac{g_1^3}{2} + a_2g_1)$$

et

$$A_0 = (-\frac{g_1^4}{2^4} + g_0^2 + h_0).$$

Par conséquent, on peut supposer que $a_3 = 0$ par le changement de variables expliqué précédemment.

On peut munir la surface $\mathscr{E}$ des fibrations suivantes.



La fibration initiale est φ_3. Pour $\mathscr{E}$, $\varphi_1 : (x, y, t) \mapsto x$ est une fibration en courbes de genre 1 (a priori sans section). L'équation de la fibre en x s'écrit sous cette forme :

$$C_x : y^2 = a_4xt^4 + a_2xt^2 + a_1xt + (a_0x + x^3).$$

C'est une courbe de genre 1 avec deux points à l'infini, notés ∞_+ et ∞_-, qui sont rationnels si et seulement si $x \in a_4\mathbb{Q}^{*2}$.

Proposition 4.2.2. *Soit $P_x = cl((\infty_+) - (\infty_-)) \in C_x(\mathbb{Q})$ pour $x \in a_4\mathbb{Q}^{*2}$.*
Alors,
— *si $a_1 = 0$, le point P_x est d'ordre 2,*
— *si $a_1 \neq 0$, P_x est d'ordre infini (sauf pour un nombre fini d'exceptions).*

Démonstration. Explicitement, si on pose $u = \frac{1}{t}$ et $v = \frac{y}{t^2}$, on a en coordonnée (u, v) :

$$\infty_+ = (0, b), \text{ et } \infty_- = (0, -b).$$

Supposons que $b^2 = a_4x$ pour un certain rationnel b. On écrit

$$C_x : y^2 = b^2t^4 + a_2xt^2 + a_1xt + a_0x + x^3.$$

On procède au changement de variables $Y = \frac{y}{\sqrt{a_4x}}$, pour obtenir l'équation :

$$C_x : Y^2 = T^4 + \frac{a_2}{a_4}T^2 + \frac{a_1}{a_4}T + \frac{a_0 + x^2}{a_4}.$$

Par conséquent, on peut écrire le côté droit de l'équation sous la forme suivante :

$$G(T)^2 + H(T),$$

où

$$G(T) = T^2 + g_0$$
$$H(T) = h_1T + h_0,$$

et où les g_j et les h_j sont donnés en termes des a_i. Explicitement, on a

$$g_0 = \frac{a_2}{2a_4},\ h_0 = \frac{2^2 a_4(a_0 + x^2) - a_2^2}{2^2 a_4^2}$$

et

$$h_1 = \frac{a_1}{a_4}.$$

L'équation de la courbe s'écrit

$$(Y + G(T))(Y - G(T)) = H(T). \tag{4.2}$$

On pose $Y + G(T) = R$, de façon à ce que

$$Y - G(T) = \frac{H(T)}{R}$$

et que

$$2G(T) = R - \frac{H(T)}{R}.$$

On pose de plus $RT = S$.

En multipliant l'équation (4.2) par R, on obtient

$$2S'^2 + 2g_0R'^2 = R'^3 - h_1S' - h_0R'. \tag{4.3}$$

Finalement, on procède au changement de variable $(R, S) = (2R', 2S')$ pour obtenir l'équation de Weierstrass générale suivante pour C_x. Ces changements de variables sont aussi décrits dans la section 1.1.3.

$$C_x : S^2 + \frac{h_1}{4}S = R^3 - g_0R^2 - \frac{h_0}{4}R. \tag{4.4}$$

Étudions vers quels points de cette nouvelle courbe sont envoyés les deux points à l'infini ∞_+ et ∞_- mentionnés précédemment. On commence par regarder la coordonnée en R de ceux-ci.

On a

$$2R = R' = Y + G(T) = \frac{y}{b} + T^2 + g_o.$$

Posons $T = \frac{1}{u}$ et $y = vT^2 = \frac{v}{u^2}$ car il sera alors plus facile d'étudier les pôles. On a

$$\begin{aligned} 2R &= \frac{v}{u^2 b} + \frac{1}{u^2} + g_0 \\ &= \frac{uv + b + g_0 u^2 b}{bu^2}. \end{aligned}$$

Pour ∞_+, on a $(u, v) = (0, b)$ et pour ∞_-, on a $(u, v) = (0, -b)$. Par conséquent, on a

$$R(\infty_+) = \infty \text{ (c'est un pôle), et } R(\infty_-) = 0.$$

À présent, étudions la valeur de leurs coordonnées en S.

Remarquons que

$$\begin{aligned} y^2 &= G(T)^2 + H(T) \\ \Rightarrow (\frac{v}{u^2 b}) &= G\left(\frac{1}{u}\right)^2 + H\left(\frac{1}{u}\right) \end{aligned}$$

$$\Rightarrow \left(\frac{v}{u^2b} - G\left(\frac{1}{u}\right)\right)\left(\frac{v}{u^2b} + G\left(\frac{1}{u}\right)\right) = H(\frac{1}{u})$$

$$\Rightarrow \left(\frac{v}{u^2b} + G(\frac{1}{u})\right) = \frac{H(\frac{1}{u})u^2b}{v - u^2G(\frac{1}{u})b} = \frac{ub(h_1 + h_0u)}{v(v - b - g_0u^2)}$$

$$\begin{aligned} 2S = S' &= T(Y + G(T)) \\ &= \frac{ub(h_1 + h_0u)}{v(v - b - g_0u^2)} \end{aligned}$$

Par conséquent, on a

$$S(\infty_+) = \infty \text{ et } S(\infty_-) = -\frac{h_1}{4}$$

Remarquons qu'il s'agit des deux points évidents sur la courbe 4.4. On pose de façon naturelle le point obtenu de ∞_+ comme point marqué de la courbe C_x, c'est-à-dire comme l'élément neutre de la loi de groupe de l'ensemble des points rationnels. On a dans cette configuration $(0, -\frac{h_1}{4}) = [-1](0, 0)$.

Dans un premier temps, on déduit que si $h_1 = \frac{a_1}{a_4} = 0$, on a que le point $(0, -\frac{h_1}{4})$ est d'ordre 2. Par la suite, on étudiera l'ordre de $Q = (0, 0)$ dans le cas où $h_1 \neq 0$. On remarque que son ordre sera le même que celui du point provenant de ∞_-.

On utilisera la proposition 1.1.3, un résultat de Lutz et Nagell présenté dans la section 1.1.2. Celle-ci dit que si $E/\mathbb{Q}$ une courbe elliptique d'équation de Weierstrass $y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Z}$ et que $P \in E(\mathbb{Q})$ est un point de torsion différent du point à l'infini, alors les propriétés suivantes sont vérifiées :

1. $x(P), y(P) \in \mathbb{Z}$.
2. On a ou bien $[2]P = O$ ou bien $x([2]P) \in \mathbb{Z}$.

Pour utiliser ce théorème, il faut commencer par s'assurer que les coefficients de la courbe elliptique que nous considérons (notons les A_i) sont bien entiers. Comme les coefficients de C_x ne sont pas forcément entier, on choisira un entier α approprié qui rend le modèle entier.

On pose u et v des entiers premiers entre eux tels que $x = \frac{u}{v}$. Si on pose $\alpha = 2 \cdot a_4 v$, les coefficients de la courbe suivante sont entiers

$$C'_x : S^2 + \alpha^3 \frac{h_1}{4} S = R^3 - \alpha^2 g_0 R^2 - \alpha^4 \frac{h_0}{4} R.$$

(En réalité, il est suffisant de prendre $\alpha = 2a_4 w$ où w est un entier tel que $v^2 \mid w$.)

On va montrer que si $h_1 \neq 0$, le point Q n'est pas de 2-torsion pour une infinité de valeurs de x. On étudie quand $R([2]Q)$ est entier. Pour tout $P \in C_x(\mathbb{Q})$, on a

$$R([2]P) = \Big(\frac{3R(P)^2 - 2\alpha^2 g_0 R(P) - \alpha^4 \frac{h_0}{4}}{2S(P) + \frac{h_1}{4}\alpha^3}\Big)^2 - 2R(P) + \alpha^2 g_0.$$

On a donc

$$R([2]Q) = \Big(\frac{4\alpha^4 h_0}{4\alpha^3 h_1}\Big)^2 + 4\alpha^2 g_0.$$

Pour que cette coordonnée soit entière, il faut que $\alpha^3 h_1$ divise $\alpha^4 h_0$.

Rappelons que $x = \frac{u}{v}$ pour des $u, v \in \mathbb{Z}$ premiers entre eux. On a

$$\alpha^4 h_0 = A\left(\frac{u}{v}\right)^2 + B,$$

où $A = 2^4 a_4^3 v^4$ et $B = 2^4 a_4^3 a_0 u^4 - 2^2 a_4^2 a_2^2 v^4$.

Quant à $\alpha^3 h_1$, c'est un entier de valeur

$$\alpha^3 h_1 = 2^3 a_4^2 a_1 v^3.$$

Si on a $\alpha^3 h_1 \mid \alpha^4 h_0$ pour tout $x \in \mathbb{Q}^{2*} a_4$, alors $\alpha^3 h_1$ divise B (on obtient ceci en prenant $x = (\alpha^3 h_1)^2 a_4$ par exemple). Par conséquent, $\alpha^3 h_1$ divise Ax^2 pour tout choix de x. Choisissons v premier à $2a_4$. Dans ce cas, on a une contradiction car $Ax^2 = 2^3 a_4^2 v^2 (2a_4 u)$ doit être divisible par $2^3 a_4^2 a_1 v^3$, mais v est supposé premier à $2a_4$ et à u. Cette contradiction montre que pour tout $x \in \mathbb{Q}^{2*} a_4$ dont le dénominateur est premier avec $2a_4$, le point Q est d'ordre infini sur la courbe C_x.

Nous complètons la démonstration grâce au théorème de spécialisation de Silverman (voir [46] et [45, Théorème 11.4, Chapitre III]). A priori, la fibration

$$\begin{aligned} \varphi_2 \colon \mathscr{E} &\to \mathbb{P}^1 \\ (x, y, t) &\mapsto x. \end{aligned}$$

n'est pas une surface elliptique sur $\mathbb{Q}$. Cependant, considérons l'application

$$\begin{aligned} \phi \colon \mathbb{P}^1 &\to \mathbb{P}^1 \\ z &\mapsto x = a_4 z^2. \end{aligned}$$

et le produit fibré $\mathscr{E}'$ de $\mathscr{E}$ par rapport à celle-ci. Par l'argument précédent, $\mathscr{E}'$ possède deux sections ∞_+ et ∞_-. C'est donc une surface elliptique sur $\mathbb{Q}$. Choisissons comme section canonique ∞_+.

Si il existe un changement de variable linéaire tel que $A = A_4 T'^4 + A_2 T^2 + A_0$, alors ∞_- est un point de torsion sur toute fibre en $x = az^2$ de $\mathscr{E}$. Par conséquent, la section $\infty_+(z)$ est de torsion pour tout z.

S'il n'existe pas de tel changement de variable, alors le point ∞_- est d'ordre infini pour une infinité de fibres de $\mathscr{E}$. Par conséquent, le théorème de spécialisation de Silverman garantit que $\infty_-(z)$ est d'ordre infini sur toute fibre de $\mathscr{E}'$ sauf un nombre fini d'entre elles. □

On déduit directement de cette proposition le théorème suivant :

Théorème 4.2.3. *Soit $\mathscr{E}$ une surface elliptique rationnelle d'équation*

$$\mathscr{E} : T^2 = X^3 + A(T)X,$$

où $A(T)$ est un polynôme de degré 4 à coefficients entiers.

On suppose qu'il n'existe pas de changement de variables linéaires $T \to T' + b$ tel que A est de la forme

$$A(T') = A_4 T'^4 + A_2 T'^2 + A_0,$$

où $A_4, A_2, A_0 \in \mathbb{Z}$.

Alors, les points rationnels de $\mathscr{E}$ sont denses pour la topologie de Zariski.

Remarque 62. Les surfaces qui ne sont pas traitées par ce théorème sont de la forme :

$$y^2 = x^3 + x(a_4 T^4 + 4ba_4 T^3 + (6b^2 a_4 + a_2)T^2 + (4b^3 + 2ba_2)T + a_4 b^4 + a_2 b^2 + a_0)$$

pour un certain $b \in \mathbb{Q}$ et $a_4, a_2, a_0 \in \mathbb{Z}$ tels que $\sqrt{a_2^2 - 4a_4 a_0} \notin \mathbb{Q}$.

Démonstration. Quitte à faire un changement de variable, on peut supposer que $a_1 = a_3 = 0$. Pour ces surfaces, l'application $(x, y, t) \mapsto x$ est une fibration en courbe de genre 1 dont une infinité de fibres (en fait toute fibre en $x \in a_4\mathbb{Q}^{*2}$ sauf un nombre fini) possédent une structure de groupe et un point d'ordre infini. Cela démontre la densité des points rationnels de $\mathscr{E}(\mathbb{Q})$. □

Supposons que la surface considérée soit telle que $A_1 = 0$. La proposition 4.2.2 démontre que pour presque tout $x \in a_4\mathbb{Q}^{*2}$ la courbe elliptique C_x possède un point d'ordre 2, mais cela ne permet pas de conclure sur la densité des points rationnels.

Des différents arguments permettent toutefois de démontrer la densité.

Théorème 4.2.4. *Soit $\mathscr{E}$ une surface elliptique rationnelle qui admet l'équation de Weierstrass*

$$y^2 = x^3 + A(T^2 - \alpha)(T^2 - \beta)x,$$

où $A, \alpha, \beta \in \mathbb{Q}$.

Alors les points rationnels sont Zariski-dense.

Démonstration. Par le changement de variable $X = (T^2 - \alpha)x$ et $Y = (T^2 - \alpha)^2 y$, on obtient l'équation

$$Y^2 = (T^2 - \alpha)X^3 + A(T^2 - \beta)(T^2 - \alpha)^4 X$$

qui est isomorphe à

$$Y^2 = (T^2 - \alpha)X^3 + A(T^2 - \beta)X.$$

Un remaniement permet ensuite d'obtenir pour $\mathscr{E}$ l'équation

$$Y^2 - T^2(X^3 - AX) + (\alpha X^3 + XA\beta) = 0$$

qui est un fibré en conique.

Ce fibré a moins de 6 fibres singulières. Le corollaire 8 de l'article de Kollár et Mella [23] démontre donc l'unirationnalité de $\mathscr{E}$. Par conséquent, les points rationnels sont denses. □

Pour conclure cette section, remarquons qu'un argument général permet de démontrer la densité des points rationnels pour toutes les surfaces elliptiques rationnelles isotriviales de j-invariant 1728.

Théorème 4.2.5. *Soit $\mathscr{E}$ une surface elliptique rationnelle isotriviale d'invariant $j(T) = 1728$.*

Alors les points rationnels sont Zariski-denses.

Démonstration. Soit $\mathscr{E}$ une surface elliptique rationnelle isotriviale de j-invariant $J(T) = 1728$.

Rappelons le théorème d'Iskovskih présenté en section 1.2.7 qui dit qu'une surface elliptique rationnelle possède un modèle minimal $X/\mathbb{Q}$ qui est :

1. soit un fibré en coniques de degré 1,
2. soit une surface de Del Pezzo.

Soit X le modèle minimal de $\mathscr{E}$.

Par la remarque 58, X n'est en aucun cas une surface de Del Pezzo de degré 1.

Dans les cas où le modèle minimal est un fibré en conique de degré 1, l'article de Kollár et Mella [23] démontre l'unirationalité de X, et donc la densité de ses points rationnels. Par conséquent, il en est de même pour $\mathscr{E}$.

Dans les cas où le modèle minimal est une surface de Del Pezzo de degré ≥ 3, les travaux de Segre et Manin [28] démontrent l'unirationnalité de X et de $\mathscr{E}$.

Il reste à traiter le cas où X est une surface de Del Pezzo de degré 2. Dans ce cas, étudions les sections de $\mathscr{E}$:

1. La section des points à l'infini $[0, y, 0, 0]$.
2. La section exhibée par la proposition 4.2.2 $[x, \frac{-b}{u^2}, \frac{1}{u}, 1]$ où $u = 0$, $b = \sqrt{a_4 x}$ et $x \in a_4 \mathbb{Q}^{*2}$.
3. La section $[0, 0, t, 1]$.

Si la contraction de deux d'entre elles donne une surface de Del Pezzo de degré 2, alors l'image de la troisième est une courbe rationnelle. Si c'est une courbe exceptionnelle, on peut la contracter pour obtenir une surface de Del Pezzo de degré 3, sur laquelle les points rationnels sont denses. Si ce n'est pas une courbe exceptionnelle, elle permet toutefois de trouver une infinité de point sur X. Par conséquent, il en existe qui ne sont ni sur une courbe exceptionnelle si sur une quartique distinguée. On peut donc appliquer les travaux de Salgado, Testa et Várilly-Alvarado qui démontre l'unirationalité et la densité des points rationnels de X et de $\mathscr{E}$.

□

4.2.3 Surfaces avec $j(T) = 0$: variation du signe

Soit X une surface elliptique rationnelle d'équation de Weierstrass

$$X : y^2 = x^3 + F(T, 1).$$

On ne connait pas d'argument géométrique général comme ceux présentés dans les sections précédentes pour démontrer la densité des points rationnels. On peut toutefois s'intéresser à la variation du signe des fibres de la surface. Plus précisément, on souhaite étudier la cardinalité des ensembles

$$W_{\pm}(\mathscr{E}) = \{t \in \mathbb{Q} | W(\mathscr{E}_t)\}.$$

Si la cardinalité de W_-, est infinie, le théorème 1.2.1 permet ensuite de conclure la densité des points rationnels conditionnellement à la conjecture de parité.

Nous avons établi des formules pour le signe dans la section 3.2. Par ces formules, nous savons que le signe sur ces surfaces peut être constant dans certain cas.

Dans la suite de cette section, nous cernons des conditions pour que le signe des fibres de la surface elliptique sous-jacente soit invariant et déterminerons quel est ce signe.

Notation 6. Pour un entier N et un nombre premier p, on notera N_p l'entier tel que $N = p^{v_p(N)} N_p$.

Théorème 4.2.6. *Soit $\mathscr{E}$ une surface elliptique d'équation de Weierstrass*

$$\mathscr{E} : y^2 = x^3 + aT^6 + b,$$

où $a, b \in \mathbb{Z}$ et $C = (a, b)$.

Alors la fonction du signe est constante si et seulement si on a $a/C = 3A^2$ et $b/C = B^2$ pour des entiers A et B qui respectent une des options de chacune des listes suivantes.

En particulier, si on pose

$$\sigma = \#\{p \text{ tel que } p^2 | C \text{ et } p \equiv 2 \mod 3\},$$

le signe de la surface elliptique $\mathscr{E}$ est égal à $W(\mathscr{E}_t) = +1$ pour toute fibre $\mathscr{E}_t$ non singulière ($t \in \mathbb{Q}$) si et seulement si

1. *σ est pair et les entiers A, B, C relatifs à la surface satisfont*
   (a) *une option de A. et une option de 2 ;*
   (b) *une option de B. et une option de 1,*
2. *σ est impair et les entiers A, B, C relatifs à la surface satisfont*
   (a) *une option de A. et une option de 1 ;*
   (b) *une option de B. et une option de 2.*

Première liste :

A. *On a et* $C_2 \equiv 3 \mod 4$ *et un des cas suivants :*
   (a) $v_2(A)$ *et* $v_2(B) \equiv 0 \mod 3$ *et* $v_2(C) \equiv 0 \mod 6$
   (b) $v_2(A) \equiv 1 \mod 3$ *et*
      i. $v_2(C) \equiv 0 \mod 6$
      ii. $v_2(C) \equiv 4 \mod 6$
   (c) $v_2(B) \equiv 1 \mod 3$ *et*
      i. $v_2(C) \equiv 0 \mod 6$
      ii. $v_2(C) \equiv 2 \mod 6$
   (d) $v_2(A) \equiv 2 \mod 3$ *et*
      i. $v_2(C) \equiv 2 \mod 6$
      ii. $v_2(C) \equiv 4 \mod 6$
   (e) $v_2(B) \equiv 2 \mod 3$ *et*
      i. $v_2(C) \equiv 0 \mod 6$
      ii. $v_2(C) \equiv 2 \mod 6$

B. *On a* $C_2 \equiv 1 \mod 4$ *et un des cas suivants :*
   (a) $v_2(A)$ *et* $v_2(B) \equiv 0 \mod 3$ *et* $v_2(C) \equiv 0 \mod 6$
   (b) $v_2(A) \equiv 1 \mod 3$ *et*
      i. $v_2(C) \equiv 0 \mod 6$
      ii. $v_2(C) \equiv 2 \mod 6$
   (c) $v_2(B) \equiv 1 \mod 3$ *et*
      i. $v_2(C) \equiv 0 \mod 6$
      ii. $v_2(C) \equiv 4 \mod 6$
   (d) $v_2(A) \equiv 2 \mod 3$ *et*
      i. $v_2(C) \equiv 0 \mod 6$
      ii. $v_2(C) \equiv 2 \mod 6$
   (e) $v_2(B) \equiv 2 \mod 3$ *et*
      i. $v_2(C) \equiv 2 \mod 6$
      ii. $v_2(C) \equiv 4 \mod 6$

Seconde liste :

Notation : Si $v_2(A) = 0$, *on pose* $k = v_2(B) - 1$ *et* $A' = B_2, B' = A_2$. *Sinon, on pose* $k = v_2(A)$ *et* $A' = A_2$, $B' = B_2$.

1. (a) $k \equiv 0 \mod 3$,
      i. $v_3(C) \equiv 3 \mod 6$

A. $B'^2 \equiv 1 \mod 9$ *et* $C_3 \equiv 4 \mod 9$,
B. $B'^2 \equiv 4 \mod 9$ *et* $C_3 \equiv 1 \mod 9$,
C. $B'^2 \equiv 7 \mod 9$ *et* $C_3 \equiv 7 \mod 9$,

ii. $v_3(C) \equiv 5 \mod 6$
A. $A'^2 \equiv 1 \mod 9$ *et* $C_3 \equiv 2, 8 \mod 9$,
B. $A'^2 \equiv 4 \mod 9$ *et* $C_3 \equiv 2, 5 \mod 9$,
C. $A'^2 \equiv 7 \mod 9$ *et* $C_3 \equiv 5, 8 \mod 9$,

iii. $v_3(C) \equiv 0 \mod 6$
A. $B'^2 \equiv 1 \mod 9$ *et* $C_3 \equiv 1, 4 \mod 9$,
B. $B'^2 \equiv 4 \mod 9$ *et* $C_3 \equiv 1, 7 \mod 9$,
C. $B'^2 \equiv 7 \mod 9$ *et* $C_3 \equiv 4, 7 \mod 9$,

iv. $v_3(C) \equiv 2 \mod 6$
A. $A'^2 \equiv 1 \mod 9$ *et* $C_3 \equiv 2 \mod 9$,
B. $A'^2 \equiv 4 \mod 9$ *et* $C_3 \equiv 5 \mod 9$,
C. $A'^2 \equiv 7 \mod 9$ *et* $C_3 \equiv 8 \mod 9$,

(b) $k \equiv 1 \mod 3$,

i. $v_3(C) \equiv 0 \mod 6$
A. $C_3 \equiv 1 \mod 9$. $A'^2 \equiv 1, 4 \mod 9$ *et* $B'^2 \equiv 7 \mod 9$,
B. $C_3 \equiv 2 \mod 9$. $A'^2 \equiv 1, 4 \mod 9$ *et* $B'^2 \equiv 7 \mod 9$,
C. $C_3 \equiv 4 \mod 9$. $A'^2 \equiv 1, 7 \mod 9$ *et* $B'^2 \equiv 4 \mod 9$,
D. $C_3 \equiv 5 \mod 9$. $A'^2 \equiv 4, 7 \mod 9$ *et* $B'^2 \equiv 1 \mod 9$,
E. $C_3 \equiv 7 \mod 9$. $A'^2 \equiv 4, 7 \mod 9$ *et* $B'^2 \equiv 1 \mod 9$,
F. $C_3 \equiv 8 \mod 9$. $A'^2 \equiv 1, 7 \mod 9$ *et* $B'^2 \equiv 4 \mod 9$,

ii. $v_3(C) \equiv 1, 4 \mod 6$ *et* $C_3 \equiv 1 \mod 3$,

iii. $v_3(C) \equiv 2, 5 \mod 6$ *et* $C_3 \equiv 2 \mod 3$,

iv. $v_3(C) \equiv 3 \mod 6$
A. $C_3 \equiv 1 \mod 9$. $B'^2 \equiv 1, 4 \mod 9$ *et* $A'^2 \equiv 4 \mod 9$,
B. $C_3 \equiv 2 \mod 9$. $B'^2 \equiv 1, 4 \mod 9$ *et* $A'^2 \equiv 1 \mod 9$,
C. $C_3 \equiv 4 \mod 9$. $B'^2 \equiv 1, 7 \mod 9$ *et* $A'^2 \equiv 1 \mod 9$,
D. $C_3 \equiv 5 \mod 9$. $B'^2 \equiv 4, 7 \mod 9$ *et* $A'^2 \equiv 4 \mod 9$,
E. $C_3 \equiv 7 \mod 9$. $B'^2 \equiv 4, 7 \mod 9$ *et* $A'^2 \equiv 7 \mod 9$,
F. $C_3 \equiv 8 \mod 9$. $B'^2 \equiv 1, 7 \mod 9$ *et* $A'^2 \equiv 7 \mod 9$,

(c) $k \equiv 2 \mod 3$

i. $v_3(C) \equiv 1 \mod 6$
A. $A'^2 \equiv 1 \mod 9$ *et* $C_3 \equiv 1, 4 \mod 9$,
B. $A'^2 \equiv 4 \mod 9$ *et* $C_3 \equiv 1, 7 \mod 9$,
C. $A'^2 \equiv 7 \mod 9$ *et* $C_3 \equiv 4, 7 \mod 9$,

ii. $v_3(C) \equiv 3 \mod 6$
A. $B'^2 \equiv 1 \mod 9$ *et* $C_3 \equiv 2 \mod 9$,

B. $B'^2 \equiv 4 \mod 9$ *et* $C_3 \equiv 5 \mod 9$,

C. $B'^2 \equiv 7 \mod 9$ *et* $C_3 \equiv 8 \mod 9$,

iii. $v_3(C) \equiv 0 \mod 6$

A. $B'^2 \equiv 1 \mod 9$ *et* $C_3 \equiv 2, 8 \mod 9$,

B. $B'^2 \equiv 4 \mod 9$ *et* $C_3 \equiv 2, 5 \mod 9$,

C. $B'^2 \equiv 7 \mod 9$ *et* $C_3 \equiv 5, 8 \mod 9$,

iv. $v_3(C) \equiv 4 \mod 6$

A. $A'^2 \equiv 1 \mod 9$ *et* $C_3 \equiv 4 \mod 9$,

B. $A'^2 \equiv 4 \mod 9$ *et* $C_3 \equiv 1 \mod 9$,

C. $A'^2 \equiv 7 \mod 9$ *et* $C_3 \equiv 7 \mod 9$,

2. (a) $k \equiv 0 \mod 3$,

i. $v_3(C) \equiv 0 \mod 6$

A. $B'^2 \equiv 1 \mod 9$ *et* $C_3 \equiv 5 \mod 9$,

B. $B'^2 \equiv 4 \mod 9$ *et* $C_3 \equiv 8 \mod 9$,

C. $B'^2 \equiv 7 \mod 9$ *et* $C_3 \equiv 2 \mod 9$,

ii. $v_3(C) \equiv 2 \mod 6$

A. $A'^2 \equiv 1 \mod 9$ *et* $C_3 \equiv 1, 7 \mod 9$,

B. $A'^2 \equiv 4 \mod 9$ *et* $C_3 \equiv 4, 7 \mod 9$,

C. $A'^2 \equiv 7 \mod 9$ *et* $C_3 \equiv 1, 4 \mod 9$,

iii. $v_3(C) \equiv 3 \mod 6$

A. $B'^2 \equiv 1 \mod 9$ *et* $C_3 \equiv 5, 8 \mod 9$,

B. $B'^2 \equiv 4 \mod 9$ *et* $C_3 \equiv 2, 8 \mod 9$,

C. $B'^2 \equiv 7 \mod 9$ *et* $C_3 \equiv 2, 5 \mod 9$,

iv. $v_3(C) \equiv 5 \mod 6$

A. $A'^2 \equiv 1 \mod 9$ *et* $C_3 \equiv 7 \mod 9$,

B. $A'^2 \equiv 4 \mod 9$ *et* $C_3 \equiv 4 \mod 9$,

C. $A'^2 \equiv 7 \mod 9$ *et* $C_3 \equiv 1 \mod 9$,

(b) $k \equiv 1 \mod 3$,

i. $v_3(C) \equiv 0 \mod 6$

A. $C_3 \equiv 1 \mod 9$. $B'^2 \equiv 1, 4 \mod 9$ *et* $A'^2 \equiv 7 \mod 9$,

B. $C_3 \equiv 2 \mod 9$. $B'^2 \equiv 1, 4 \mod 9$ *et* $A'^2 \equiv 7 \mod 9$,

C. $C_3 \equiv 4 \mod 9$. $B'^2 \equiv 1, 7 \mod 9$ *et* $A'^2 \equiv 4 \mod 9$,

D. $C_3 \equiv 5 \mod 9$. $B'^2 \equiv 4, 7 \mod 9$ *et* $A'^2 \equiv 1 \mod 9$,

E. $C_3 \equiv 7 \mod 9$. $B'^2 \equiv 4, 7 \mod 9$ *et* $A'^2 \equiv 1 \mod 9$,

F. $C_3 \equiv 8 \mod 9$. $B'^2 \equiv 1, 7 \mod 9$ *et* $A'^2 \equiv 4 \mod 9$,

ii. $v_3(C) \equiv 1.4 \mod 6$ *et* $C_3 \equiv 2 \mod 3$,

iii. $v_3(C) \equiv 2, 5 \mod 6$ *et* $C_3 \equiv 1 \mod 3$,

iv. $v_3(C) \equiv 3 \mod 6$

A. $C_3 \equiv 1 \mod 9$. $A'^2 \equiv 4 \mod 9$ *et* $B'^2 \equiv 1, 4 \mod 9$,

B. $C_3 \equiv 2 \mod 9$. $A'^2 \equiv 1 \mod 9$ *et* $B'^2 \equiv 1, 4 \mod 9$,
C. $C_3 \equiv 4 \mod 9$. $A'^2 \equiv 1 \mod 9$ *et* $B'^2 \equiv 1, 7 \mod 9$,
D. $C_3 \equiv 5 \mod 9$. $A'^2 \equiv 4 \mod 9$ *et* $B'^2 \equiv 4, 7 \mod 9$,
E. $C_3 \equiv 7 \mod 9$. $A'^2 \equiv 7 \mod 9$ *et* $B'^2 \equiv 4, 7 \mod 9$,
F. $C_3 \equiv 8 \mod 9$. $A'^2 \equiv 7 \mod 9$ *et* $B'^2 \equiv 1, 7 \mod 9$,

(c) $k \equiv 2 \mod 3$

i. $v_3(C) \equiv 0 \mod 6$

A. $B'^2 \equiv 1 \mod 9$ *et* $C_3 \equiv 5 \mod 9$,
B. $B'^2 \equiv 4 \mod 9$ *et* $C_3 \equiv 8 \mod 9$,
C. $B'^2 \equiv 7 \mod 9$ *et* $C_3 \equiv 2 \mod 9$,

ii. $v_3(C) \equiv 1 \mod 6$

A. $A'^2 \equiv 1 \mod 9$ *et* $C_3 \equiv 5 \mod 9$,
B. $A'^2 \equiv 4 \mod 9$ *et* $C_3 \equiv 8 \mod 9$,
C. $A'^2 \equiv 7 \mod 9$ *et* $C_3 \equiv 2 \mod 9$,

iii. $v_3(C) \equiv 3 \mod 6$

A. $B'^2 \equiv 1 \mod 9$ *et* $C_3 \equiv 1, 7 \mod 9$,
B. $B'^2 \equiv 4 \mod 9$ *et* $C_3 \equiv 4, 7 \mod 9$,
C. $B'^2 \equiv 7 \mod 9$ *et* $C_3 \equiv 1, 4 \mod 9$,

iv. $v_3(C) \equiv 4 \mod 6$

A. $A'^2 \equiv 1 \mod 9$ *et* $C_3 \equiv 5, 8 \mod 9$,
B. $A'^2 \equiv 4 \mod 9$ *et* $C_3 \equiv 2, 8 \mod 9$,
C. $A'^2 \equiv 7 \mod 9$ *et* $C_3 \equiv 2, 5 \mod 9$,

Pour les surfaces qui ont un signe négatif sur toute fibre non singulière, la conjecture de parité avance que le rang des fibres de ces surfaces elliptiques est toujours strictement positif. Pour celles dont le signe est partout positif, cependant et il n'est pas possible de conclure quelque chose sur la densité des points rationnels à partir de l'étude du signe.

Exemple 2. Soit la surface elliptique définie par l'équation

$$y^2 = x^3 + 39(27T^6 + 1).$$

Par le théorème 4.2.6, la fonction du signe des fibres est constante lorsque t varie dans $\mathbb{Q}$.

En effet, on a $\sigma = 0$ (donc pair), $v_2(C) = 0$, $C_2 \equiv 3 \mod 4$ (donc $\mathscr{E}$ fait partie de la liste B.), $v_3(C) = 1$, $v_2(A) = 1$ et $C_3 \equiv 1 \mod 3$ (donc $\mathscr{E}$ fait partie de la liste 1). Par conséquent, on a

$$W(\mathscr{E}_t) = +1.$$

Exemple 3. Si on prend les mêmes hypothèses que dans l'exemple précédent, mais qu'on choisit plutôt un $C_3 \equiv 2 \mod 3$, le signe sera -1.

Par exemple, cela est vrai pour la surface définie par l'équation

$$\mathscr{E} : y^2 = x^3 + 15(27t^6 + 1).$$

Dans la démonstration de ce théorème, on utilise deux lemmes qui étudient différentes parties de la formule du signe.

Lemme 4.2.7. *Soit $\mathscr{E}$ une surface elliptique d'équation de Weierstrass*

$$\mathscr{E} : y^2 = x^3 + C(3A^2T^6 + B^2),$$

où $A, B, C \in \mathbb{Z}$ et $\mathrm{pgcd}(A, B) = 1$.

Lorsque $v_2(B) = 0$, on pose $k = v_2(A)$, $A' = A_3$ et $B' = B_3$. Si $v_2(A) = 0$, on pose $k = v_2(B) - l$, $A' = B_3$ et $B' = A_3$.

La fonction $w_3(t) = W_3(\mathscr{E}_t)(-1)^{v_3(t)}$ est constante si et seulement si

1. $k \equiv 0 \mod 3$,
   - (a) $v_3(C) \equiv 0 \mod 6$
     - i. $B'^2 \equiv 1 \mod 9$ et $C_3 \equiv 5 \mod 9$,
     - ii. $B'^2 \equiv 4 \mod 9$ et $C_3 \equiv 8 \mod 9$,
     - iii. $B'^2 \equiv 7 \mod 9$ et $C_3 \equiv 2 \mod 9$,
   - (b) $v_3(C) \equiv 2 \mod 6$
     - i. $A'^2 \equiv 1 \mod 9$ et $C_3 \equiv 1, 7 \mod 9$,
     - ii. $A'^2 \equiv 4 \mod 9$ et $C_3 \equiv 4, 7 \mod 9$,
     - iii. $A'^2 \equiv 7 \mod 9$ et $C_3 \equiv 1, 4 \mod 9$,
   - (c) $v_3(C) \equiv 3 \mod 6$
     - i. $B'^2 \equiv 1 \mod 9$ et $C_3 \equiv 4 \mod 9$,
     - ii. $B'^2 \equiv 4 \mod 9$ et $C_3 \equiv 1 \mod 9$,
     - iii. $B'^2 \equiv 7 \mod 9$ et $C_3 \equiv 7 \mod 9$,
   - (d) $v_3(C) \equiv 5 \mod 6$
     - i. $A'^2 \equiv 1 \mod 9$ et $C_3 \equiv 2, 8 \mod 9$,
     - ii. $A'^2 \equiv 4 \mod 9$ et $C_3 \equiv 2, 5 \mod 9$,
     - iii. $A'^2 \equiv 7 \mod 9$ et $C_3 \equiv 5, 8 \mod 9$,
2. $k \equiv 1 \mod 3$,
   - (a) $v_3(C) \equiv 0 \mod 6$
     - i. $C_3 \equiv 1 \mod 9$. $B'^2 \equiv 1, 4 \mod 9$ et $A'^2 \equiv 7 \mod 9$,
     - ii. $C_3 \equiv 2 \mod 9$. $B'^2 \equiv 1, 4 \mod 9$ et $A'^2 \equiv 7 \mod 9$,
     - iii. $C_3 \equiv 4 \mod 9$. $B'^2 \equiv 1, 7 \mod 9$ et $A'^2 \equiv 4 \mod 9$,
     - iv. $C_3 \equiv 5 \mod 9$. $B'^2 \equiv 4, 7 \mod 9$ et $A'^2 \equiv 1 \mod 9$,
     - v. $C_3 \equiv 7 \mod 9$. $B'^2 \equiv 4, 7 \mod 9$ et $A'^2 \equiv 1 \mod 9$,
     - vi. $C_3 \equiv 8 \mod 9$. $B'^2 \equiv 1, 7 \mod 9$ et $A'^2 \equiv 4 \mod 9$,
   - (b) $v_3(C) \equiv 1, 2 \mod 6$ et $C_3 \equiv 1 \mod 3$,
   - (c) $v_3(C) \equiv 3 \mod 6$
     - i. $C_3 \equiv 1 \mod 9$. $B'^2 \equiv 1, 4 \mod 9$ et $A'^2 \equiv 4 \mod 9$,
     - ii. $C_3 \equiv 2 \mod 9$. $B'^2 \equiv 1, 4 \mod 9$ et $A'^2 \equiv 1 \mod 9$,
     - iii. $C_3 \equiv 4 \mod 9$. $B'^2 \equiv 1, 7 \mod 9$ et $A'^2 \equiv 1 \mod 9$,
     - iv. $C_3 \equiv 5 \mod 9$. $B'^2 \equiv 4, 7 \mod 9$ et $A'^2 \equiv 4 \mod 9$,
     - v. $C_3 \equiv 7 \mod 9$. $B'^2 \equiv 4, 7 \mod 9$ et $A'^2 \equiv 7 \mod 9$,
     - vi. $C_3 \equiv 8 \mod 9$. $B'^2 \equiv 1, 7 \mod 9$ et $A'^2 \equiv 7 \mod 9$,

(d) $v_3(C) \equiv 4, 5 \mod 6$ *et* $C_3 \equiv 2 \mod 3$,

3. $k \equiv 2 \mod 3$

(a) $v_3(C) \equiv 0 \mod 6$

i. $B'^2 \equiv 1 \mod 9$ *et* $C_3 \equiv 5 \mod 9$,

ii. $B'^2 \equiv 4 \mod 9$ *et* $C_3 \equiv 8 \mod 9$,

iii. $B'^2 \equiv 7 \mod 9$ *et* $C_3 \equiv 2 \mod 9$,

(b) $v_3(C) \equiv 1 \mod 6$

i. $A'^2 \equiv 1 \mod 9$ *et* $C_3 \equiv 1, 4 \mod 9$,

ii. $A'^2 \equiv 4 \mod 9$ *et* $C_3 \equiv 1, 7 \mod 9$,

iii. $A'^2 \equiv 7 \mod 9$ *et* $C_3 \equiv 4, 7 \mod 9$,

(c) $v_3(C) \equiv 3 \mod 6$

i. $B'^2 \equiv 1 \mod 9$ *et* $C_3 \equiv 2 \mod 9$,

ii. $B'^2 \equiv 4 \mod 9$ *et* $C_3 \equiv 5 \mod 9$,

iii. $B'^2 \equiv 7 \mod 9$ *et* $C_3 \equiv 8 \mod 9$,

(d) $v_3(C) \equiv 4 \mod 6$

i. $A'^2 \equiv 1 \mod 9$ *et* $C_3 \equiv 5, 8 \mod 9$,

ii. $A'^2 \equiv 4 \mod 9$ *et* $C_3 \equiv 2, 8 \mod 9$,

iii. $A'^2 \equiv 7 \mod 9$ *et* $C_3 \equiv 2, 5 \mod 9$,

aux quels cas $w_3(t) = (-1)^{v_3(C)+1}$, *ou encore*

1. $k \equiv 0 \mod 3$,

(a) $v_3(C) \equiv 0 \mod 6$

i. $B'^2 \equiv 1 \mod 9$ *et* $C_3 \equiv 1, 4 \mod 9$,

ii. $B'^2 \equiv 4 \mod 9$ *et* $C_3 \equiv 1, 7 \mod 9$,

iii. $B'^2 \equiv 7 \mod 9$ *et* $C_3 \equiv 4, 7 \mod 9$,

(b) $v_3(C) \equiv 2 \mod 6$

i. $A'^2 \equiv 1 \mod 9$ *et* $C_3 \equiv 2 \mod 9$,

ii. $A'^2 \equiv 4 \mod 9$ *et* $C_3 \equiv 5 \mod 9$,

iii. $A'^2 \equiv 7 \mod 9$ *et* $C_3 \equiv 8 \mod 9$,

(c) $v_3(C) \equiv 3 \mod 6$

i. $B'^2 \equiv 1 \mod 9$ *et* $C_3 \equiv 5, 8 \mod 9$,

ii. $B'^2 \equiv 4 \mod 9$ *et* $C_3 \equiv 2, 8 \mod 9$,

iii. $B'^2 \equiv 7 \mod 9$ *et* $C_3 \equiv 2, 5 \mod 9$,

(d) $v_3(C) \equiv 5 \mod 6$

i. $A'^2 \equiv 1 \mod 9$ *et* $C_3 \equiv 7 \mod 9$,

ii. $A'^2 \equiv 4 \mod 9$ *et* $C_3 \equiv 4 \mod 9$,

iii. $A'^2 \equiv 7 \mod 9$ *et* $C_3 \equiv 1 \mod 9$,

2. $k \equiv 1 \mod 3$,

(a) $v_3(C) \equiv 0 \mod 6$

i. $C_3 \equiv 1 \mod 9$. $A'^2 \equiv 1, 4 \mod 9$ *et* $B'^2 \equiv 7 \mod 9$,

ii. $C_3 \equiv 2 \mod 9$. $A'^2 \equiv 1, 4 \mod 9$ *et* $B'^2 \equiv 7 \mod 9$,

iii. $C_3 \equiv 4 \mod 9$. $A'^2 \equiv 1,7 \mod 9$ *et* $B'^2 \equiv 4 \mod 9$,
iv. $C_3 \equiv 5 \mod 9$. $A'^2 \equiv 4,7 \mod 9$ *et* $B'^2 \equiv 1 \mod 9$,
v. $C_3 \equiv 7 \mod 9$. $A'^2 \equiv 4,7 \mod 9$ *et* $B'^2 \equiv 1 \mod 9$,
vi. $C_3 \equiv 8 \mod 9$. $A'^2 \equiv 1,7 \mod 9$ *et* $B'^2 \equiv 4 \mod 9$,

(b) $v_3(C) \equiv 1,2 \mod 6$ *et* $C_3 \equiv 2 \mod 3$,

(c) $v_3(C) \equiv 3 \mod 6$

i. $C_3 \equiv 1 \mod 9$. $A'^2 \equiv 4 \mod 9$ *et* $B'^2 \equiv 1,4 \mod 9$,
ii. $C_3 \equiv 2 \mod 9$. $A'^2 \equiv 1 \mod 9$ *et* $B'^2 \equiv 1,4 \mod 9$,
iii. $C_3 \equiv 4 \mod 9$. $A'^2 \equiv 1 \mod 9$ *et* $B'^2 \equiv 1,7 \mod 9$,
iv. $C_3 \equiv 5 \mod 9$. $A'^2 \equiv 4 \mod 9$ *et* $B'^2 \equiv 4,7 \mod 9$,
v. $C_3 \equiv 7 \mod 9$. $A'^2 \equiv 7 \mod 9$ *et* $B'^2 \equiv 4,7 \mod 9$,
vi. $C_3 \equiv 8 \mod 9$. $A'^2 \equiv 7 \mod 9$ *et* $B'^2 \equiv 1,7 \mod 9$,

(d) $v_3(C) \equiv 4,5 \mod 6$ *et* $C_3 \equiv 2 \mod 3$,

3. $k \equiv 2 \mod 3$

(a) $v_3(C) \equiv 0 \mod 6$

i. $B'^2 \equiv 1 \mod 9$ *et* $C_3 \equiv 2,8 \mod 9$,
ii. $B'^2 \equiv 4 \mod 9$ *et* $C_3 \equiv 2,5 \mod 9$,
iii. $B'^2 \equiv 7 \mod 9$ *et* $C_3 \equiv 5,8 \mod 9$,

(b) $v_3(C) \equiv 1 \mod 6$

i. $A'^2 \equiv 1 \mod 9$ *et* $C_3 \equiv 5 \mod 9$,
ii. $A'^2 \equiv 4 \mod 9$ *et* $C_3 \equiv 8 \mod 9$,
iii. $A'^2 \equiv 7 \mod 9$ *et* $C_3 \equiv 2 \mod 9$,

(c) $v_3(C) \equiv 3 \mod 6$

i. $B'^2 \equiv 1 \mod 9$ *et* $C_3 \equiv 1,7 \mod 9$,
ii. $B'^2 \equiv 4 \mod 9$ *et* $C_3 \equiv 4,7 \mod 9$,
iii. $B'^2 \equiv 7 \mod 9$ *et* $C_3 \equiv 1,4 \mod 9$,

(d) $v_3(C) \equiv 4 \mod 6$

i. $A'^2 \equiv 1 \mod 9$ *et* $C_3 \equiv 4 \mod 9$,
ii. $A'^2 \equiv 4 \mod 9$ *et* $C_3 \equiv 1 \mod 9$,
iii. $A'^2 \equiv 7 \mod 9$ *et* $C_3 \equiv 7 \mod 9$,

aux quels cas $w_3(t) = (-1)^{v_3(C)}$.

Démonstration. Soit $\delta = C(3A^2m^6 + B^2n^6)$.

Supposons que $v_3(A) = k$ et $v_3(B) = 0$.

Soit (m, n) un couple d'entiers premiers entre eux tels que $6v_3(n) < 2k + 1$. On a $v_3(\delta) \equiv v_3(C) \mod 6$ et $\delta_3 \equiv C_3B^2n^6 \mod 9$. Sur ce choix de (m, n), la fonction w_2 est constante :

$$w_3(t) = \begin{cases} (-1)^{v_3(C)+1} & \text{si } v_3(C) \equiv 1,2 \mod 6 \text{ et } C_3 \equiv 1 \mod 3 \\ & \text{et si } v_3(C) \equiv 4,5 \mod 6 \text{ et } C_3 \equiv 2 \mod 3, \\ & \text{si } v_3(C) \equiv 0 \mod 6 \text{ et } C_3B^2 \equiv 5,7 \mod 9 \\ & \text{si } v_3(C) \equiv 3 \mod 6 \text{ et } C_3B^2 \equiv 2,4 \mod 9 \\ (-1)^{v_3(C)} & \text{sinon.} \end{cases}$$

Supposons à présent que $6v_3(n) > 2k+1$. On a dans ce cas $v_3(\delta) = v_3(C) + 2k + 1$ et $\delta_3 \equiv C_3 A_3^2 m^4$. De même que précédement, on trouve que sur ce choix de (m,n), la valeur de w_3 est

$$w_3(t) = \begin{cases} (-1)^{v_3(C)} & \text{si } v_3(C)+2k \equiv 0,2 \mod 6 \text{ et } C_3 \equiv 1 \mod 3 \\ & \text{et si } v_3(C)+2k \equiv 3,4 \mod 6 \text{ et } C_3 \equiv 2 \mod 3, \\ & \text{si } v_3(C)+2k \equiv 5 \mod 6 \text{ et } C_3B^2 \equiv 5,7 \mod 9 \\ & \text{si } v_3(C)+2k \equiv 2 \mod 6 \text{ et } C_3B^2 \equiv 2,4 \mod 9 \\ (-1)^{v_3(C)} & \text{sinon.} \end{cases}$$

En remarquant que $C_3B^2 \equiv 5,7 \mod 9$ dans les cas suivants :

1. $B^2 \equiv 1 \mod 9$ et $C_3 \equiv 5,7 \mod 9$
2. $B^2 \equiv 4 \mod 9$ et $C_3 \equiv 4,8 \mod 9$
3. $B^2 \equiv 7 \mod 9$ et $C_3 \equiv 1,2 \mod 9$

et que $C_3B^2 \equiv 2,4 \mod 9$ dans les cas suivants :

1. $B^2 \equiv 1 \mod 9$ et $C_3 \equiv 2,4 \mod 9$
2. $B^2 \equiv 4 \mod 9$ et $C_3 \equiv 1,5 \mod 9$
3. $B^2 \equiv 7 \mod 9$ et $C_3 \equiv 7,8 \mod 9$

on en déduit que la fonction w_3 est constante dans les cas de l'énoncé. On procède pour ce faire en comparant les deux formules pour chaque cas de $k \mod 3$.

Lorsque $v_2(A) = 0$ et $v_2(B) = l$, on procède d'une manière similaire pour obtenir les conditions précédentes, où $k = l-1$ et en interchangeant A et B, afin d'obtenir une fonction w_3 est constante. □

Lemme 4.2.8. *Soit $\mathscr{E}$ une surface elliptique d'équation de Weierstrass*

$$\mathscr{E} : y^2 = x^3 + C(3A^2T^6 + B^2)x,$$

où $A, B, C \in \mathbb{Z}$ et $\operatorname{pgcd}(A,B) = 1$. Pout $t = \frac{u}{v} \in \mathbb{Q}$, on pose $\delta = C(A^2u^4 + B^2v^4)$. On note δ_2 l'entier tel que $\delta = 2^{\operatorname{ord}_2\delta}\delta_2$. La valeur de la fonction $w_2(t) := W_2(\mathscr{E}_t)\left(\frac{-1}{\delta_2}\right)$ est constante égale à $\left(\frac{-1}{C_2}\right)$ lorsque $t \in \mathbb{Q}$ varie si et

1. *$v_2(A)$ et $v_2(B) \equiv 0 \mod 3$ et $v_2(C) \equiv 0 \mod 6$*
2. *$v_2(A) \equiv 1 \mod 3$ et*
   - *(a) $v_2(C) \equiv 0 \mod 6$*
   - *(b) $v_2(C) \equiv 2 \mod 6$ et $C_2 \equiv 1 \mod 4$*
   - *(c) $v_2(C) \equiv 4 \mod 6$ et $C_2 \equiv 3 \mod 4$*
3. *$v_2(B) \equiv 1 \mod 3$ et*
   - *(a) $v_2(C) \equiv 0 \mod 6$*
   - *(b) $v_2(C) \equiv 2 \mod 6$ et $C_2 \equiv 3 \mod 4$*
   - *(c) $v_2(C) \equiv 4 \mod 6$ et $C_2 \equiv 1 \mod 4$*
4. *$v_2(A) \equiv 2 \mod 3$ et*
   - *(a) $v_2(C) \equiv 0 \mod 6$ et $C_2 \equiv 1 \mod 4$*
   - *(b) $v_2(C) \equiv 2 \mod 6$*
   - *(c) $v_2(C) \equiv 4 \mod 6$ et $C_2 \equiv 3 \mod 4$*

5. $v_2(B) \equiv 2 \mod 3$ *et*
   (a) $v_2(C) \equiv 0 \mod 6$ *et* $C_2 \equiv 3 \mod 4$
   (b) $v_2(C) \equiv 2 \mod 6$
   (c) $v_2(C) \equiv 4 \mod 6$ *et* $C_2 \equiv 1 \mod 4$

Démonstration. Supposons que $v_2(A) = k \in \mathbb{N}$ et $v_2(B) = 0$.

Soit (m, n) un couple d'entiers premiers entre eux.

Si $6v_2(n) < 2k$, alors $v_2(\delta) \equiv v_2(C) \mod 6$ et $\delta_3 \equiv C_2 \mod 4$. On a donc

$$w_2(t) = \begin{cases} \left(\frac{-1}{C_2}\right) & \text{si } v_2(C\delta) \equiv 1,3,4,5 \mod 6 \text{ et } C_2 \equiv 1 \mod 4 \\ -\left(\frac{-1}{C_2}\right) & \text{si } v_2(C\delta) \equiv 0,2 \\ & \text{ou si } v_2(C\delta) \equiv 1,3,4,5 \mod 6 \text{ et } C_2 \equiv 3 \mod 4 \end{cases}$$

Remarquons que cette formule s'applique aussi aux $(m, n) \in \mathbb{Z}^2$ tels que $2 \mid m$.

Si $6v_2(n) \geq 2k$, alors $v_2(\delta) \equiv v_2(C) + 2k \mod 6$ et $\delta_2 \equiv 3C_2 \mod 4$. On a donc

$$w_2(t) = \begin{cases} \left(\frac{-1}{C_2}\right) & \text{si } v_2(C\delta) + 2k \equiv 1,3,4,5 \mod 6 \text{ et } C_2 \equiv 3 \mod 4 \\ -\left(\frac{-1}{C_2}\right) & \text{si } v_2(C\delta) + 2k \equiv 0,2 \\ & \text{ou si } v_2(C\delta) \equiv 1,3,4,5 \mod 6 \text{ et } C_2 \equiv 1 \mod 4 \end{cases}$$

De ces formules, on déduit le comportement suivant de la fonction $w_2(t)$ lorsque $6v_2(n) \neq 2k$.

Lorsque k est divisible par 3, alors la fonction w_2 est constante égale à $-\left(\frac{-1}{C_2}\right)$ si $v_2(C) = 0, 2 \mod 6$.

Lorsque $k \equiv 1 \mod 3$, alors la fonction w_2 est constante égale à $-\left(\frac{-1}{C_2}\right)$ si et seulement si la surface fait partie des cas suivants :

1. $v_2(C) \equiv 0 \mod 6$
2. $v_2(C) \equiv 2 \mod 6$ et $C_2 \equiv 1 \mod 4$
3. $v_2(C) \equiv 4 \mod 6$ et $C_2 \equiv 3 \mod 4$

Si $k \equiv 2 \mod 3$, alors la fonction w_2 est constante égale à $-\left(\frac{-1}{C_2}\right)$ si et seulement si la surface fait partie des cas suivants :

1. $v_2(C) \equiv 0 \mod 6$ et $C_2 \equiv 1 \mod 4$
2. $v_2(C) \equiv 2 \mod 6$
3. $v_2(C) \equiv 4 \mod 6$ et $C_2 \equiv 3 \mod 4$

Lorsque $k \equiv 0 \mod 3$, on doit procéder à un tri plus fin car il est possible que le signe varie lorsqu'on considère de plus les n tels que $6v_2(n) = 2k$. Lorsqu'on a une paire (m, n) avec n de telle sorte, alors $v_2(C\delta) = v_2(C) + 2$. Remarquons qu'en remplaçant n_2 par n' tel que $n' \equiv n_2 + 8 \mod 16$, alors on fait passer la valeur de $\delta_2 \mod 4$ de C_2 à $3C_2$ et vice-versa. Par conséquent, le signe varie quand on prend n tel que $6v_2(n) = 2k$ dans les cas où $v_2(C) \equiv 1,2,3,5 \mod 6$. Il est constant sur de telles paires lorsque $v_2(C) \equiv 0,4 \mod 6$.

Par conséquent, lorsque $3 \mid k$, le signe est constant si et seulement si $v_2(C) \equiv 0 \mod 6$

Supposons maintenant que $v_2(A) = 0$ et $v_2(B) = k$. Alors par un raisonnement similaire à ce qui précède, on trouve que $w_2(t)$ est constante et égale à $-\left(\frac{-1}{C_2}\right)$ si et seulement si

1. $k \equiv 0 \mod 3$ et $v_2(C) \equiv 0 \mod 6$
2. $k \equiv 1 \mod 3$ et
   (a) $v_2(C) \equiv 0 \mod 6$
   (b) $v_2(C) \equiv 2 \mod 6$ et $C_2 \equiv 3 \mod 4$
   (c) $v_2(C) \equiv 4 \mod 6$ et $C_2 \equiv 1 \mod 4$
3. $k \equiv 2 \mod 3$ et
   (a) $v_2(C) \equiv 0 \mod 6$ et $C_2 \equiv 3 \mod 4$
   (b) $v_2(C) \equiv 2 \mod 6$
   (c) $v_2(C) \equiv 4 \mod 6$ et $C_2 \equiv 1 \mod 4$

□

Démonstration. (de la prop. 4.2.6) Soit $C = \text{pgcd}(A, B)$.

Si $3A/B$ n'est pas un carré rationnel, alors le théorème 1.2.14 [51, Thm 2.1] assure que le signe varie. Supposons que ce n'est pas le cas, c'est-à-dire qu'il existe $a, b \in \mathbb{Z}$ tels que $3a^2 = \frac{A}{C}$ et $b^2 = \frac{B}{C}$.

Soit $\mathscr{E} : y^2 = x^3 + C(3A^2m^6 + B^2n^6)$, la fibre en $t = (m, n) \in \mathbb{P}$. associée à X une surface de Del Pezzo de la forme $w^2 = z^3 + Ax^6 + By^6$.

On pose

$$\delta = c(3a^2m^6 + b^2n^6) = 2^{v_2(\delta)}3^{v_3(\delta)}p_1^{e^1}...p_n^{e^n} = 2^{v_2(\delta)}3^{v_3(\delta)}d_1(d_2)^2$$

où $d_1 = \prod_{e_i \text{ impair}} p_i^{e^i}$ et $d_2 = \prod_{e_i \text{ pair}} p_i^{e^i/2}$. Comme $\mathscr{E}$ est de la forme $E_\delta : y^2 = x^3 + \delta$, le théorème 3.2.1 indique que la formule du signe est

$$W(E_t) = -W_2(E_t)W_3(E_t)(\frac{-1}{d_1})(\frac{-3}{d_2}).$$

Remarquons que l'on a $\left(\frac{-1}{d_1}\right) = \left(\frac{-1}{\delta_2}\right)(-1)^{v_3(\delta)}$, où δ_2 est l'entier tel que $\delta = 2^{v_2(\delta)}\delta_2$.

Pour la suite, on utilisera les notations suivantes :

$\mathscr{P}(t) := \left(\frac{-3}{d_2}\right)$, $w_2(t) := W_2(E_\delta)(\frac{-1}{\delta_2})$ et $w_3(t) := W_3(E_\delta)(-1)^{v_3(\delta)}$.

Nous étudierons la variation de $\mathscr{P}$, w_2 et w_3, les différentes parties de la formule du signe, selon les valuations 2 et 3-adique de a, b et c, les valeurs de $c_2 \mod 4$ et $c_3 \mod 9$ et la factorisation en nombres premiers de c, afin de cerner les cas où ces composantes sont constantes. Cette étude servira à comprendre le comportement global de la fonction signe.

Pour tout a, b et c, $\mathscr{P}(t)$ est une constante. Celle-ci est égale à $\mathscr{P} = (-1)^\sigma$, où

$$\sigma = \#\{p \text{ tel que } p^2|C \text{ et } p \equiv 2 \mod 3\},$$

En effet, les conditions qui déterminent le signe local en 3 font intervenir $v_3(\delta) \mod 6$, et $\delta_3 \mod 9$, alors que celles pour le signe local en 2 font intervenir $v_2(\delta) \mod 4$ et $\delta_2 \mod 4$. Par conséquent, si l'une des valeurs w_2 ou w_3 présente une variation, alors le signe global n'est pas constant. Dans le cas où une de w_2 ou w_3 est fixée et l'autre varie, on a forcément une variation du signe. De plus, lorsque les deux présentent une variation, celles-ci ne se produisent pas simultanément (et donc la surface elliptique ne peut pas avoir un signe constant dans ces cas).

Par conséquent, le signe varie en dehors des surfaces telles que A, B, C respectent une des conditions du lemme 4.2.8, et une de lemme 4.2.7. □

Remarque 63. L'indépendance de w_2 et de w_3 mentionnée à la fin de la démonstration est également prédite par la formule du signe moyen de Helfgott pour une surface elliptique isotriviale (Proposition 2.5.2), d'une façon similaire à celle mentionnée dans la section 2.6.1 de j-invariant 0.

Remarque 64. Le choix de s'intéresser à une surface de la forme

$$y^2 = x^3 + AT^6 + B$$

vient du théorème de Várilly-Alvarado [51, Théorème 2.1] qui démontre que la variation du signe des fibres sur une surface elliptique rationnelle de la forme

$$y^2 = x^3 + F(T)$$

où F a un facteur primitif f_i qui est tel que $\mu_3 \not\subseteq \mathbb{Q}[T]/f_i$ où μ_3 est le groupe des racines troisièmes de l'unité. Le contre-exemple le plus naturel à cette propriété est

$$F(T) = C(3A^2T^6 + B^2).$$

Remarquons que le théorème 4.2.6 est la suite logique des travaux de Várilly-Alvarado, en particulier celle de [51, Théorème 1.1] qui marquait le début de la tentative de cerner les surfaces elliptique rationnelles isotriviales de cette forme dont les fibres ont toutes le même signe.

4.2.4 Surfaces avec $j(T) = 1728$: variation du signe

La densité des points rationnels sur certaines surfaces elliptiques de la forme $\mathscr{E} : y^2 = x^3 + g(T)x$ est assurée par l'argument en section 4.2.2. Pour ce faire, on construit un point générique d'ordre infini sur une fibration elliptique de $\mathscr{E}$. Il arrive toutefois que cet argument ne fonctionne pas, en particulier quand la fonction est de la forme $g(T) = AT^4 + B$. Dans cette section, on trouve de la même façon que dans la section précédente des surfaces elliptiques rationnelles de cette forme dont le signe est constant.

Théorème 4.2.9. *Soit $\mathscr{E}$ une surface elliptique d'équation de Weierstrass*

$$\mathscr{E} : y^2 = x^3 + C(A^2T^4 + B^2)x,$$

où $A, B, C \in \mathbb{Z}$ et $(A, B) = 1$.

Alors la fonction du signe est constante si et seulement si $v_3(AB)$ est pair et si une des options de la liste suivante est vérifiée :

1. *(a) k est impair*
   - *i. $v_2(C) \equiv 0 \mod 4$*
     - *A. $C_2 \equiv 3 \mod 16$, $A^2 \equiv B^2 \equiv 1 \mod 16$*
     - *B. $C_2 \equiv 11 \mod 16$, $A^2 \equiv B^2 \equiv 9 \mod 16$*
   - *ii. $v_2(C) \equiv 1, 3 \mod 4$*
     - *A. $C_2 \equiv 3 \mod 16$,*
   - *iii. $v_2(C) \equiv 2 \mod 4$ et*
     - *A. $C_2 \equiv 9 \mod 16$, $A^2 \equiv B^2 \equiv 9 \mod 16$*

   (b) k est impair et
   - *i. $v_2(C) \equiv 0 \mod 4$*

A. $C_2 \equiv 5, 13 \mod 16$
B. $C_2 \equiv 7 \mod 16$, $B^2 \equiv A^2 \equiv 9 \mod 16$
C. $C_2 \equiv 15 \mod 16$, $A^2 \equiv B^2 \equiv 1 \mod 16$

ii. $v_2(C) \equiv 2 \mod 4$ *et*
A. $C_2 \equiv 7, 15 \mod 16$
B. $C_2 \equiv 5 \mod 16$, $A^2 \equiv B^2 \equiv 1 \mod 16$
C. $C_2 \equiv 13 \mod 16$, $A^2 \equiv B^2 \equiv 9 \mod 16$

2. (a) *k est impair*
i. $v_2(C) \equiv 0 \mod 4$
A. $C_2 \equiv 7 \mod 16$, $A^2 \equiv B^2 \equiv 1 \mod 16$
B. $C_2 \equiv 15 \mod 16$, $A^2 \equiv B^2 \equiv 9 \mod 16$

ii. $v_2(C) \equiv 1, 3 \mod 4$
A. $C_2 \equiv 7 \mod 16$,

iii. $v_2(C) \equiv 2 \mod 4$ *et*
A. $C_2 \equiv 5, 7 \mod 16$, $A^2 \equiv B^2 \equiv 1 \mod 16$

(b) *k est pair et*
i. *Si* $v_2(C) = 0, 2$
A. $C_2 \equiv 7 \mod 8$ *et* $A^2 \equiv B^2 \equiv 9 \mod 16$

ii. $v_2(C) = 1$
A. $C_2 \equiv 7, 15 \mod 16$ *et* $A^2 \equiv B^2 + 8 \mod 16$,

iii. $v_2(C) = 3$
A. $C_2 \equiv 5 \mod 8$ *et* $A^2 \equiv B^2 + 8 \mod 16$,

(c) *k est impair et*
i. $v_2(C) \equiv 0 \mod 4$
A. $C_2 \equiv 1, 9 \mod 16$
B. $C_2 \equiv 3 \mod 16$, $B^2 \equiv A^2 \equiv 9 \mod 16$
C. $C_2 \equiv 11 \mod 16$, $A^2 \equiv B^2 \equiv 1 \mod 16$

ii. $v_2(C) \equiv 1, 3 \mod 4$
A. $C_2 \equiv 1, 3 \mod 8$

iii. $v_2(C) \equiv 2 \mod 4$ *et*
A. $C_2 \equiv 3, 11 \mod 16$
B. $C_2 \equiv 1 \mod 16$, $A^2 \equiv B^2 \equiv 1 \mod 16$
C. $C_2 \equiv 9 \mod 16$, $A^2 \equiv B^2 \equiv 9 \mod 16$

(d) *k est pair et*
i. *Si* $v_2(C) = 0$
A. $C_2 \equiv 1 \mod 16$ *et* $B^2 \equiv 1 \mod 16$
B. $C_2 \equiv 3 \mod 16$ *et* $A^2 \equiv 9 \mod 16$
C. $C_2 \equiv 9 \mod 16$ *et* $B^2 \equiv 9 \mod 16$
D. $C_2 \equiv 11 \mod 16$ *et* $A^2 \equiv 1 \mod 16$

ii. $v_2(C) = 1$

A. $C_2 \equiv 3, 11 \mod 16$ *et* $A^2 \equiv B^2 \mod 16$

iii. Si $v_2(C) = 2$

A. $C_2 \equiv 1 \mod 16$ *et* $A^2 \equiv 1 \mod 16$,

B. $C_2 \equiv 3 \mod 16$ *et* $B^2 \equiv 9 \mod 16$,

C. $C_2 \equiv 9 \mod 16$ *et* $A^2 \equiv 9 \mod 16$,

D. $C_2 \equiv 11 \mod 16$ *et* $B^2 \equiv 1 \mod 16$,

iv. si $v_2(C) = 3$

A. $C_2 \equiv 1 \mod 8$ *et* $A^2 \equiv B^2 \mod 16$

Soit $\sigma = \#\{p \text{ nombre premier} \mid p^2 \mid C \text{ et } p \equiv 2 \mod 3\}$.
Dans ce cas, le signe sera de valeur

$$W(\mathscr{E}_t) = +1$$

si et seulement si

1. σ *est pair,*
   (a) $v_3(C) = 2 \mod 4$ *et les coefficients respectent une option de la liste* 1
   (b) $v_3(C) \neq 2 \mod 4$ *et les coefficients respectent une option de la liste* 2
2. σ *est impair*
   (a) $v_3(C) = 2 \mod 4$ *et les coefficients respectent une option de la liste* 2
   (b) $v_3(C) \neq 2 \mod 4$ *et les coefficients respectent une option de la liste* 1

Exemple 4. La surface

$$\mathscr{E} : y^2 = x^3 + 7(9T^4 + 25)x$$

est de signe -1 sur toute fibre en $t \in \mathbb{Q}$.

La surface

$$\mathscr{E} : y^2 = x^3 + 11(9T^4 + 25)x,$$

quant à elle est de signe $+1$ sur toute fibre en $t \in \mathbb{Q}$.

Dans la démonstration de ce théorème, on utilise deux lemmes qui étudient différentes parties de la formule du signe.

Lemme 4.2.10. *Soit* $\mathscr{E}$ *une surface elliptique d'équation de Weierstrass*

$$\mathscr{E} : y^2 = x^3 + C(A^2T^4 + B^2)x,$$

où $A, B, C \in \mathbb{Z}$ *et* $(A, B) = 1$.

Le signe local en 3 est constant si et seulement si $v_3(AB)$ *est pair. Dans ce cas, on a*

$$W_3(\delta) = \begin{cases} -1 & \text{si } v_3(C) \equiv 2 \mod 4 \\ +1 & \text{sinon} \end{cases}$$

Démonstration. Rappelons la formule dans ce cas (voir [51, Lemme 4.7]) :

$$W_3(\delta) = \begin{cases} -1 & \text{si } v_3(\delta) \equiv 2 \mod 4 \\ +1 & \text{sinon} \end{cases}$$

Pour chaque fibre $\mathscr{E}_t$, on étudiera la courbe $\mathscr{E}_{m,n} : y^2 = x^3 + C(A^2m^4 + B^2n^4)x$ qui lui est $\mathbb{Q}$-isomorphe. On pose $\delta(m, n) = A^2m^4 + B^2n^4$. Le signe local en 3 de $E_{m,n}$ dépend

uniquement de $v_3(C\delta(m,n)$. Comme $v_3(C)$ est fixe, on étudiera la variation de $v_3(\delta(m,n)$ selon les cas de A et de B.

Pour tout $l \in \mathbb{Z}$, on notera l_3, l'entier tel que $l = 3^{v_3(l)}l_3$.

Étant donné que par hypothèse A et B sont premiers entre eux, cela signifie que 3 ne peut diviser que l'un de $v_3(A)$ ou $v_3(B)$ à la fois. Quitte à échanger les rôles de A et de B, on peut supposer $3 \nmid B$ et $v_3(A) = k$ pour un certain $k \in \mathbb{Z}$. Pour tout m, n premiers entre eux, on a $\delta(m,n) = 3^{2k+4v_3(m)}A_3^2m_3^4 + B^2 3^{4v_3(n)}n_3^4$.

Dans le cas où $v_3(n) = 0$, on a $\delta(m,n) \equiv 1 \mod 4$ et $v_3(\delta) = 0$. Dans le cas où $0 < v_3(n) \leq \frac{k}{2} - 1$, on a $\delta(m,n)_3 \equiv 3^{2k-4v_3(n)} + 1 \equiv 1 \mod 3$ et $v_3(\delta) \equiv 2k - 4v_3(n) \equiv k \mod 4$. Dans le cas où $v_3(n) = \frac{k}{2}$ (ce qui se produit uniquement si $k \equiv 0, 2 \mod 4$), on a $v_3(\delta) \equiv 2k \mod 4$ et $\delta_3 \equiv 2 \mod 4$. Dans le cas où $v_3(n) \geq \frac{k}{2} + 1$, on a $v_3(\delta) \equiv -2k \mod 4$ et $\delta_3 \equiv 1 \mod 3$

Supposons que $v_3(AB)$ est impair. Soit m_1, n_1 non divisible par 3 et premiers entre eux. On a $\delta(m_1, n_1) \equiv 0 \mod 4$. Soit m, n premiers entre eux tel que $3 \mid n$. On a $\delta(m_2, n_2) \equiv 2 \mod 4$. Par conséquent, on a

$$W(\mathscr{E}_{m_1,n_1}) = -W(\mathscr{E}_{m_2,n_2}).$$

Supposons que $v_3(AB)$ est pair. Alors $2k \equiv -2k \equiv 0 \mod 4$. Par conséquent, $v_3(\delta(m,n))$ est constant pour toute valeur de $m, n \in \mathbb{Z}$ premiers entre eux. On a dans ce cas :

$$W(\mathscr{E}_{m,n}) = -1 \Leftrightarrow v_3(C) \equiv 2 \mod 4.$$

□

Lemme 4.2.11. *Soient $A, B, C \in \mathbb{Z}$ des entiers premiers entre eux et tels que $2 \nmid B$. Soit $\mathscr{E}$ une surface elliptique d'équation de Weierstrass*

$$\mathscr{E} : y^2 = x^3 + C(A^2T^4 + B^2)x.$$

Pour $t = \frac{u}{v} \in \mathbb{Q}$, on pose $\delta = C(A^2u^4 + B^2v^4)$. On note δ_2 l'entier tel que $\delta = 2^{\mathrm{ord}_2\delta}\delta_2$. Si $v_2(A) = 0$, on pose $k = v_2(B)$ et $A' = B_3$ et $B' = A_3$. Sinon, on pose $k = v_2(A)$ et $A' = A_3$ et $B' = B_3$.

La valeur de $w_2(\mathscr{E}_t) := W_2(\mathscr{E}_t)\left(\frac{-2}{\delta_2}\right)$ est constante lorsque $t \in \mathbb{Q}$ varie si et seulement si

1. *k est impair*
   - *(a) $v_2(C) \equiv 0 \mod 4$*
     - *i. $C_2 \equiv 3, 7 \mod 16$, $A^2 \equiv B^2 \equiv 1 \mod 16$*
     - *ii. $C_2 \equiv 11, 15 \mod 16$, $A^2 \equiv B^2 \equiv 9 \mod 16$*
   - *(b) $v_2(C) \equiv 1, 3 \mod 4$*
     - *i. $C_2 \equiv 3, 7 \mod 16$,*
   - *(c) $v_2(C) \equiv 2 \mod 4$ et*
     - *i. $C_2 \equiv 5, 7 \mod 16$, $A^2 \equiv B^2 \equiv 1 \mod 16$*
     - *ii. $C_2 \equiv 9, 13 \mod 16$, $A^2 \equiv B^2 \equiv 9 \mod 16$*
2. *k est pair et*
   - *(a) Si $v_2(C) = 0, 2$*
     - *i. $C_2 \equiv 7 \mod 8$ et $A^2 \equiv B^2 \equiv 9 \mod 16$*
   - *(b) $v_2(C) = 1$*

i. $C_2 \equiv 7, 15 \mod 16$ *et* $A^2 \equiv B^2 + 8 \mod 16$,

(c) $v_2(C) = 3$

i. $C_2 \equiv 5 \mod 8$ *et* $A^2 \equiv B^2 + 8 \mod 16$,

auxquels cas $w_2(\mathscr{E}_t) = \left(\frac{-2}{C_2}\right)$ *et les cas suivants :*

1. k est impair et

(a) $v_2(C) \equiv 0 \mod 4$

i. $C_2 \equiv 1, 5, 9, 13 \mod 16$

ii. $C_2 \equiv 3, 7 \mod 16$, $B^2 \equiv A^2 \equiv 9 \mod 16$

iii. $C_2 \equiv 11, 15 \mod 16$, $A^2 \equiv B^2 \equiv 1 \mod 16$

(b) $v_2(C) \equiv 1, 3 \mod 4$

i. $C_2 \equiv 1, 3 \mod 8$

(c) $v_2(C) \equiv 2 \mod 4$ *et*

i. $C_2 \equiv 3, 7, 11, 15 \mod 16$

ii. $C_2 \equiv 1, 5 \mod 16$, $A^2 \equiv B^2 \equiv 1 \mod 16$

iii. $C_2 \equiv 9, 13 \mod 16$, $A^2 \equiv B^2 \equiv 9 \mod 16$

2. k est pair et

(a) Si $v_2(C) = 0$

i. $C_2 \equiv 1 \mod 16$ *et* $B^2 \equiv 1 \mod 16$

ii. $C_2 \equiv 3 \mod 16$ *et* $A^2 \equiv 9 \mod 16$

iii. $C_2 \equiv 9 \mod 16$ *et* $B^2 \equiv 9 \mod 16$

iv. $C_2 \equiv 11 \mod 16$ *et* $A^2 \equiv 1 \mod 16$

(b) $v_2(C) = 1$

i. $C_2 \equiv 3, 11 \mod 16$ *et* $A^2 \equiv B^2 \mod 16$

(c) Si $v_2(C) = 2$

i. $C_2 \equiv 1 \mod 16$ *et* $A^2 \equiv 1 \mod 16$,

ii. $C_2 \equiv 3 \mod 16$ *et* $B^2 \equiv 9 \mod 16$,

iii. $C_2 \equiv 9 \mod 16$ *et* $A^2 \equiv 9 \mod 16$,

iv. $C_2 \equiv 11 \mod 16$ *et* $B^2 \equiv 1 \mod 16$,

(d) si $v_2(C) = 3$

i. $C_2 \equiv 1 \mod 8$ *et* $A^2 \equiv B^2 \mod 16$

auxquels cas $w_2(\mathscr{E}_t) = -\left(\frac{-2}{C_2}\right)$.

Démonstration. Pour tout $m, n \in \mathbb{Z}$ premiers entre eux, soit $\mathscr{E}_{m,n} : y^2 = x^3 + C(A^2m^4 + B^2n^4)x$ une courbe elliptique $\mathbb{Q}$-isomorphe à $E_{\frac{m}{n}}$. On connait la formule du signe local en 2 grâce à [51, Lemme 4.7] (un résultat aussi présenté dans le lemme 3.2.3). De plus, on se rappelle que si t est un entier impair, on a

$$(\frac{-2}{t}) = \begin{cases} +1 & \text{si } t \equiv 1, 3 \mod 8, \\ -1 & \text{sinon.} \end{cases}$$

On pose

On pose pour tout $m, n \in \mathbb{Z}$ premiers entre eux l'entier $\alpha(m,n) = A^2m^4 + B^2n^4$, c'est-à-dire que $\delta(m,n) = C \cdot \alpha(m,n)$. On va étudier les valeurs de $v_2(\delta)$ et de $\delta_2 \mod 16$. On en déduira la valeur de w_2 pour chaque cas.

Comme on a supposé que A et B sont premiers entre eux, il ne peut y en avoir un seul qui soit divisible par 2. Quitte à inverser les rôles de A et de B, on peut supposer que $v_2(A) = k$ pour un entier $k \in \mathbb{Z}$ et que $v_2(B) = 0$.

On écrit

$$\alpha(m,n) = 2^{2k}A_2^2m^4 + B^2 2^{4v_2(n)}n_2^4,$$

pour (m,n) un couple d'entier premiers entre eux.

Supposons que $2k > 4v_2(n)$. Dans ce cas, $v_2(\delta(m,n)) = 4v_2(n)+v_2(C) \equiv v_2(C) \mod 4$ et $\delta(m,n)_2 \equiv B^2C_2 \mod 16$. Dans ce cas,

$$W_2(\mathscr{E}_{m,n}) = \begin{cases} +1 & \text{si } v_2(C) \equiv 0 \mod 4 \text{ et } B^2C_2 \equiv 3,7 \mod 16, \\ & \text{si } v_2(C) \equiv 2 \mod 4 \text{ et } B^2C_2 \equiv 9,13 \mod 16, \\ & \text{si } v_2(C) \equiv 1,3 \mod 4 \text{ et } B^2C_2 \equiv 5,7 \mod 8, \\ -1 & \text{sinon.} \end{cases} \tag{4.5}$$

Supposons que $2k > 4v_2(n)$. Dans ce cas, $v_2(\delta(m,n)) = 2k + v_2(C) \mod 4$. On a $\delta_2 \equiv C_2A_2^2 \mod 16$. Par conséquent, le signe est

$$W_2(\mathscr{E}_{m,n}) = \begin{cases} +1 & \text{si } v_2(C) \equiv 2k \mod 4 \text{ et } C_2A_2^2 \equiv 3,7 \mod 16, \\ & \text{si } v_2(C) \equiv 2k-2 \mod 4 \text{ et } C_2A_2^2 \equiv 9,13 \mod 16, \\ & \text{si } v_2(C) \equiv 1,3 \mod 4 \text{ et } C_2A_2^2 \equiv 5,7 \mod 8, \\ -1 & \text{sinon.} \end{cases} \tag{4.6}$$

Supposons que k est impair.

On en déduit que, si k est impair, alors la fonction w_2 est constante dans les cas suivants :

1. $v_2(C) \equiv 0 \mod 4$
   (a) $C_2 \equiv 3,7 \mod 16$, $A^2 \equiv B^2 \equiv 1 \mod 16$
   (b) $C_2 \equiv 11,15 \mod 16$, $A^2 \equiv B^2 \equiv 9 \mod 16$
2. $v_2(C) \equiv 1,3 \mod 4$
   (a) $C_2 \equiv 3,7 \mod 16$,
3. $v_2(C) \equiv 2 \mod 4$ et
   (a) $C_2 \equiv 5,7 \mod 16$, $A^2 \equiv B^2 \equiv 1 \mod 16$
   (b) $C_2 \equiv 9,13 \mod 16$, $A^2 \equiv B^2 \equiv 9 \mod 16$

auquel cas $w_2(t) = (\frac{-2}{C_2})$ ou encore

1. $v_2(C) \equiv 0 \mod 4$
   (a) $C_2 \equiv 1,5,9,13 \mod 16$
   (b) $C_2 \equiv 3,7 \mod 16$, $B^2 \equiv A^2 \equiv 9 \mod 16$
   (c) $C_2 \equiv 11,15 \mod 16$, $A^2 \equiv B^2 \equiv 1 \mod 16$
2. $v_2(C) \equiv 1,3 \mod 4$
   (a) $C_2 \equiv 1,3 \mod 8$
3. $v_2(C) \equiv 2 \mod 4$ et

(a) $C_2 \equiv 3, 7, 11, 15 \mod 16$

(b) $C_2 \equiv 1, 5 \mod 16$, $A^2 \equiv B^2 \equiv 1 \mod 16$

(c) $C_2 \equiv 9, 13 \mod 16$, $A^2 \equiv B^2 \equiv 9 \mod 16$

auquel cas $w_2 = -\left(\frac{-2}{C_2}\right)$.

On suppose maintenant que k est pair.

Remarquons que si $k = 0$, alors il n'est pas possible que $k = 2k > 4v_2(n)$. Cependant, lorsqu'on prend (m, n) un couple d'entiers premiers entre eux tels que $2 \mid m$, alors on obtient la formule (4.6).

On trouve les cas suivants, où le signe peut être constant lorsque $v_2(n), v_2(m) \neq 2k$.

1. $v_2(C) \equiv 0, 2 \mod 4$
   (a) $C_2 \equiv 7 \mod 16$, $A^2 \equiv B^2 \equiv 9 \mod 16$
2. $v_2(C) \equiv 1, 3 \mod 4$
   (a) $C_2 \equiv 5, 7 \mod 8$,

auquel cas $w_2(t) = (\frac{-2}{C_2})$ ou encore

1. $v_2(C) \equiv 0 \mod 4$
   (a) $C_2 \equiv 1, 5 \mod 16$, $B^2 \equiv 1 \mod 16$
   (b) $C_2 \equiv 3, 7 \mod 16$, $A^2 \equiv 9 \mod 16$
   (c) $C_2 \equiv 5 \mod 16$, $B^2 \equiv 1 \mod 16$,
   (d) $C_2 \equiv 9, 13 \mod 16$ $B^2 \equiv 9 \mod 16$
   (e) $C_2 \equiv 11, 15 \mod 16$, $A^2 \equiv 1 \mod 16$
2. $v_2(C) \equiv 1, 3 \mod 4$
   (a) $C_2 \equiv 1, 3 \mod 8$,
3. $v_2(C) \equiv 2 \mod 4$
   (a) $C_2 \equiv 1, 5 \mod 16$, $A^2 \equiv 1 \mod 16$
   (b) $C_2 \equiv 3, 7 \mod 16$, $B^2 \equiv 9 \mod 16$
   (c) $C_2 \equiv 5 \mod 16$, $A^2 \equiv 1 \mod 16$,
   (d) $C_2 \equiv 9, 13 \mod 16$ $A^2 \equiv 9 \mod 16$
   (e) $C_2 \equiv 11, 15 \mod 16$, $B^2 \equiv 1 \mod 16$

auquel cas $w_2 = -\left(\frac{-2}{C_2}\right)$.

Pour ces exceptions, on procède à un tri plus fin.

Selon les valeurs de $A^2m^4, B^2n_2^4$ (qui se trouvent parmi $1, 9, 17, 25 \mod 32$), on détermine les valeurs possibles de δ_2 et $v_2(\delta)$.

Dans tous les cas, $v_2(\delta) = v_2(C)+2k+1 \equiv v_2(C)+1 \mod 4$. Remarquons que m^4 et n_2^4 peuvent prendre les valeurs $1, 17 \mod 32$. Par conséquent, on pourra, en choisissant une valeur $n'^4 \equiv 17n^4 \mod 32$, on a $\delta_2' \equiv 9\delta_2 \mod 16$. Par conséquent, on aura, si $A^2 \equiv B^2 \mod 16$, $\delta_2 \in \{1, 9 \mod 16\}$ et si $A^2 \not\equiv B^2 \mod 16$, $\delta_2 \in \{5, 13\}$.

Soient, s'ils existent, des rationnels t_1, t_5, t_9, t_{13} associés à des couples d'entiers premiers entre eux (m_i, n_i) tels que $\delta_2(m_i, n_i) = i$. On a l'existence de t_1, t_9 si et seulement si $A^2 \equiv B^2 \mod 16$ et l'existence de t_5, t_{13} si et seulement si $A^2 \equiv B^2 + 8 \mod 16$.

Supposons que $v_2(C) = 0, 2$. Alors

$$w_2(t^i) = \left(\frac{-2}{C_2}\right) \Leftrightarrow C_2 \equiv 5, 7 \mod 8, \text{ lorsque } i = 1, 9$$
$$w_2(t^i) = \left(\frac{-2}{C_2}\right) \Leftrightarrow C_2 \equiv 1, 3 \mod 8, \text{ lorsque } i = 5, 13.$$

Si l'on compare le comportement de la fonction w_2 lorsque $4v_2(n) = 2k$ avec celui où $4v_2(n) \neq 2k$, on ne retient que les cas suivant où le signe est constant :

1. Si $v_2(C) = 0, 2$
   (a) $C_2 \equiv 7 \mod 8$ et $A^2 \equiv B^2 \equiv 9 \mod 16$

auxquels cas $w_2(\mathscr{E}_t) = \left(\frac{-2}{C_2}\right)$ et les cas suivants :

1. Si $v_2(C) = 0$
   (a) $C_2 \equiv 1 \mod 16$ et $B^2 \equiv 1 \mod 16$
   (b) $C_2 \equiv 3 \mod 16$ et $A^2 \equiv 9 \mod 16$
   (c) $C_2 \equiv 9 \mod 16$ et $B^2 \equiv 9 \mod 16$
   (d) $C_2 \equiv 11 \mod 16$ et $A^2 \equiv 1 \mod 16$
2. Si $v_2(C) = 2$
   (a) $C_2 \equiv 1 \mod 16$ et $A^2 \equiv 1 \mod 16$,
   (b) $C_2 \equiv 3 \mod 16$ et $B^2 \equiv 9 \mod 16$,
   (c) $C_2 \equiv 9 \mod 16$ et $A^2 \equiv 9 \mod 16$,
   (d) $C_2 \equiv 11 \mod 16$ et $B^2 \equiv 1 \mod 16$,

auxquels cas $w_2(\mathscr{E}_t) = -\left(\frac{-2}{C_2}\right)$.

Supposons que $v_2(C) = 1$. Alors

$$w_2(t_1) = \left(\frac{-2}{C_2}\right) \Leftrightarrow C_2 \equiv 9, 13 \mod 16$$
$$w_2(t_9) = \left(\frac{-2}{C_2}\right) \Leftrightarrow C_2 \equiv 1, 5 \mod 16$$

$$w_2(t_5) = \left(\frac{-2}{C_2}\right) \Leftrightarrow C_2 \equiv 1, 3, 7, 11, 13, 15 \mod 16$$
$$w_2(t_{13}) = \left(\frac{-2}{C_2}\right) \Leftrightarrow C_2 \equiv 3, 5, 7, 9, 11, 15 \mod 16$$

Si l'on compare le comportement de la fonction w_2 lorsque $4v_2(n) = 2k$ avec celui où $4v_2(n) \neq 2k$, on ne retient que les cas suivant où le signe est constant pour tout t :

1. $C_2 \equiv 7, 15 \mod 16$ et $A^2 \equiv B^2 + 8 \mod 16$,

auxquels cas $w_2(\mathscr{E}_t) = \left(\frac{-2}{C_2}\right)$ et les cas suivants :

2. $C_2 \equiv 3, 11 \mod 16$ et $A^2 \equiv B^2 \mod 16$

auxquels cas $w_2(\mathscr{E}_t) = -\left(\frac{-2}{C_2}\right)$.

Supposons que $v_2(C) = 3$. Alors

$$w_2(t_1) = \left(\frac{-2}{C_2}\right) \Leftrightarrow C_2 \equiv 3, 7 \mod 16$$
$$w_2(t_9) = \left(\frac{-2}{C_2}\right) \Leftrightarrow C_2 \equiv 11, 15 \mod 16$$

$$w_2(t_5) = \left(\frac{-2}{C_2}\right) \Leftrightarrow C_2 \equiv 1, 3, 5, 9, 13, 15 \mod 16$$
$$w_2(t_13) = \left(\frac{-2}{C_2}\right) \Leftrightarrow C_2 \equiv 1, 5, 7, 9, 11, 13 \mod 16$$

Si l'on compare le comportement de la fonction w_2 lorsque $4v_2(n) = 2k$ avec celui où $4v_2(n) \neq 2k$, on ne retient que les cas suivant où le signe est constant pour tout t :

1. $C_2 \equiv 5 \mod 8$ et $A^2 \equiv B^2 + 8 \mod 16$,

auxquels cas $w_2(\mathscr{E}_t) = \left(\frac{-2}{C_2}\right)$ et les cas suivants :

2. $C_2 \equiv 1 \mod 8$ et $A^2 \equiv B^2 \mod 16$

auxquels cas $w_2(\mathscr{E}_t) = -\left(\frac{-2}{C_2}\right)$.

□

Démonstration. (du théorème 4.2.9)

Soit une surface elliptique isotriviale de la forme

$$\mathscr{E} : y^2 = x^3 + C^2(A^2m^4 + B^2n^4),$$

où $A, B, C \in \mathbb{Z}$ et $(A, B) = 1$.

Par le théorème 3.2.2, le signe en t d'une telle surface est donnée par la formule

$$W(\mathscr{E}) = -W_2(\mathscr{E}_t)W_3(\mathscr{E}_t)\left(\frac{-2}{t_1}\right)\left(\frac{-1}{\tau_2}\right),$$

où t_1 et τ_2 sont tels que définis dans ce même théorème. On pose $\delta = A^2m^4 + B^2n^4$.

On remarque qu'on a $\left(\frac{-2}{t_1}\right) = (\frac{-2}{t'})$, où t' est l'entier tel que $t' = 2^{v_2(t)}t'$

Pour la suite, on utilisera les notations suivantes :

$\mathscr{P}(t) := \left(\frac{-1}{t_2}\right)$, $w_2(t) := W_2(E_\delta)\left(\frac{-2}{t'}\right)$ et $w_3(t) := W_3(E_t)$.

La variation de $\mathscr{P}$, w_2 et w_3, les différentes parties de la formule du signe, selon les valuations 2 et 3-adique de a, b et c, les valeurs de $c_2 \mod 16$ et $c_3 \mod 3$ et la factorisation en nombres premiers de c, permet de cerner les cas où ces composantes sont constantes.

Pour tout A, B et C, la valeur de $\mathscr{P}(t)$ est constante sur toute fibre. Explicitement, on a

$$\mathscr{P} = (-1)^\sigma,$$

où

$$\sigma = \#\{p \text{ tel que } p^2|c \text{ et } p \equiv 3 \mod 4\}.$$

Le lemme 4.2.11 donne les conditions pour que w_2 soit constant et le lemme 4.2.10 donne celles pour que W_3 soit constant. En combinant, on obtient bien les conditions et conclusions du théorème.

□

4.3 Densité des points rationnels sur des surfaces elliptiques rationnelles non isotriviales

Dans cette section, nous classifierons les surfaces elliptiques rationnelles non isotriviales pour lesquelles les travaux de Helfgott abordés dans le chapitre 2 s'appliquent inconditionnellement. Puis, nous donnerons des arguments géométriques démontrant la densité des points rationnels inconditionnellement pour davantage de surfaces elliptiques rationnelles non isotriviales et de surfaces de Del Pezzo de degré 1.

4.3.1 Où les travaux de Helfgott sont inconditionnels

Soit $\mathscr{E}$ une surface elliptique rationnelle représentée par l'équation

$$\mathscr{E} : y^2 = x^3 + F(u,1)x + G(u,1),$$

où F et G sont des polynômes homogènes de degré respectif 4 et 6 qui définissent un modèle minimal. On la suppose non isotriviale, et donc en particulier $FG \neq 0$. On pose $\Delta = 4F^3 + 27G^2 = \prod_{i=0}^{s} P_i^{m_i}$ (le discriminant de $\mathscr{E}$) et $M(u,v) = \prod_{i \in I'} P_i(u,v)$ où $I' = \{i$ tel que $P_i \nmid F\}$ (le produit des places multiplicatives).

Les travaux de Helfgott ([15]) imposent que Δ respecte la conjecture du crible des valeurs sans facteur carré, et que $M_{\mathscr{E}}$ respecte la conjecture de Chowla. Nous pouvons utiliser ces conjectures sous deux formes :

A. la variante homogène, qui est vérifiée si
   (a) $\deg P_i \leq 6$ (conjecture du crible des valeurs sans facteur carré) et
   (b) $\deg M_{\mathscr{E}} \leq 3$ ou si $M_{\mathscr{E}}$ est un produit de facteurs linéaires (conjecture de Chowla) ;

B. la variante à une variable, qui est vérifiée si
   (a) $\deg P_i \leq 3$ (conjecture du crible des valeurs sans facteur carré) et
   (b) $\deg M_{\mathscr{E}} \leq 1$ (conjecture de Chowla).

Les cas vérifiés par la seconde sont inclus dans les cas vérifiant la première.

Rappelons que $\mathscr{M}_{\mathscr{E}}$ désigne l'ensemble des places de réduction multiplicative.

Proposition 4.3.1. *Soit $\mathscr{E}$ une surface elliptique rationnelle non isotriviale d'équation*

$$\mathscr{E} : y^2 = x^3 + F(T,1)X + G(T,1),$$

où F et G sont des polynômes homogènes de degré respectif 4 et 6.

On suppose que $\mathscr{E}$ respecte l'une des propriétés suivantes :

1. *$\mathscr{M} = \emptyset$;*
2. *les places de $\mathscr{M}$ sont toutes rationnelles ;*
3. *$\mathscr{M} = \{P\}$ pour $P \in \mathbb{Z}[T]$ un polynôme de degré 3 ;*
4. *$\mathscr{M} = \{P_1, P_2\}$ pour $P_1, P_2 \in \mathbb{Z}[T]$ des polynômes de degré respectivement 1 et 2 ;*
5. *$\mathscr{M} = \{\frac{1}{T}, P_2\}$ où $P_2 \in \mathbb{Z}[T]$ un polynôme de degré 2.*

Alors les ensembles $W_{\pm}$ sont tous deux de cardinalité infinie.

Remarque 65. Cette proposition recense toutes les surfaces elliptiques rationnelles pour lesquelles les travaux de Helfgott s'appliquent inconditionnellement.

Remarque 66. Une rapide étude permet de vérifier qu'il existe bien des surfaces elliptiques rationnelles dans tous les cas listés.

Lorsque $\mathscr{M} = \emptyset$, la surface obtenue par la contraction de la section à l'infini n'est jamais une surface de Del Pezzo de degré 1. En effet, une surface elliptique sans place de réduction multiplicative est automatiquement pourvue d'une place de réduction potentiellement multiplicative. Dans ce cas, le corollaire 4.1.1 informe que $\mathscr{E}$ ne provient pas d'une surface de Del Pezzo de degré 1.

Dans les autres cas, on peut toujours trouver des surfaces de Del Pezzo de degré 1.

Remarque 67. Les arguments géométriques présentés dans la section 4.3.3 démontrent la densité sur certains cas pour lesquels on ne peut pas appliquer inconditionnellement les travaux de Helfgott.

La proposition 4.3.4 demande qu'il existe une place rationnelle de type I_m^*, II^*, III^* IV^* ou I_0^*.

Démonstration. (de la proposition 4.3.1)

Soient les polynômes

1. $B_{\mathscr{E}}$ le produit des polynômes associées aux places de mauvaises réductions de $\mathscr{E}$ qui ne sont pas de type I_0^*,
2. $M_{\mathscr{E}}$ le produit des polynômes associés aux places de réduction multiplicative de $\mathscr{E}$.

Le théorème 2.6.3 et la conjecture de parité démontrent la variation du signe des fibres lorsque $\mathscr{E}$ est une surface non isotriviale dont les polynômes associés sont tels que

1. $B_{\mathscr{E}}$ respecte la conjecture du crible sans facteurs carrés en version homogène,
2. $M_{\mathscr{E}}$ respecte la conjecture de Chowla en version homogène.

Il suffit de vérifier dans quels cas ces hypothèses sont vérifiées.

S'il n'existe pas de place de réduction multiplicative sur $\mathscr{E}$, alors $M_{\mathscr{E}} = 1$. Il n'y a donc pas besoin de recourir à la conjecture de Chowla. De plus, les facteurs irréductibles de Δ apparaissent avec l'exposant ≥ 2. Ils sont donc de degré ≤ 6. Par conséquent, la conjecture du crible des facteurs carrés en version homogène est vérifiée.

Supposons maintenant qu'il existe une place de réduction multiplicative sur $\mathscr{E}$.

Soit l'équation de Weierstrass pour $\mathscr{E}$

$$y^2 = x^3 + F(T,1)x + G(T,1),$$

où $F, G \in \mathbb{Z}[U,V]$ sont des polynômes homogènes de degré respectifs 4 et 6 qui définissent un modèle de Weierstrass minimal. Soit C, le plus grand polynôme primitif tel que $C \mid F$ et $C^2 \mid G$. On écrit $F = aCF_1$ et $G = bC^2G_1$ pour F_1 et G_1 des polynômes primitifs adéquats et a, b les constantes adéquates. Soit $R := \mathrm{pgcd}(F_1, G_1)$. Remarquons que le polynôme R est séparable par construction. On écrit $F = aCRF_2$ et $G = bC^2RG_2$ pour F_2, G_2 des polynômes adéquats.

Le discriminant s'écrit

$$\Delta = C^3R^2(4a^3RF_2^3 + 27b^2CG_2^2).$$

Remarquons que si la surface est non isotriviale, alors s'il existe P un polynôme tel que $P^4 \mid F$, alors $P^6 \nmid G$, et donc $\mathrm{ord}_P C \leq 3$.

Remarquons que R, C, F_2 et G_2 vérifient la conjecture du crible des facteurs carrés en version homogène, car de degré ≤ 6.

On définit $M_0 = (4RF_2^3 - 27CG_2^2)$ et on remarque que $\Delta = C^2R^3M_0$.

Le polynôme M_o est un produit de puissances de polynômes associés à des places de réduction multiplicative ou additive.

Il est possible que M_o soit divisible par les polynômes dont la réduction est de type additive. Celles-ci sont associées à un facteur de C ou de R.

Il existe donc, pour $F = P_1^{\alpha_1} \dots P_r^{\alpha_r}$ (la décomposition en facteurs irréductibles de F) des entiers $\beta_i \in \mathbb{N}$ tels que

$$M_1 = \frac{M_o}{P_1^{\beta_1} \dots P_r^{\beta_r}}.$$

On utilise le lemme 4.3.2 (qui suit) sur $red(M_1) = \prod_{P|M_1} P$ pour conclure. Par conséquent, on aura également que M_o vérifie la version pour les polynômes en une variable de la conjecture du crible des valeurs sans facteurs carrés, et donc également la version pour les polynômes homogènes en deux variables.

□

Lemme 4.3.2. *Soit M un polynôme homogène.*

Alors M satisfait la conjecture de Chowla en version homogène si

1. *c'est un produit de polynômes linéaires ;*
2. *c'est le produit d'une puissance d'un polynôme quadratique et d'une puissance d'un polynôme linéaire ; ou*
3. *c'est une puissance d'un polynôme de degré 3.*

Démonstration. Ceci se déduit aisément du théorème 1.3.6. □

4.3.2 Forme des surfaces elliptiques rationnelles sans place de réduction multiplicative

Proposition 4.3.3. *Soit X une surface elliptique rationnelle non isotriviale et n'admet pas de place de réduction de type I_m. Alors X peut être décrite par l'une des équations suivantes :*

$$\mathscr{E}_1 : y^2 = x^3 + aL_1^2 Q x + bL_1^3 Q M, \tag{4.7}$$

où de plus $Q = \frac{cL_1^2 - 27b^2M^2}{4a^3}$; et

$$\mathscr{E}_2 : y^2 = x^3 + aL_1^2 L_2 L_3 x + bL_1^3 L_2^2 L_3, \tag{4.8}$$

où de plus, $L_1 = 4a^3 L_3 - 27b^2 L_2$; pour $a, b \in \mathbb{Z}$, L_1, L_2, L_3 et M des polynômes linéaires et Q un polynôme quadratique.

Remarque 68. Les conjectures en version homogène et en version une variable sont vérifiées sur les surfaces $\mathscr{E}_a$ et $\mathscr{E}_b$. En effet, la conjecture de Chowla est vraie car $M_{\mathscr{E}} = 1$, et comme tous les polynômes impliqués sont linéaires, la conjecture du crible des facteurs carrés est également vérifiée.

Remarque 69. Dans le premier cas, les places de mauvaises réductions sont celle associée à L_1, de type I_2^*, et celles associées aux facteurs irréductible de Q, de type II.

Dans le second cas, on a trois places de mauvaise réduction rationnelles : celle associée à $4a^3L_2 - 27b^2L_3$ est de type I_1^*, celle associée à L_2 est de type III et celle associée à L_3 est de type II.

Ceci donne une piste pour démontrer la densité des points rationnels sur (4.8) qui sera développée dans la section 4.3.3.

Démonstration. Soit $\mathscr{E}$ la surface elliptique rationnelle associée à X d'équation de Weierstrass :

$$\mathscr{E} : y^2 = x^3 - 27c_4(T)x - 54c_6(T),$$

où $c_4(T), c_6(T) \in \mathbb{Z}[T]$ sont de degré respectivement inférieur à 4 et à 6. Soit Δ son déterminant. Cette surface est pourvue d'une place de réduction de type I_m^* car l'invariant $j = \frac{c_4^3}{\Delta}$ possède obligatoirement un pôle (en un polynôme irréductible $P \in \mathbb{Z}[T]$ ou en $\frac{1}{T}$).

Chaque fibre en $t = \frac{m}{n}$ a aussi pour équation :

$$\mathscr{E}_t = \mathscr{E}_{m,n} : y^2 = x^3 + n^{4-\deg c_4} c_4\left(\frac{m}{n}\right) x + n^{6-\deg c_6} c_6\left(\frac{m}{n}\right).$$

Supposons que P soit le polynôme associé à une place de réduction de type I_m^*, alors on écrit $F = P^2F_1$ et $G = P^3G_1$ pour certains polynômes F_1, G_1. On a que $P \mid (F_1^3 - G_1^2)$.

On doit avoir $\deg P = 1$. En effet, si $\deg P = 2$, alors G_1 et F_1 sont constants et par conséquent $\mathscr{E}$ est isotriviale. Le cas où $\deg P > 2$ est impossible car on aurait alors $\deg G > 6$.

Par conséquent, une surface rationnelle non isotriviale sans place de réduction de type I_m possède une place rationnelle de réduction I_m^*. On a $\deg P = 1$, $\deg F_1 = 2$ et $\deg G_1 = 3$.

Le cas où $(F_1, G_1) = 1$ est impossible. En effet, on devrait avoir $P^6 \mid F_1^3 - G_1^2$ et la surface serait isotriviale. Par conséquent, F_1 et G_1 ont un facteur commun, que nous notons A. On écrit $F_1 = AF_2$ et $G_1 = AG_2$ pour les polynômes appropriés F_2 et G_2. On a $\Delta = P^6A^2(AF_2^3 - G_2^2)$. La réduction en A est donc additive.

Supposons que $\deg A = 2$. Dans ce cas, si $(A, G_2) = 1$, on doit avoir l'égalité

$$A = \gamma P^2 + G_2^2.$$

Si $(A, G_2) = A_2$ pour un polynôme linéaire A_2, alors on doit avoir

$$P = \frac{A_1 - A_2}{\gamma}.$$

Supposons que $\deg A = 1$. Si $A \mid G_2$, on doit avoir

$$A = \frac{F_2^3 - \gamma P^3}{G_3^2}.$$

Cependant, il n'existe pas de polynômes $A, P, G_2, F_2 \in \mathbb{Z}[T]$ respectant cette propriété. En effet, en changeant de variable linéaire $v = P(t)$, et posant $\nu = \frac{u}{v}$, on se ramène à résoudre

$$4a^3F_2(\nu)^3 + 27b^2A(\nu)M(\nu)^2 = c.$$

Comme $F_2 \neq P$, $F_2(\nu)$ est non constant. Soit u_0 tel que $F_2(u_0) = 0$. On a

$$27b^2A(u_0)G_3(u_0)^2 = c \neq 0.$$

En dérivant en u_0, on obtient :

$$2A(u_0)G_3(u_0)G_3'(u_0) + A'(u_0)G_3(u_0)^2 = 0.$$

En dérivant une seconde fois on a :

$$2A(u_0)G_3'(u_0)^2 + 2A(u_0) + 4A'(u_0)G_3'(u_0)G_3(u_0) + A''(u_0)G_3(u_0)^2 = 0.$$

En remarquant que G_3 est linéaire, on a :

$$2A(u_0)G_3'(u_0) + 4A'(u_0)G_3(u_0) = 0.$$

Par conséquent, A est proportionnel à G_3. Pour tout $P \in \mathbb{Z}[T]$ linéaire, le polynôme $P(T)^3 - c$ n'a pas de racine double. Donc, F_2 doit être constant. Par conséquent G_3, F_2, A et P sont proportionnels et la surface $\mathscr{E}$ est isotriviale.

Si $A \nmid G_2$, on doit avoir l'égalité

$$A = \frac{\gamma P^4 + G_2^2}{F_2^3}.$$

Par un raisonnement similaire au cas précédent, ce cas n'est pas possible non plus. □

4.3.3 Arguments géométriques

Nous démontrerons dans cette section deux résultats qui traitent davantage de surfaces elliptiques rationnelles non isotriviales que l'article de Helfgott et ce d'une manière inconditionnelle.

Proposition 4.3.4. *Soit $\mathscr{E}$ une surface elliptique d'équation*

$$\mathscr{E} : y^2 = x^3 + L^2Qx + L^3C,$$

où $L, Q, C \in \mathbb{Z}[u, v]$ sont de degrés respectifs 1, 2 et 3. La surface $\mathscr{E}$ est unirationnelle.

En particulier, on a la densité des points rationnels de $\mathscr{E}$ au sens de Zariski.

Remarque 70. Le polynôme L de la surface $\mathscr{E}$ du théorème précédent est tel que $L^6 \mid \Delta$. Comme on a pris un modèle de Weierstrass minimal pour $\mathscr{E}$, cela signifie que la réduction en L est de type I_0^*, II^*, III^*, IV^* ou I_m^*. Inversement, si on a une surface possédant une place rationnelle d'un de ces types, on peut lui trouver une équation de la forme de la proposition. On en déduit directement le corollaire suivant :

Corollaire 4.3.5. *Si une surface elliptique rationnelle $\mathscr{E}$ possède une place rationnelle de type I_0^*, II^*, III^*, IV^* ou I_m^*, alors les points rationnels de X sont denses pour la topologie de Zariski.*

En particulier, si $\mathscr{E}$ est une surface elliptique non isotriviale sans place de réduction multiplicative, alors ses points rationnels sont denses.

Démonstration. Soit S une surface elliptique représentée par l'équation

$$S : y^2 = x^3 + L(t,1)^2Q(t,1)x + L(t,1)^3C(t,1),$$

où $L, Q, C \in \mathbb{Z}[u, v]$ sont de degrés respectifs 1, 2 et 3. Remarquons que cette surface est rationnelle.

On étudie la surface qui lui est birationnelle

$$\Big(\frac{y}{L^3}\Big)^2 = \Big(\frac{x}{L^2}\Big)^3 + \frac{Q}{L^2}\Big(\frac{x}{L^2}\Big) + \Big(\frac{C}{L^3}\Big). \tag{4.9}$$

Quitte à faire un changement linéaire sur u, v, on peut supposer que $L(u, v) = v$. On pose donc $t = \frac{u}{v}$, $x' = \frac{x}{v^2}$ et $y' = \frac{y}{v^3}$, dont la transformation inverse est $x = x'v^2$, $y = y'v^3$, $u = tv$. Par ce changement de variable, 4.9 devient

$$S' : y'^2 = x'^3 + q(t)x' + c(t) \subset \mathbb{P}^3,$$

avec $Q(t,1) = q(t)$ et $C(t,1) = c(t)$, qui est une surface cubique avec un nombre fini de points singuliers donnés par le théorème 1.2.8.

Remarquons que sur une surface cubique qui n'est pas un cône sur une courbe cubique, l'existence d'un point rationnel équivaut à la densité de ces points rationnels. Ceci est démontré par l'article de Kollar [22], qui est une généralisation des travaux de Segre et Manin [28].

Géométriquement, cette surface est obtenue par la contraction de deux courbes exceptionnelles. Pour une surface obtenue par contraction successive de deux courbes exceptionnelles d'intersection vide (ce qui est le cas de S'), il nous est garanti d'avoir un point rationnel : celui qui est associé au point $[0,0,1,1]$ (qui n'est pas un point singulier). □

Dans la section précédente, on démontre qu'une surface elliptique rationnelle sans place de réduction multiplicative est d'une des deux formes suivantes :

$$\mathscr{E}_1 : y^2 = x^3 + aL_1^2Qx + bL_1^3QM \tag{4.10}$$

et

$$\mathscr{E}_2 : y^2 = x^3 + a(4a^3L_3 - 27b^2L_2)^2L_2L_3x + b(4a^3L_3 - 27b^2L_2)^3L_2^2L_3, \tag{4.11}$$

pour $a, b \in \mathbb{Z}$, L_1, L_2, L_3 et M des polynômes linéaires et Q un polynôme quadratique. Dans le premier cas, on impose de plus que M soit tel que $M^2 = (\frac{L_1^2 - 4a^3Q}{27b^2})$.

Dans le premier cas, les places de mauvaises réductions sont celle associée à L_1, de type I_2^*, et celles associées aux facteurs irréductible de Q, de type II.

Dans le second cas, on a trois places de mauvaise réduction rationnelles : celle associée à $4a^3L_2 + 27b^2L_3$ est de type I_1^*, celle associée à L_2 est de type III et celle associée à L_3 est de type II.

Par conséquent, les résultats présentés précédemment démontrent la densité des points rationnels sur ces surfaces. Les travaux de Helfgott démontrent aussi la densité des points rationnels, mais sous l'hypothèse de la conjecture de parité dont nous nous passons ici.

Il y a une quatrième méthode pour démontrer la densité, au moins sur la surface 4.11.

Rappelons la relation fondamentale du rang de Shioda-Tate rappelée dans la section 1.2.5.

Soit $\mathscr{E}$ une surface elliptique et E sa fibre générique (c'est-à-dire $\mathscr{E}$ vue comme une courbe elliptique sur $\mathbb{Q}[T]$). On a

$$\mathrm{rg}NS(\mathscr{E}_{\overline{\mathbb{Q}}}) = 2 + \mathrm{rg}E(\overline{\mathbb{Q}}(T)) + \sum_v (m_v - 1).$$

Sur les surfaces que nous considérons, qui sont des surfaces elliptiques obtenues par l'éclatement de $\mathbb{P}^2$ en 9 points en position générale, le rang de Néron-Séveri est $\mathrm{rg}NS(\mathscr{E}) = 10$.

Dans le premier cas, la formule de Shioda-Tate nous indique que $\mathrm{rg}E(\overline{\mathbb{Q}}(T)) = 4$. Malheureusement, bien que donnant une majoration intéressante : $\mathrm{rg}(E(\mathbb{Q}(T))) \leq 4$, cela n'est pas assez précis pour conclure sur la densité. En effet, il y a une indécision à ce sujet, hormi dans le cas où on peut borner ainsi : $\mathrm{rg}(E(\mathbb{Q}(T))) \geq 1$.

C'est justement ce qui se produit dans le second cas. En effet, celle-ci donne $\mathrm{rg}E(\overline{\mathbb{Q}}(T)) = 1$.

On a $\mathscr{E}(\overline{\mathbb{Q}}(T)) = \mathbb{Z} \cdot P_o$, pour un certain point P_o. On a par conséquent qu'il existe une extension quadratique K de $\mathbb{Q}$ telle que $P_o \in \mathscr{E}(K(T))$. En effet, si pour tout $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) = G_{\mathbb{Q}}$ l'on pose $\sigma P_o := \varepsilon(\sigma) \cdot P_o$ où $\varepsilon : G_{\mathbb{Q}} \to \pm 1$. Dans ce cas,

1. ou bien ε est trivial et $P_o \in E(\mathbb{Q}(T))$,

2. ou bien ε est non trivial et dans ce cas, $\overline{\mathbb{Q}}^{\mathrm{Ker}\varepsilon} = K$, le sous-corps de $\overline{\mathbb{Q}}$ laissé stable par ε, est un corps quadratique tel que $P_o \in E(K(T))$.

On remarque, d'une façon similaire à la proposition 4.3.4, que $\mathscr{E}_2$ est birationnelle à une surface cubique.

On utilise ensuite la proposition suivante pour conclure :

Proposition 4.3.6. *Soit S une surface cubique non singulière sur un corps de nombres k. On suppose que S n'est pas un cône sur une courbe cubique.*

1. *Si $S(k) \neq \varnothing$, alors $S(k)$ est Zariski-dense.*
2. *Soit k_1 une extension quadratique de k. Alors si $S(k_1) \neq \varnothing$, l'ensemble des points rationnels, est Zariski-dense, alors $S(k)$ est Zariski-dense.*

Démonstration. Le premier point de l'énoncé est démontré par les travaux de Segre et Manin (voir [28]). Ceux-ci démontrent en réalité un résultat plus fort : si k est un corps quelconque et que $S(k) \neq \varnothing$, alors S est k-unirationnelle. Lorsque k est infini, cela implique la Zariski-densité des points rationnels.

On démontre maintenant le deuxième point de l'énoncé. Soit $P \in S(k_1)$. Si $P \in S(k)$, alors les points rationnels sont denses. Supposons donc que $P \notin S(k_1)$. On considère la droite D passant par P et P^σ ou σ est l'automorphisme de k_1 fixant k.

Si $D \subset S$, alors $D(k) \subset S(k)$ et par conséquent S est pourvue de points rationnels.

Sinon, l'intersection $D \cap S$ est formée de trois points : P, P^σ, et un troisième point qui est forcément dans $S(k)$. □

Nous complétons la section par la présentation d'un autre résultat, valable sur les surfaces elliptiques rationnelles sans point singulier, c'est-à-dire celles qui sont associées à une surface de Del Pezzo de degré 1.

Soit X une surface de del Pezzo de degré 1. En général, s'il existe C_1 et C_2 une paire de courbes exceptionnelles définies sur $\mathbb{Q}$ sur X dont l'intersection est vide, on peut contracter ces courbes pour obtenir une surface de del Pezzo de degré 3. Sur cette nouvelle surface, on sait que l'existence d'un point rationnel garantit la densité de $X(k)$ au sens de Zariski.

Dans la suite, nous nous inspirons de cette idée pour démontrer la densité de certaines autres surfaces sur lesquelles on trouve des courbes exceptionnelles dont l'intersection n'est pas vide.

Proposition 4.3.7. *Soit X une surface de Del Pezzo de degré 1 sur laquelle se trouve $\mathscr{C}_1$ et $\mathscr{C}_2$ deux courbes exceptionnelles rationnelles distinctes avec possiblement des points en commun.*

Alors les points rationels de X sont denses pour la topologie de Zariski.

Démonstration. La contraction de $\mathscr{C}$ donne X' une surface de del Pezzo de degré 2. On sait que sur ces surfaces, la densité des points rationnels de X' est équivalente à l'existence d'un point rationnel de X' qui ne soit ni sur une courbe exceptionnelle ni sur une quartique distinguée. Posons $\mathscr{E}$ l'union des points de cette quartique et des courbes exceptionnelles. La contraction envoie $\mathscr{C}_2$ sur une courbe rationnelle de X' que nous noterons $\mathscr{C}$.

Notons que $\mathscr{C}$ n'est pas une courbe exceptionnelle sur X'. Cela est impossible car elle est la contraction d'une courbe qui a un point en commun avec $\mathscr{C}_1$.

Dans le cas où $\mathscr{C} \cap \mathscr{E}$ est fini, on peut trouver un point rationnel hors de $\mathscr{E}$, et la densité des points rationnels est donc garantie. □

5

Surfaces elliptiques non isotriviales

Dans les articles [15] et [27], on étudie le signe de l'équation fonctionnelle associée aux fibres d'une surface elliptique non isotriviale. On démontre que celui-ci varie lorsque les polynômes associés aux places de mauvaise réduction respectent la conjecture du crible des facteurs carrés et ceux associés aux places multiplicatives respectent la conjecture de Chowla. Le premier de ces articles est étudié dans le chapitre 2 de cette thèse. Nous étendrons les résultats de variation du signe à davantage de surfaces elliptiques. Notre théorème principal est le suivant. (On rappelle que $M_{\mathscr{E}}$ est le produit des polynômes associés à une place de réduction multiplicative.)

Théorème 5.0.8. *Soit $\mathscr{E}_T$ une surface elliptique non isotriviale. Soit $\Delta = d \cdot P_1^{e_1} \dots P_r^{e_r}$ la factorisation en facteurs irréductibles du discriminant de $\mathscr{E}$. On suppose que*

1. *pour tout P_i de réduction de type II, II^*, IV ou IV^*, on a*
$$\mu_3 \subseteq \mathbb{Q}[t]/P_i(t);$$
2. *pour tout P_i de type III ou III^* on a*
$$\mu_4 \subseteq \mathbb{Q}[t]/P_i(t),$$
3. $\deg M_{\mathscr{E}} \leq 3$*, ou $M_{\mathscr{E}}$ est un produit de degré arbitraire de formes linéaires,*
4. *et tout P_i de réduction I_m^* vérifie* $\deg P_i \leq 6$ *;*

Alors les ensembles
$$W_{\pm}(\mathscr{E}) = \{t \in \mathbb{Q} | W(\mathscr{E}_t) = \pm 1\}$$
sont tous deux infinis.

Remarque 71. La démonstration de ce théorème montre en fait que si 1 et 2 sont vérifiés, si $M_{\mathscr{E}}$ vérifie la conjecture de Chowla et si chaque P de type I_m^* vérifie la conjecture du crible des facteurs carrés, alors les ensembles $W_{\pm}$ sont infinis.

Ce résultat permet d'obtenir un corollaire direct.

Corollaire 5.0.9. *Soit $\mathscr{E}$ une surface respectant les hypothèses 1 à 4 du théorème 5.0.8. On suppose vraie la conjecture de parité. Alors l'ensemble des points rationnels de $\mathscr{E}$ est dense pour la topologie de Zariski.*

Remarque 72. La condition sur le degré des polynômes dont la réduction est de type I_m^* est là pour assurer qu'il soit possible de contrôler les facteurs carrés de ces polynômes. Toutefois, contrairement aux résultats antérieurs précités, on ne met pas de telle restriction sur les autres places. Leurs polynômes associés peuvent être de degré arbitrairement grand tel que l'illustre l'exemple suivant :

Exemple 5. Soit $Q(T) \in \mathbb{Z}[T]$ un produit de facteurs irréductibles distincts Q_i de degré inférieur ou égal à 6, et tel que $Q(0) \neq 0$. On fixe $N \in \mathbb{N}$ et on définit

$$P(T) = 3\alpha^2 Q(T)^2 + \beta^2 T^{2N},$$

où $\alpha, \beta \in \mathbb{Z}$ premiers entre eux. Soit la surface elliptique décrite par l'équation

$$\mathscr{E} : y^2 = x^3 - 27P(T)Q(T)^2 x - 54\beta P(T)Q(T)^3 T^N.$$

Cette surface respecte les hypothèses du théorème 0.2.3. Par conséquent, le corollaire 0.2.4 implique la Zariski-densité des points rationnels sur $\mathscr{E}$, si l'on admet la conjecture de parité.

Dans cet exemple, on a $\deg P = 2\max(\deg Q, N)$. Par conséquent, dès que $N \geq 4$, on ne sait pas en général si P respecte la conjecture du crible des facteurs carrés. La surface $\mathscr{E}$ définie ci-dessus ne vérifie donc pas les hypothèses du théorème 0.1.13 de Helfgott.

5.1 Places associées à une surface elliptique

5.1.1 Symboles de Kodaira

Soit une surface elliptique $\mathscr{E}$ sur $\mathbb{Q}$ et soit $\Delta(t)$ son discriminant. Nous allons décrire la réduction de $\mathscr{E}$ en w_P une place de $\mathbb{Q}[T]$ associée à un polynôme $P(T) \in \mathbb{Z}[T]$ par un symbole de Kodaira.

Pour que les conditions déterminent aussi le type de la place à l'infini, nous allons écrire $\mathscr{E}_T$ différemment. Soit $(m, n) \in \mathbb{Z}$ des entiers copremiers, $n \neq 0$, tels que $t = \frac{m}{n}$. Soit k le plus petit entier tel que $12k \geq \deg \Delta_T$ comme dans la section 1.2.1. Une fibre $\mathscr{E}_t$ en t qui est non singulière est isomorphe à la courbe

$$\mathscr{E}_{m,n} : y^2 = x^3 - 27n^{4k} c_4(m/n)x - 54n^{6k} c_6(m/n),$$

qui est de discriminant $\Delta_{m,n} = n^{12k}\Delta(m/n)$.

On a que
- la réduction de $\mathscr{E}$ en $P(T)$ est de type I_m si et seulement si $P(T) \nmid c_4(T)$, $P(T) \mid \Delta(T)$ et $m = \mathrm{ord}_{w_P}\Delta(T) = -\mathrm{ord}_{w_P} j(T)$;
- de type I_m^* si et seulement si $P(T) \mid c_4(T)$, $P(T) \mid \Delta(T)$, $-\mathrm{ord}_{w_P} j = m$ et $\mathrm{ord}_{w_P}\Delta(T) = m + 6$;
- de type II si et seulement si $P(T) \mid c_4(T)$, $\mathrm{ord}_{w_P}\Delta(T) = 2$;
- de type III si et seulement si $P(T) \mid c_4(T)$, $\mathrm{ord}_{w_P}\Delta(T) = 3$;
- de type IV si et seulement si $P(T) \mid c_4(T)$, $\mathrm{ord}_{w_P}\Delta(T) = 4$;
- de type I_o^* si et seulement si $P(T) \mid c_4(T)$, $\mathrm{ord}_{w_P}\Delta(T) = 6$;
- de type IV^* si et seulement si $P(T) \mid c_4(T)$, $\mathrm{ord}_{w_P}\Delta(T) = 8$;
- de type III^* si et seulement si $P(T) \mid c_4(T)$, $\mathrm{ord}_{w_P}\Delta(T) = 9$;
- de type II^* si et seulement si $P(T) \mid c_4(T)$, $\mathrm{ord}_{w_P}\Delta(T) = 10$;
- de type I_o si $P \nmid \Delta$.

5.1.2 Notations

Pour alléger les notations, on utilisera la convention suivante.

On note $\mathscr{A}_2(\mathscr{E})$ l'ensemble des places de réduction de type II et II^*, $\mathscr{A}_3(\mathscr{E})$ l'ensemble des places de type III et III^*, $\mathscr{A}_4(\mathscr{E})$ celui des places de type IV et IV^*, $\mathscr{A}_m$ celui des places de type I_m^*. L'ensemble de toutes les places additives sera noté $\mathscr{A}(\mathscr{E})$.

On définit $\mathscr{M}(\mathscr{E})$, comme l'ensemble des places v de $\mathbb{Q}(T)$ pour lesquelles la réduction de $\mathscr{E}$ en v est de type I_m.

On définira aussi $\mathscr{B}(\mathscr{E})$, l'ensemble des places v de $\mathbb{Q}(T)$ pour lesquelles la réduction de $\mathscr{E}$ en v n'est ni de type I_0, ni de type I_0^*. Finalement, on définit $\mathscr{B}'(\mathscr{E})$, l'ensemble des places qui ne sont pas de type I_0.

Remarquons que

$$\mathscr{M}(\mathscr{E}) \subseteq \mathscr{B}(\mathscr{E}) \subseteq \mathscr{B}'(\mathscr{E}).$$

On définit les polynômes homogènes

$$M_{\mathscr{E}}(x,y) = \prod_{v \in \mathscr{M}_{\mathscr{E}}} P_v(x,y)$$

et

$$B_{\mathscr{E}}(x,y) = \prod_{v \in \mathscr{B}_{\mathscr{E}}} P_v(x,y).$$

Avec ces définitions, on a que $M_{\mathscr{E}}(x,y)$ divise $B_{\mathscr{E}}(x,y)$ (qui divise $\Delta(x,y)$).

On fera souvent un abus de notation en omettant de préciser la surface si celle-ci est évidente.

5.2 Étude de la décomposition du signe selon les places de réduction

On rappelle ce qui est davantage détaillé dans la section 2.3 de cette thèse.

Soit $\mathscr{E}$ une surface elliptique non isotriviale représentée par l'équation

$$\mathscr{E} : y^2 = x^3 - 27c_4(T)x - 54c_6(T).$$

Soit $\frac{d_0}{d_1}$, $\frac{d_2}{d_3}$ et $\frac{d_4}{d_5}$ les contenus respectifs de $c_4(T)$, $c_6(T)$ et $\Delta(T)$ écrit sous forme de fractions irréductibles. On pose

$$\delta = 2 \cdot 3 \cdot d_1 \dots d_5 \prod_{Q,Q' \in \mathscr{B}} Res(Q,Q'). \tag{5.1}$$

Soit (m,n) une paire d'entiers premiers entre eux. Par le théorème 2.3.2, le signe de E_t la fibre en $t = \frac{m}{n} \in \mathbb{Q}$ s'écrit

$$W(E_t) = -\lambda(M_{\mathscr{E}}(x,y)) \prod_{p|\delta} W_p(\mathscr{E}_t) \cdot \prod_{P \in \mathscr{B}'} g_{\mathscr{E},\delta,P}(x,y) \cdot \prod_{p \in \mathscr{B}'} h_{\mathscr{E},\delta,P}(x,y),$$

où les fonctions $g_{\mathscr{E},\delta,P}$ et $h_{\mathscr{E},\delta,P}$ sont décrites par le tableau 2.2 qu'on rappelle en tableau 5.1 par commodité de lecture.

Dans la suite de cette section, on étudiera la variation des différentes parties de cette formule.

Type	Forme de $g_{\mathscr{E},\delta,P}(x,y)$	Forme de $h_{\mathscr{E},\delta,P}(x,y)$
I_0	1	1
I_0^*	$(-1\|P(x,y))_\delta$	1
II, II^*	$(-1\|P(x,y))_\delta$	$\prod_{\substack{p\nmid\delta \\ p^2\|P(x,y)}} \begin{cases}(-3/p) & v_p(P(x,y))\equiv 2,4 \mod 6\\ +1 & \text{sinon.}\end{cases}$
III, III^*	$(-2\|P(x,y))_\delta$	$\prod_{\substack{p\nmid\delta \\ p^2\|P(x,y)}} \begin{cases}(-1/p) & v_p(P(x,y))\equiv 2 \mod 4\\ +1 & \text{sinon.}\end{cases}$
IV, IV^*	$(-3\|P(x,y))_\delta$	$\prod_{\substack{p\nmid\delta \\ p^2\|P(x,y)}} \begin{cases}(-3/p) & v_p(P(x,y))\equiv 2,3,4 \mod 6\\ +1 & \text{sinon.}\end{cases}$
I_v^*	$(-1\|P(x,y))_\delta$	$\prod_{\substack{p\nmid\delta \\ p^2\|P(x,y)}} (-(-c_6(x,y)/p))^{v_p(P(x,y))-1}$
I_v	$\left(\prod_{p\|\delta}(-1)^{v_p(P(x,y))}\right)$ $\cdot(-c_6(x,y)\|P(x,y))$	$\prod_{\substack{p\nmid\delta \\ p^2\|P(x,y)}} (-(-c_6(x,y)/p))^{v_p(P(x,y))-1}$

TABLE 5.1 – Contribution d'une place au signe selon le type de réduction : $W_{\mathscr{E},\delta,P}(x,y)$

5.2.1 Signes locaux

On étudie dans cette sous-section le comportement d'un signe local. Nous démontrerons que sur une surface elliptique, le signe local des fibres $W_p(E_t)$ est une fonction localement constante pour la topologie p-adique.

Lemme 5.2.1. *Soit un nombre premier p.*
Pour $c_4, c_6 \in \mathbb{Z}$, on définit la courbe elliptique associée

$$E_{c_4,c_6} : y^2 = x^3 - 27c_4x - 54c_6.$$

On pose

$$\mathscr{U} = \{(c_4,c_6) \in \mathbb{Z}_p \times \mathbb{Z}_p | c_4^3 - c_6^2 \neq 0\}.$$

1. *L'application $\mathscr{U} \longrightarrow \{\pm 1\}$ induite par le signe (c'est-à-dire $(c_4,c_6) \mapsto W_p(E_{c_4,c_6})$) est localement constante pour la topologie p-adique. C'est-à-dire que pour presque tout $c_4, c_6 \in \mathbb{Z}$, il existe un entier $A_p > 0$ tel que pour tout $c_4', c_6' \in \mathbb{Z}$ avec $v(c_j' - c_j) > A_p$, $E' : y^2 = x^3 - 27c_4'x - 54c_6'$ est telle que $W(E) = W(E')$.*
2. *Lorsque $(c_4,c_6) \in \mathbb{Z}_p \times \mathbb{Z}_p$ est tel que $(c_4,c_6) \neq (0,0)$ et $c_4^3 - c_6^2 = 0$, nous étudions le comportement de la fonction signe au voisinage de ce point.*
   Remarquons qu'il existe $t \in \mathbb{Z}_p$ tel que $c_4 = t^2$ et $c_6 = t^3$ et que l'ensemble des courbes singulières est décrit par l'équation suivante (qui est elle-même une courbe singulière) :

$$E_{c_4,c_6} : y^2 = x^3 - 27t^2x - 54t^3.$$

   Alors, il existe V un voisinage de (c_4,c_6) dans $\mathbb{Z}_p$ pour lequel le signe est constant sur $V \cap \mathscr{U}$.

Remarque 73. Lorsque $(c_4,c_6) = (0,0)$, le signe au voisinage de ce point ne peut être constant.

Démonstration. 1) Soit $(c_4, c_6) \in \mathscr{U}$ et E_{c_4,c_6} la courbe elliptique associée à cette paire. Puisque $\Delta(c_4, c_6) \neq 0$, on peut trouver un voisinage sur lequel on a également $\Delta(c_4', c_6') \neq 0$.

De plus, si $\Delta(c_4, c_6)$ est divisible par p, on peut trouver un voisinage sur lequel $\Delta(c_4', c_6')$ a la même valuation p-adique que $\Delta(c_4, c_6)$.

Si la réduction de E_{c_4,c_6} est bonne, potentiellement bonne, ou encore si elle est potentiellement multiplicative et que $p \neq 2$, alors le signe est constant sur un voisinage.

Dans les autres cas, le signe dépend de la classe de $-c_6'$ dans $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$. On cherche donc un voisinage de (c_4, c_6) sur lequel cette classe est constante. Si on prend c_6' tel que $|c_6' - c_6| < p^{-A-1}$, on aura $c_6 \equiv c_6' \mod p$.

2) On suppose $(c_4, c_6) \notin \mathscr{U}$ et on souhaite étudier le comportement de la fonction signe autour de ce point. Soit t tel que $c_4 = t^2$ et $c_6 = t^3$.

(a) Supposons que $t \neq 0$.

Le premier cas que nous allons considérer est celui où $p \nmid t$. On considère alors $E_{\overline{c_4},\overline{c_6}}$ la courbe elliptique sur $\mathbb{F}_p$ dont les coefficients sont les réductions modulo p de c_4 et c_6. Alors $E_{\overline{c_4},\overline{c_6}}$ a un certain type de réduction, qui reste constant sur un certain voisinage, par un argument similaire à celui utilisé pour démontrer 1).

Étudions à présent le cas où $ord_p(t) = 1$. On a $ord_p(c_4) = 2$ et $ord_p(c_6) = 3$, ce qui implique que l'on peut écrire $c_4 = p^2u_0^2$ et $c_6 = p^3u_0^3$ avec un certain u_0 qui est une unité de $\mathbb{Q}_p$. Alors si $(c_4', c_6') \in \mathbb{Q}_\text{ı}$ est tel que $|c_i - c_i'| < \varepsilon$, cela implique que $c_4' = p^2u_4$ et $c_6' = p^3u_6$ où $u_4 \equiv u_0^2 \mod p^N$ et $u_6 \equiv u_0^3 \mod p^N$, pour un certain entier N. De ce fait, $1728\Delta = p^6(u_4^3 - u_6^2) \equiv p^6(u_0^6 - u_0^6) \mod p^{N+6} \equiv 0 \mod p^{N+6}$. On a donc que $E_{c_4',c_6'} \cong E_{u_4,u_6}$ sur $\mathbb{Q}[\sqrt{p}]$.

Si $N = 0$, la réduction de $E_{c_4',c_6'}$ est de type I_m^* $(m \geq 0)$ car $ord_p(\Delta) \geq 6$ et $ord_p(c_4) = 2$ et $ord_p(c_6) = 3$. Ceci est valide pour tout choix de $u_4, u_6)$ dans ce voisinage.

Si $N \geq 1$, pour tout choix de (u_4, u_6) dans le voisinage, la réduction de $E_{c_4',c_6'}$ est de type I_m^* $(m \geq 1)$.

Si $ord(t) = s$, on peut se ramener à un des deux cas précédent selon la parité de s.

□

Corollaire 5.2.2. *Soit $\mathscr{E}$ est une surface elliptique de fibre $\mathscr{E}_t$ en $t \in \mathbb{P}^1$ et soit S l'ensemble des points pour lesquels la fibre n'est pas une courbe elliptique. On pose $U = \mathbb{P}^1 - S$.*

1. *L'application $U(\mathbb{Q}_p) \longrightarrow \{\pm 1\}$ induite par le signe (i.e. $t \mapsto W_p(\mathscr{E}_t)$) est localement constante.*
2. *Lorsque $t_0 \in S$, nous étudions le comportement de la fonction signe au voisinage de ce point.*

   a) Si $(T - t_0)$ est une place de réduction multiplicative alors il existe un voisinage épointé sur lequel le signe est constant.

   b) Si $(T - t_0)$ est une place de réduction additive potentiellement multiplicative, le signe ne dépend que de $(t - t_0) \mod K^{*2}$.

   c) Si $(T - t_0)$ est une place de réduction additive potentiellement bonne, le signe ne dépend que de $(t - t_0) \mod K^{*12}$.

Démonstration. 1. Soit $t_0 \in U(\mathbb{Q}_p)$ alors $\mathscr{E}_{t_0}$ est bien définie. On a un voisinage de $(c_4(t_0), c_6(t_0))$ dans $\mathbb{Z}_p^2$ sur lequel le signe est constant. Soit $t \in U(\mathbb{Q}_p)$ proche de t_0 (dans un certain voisinage). Alors on a $t \equiv t_0 \mod p^N$ pour un certain N. De plus, on aura également $c_4(t) \equiv c_4(t_0) \mod p^N$ et $c_6(t) \equiv c_6(t_0) \mod p^N$. On peut donc contrôler le voisinage dans lequel se situe $(c_4(t), c_6(t))$ et choisir t de façon à ce que la paire de coefficients associée soit dans le voisinage sur lequel le signe est constant.

2. Soit $t_0 \in S$.

a) Supposons que $\mathscr{E}$ ait une place multiplicative en $(T-t_0)$. Alors, $(T-t_0) \not| c_i(t)$, $i=4,6$ et $(T-t_0)|\Delta(t)$ (si on suppose que $\mathscr{E}$ est un modèle minimal). On a donc $c_i(t_0)\neq 0$, $i=4,6$. Par le point 2 de la proposition 2.3.4 et un argument similaire à précédemment, on a un voisinage épointé de t_0 sur lequel le signe est constant.

b) Supposons que $\mathscr{E}$ ait une place additive potentiellement multiplicative en $(T-t_0)$. Alors dans un voisinage épointé de t_0, le signe sera de la forme :

$$\begin{cases} +1 & \text{si } t \text{ est un cube;} \\ \left(\frac{-1}{p}\right), & \text{sinon.} \end{cases}$$

c) Supposons que $\mathscr{E}$ ait une place additive potentiellement bonne en $(T-t_0)$. Alors dans un voisinage épointé de t_0, le signe sera de la forme :

$$\begin{cases} +1 & \text{si } t \text{ est une puissance douzième;} \\ \left(\frac{-1}{p}\right) & \text{si } t \text{ est tel que } v_p(\Delta(\mathscr{E}_t)) \equiv 2 \mod 4; \\ \left(\frac{-2}{p}\right) & \text{si } t \text{ est tel que } v_p(\Delta(\mathscr{E}_t)) \equiv 3 \mod 6; \\ \left(\frac{-3}{p}\right) & \text{si } t \text{ est tel que } v_p(\Delta(\mathscr{E}_t)) \equiv 4 \text{ ou } 8 \mod 12. \end{cases}$$

□

5.2.2 Étude de la fonction $\prod_{p|\delta} W_p(\mathscr{E}_t) \prod_P g_{\mathscr{E},\delta,P}$ selon la surface

Proposition 5.2.3. *Soit $\mathscr{E}$ une surface elliptique. Soit δ défini comme dans* (5.1).

Alors, il existe $N_{\mathscr{E}} \in \mathbb{Z}$ tel que la fonction $\phi : \mathbb{Q} \to \{-1,+1\}$ définie par

$$t = \frac{x}{y} \mapsto \phi_{\mathscr{E}}(x/y) := \prod_{p|\delta} W_p(\mathscr{E}_{\frac{x}{y}}) \prod_{P\in\mathscr{B}} g_{\mathscr{E},\delta,P}(x,y)$$

est telle que $\phi(x/y) = \phi(x'/y')$ pour tous couple de paires d'entiers premiers entre eux tels que $(x,y) \equiv (x',y') \mod N_{\mathscr{E}}$.

Démonstration. Soit $\mathscr{E}$ une surface elliptique et soit $P \in \mathscr{B}$ un polynôme associé à une place de mauvaise réduction sur $\mathscr{E}$.

Dans le cas où la surface $\mathscr{E}$ n'est pas de réduction de type I_m en P, on a

$$g_{\mathscr{E},\delta,P}(m,n) = \left(\frac{\varepsilon_P}{P(m,n)}\right)_\delta$$

où

$$\varepsilon_P = \begin{cases} -1 & \text{si } P \text{ est de type } II,\ II^*,\ I_0^* \text{ ou } I_m^*; \\ -2 & \text{si } P \text{ est de type } III,\ III^*; \\ -3 & \text{si } P \text{ est de type } IV \text{ ou } IV^*, \end{cases}$$

ce qui dépend respectivement de la valeur de $P(x,y)_\delta$ modulo 4, 8 et 12.

Dans le cas où la surface a réduction multiplicative en P, on a

$$g_{\mathscr{E},\delta,P}(x,y) = (-c_6(x,y)|P(x,y))_\delta,$$

pour lesquelles la proposition 2.3.4 donne des entiers N_P sur lesquels les $g_{\mathscr{E},\delta,P}$ sont localement constantes.

Par conséquent, $\prod g_{\mathscr{E},\delta,P}$ est constant sur une classe de (m,n) modulo $24\prod_{P\in\mathscr{M}} N_P$.

On termine la démonstration en remarquant que, par le corollaire 5.2.2, les signes locaux en $p \mid \delta$ des fibres sont localement constants pour la topologie p-adique. Soit pour chaque $p \mid \delta$ le plus petit entier α_p tel que $W_p(E_t) = W_p(E'_t)$ si et seulement si $t \equiv t' \mod p^{\alpha_p}$.

La fonction ϕ est donc constante sur une classe de (m,n) modulo

$$N_{\mathscr{E}} = 24 \prod_{p|\delta} p^{\alpha_p} \prod_{P \in \mathscr{M}} N_P.$$

□

5.2.3 Étude de la fonction $h_{\mathscr{E},\delta,P}$ en une place II, II^*, IV ou IV^*

Lemme 5.2.4. *Soit P un polynôme associé à une place de type II, II^* IV ou IV^*. On suppose que pour tout P_i, facteur irréductible primitif de P,*

$$\mu_3 \subseteq \mathbb{Q}[T]/P(T),$$

où μ_3 est le groupe des racine troisième de l'unité.

Alors pour tout $t = \frac{m}{n} \in \mathbb{Q}$ on a $h_{\mathscr{E},\delta,P}(m,n) = +1$.

Démonstration. Soit $f(T) \in \mathbb{Z}[T]$ un polynôme irréductible non constant, et soit $N = \mathbb{Q}[T]/f(T)$. Soit μ_3 le groupe des racines troisièmes de l'unité, et supposons que $\mathbb{Q}(\mu_3) \subseteq N$. Alors soit un nombre premier p tels que $p \equiv 2 \mod 3$. Un tel p est inerte dans $\mathbb{Q}(\mu_3)/\mathbb{Q}$.

Par conséquent, pour toute paire (m,n) d'entiers premiers entre eux, il n'existe aucun nombre premier $p \equiv 2 \mod 3$ qui divise $P(m,n)$. En d'autres termes, si $p \mid P(m,n)$ alors $p \equiv 1 \mod 3$.

On a donc

$$\begin{aligned} h_{\mathscr{E},\delta,P}(m,n) &= \prod_{p^2 | P(m,n); p \nmid \delta} \begin{cases} \left(\frac{-3}{p}\right) & \text{si } v_p(P(m,n)) \equiv 2,4 \mod 6 \\ +1 & \text{sinon.} \end{cases} \\ &= +1. \end{aligned}$$

□

Remarque 74. On peut facilement donner des exemple de polynômes vérifiant l'hypothèse $\mu_3 \subseteq \mathbb{Q}[T]/(P_i)$ pour chaque facteur. On a en particulier ceux de la forme

$$P(T) = 3A(T)^2 + B(T)^2,$$

où $A(T), B(T) \in \mathbb{Z}[T]$ sont premiers entre eux.

Bien que ce polynôme ne soit pas irréductible en général,ses facteurs vérifient l'hypothèse.

Soit P_i un facteur irréductible de P et $K_i = \mathbb{Q}[T]/(P_i) = \mathbb{Q}(\alpha_i)$ où α_i est une racine de P_i. On a $3A(\alpha_i)^2 + B(\alpha_i) = 0$, donc $-3 = (B(\alpha_i)A(\alpha_i)^{-1})^2$ et par conséquent $\mu_3 \subset K_i$.

Remarque 75. Le raisonnement de la démonstration est inspiré d'un résultat plus général dû à Bauer (voir le livre [36, p.548]). Pour L une extension d'un corps K, on note

$$P(L/K) := \{p \text{ premier de } K \mid \exists \mathfrak{p} \text{ premier de } L \text{ de degré 1 au dessus de } p\}.$$

Théorème 5.2.5. *(Bauer) Soit L/K une extension galoisienne et M/K une extension finie. Alors,*

$$P(L/K) \supseteq P(M/K) \Leftrightarrow L \subseteq M.$$

5.2.4 Étude de $h_{\mathscr{E},\delta,P}$ en une place III ou III^*

Lemme 5.2.6. *Soit P un polynôme associé à une place de type II, II^* IV ou IV^*. On suppose que pour tout P_i, facteur irréductible primitif de P,*

$$\mu_4 \subseteq \mathbb{Q}[T]/P_i(T),$$

où μ_4 est le groupe des racine quatrième de l'unité.

Alors pour tout $t = \frac{m}{n} \in \mathbb{Q}$ on a $h_{\mathscr{E},\delta,P}(m,n) = +1$.

Démonstration. Similaire au lemme 5.2.4. □

Remarque 76. On peut facilement donner des exemples de polynômes dont les facteurs vérifient l'hypothèse $\mu_4 \subseteq \mathbb{Q}[T]/P_i$ pour chaque facteur irréductible. On a ceux de la forme

$$P(T) = A(T)^2 + B(T)^2,$$

où $A(T)$ et $B(T)$ sont des polynômes premiers entre eux.

5.2.5 Étude de $h_{\mathscr{E},\delta,P}$ en une place I_m^* ou I_m

Constance

Lemme 5.2.7. *Soit une surface elliptique admettant une place de réduction I_m^* ou I_m dont le polynôme associé est Q.*

Soit (x,y) et (x',y') des paires d'entiers premiers entre eux telles que $(x,y) \equiv (x',y') \mod N_{\mathscr{E}}$, où $N_{\mathscr{E}}$ est l'entier de la proposition 5.2.3. Pour celles-ci on note $\alpha := Q(x,y)$ et $\beta := Q(x',y')$.

Supposons qu'on a

(1) $\alpha = c^2 l$, où l est sans facteur carré qui divise $N_{\mathscr{E}}$ et $\gcd(c,l) = 1$,

(2) $\beta = c^2\eta$, où η est sans facteur carré qui divise $N_{\mathscr{E}}$, $\gcd(c,\eta) = 1$,

Alors $h_{\mathscr{E},\delta,Q}(x,y) = h_{\mathscr{E},\delta,Q}(x',y')$.

Démonstration. Le lemme découle directement de la forme de la fonction $h_{\mathscr{E},\delta,P}$. □

Variation

Un résultat général sur les polynômes nous permettra de faire varier la fonction $h_{\mathscr{E},\delta,Q}(x,y)$ associée à une place de réduction I_m^*.

Lemme 5.2.8. *[27, Lemme 2.3] Soit $Q(T)$ et $P(T) \in \mathbb{Z}[T]$ avec $Q(T)$ non constant. Soit $R = Res(P,Q)$ le résultant de P et de Q, et soit Δ_Q, le discriminant de Q. On suppose que R et Δ_Q sont non nuls. Soit $\mathscr{P}_0$ un ensemble fini de nombres premiers.*

Alors il existe un nombre premier $p_0 \notin \mathscr{P}_0$ et n un entier positif tel que $p_0^2 \mid Q(n)$ et $p_0^{-2}P(n)Q(n) \equiv 1 \mod p_0$.

En particulier, $p_0^2 \,||\, Q(n)$ et $p_0 \nmid P(n)$.

Nous renvoyons à [27] pour une démonstration élémentaire de ce lemme.

Remarque 77. Il n'est nul besoin que la conjecture du crible des facteurs carrés soit respectée pour que le lemme fonctionne.

Lemme 5.2.9. *Soit une surface elliptique admettant une place de réduction I_m^* dont le polynôme associé est Q. On pose $P = -\frac{c_6(x,y)}{Q(x,y)^3}$.*

Soit (x,y) et (x',y') des paires d'entiers premiers entre eux telles que $(x,y) \equiv (x',y') \mod N_{\mathscr{E}}$, où $N_{\mathscr{E}}$ est l'entier de la proposition 5.2.3. Pour celles-ci on note $\alpha := Q(x,y)$ et $\beta := Q(x',y')$.

Supposons qu'il existe q_0 tel qu'on a

(1) $\alpha = c^2 l$, où l est sans facteur carré qui divise $N_{\mathscr{E}}$ et $\mathrm{pgcd}(c, l, q_0) = 1$,

(2) $\beta = c^2 q_0^2 \eta$, où η est sans facteur carré qui divise $N_{\mathscr{E}}$, $\mathrm{pgcd}(c,\eta) = \mathrm{pgcd}(q_0, c\eta) = 1$,

(3) $q_0 \nmid \delta$ et $q_0^{-2} P(x,y)Q(x,y) \equiv q_0^{-2} P(x',y')Q(x',y') \equiv 1 \mod q_0$

Alors $h_{\mathscr{E},\delta,Q}(x,y) = -h_{\mathscr{E},\delta,Q}(x',y')$.

Démonstration. Soit Q, une place de réduction de type I_m^* de $\mathscr{E}$. On pose $Q(x,y) =: \alpha = c^2 l$ et $Q(x',y') =: \beta = c^2 q_0^2 \eta$ comme dans l'énoncé. Alors par le théorème 2.3.2, on a

$$\begin{aligned} h_{\mathscr{E},\delta,Q}(x',y') &= \prod_{p\nmid\delta; p\mid cq} \begin{cases} -\left(\frac{-c_6(x,y)}{p}\right) & \text{si } 2v_p(qc) \equiv 2,4 \mod 6 \\ +1 & \text{sinon.} \end{cases} \\ &= \left(\frac{-c_6(x,y)}{q_0}\right) \prod_{p\nmid\delta; p\mid c} \begin{cases} -\left(\frac{-c_6(x,y)}{p}\right) & \text{si } v_p(c) \text{ est pair,} \\ +1 & \text{sinon.} \end{cases} \\ &= -\left(\frac{-c_6(x,y)}{q_0}\right) h_{\mathscr{E},\delta,Q}(x,y). \end{aligned}$$

Par hypothèse sur q_0, on a $q_0^{-2}\frac{c_6(x,y)}{Q(x,y)^2} \equiv 1 \mod q_0$. En posant $Q(x,y) = q_0^2 Q'$ où Q' est un entier approprié premier à q_0, on a $q_0^{-6} c_6(x,y) \equiv Q'^2 \mod q_0$. Par conséquent, on a $(\frac{-c_6(x,y)}{q_0}) = +1$ pour tout (x,y).

Donc on a bien

$$h_{\mathscr{E},\delta,Q}(x,y) = -h_{\mathscr{E},\delta,Q}(x',y').$$

□

5.2.6 Étude du signe global sur les surfaces du théorème 5.0.8

Étude du signe en général

Lemme 5.2.10. *Soit $\mathscr{E}$ une surface elliptique respectant les hypothèses du théorème 5.0.8. Soit l'entier $N_{\mathscr{E}}$ donné par la proposition 5.2.3. Soit x, x' deux entiers tels que $x \equiv x' \mod N_{\mathscr{E}}$. Soit n_0 et n_1 tels que $n_0 \equiv n_1 \mod N_{\mathscr{E}}$ et que les valeurs $M_{\mathscr{E}}(x,n_0)$ et $M_{\mathscr{E}}(x',n_1)$ sont des entiers sans facteurs carrés.*

On fait de plus la supposition que pour tout Q de type I_m^* ou I_m, il existe un entier c_Q tel qu'on a $Q(x,n_0) = c_Q^2 l$ et $Q(x',n_1) = c_Q^2 l'$ où l et l' sont des entiers sans facteur carré et premier avec $N_{\mathscr{E}}$.

Alors

$$W(x,n_0) = \lambda(M_{\mathscr{E}}(x,n_0)M_{\mathscr{E}}(x',n_1))W(x',n_1).$$

Remarque 78. Lorsque la seule place de type I_m est celle à l'infini, on prend $n_0 \equiv n_1 \mod N_{\mathscr{E}}$ des entiers sans facteur carré, et la conclusion du lemme s'écrit

$$W(x,n_0) = \lambda(n_0 n_1)W(x,n_1).$$

Lorsqu'il n'y a pas de place I_m, la conclusion de ce lemme est

$$W(x,n_0) = W(x',n_1).$$

Démonstration. Par le théorème 2.3.2, on a pour tout $n \in \mathbb{Z}$,

$$W(x,n) = \lambda(M_{\mathscr{E}}(x,n)) \prod_{p|\delta} W_p(x,n) \prod_{P \in \mathscr{M}} g_{\mathscr{E},\delta,P}(x,n) \prod_{P \in \mathscr{A}} h_{\mathscr{E},\delta,P}(x,n) \cdot h_{\mathscr{E},\delta,\infty}(x,n).$$

Le reste de la démonstration se basera sur le fait que les autres parties de la formule sont constantes.

On sait par construction de l'entier $N_{\mathscr{E}}$ que

$$\prod_{p|\delta} W_p(x,n_0) \prod_{P \in \mathscr{M}} g_{\mathscr{E},\delta,P}(x,n_0) = \prod_{p|\delta} W_p(x',n_1) \prod_{P \in \mathscr{M}} g_{\mathscr{E},\delta,P}(x',n_1).$$

Par le contrôle des facteurs carrés de Q de type I_m^*, et les propositions 5.2.4 et 5.2.6, on a l'égalité

$$\prod_{P \in \mathscr{A}} h_{\mathscr{E},\delta,P}(x,n_0) = \prod_{P \in \mathscr{A}} h_{\mathscr{E},\delta,P}(x,n_0).$$

Finalement, on observe que

$$h_{\mathscr{E},\delta,\infty}(x,n_0) = h_{\mathscr{E},\delta,\infty}(x',n_1) = +1.$$

□

Lorsqu'il n'y a pas de place I_m

Proposition 5.2.11. *Soit E une surface elliptique respectant les hypothèses du théorème 5.0.8 qui n'admet pas de place de type I_m. Soit aussi $N_{\mathscr{E}}$ l'entier correspondant à $\mathscr{E}$ donné par le théorème 2.3.2.*

Soit $t_1 = \frac{m_1}{n_1} \in \mathbb{Q}$ et $t_2 = \frac{m_2}{n_2} \in \mathbb{Q}$ des entiers satisfaisant aux propriétés suivantes.

1. $(m_1,n_1) \equiv (m_2,n_2) \mod N_{\mathscr{E}}$ *une classe de congruence non nulle,*
2. *Pour un certain Q_0 de type I_m^*, on a*
   (a) $Q_0(m_1,n_1) = c^2 l$ *où l est un entier premier à $N_{\mathscr{E}}$ qui est sans facteur carré,*
   (b) $Q_0(m_2,n_2) = c^2 q_0^2 l'$ *où l' est premier à $N_{\mathscr{E}}$ et sans facteur carré, et q_0 est un nombre premier qui ne divise pas δ et tel que $-p_0^{-6} c_6(x_i,y_i)$ est un carré mod q_0 pour $i = 1,2$.*
3. *Pour tout $Q \neq Q_0$ de type I_m^*,*
   (a) $Q(m_1,n_1) = c_Q^2 l_Q$ *où l_Q est un entier premier à $N_{\mathscr{E}}$ qui est sans facteur carré,*
   (b) $Q(m_2,n_2) = c_Q^2 l'_Q$ *où l'_Q est premier à $N_{\mathscr{E}}$ et sans facteur carré,.*

Alors, on a

$$W(E_{t_1}) = -W(E_{t_2}).$$

Démonstration. La proposition se démontre comme le lemme 5.2.10, hormis que pour la fonction associée au polynôme Q_0, on utilise la proposition 5.2.9 pour voir que

$$h_{\mathscr{E},\delta,Q_0}(m_1,n_1) = -h_{\mathscr{E},\delta,Q_0}(m_2,n_2).$$

□

5.3 Surfaces telles que $M_{\mathscr{E}} = 1$

Théorème 5.3.1. *Soit $\mathscr{E}$ une surface elliptique non isotriviale qui satisfait aux hypothèses du théorème 5.0.8 et qui de plus n'admet pas de place de réduction de type I_m.*

Alors l'ensembles $W_\pm$ sont tous deux infinis.

Démonstration. Soit $\frac{d_0}{d_1}$, $\frac{d_2}{d_3}$, $\frac{d_4}{d_5}$ les contenus respectifs des polynômes $c_4(T)$, $c_6(T)$, $\Delta(T)$ associés à $\mathscr{E}$. On pose

$$\delta = 2 \cdot 3 \cdot d_1 \dots d_5 \prod_{Q,Q' \in \mathscr{B}} Res(Q, Q').$$

Soit $N = N_{\mathscr{E}}$ l'entier donné par la proposition 5.2.3 (on le choisit de sorte qu'il soit minimal). La fonction $t \mapsto \prod_{p|\delta} W_p(\mathscr{E}_{\frac{m}{n}}) \prod_{P \in \mathscr{B}} g_{\mathscr{E},\delta,P}(m,n)$ est constante chaque classe de congruence modulo N.

Pour chaque $p \mid N$, on pose $\alpha_p = v_p(N)$.

On pose

$$S = \{2, 3, p_1, \dots, p_r\},$$

et

$$T = \{0, \dots, 0\}.$$

Soit une classe $(\mathfrak{a}_2, \mathfrak{b}_2) \mod 2^{\alpha_2}$ telle que

$$P_i(\mathfrak{a}_2, \mathfrak{b}_2) \not\equiv 0 \mod 2^{\alpha_2}$$

pour tout $P_i \in \mathscr{A}$.

Soit une classe $(\mathfrak{a}_3, \mathfrak{b}_3) \mod 3^{\alpha_3}$ tel que

$$P_i(\mathfrak{a}_3, \mathfrak{b}_3) \not\equiv 0 \mod 3^{\alpha_3}$$

pour tout $P_i \in \mathscr{A}$

Soient aussi des classes $(a_p, b_p) \mod p^{\alpha_p}$ pour chaque $p \mid N$ tel que $p \neq 2, 3$ on a pour tout $P \in \mathscr{A}$

$$P(a_p, b_p) \not\equiv 0 \mod p^{\alpha_p}.$$

Comme P est de contenu 1 par hypothèse, de telles classes (a_p, b_p) existent pour tout $p \mid N$.

Par le théorème des restes chinois, il existe une classe de congruence (a, b) modulo M respectant

$$(a,b) \equiv \begin{cases} (\mathfrak{a}_2, \mathfrak{b}_2) & \mod 2^{\alpha_2}, \\ (\mathfrak{a}_3, \mathfrak{b}_3) & \mod 3^{\alpha_3}, \\ (a_p, b_p) & \mod p^{\alpha_p} \quad \text{pour tout } p \mid \delta, \end{cases} \tag{5.2}$$

On pose $Q_0 = \prod_{Q \in \mathscr{A}'} Q$.

Par le crible des facteurs carrés 1.3.5 appliqué à Q_0, S, T, N, a et b comme précédemment, il existe un ensemble infini $\mathscr{F}_1$ de paires $(m, n) \in \mathbb{Z}^2$ telles que

$$Q_0(m, n) = l,$$

où l est un entier sans facteur carré premier avec tout $p \in S$ par nos choix de S et de T.

Par la proposition 5.2.11, pour tout $(x, y), (x', y') \in \mathscr{F}_1$,

$$W(x, y) = W(x', y').$$

On choisit Q_1 un polynôme associé à une des places de type I_m^*.

On pose $R(m,n) = -c_6(x,y)/Q(x,y)^3$. Par le lemme 5.2.8 appliqué à $R(t,1), Q(t,1)$ et S, il existe $q_0 \notin S$ et m_0 un entier positif tels que $q_0^2 \mid Q(m_0,1)$ et $-q_0^{-2}P(m_0,1)Q(m_0,1)$ est un carré modulo q_0.

Soit l'ensemble

$$S' = \{2, 3, p_1, \ldots, p_r, q_0\}$$

et

$$T' = \{0, \ldots, 0, 2\}.$$

Par le lemme chinois, il existe une paire d'entiers (a', b') respectant simultanément (5.4) et

$$a' \equiv m_0 \mod q_0^3,\ b' \equiv 1 \mod q_0^3.$$

En appliquant le crible 1.3.5 à

$$Q_1,\ S',\ T',\ a' \text{ et } b',$$

on obtient $\mathscr{F}_2$ un ensemble infini de paires telles que

$$Q_1(x,y) = q_0^2 l,$$

où l est un entier sans facteur carré premier avec tout élément de S' et où $q_0^{-6}c_6(x,y)$ un carré modulo q_0. Par la proposition 5.2.11, tous les éléments de $\mathscr{F}_2$ ont le même signe.

Enfin, par la proposition 5.2.11, pour tout $(x,y) \in \mathscr{F}_1$, et tout $(x',y') \in \mathscr{F}_2$, on a

$$W(\mathscr{E}_{\frac{x}{y}}) = -W\left(\mathscr{E}_{\frac{x'}{y'}}\right).$$

□

5.4 Surfaces avec des places de type I_m

Pour démontrer $\#W_\pm = \infty$ sur des surfaces possédant des places de réduction multiplicative, une difficulté supplémentaire se présente. Il faut contrôler les deux quantités suivantes simultanément :

1. les facteurs carrés de $M_{\mathscr{E}}(x,y)$.
2. le nombre de facteurs de $M_{\mathscr{E}}(x,y)$, comptés avec multiplicité.

Dans la section 1.3.3, on a démontré le résultat suivant, qui règle ce problème.

Théorème 5.4.1. *Soit $f \in \mathbb{Z}[X,Y]$ polynôme homogène à coefficients entiers, sans facteurs carrés. Supposons la conjecture du crible des facteurs carrés et la conjecture de Chowla vraies pour f, alors l'estimation suivante vaut pour tout réseau $\mathcal{A}'$, où $\epsilon = \pm 1$:*

$$\sharp\left\{(m,n) \in \mathcal{A}'(X) \mid \frac{f(m,n)}{d_{f,\mathcal{A}'}} \text{ est sans facteur carré et } \lambda(f(m,n)) = \epsilon\right\} = \frac{c_{f,\mathcal{A}'}}{2}\mathrm{A}'(X) + o(A'(X)). \tag{5.3}$$

Remarque 79. La conclusion du théorème vaut donc inconditionnellement si $\deg f \leq 3$ ou si f est produit de formes linéaires.

Notation 7. Rappelons qu'un réseau est un ensemble de la forme

$$\mathcal{A} = \{(ax + by, cx + dy) \in \mathbb{Z}^2 |\ (x, y) \in \mathbb{Z}^2\}$$

où $ad - bc \neq 0$. On note $\mathrm{A}(X) := \{(m, n) \in \mathcal{A} \mid |(m, n)| \leq X\}$ et $A(X) := \sharp\mathrm{A}(X)$.

Rappelons aussi que $d_{f,\mathcal{A}}$ est le plus petit entier tel que $\frac{\delta_{f,\mathcal{A}}}{d_{f,\mathcal{A}}}$ est sans facteur carré, où $\delta_{f,\mathcal{A}} = pgcd(f(m, n), (m, n) \in \mathcal{A})$.

Cela nous permet de compléter la démonstration du théorème 5.0.8 :

Théorème 5.4.2. *Soit $\mathscr{E}_T$ une surface elliptique non isotriviale qui respecte les hypothèses du théorème 5.0.8. On suppose que $M_{\mathscr{E}} \neq 1$, c'est-à-dire qu'il existe des places génériques de réduction multiplicative.*

Alors les ensembles $W_{\pm}(\mathscr{E})$ sont tous deux infinis.

Démonstration. On étudiera une surface dont la place à l'infini n'est pas I_m (quitte à faire un changement de variables, on peut faire cette supposition).

Soit $N_{\mathscr{E}}$ l'entier correspondant à $\mathscr{E}$ donné par la proposition 5.2.3. Pour chaque $p \mid M$, soit $\alpha_p = v_p(N_{\mathscr{E}})$, de sorte que

$$N_{\mathscr{E}} = 2^{\alpha_2} 3^{\alpha_3} \cdot p_1^{\alpha_{p_1}} \dots p_r^{\alpha_{p_r}}.$$

On pose

$$S = \{2, 3, p_1, \dots, p_r\}$$

et

$$T = \{0, \dots, 0\}.$$

De la même façon que dans la démonstration du théorème, le théorème des restes chinois permet d'obtenir (a, b), une classe modulo $N_{\mathscr{E}}$ telle que

$$\begin{cases} B_{\mathscr{E}}(a, b) \not\equiv 0 \mod 2^{\alpha_2}, \\ B_{\mathscr{E}}(a, b) \not\equiv 0 \mod 3^{\alpha_3}, \\ B_{\mathscr{E}}(a, b) \not\equiv 0 \mod p^{\alpha_p} \quad \text{pour tout } p \mid \delta, \end{cases} \tag{5.4}$$

Par le crible des facteurs carrés 1.3.5 appliqué à $B_{\mathscr{E}}, S, T, N_{\mathscr{E}}, a$ et b, il existe un ensemble infini $\mathscr{F}$ de paires $(m, n) \in \mathbb{Z}^2$ telles que

$$B_{\mathscr{E}}(m, n) = l,$$

où l est un entier sans facteur carré premier avec tout $p \in S$ par nos choix de S et de T.

Par le lemme 5.2.11, pour tout $(x, y), (x', y') \in \mathscr{F}$ on a

$$W(x, y) = \lambda(M_{\mathscr{E}}(x, y) M_{\mathscr{E}}(x', y)) W(x', y).$$

Grâce au théorème 5.4.1, on extrait de cet ensemble des sous-ensembles infinis $\mathscr{F}_1$ et $\mathscr{F}_2$ tels que

1. $(m, n) \in \mathscr{F}_1$ est tel que $\lambda(M_{\mathscr{E}}(m, n)) = +1$,
2. $(m', n') \in \mathscr{F}_2$ est tel que $\lambda(M_{\mathscr{E}}(m', n')) = -1$.

Pour tout $(m, n) \in \mathscr{F}_1$, $(m', n') \in \mathscr{F}_2$, on a

$$W(m, n) = -W(m', n').$$

□

5.5 Exemples

Il existe de nombreuses surfaces respectant les hypothèses du théorème 5.0.8 comme en témoigne le théorème suivant.

Théorème 5.5.1. *Soit Q un polynôme sans facteur carré dont les facteurs irréductibles sont de degré inférieur ou égal à 6 et différents de T. Soit $N \in \mathbb{N}$. On pose*

$$P(T) = 3\alpha^2 Q(T)^2 + \beta^2 T^{2N},$$

et $\alpha, \beta \in \mathbb{Z}$ premiers entre eux.

Soit $\mathscr{E}$ la surface elliptique décrite par l'équation

$$\mathscr{E} : y^2 = x^3 - 27P(T)Q(T)^2 x - 54\beta P(T)Q(T)^3 T^N.$$

Alors W_+ et W_- sont infinis.

De plus, si on suppose la conjecture de parité, alors les points rationnels de $\mathscr{E}$ sont Zariski-denses.

Remarque 80. Lorsque $N \geq 4$, la conjecture du crible des facteurs carrés n'est pas démontrée en général sur P. Les surfaces étudiées ne sont donc pas incluses dans les travaux d'Helfgott.

Démonstration. Pour $t \in \mathbb{Q}$ qu'on écrit $t = \frac{m}{n}$ pour $m, n \in \mathbb{Z}$ premiers entre eux, on note $\mathscr{E}_{m,n}$ la courbe elliptique isomorphe à $\mathscr{E}_t$ la fibre en t de $\mathscr{E}$:

$$\mathscr{E}_{m,n} : y^2 = x^3 - 27n^{4k-\deg P-2\deg Q} P(m,n)Q(m,n)^2 - 54\beta n^{6k-\deg P-3\deg Q-N} P(m,n)Q(m,n)^3 m^N,$$

où k est le plus petit entier tel que $4k \geq \deg c_4(T)$ et $6k \geq \deg c_6(T)$.

Cette courbe elliptique est de discriminant $\Delta(m,n) = \gamma n^{12k-2\deg P-8\deg Q} P(m,n)^2 Q(m,n)^8$, pour une certaine constante $\gamma \in \mathbb{Q}$. On cherche quel est la valeur de k, et celle de $12k - 2\deg P - 8\deg Q$ qui nous donnera le type de la réduction en la place à l'infini.

Supposons que $N \leq \deg Q$. On a $\deg P = 2\deg Q$ et par conséquent

$$\deg c_4(T) = 4\deg Q,$$

$$\deg c_6(T) = 5\deg Q + N,$$

$$\deg \Delta(T) = 12\deg Q.$$

On a $k = \deg Q$ et $12k - 2\deg P - 8\deg Q = 0$. La place à l'infini est donc de bonne réduction. Les places de mauvaises réduction de la surface $\mathscr{E}$ sont les suivantes :

— les places associées aux P_i, les facteurs irréductibles de $P(T) = P_1^{e_1} \dots P_n^{e_n}$ qui sont de type II, IV, I_0^*, IV^*, II^* ou I_0 selon $e_i \mod 6$;

— les places associées aux facteurs de $Q(T)$ de type I_2^* ; et

Supposons maintenant que $N \geq \deg Q$ et posons $N = \deg Q + a$ pour un certain $a \in \mathbb{N}$. Remarquons que $\deg P = 2N$. On a

$$\deg c_4(T) = 4\deg Q + 2a,$$

$$\deg c_6(T) = 6\deg Q + 3a,$$

$$\deg \Delta(T) = 12\deg Q + 4a.$$

La surface $\mathscr{E}$ admet les places de mauvaise réduction suivantes :

— les places associées aux P_i, les facteurs irréductibles de $P(T) = P_1^{e_1} \dots P_n^{e_n}$ qui sont de type II, IV, I_0^*, IV^*, II^* ou I_0 selon $e_i \mod 6$;
— les places associées aux facteurs de $Q(T)$ de type I_2^* ; et
— la place à l'infini est I_{2a}^* ou I_{2a} selon la parité de a.

Pour commencer, remarquons que pour tout $p \mid P(m,n)$, on a

$$3\alpha^2 Q(m,n)^2 + \beta^2 m^{\deg Q} \equiv 0 \mod p$$

$$\Rightarrow \left(\frac{\beta m^{\deg Q}}{\alpha Q(m,n)}\right)^2 \equiv -3 \mod p.$$

Cela signifie que pour tout $p \mid P(m,n)$, on a $(\frac{-3}{p}) = +1$. Soit R un facteur irréductible de P. On a $3\alpha^2 Q(T)^2 + \beta^2 T^{2n} = R(T)P_1(T)$, pour un certain polynôme P_1 tel que $R(T)P_1(T) = P(T)$. Le corps $\mathbb{Q}[T]/R(T)$ est engendré par ξ, qui est une racine de R. De plus, ξ est telle que $3\alpha^2 Q(\xi)^2 + \beta^2 \xi^{2N} = 0$. Par conséquent, on a $-3 = (\frac{\beta \xi^N}{\alpha Q(\xi)})^2$ et $\mathbb{Q}(\mu_3) \subset K$.

Si a est pair, la valeur de k est $\deg Q + \frac{a}{2}$, on a $12k - 2\deg P - 8\deg Q = 2a$ et $\deg c_4 \equiv 0 \mod 4$. Par conséquent, la place à l'infini est de type I_{2a}. Comme c'est la seule place de type multiplicatif et que P et Q (associés aux deux autres places) respectent les hypothèses du théorème 5.0.8, la densité des points rationnels est démontrée conditionnellement à la conjecture de parité.

Si a est impair, la valeur de k est $\deg Q + \frac{a+1}{2}$, on a $12k - 2\deg P - 8\deg Q = 2a$ et $\deg c_6 \equiv 2 \mod 4$. Par conséquent, la place à l'infini est de type I_{2a}^*. Dans ce cas aussi, on obtient la conclusion du théorème par l'application du théorème 5.0.8. □

Remarque 81. Les hypothèses du théorème peuvent être assouplies.

1. On peut alléger l'hypothèse sur Q, plutôt que le supposer sans facteur carré. On peut l'autoriser à prendre la forme

$$Q = R(T) \prod_{j=1}^{s} (T - a_j)^{e_j},$$

où pour tout $j = 1, \cdots, s$, $a_j \in \mathbb{Q}$ et $e_j \in \mathbb{N}$, et où $R(T)$ est un polynôme sans facteur carré dont les facteurs irréductibles sont de degré ≤ 6.

Dans ce cas, les places multiplicatives sont

(a) éventuellement la place à l'infini,

(b) les places associées aux $T - a_j$ dont l'exposant e_j est pair.

Par conséquent, le polynôme M_E est un produit de facteurs linéaires et respecte bien la conjecture de Chowla.

2. On peut remplacer T^N par un polynôme $S(T) \in \mathbb{Z}[T]$ tel que $Res(S,Q) \neq 0$. Précisément, on définit

$$P = 3\alpha^2 Q^2 + \beta^2 S^2,$$

où $\alpha, \beta \in \mathbb{Q}$, et on considère la surface elliptique d'équation de Weierstrass

$$y^2 = x^3 - 27PQ^2 x - 54\beta PQ^3 S.$$

Bibliographie

[1] J. Browkin, M. Filaseta, G. Greaves et A. Schinzel : *Sieve Methods, Exponential Sums, and their Applications in Number Theory (Cardiff, 1995)*, chap. Squarefree values of polynomials and the abc-conjecture, p. 65–85. 237. London Mathematical Society Lecture Note, Cambridge, 1997.

[2] J. W. S. Cassels : *Lectures on elliptic curves*, vol. 24 de *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1991.

[3] J. W. S. Cassels et A. Schinzel : Selmer's conjecture and families of elliptic curves. *Bull. London Math. Soc.*, 14(4):345–348, 1982.

[4] B. Conrad, K. Conrad et H. Helfgott : Root numbers and ranks in positive characteristic. *Adv. Math.*, 198(2):684–731, 2005.

[5] H. Darmon : Wiles' theorem and the arithmetic of elliptic curves. *In Modular forms and Fermat's last theorem (Boston, MA, 1995)*, p. 549–569. Springer, New York, 1997.

[6] P. Deligne : Les constantes des équations fonctionnelles des fonctions L. *In Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, p. 501–597. Lecture Notes in Math., Vol. 349. Springer, Berlin, 1973.

[7] T. Dokchitser et V. Dokchitser : On the Birch-Swinnerton-Dyer quotients modulo squares. *Ann. of Math. (2)*, 172(1):567–596, 2010.

[8] A. Granville : *ABC* allows us to count squarefrees. *Internat. Math. Res. Notices*, (19):991–1009, 1998.

[9] G. Greaves : Power-free values of binary forms. *Quart. J. Math. Oxford Ser. (2)*, 43(169):45–65, 1992.

[10] B. Green et T. Tao : Linear equations in the primes. *Annals of mathematics*, 171:1753–1850, 2010.

[11] B. Green et T. Tao : The Möbius function is strongly orthogonal to nilsequences. *Ann. of Math. (2)*, 175(2):541–566, 2012.

[12] B. Green, T. Tao et T. Ziegler : An inverse theorem for the gowers $u_{s+1}[n]$-norm. *Annals of Mathematics (2)*, 176(2):1231–1372, 2012.

[13] E. Halberstadt : Signes locaux des courbes elliptiques en 2 et 3. *C. R. Acad. Sci. Paris Sér. I Math.*, 326(9):1047–1052, 1998.

[14] R. Hartshorne : *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.

[15] H. A. Helfgott : On the behaviour of root numbers in families of elliptic curves. arXiv :math/0408141v3, 2003.

[16] H. A. Helfgott : The parity problem for irreducible polynomials. arXiv :math/0501177, 2005.

[17] H. A. Helfgott : The parity problem for reducible cubic forms. *J. London Math. Soc. (2)*, 73(2):415–435, 2006.

[18] C. Hooley : On the power free values of polynomials. *Mathematika*, 14:21–26, 1967.

[19] V. A. Iskovskih : Minimal models of rational surfaces over arbitrary fields. *Izv. Akad. Nauk SSSR Ser. Mat.*, 43(1):19–43, 237, 1979.

[20] K. Kodaira : On compact analytic surfaces. I, II, III. *Ann. of Math. (2) 77 (1963), 563–626 ; ibid.*, 78:1–40, 1963.

[21] J. Kollár : *Rational curves on algebraic varieties*, vol. 32 de *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics*. Springer-Verlag, Berlin, 1996.

[22] J. Kollar : Unirationality of cubic hypersurfaces. *J. Inst. Math. Jussieu*, 1(3):467–476, 2002.

[23] J. Kollár et M. Mella : Quadratic families of elliptic curves and unirationnality of degree 1 conic bundles. arXiv :1412.3673, 2014.

[24] A. Lachand : *Entiers friables et formes binaires*. Thèse de doctorat, Université de Lorraine, 2014.

[25] A. Lachand : Fonctions arithmétiques et formes binaires irréductibles de degré 3. 2014.

[26] E. Liverance : A formula for the root number of a family of elliptic curves. *J. Number Theory*, 51(2):288–305, 1995.

[27] E. Manduchi : Root numbers of fibers of elliptic surfaces. *Compositio Math.*, 99(1): 33–58, 1995.

[28] Y. I. Manin : *Cubic forms : algebra, geometry, arithmetic*. North-Holland Publishing Co., Amsterdam-London ; American Elsevier Publishing Co., New York, 1974. Translated from the Russian by M. Hazewinkel, North-Holland Mathematical Library, Vol. 4.

[29] K. Matomäki, M. Radziwiłł et T. Tao : An averaged form of Chowla's conjecture. *Algebra Number Theory*, 9(9):2167–2196, 2015.

[30] B. Mazur : Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, (47):33–186 (1978), 1977.

[31] B. Mazur : Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.

[32] B. Mazur : Topology of rational points. *Experiment. Math.*, 1(1):35–45, 1992.

[33] R. Miranda : *The Basic Theory of elliptic surfaces*. ETS Editrice Pisa, 1989.

[34] J. Nekovář : On the parity of ranks of Selmer groups. II. *C. R. Acad. Sci. Paris Sér. I Math.*, 332(2):99–104, 2001.

[35] A. Néron : Modèles minimaux des variétés abéliennes sur les corps locaux et globaux. *Inst. Hautes Études Sci. Publ. Math. No.*, 21:128, 1964.

[36] J. Neukirch : *Algebraic number theory*, vol. 322. Grundlehren der Mathematischen Wissenschften, Berlin, 1999.

[37] O. G. Rizzo : Average root numbers for a nonconstant family of elliptic curves. *Compositio Math.*, 136(1):1–23, 2003.

[38] D. E. Rohrlich : Variation of the root number in families of elliptic curves. *Compositio Math.*, 87(2):119–151, 1993.

[39] D. E. Rohrlich : Galois theory, elliptic curves, and root numbers. *Compositio Math.*, 100(3):311–349, 1996.

[40] C. Salgado : On the rank of the fibres of rational elliptic surfaces. *Algebra and Number Theory*, 6(7):1289–1309, 2012.

[41] C. Salgado, D. Testa et A. Várilly-Alvarado : On the unirationality of del Pezzo surfaces of degree two. *J. London Math. Soc.*, 90:121–139, 2014.

[42] C. Salgado et R. van Luijk : Density of rational points on del Pezzo surfaces of degree one. *Adv. Math.*, 261:154–199, 2014.

[43] J.-P. Serre : *Cours d'arithmétique*. Presses Universitaires de France, Paris, 1977. Deuxième édition revue et corrigée, Le Mathématicien, No. 2.

[44] T. Shioda : On elliptic modular surfaces. *J. Math. Soc. Japan*, 24:20–59, 1972.

[45] J. H. Silverman : *Advanced Topics in the Arithmetic of Elliptic Curves*. Graduate Texts in Mathematics.

[46] J. H. Silverman : Heights and the specialization map for families of abelian varieties. *J. Reine Angew. Math.*, 342:197–211, 1983.

[47] J. H. Silverman : *The Arithmetic of Elliptic Curves*, vol. 106. Springer-Verlag, New-York, 1994.

[48] J. Tate : Algorithm for determining the type of a singular fibre in an elliptic pencil. *Lect. Notes in Math.*, Modular functions of one variable IV (Antwerpen 1972)(476):33–52, 1975.

[49] J. Tate : *Number theoretic background, Automorphic forms, representations and L-functions*. Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977.

[50] M. Ulas : Rational points on certain del Pezzo surfaces of degree one. *Glasg. Math. J.*, 50(3):557–564, 2008.

[51] A. Várilly-Alvarado : Density of rational points on isotrivial rational elliptic surfaces. *Algebra & Number Theory*, 5:659–690, 2011.

[52] A. Wiles : Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.