PONTIFICIA
UNIVERSIDAD
CATÓLICA
DE CHILE

FACULTAD DE MATEMÁTICAS

SOME ADVANCES IN A CONJECTURE OF WATKINS AND AN ANALOGUE OVER FUNCTION FIELDS

by
JERSON CARO REYES

Tesis presentada a la Facultad de Matemáticas de la
Pontificia Universidad Católica de Chile
para optar al grado académico de Doctor en Matemática

Thesis advisor
Prof. HECTOR PASTEN VASQUEZ

ASSESSMENT COMMITTEE:
Prof. RICARDO MENARES VALENCIA
Prof. FABIEN MEHDI PAZUKI

March, 2023
Santiago Chile

Acknowledgements

First of all, I would like to express my sincere gratitude to my advisor Hector Pasten. His office was always open whenever I needed advice and guidance in solving all the problems that arose while writing this thesis. Thanks for your guidance as a mathematician and as a person.

I am very grateful for financial support from ANID (ex CONICYT) Doctorado Nacional 2019, 21190304.

In my whole career, I have had excellent Professors, Prof. Natalia Garcia, Prof. Ricardo Menares, and Prof. Guillermo Mantilla-Soler. All of them have helped me and have been an inspiration to me.

I would also like to thank my friends and classmates: Matias Alvarado, Nicolas Arevalo, Jaime Gomez, David Jaramillo, Patricio Perez, and Danilo Polo who gave me support in many opportunities when I wanted to put aside mathematics for personal problems.

I must express my profound gratitude to my mother, my brother, and Teresa Jimenez for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of creating this thesis. This accomplishment would not have been possible without them.

Finally, I heartily thank the assessment committee for carefully reading this thesis and for several useful comments on an earlier version of it. Thank you.

Abstract

Our results are divided into two main parts, both related to a conjecture by Watkins. In 2002, Watkins conjectured that the rank of an elliptic curve defined over $\mathbb{Q}$ is at most the 2-adic valuation of its modular degree.

The first part is related to presenting some approaches to Watkins's conjecture in its original version. We prove this conjecture for semistable elliptic curves having exactly one rational point of order 2, provided that they have an odd number of primes of non-split multiplicative reduction or no primes of split multiplicative reduction. In addition, we show that this conjecture is satisfied when E is any quadratic twist of an elliptic curve with non-trivial rational 2-torsion and prime power conductor, in particular, for the congruent number elliptic curves.

In the second part, we consider the analogous problem over function fields of positive characteristic, and we prove it in several cases. More precisely, every modular semistable elliptic curve over $\mathbb{F}_q(T)$ after extending constant scalars and every quadratic twist of a modular elliptic curve over $\mathbb{F}_q(T)$ by a polynomial with sufficiently many prime factors satisfy this version of Watkins's conjecture. Additionally, we prove the analogue of Watkins's conjecture for a well-known family of elliptic curves with unbounded rank due to Ulmer.

In addition, we include a final appendix describing joint work with Hector Pasten [16] on a generalization of the Chabauty-Coleman bound for surfaces. While this is not directly related to the core of the thesis, it is a report on work that was performed during my time as a Ph.D. student.

Contents

Chapter 1

Introduction

1.1 Introduction to Watkins's conjecture

Let E be an elliptic curve defined over $\mathbb{Q}$. The modularity theorem [12, 85, 92] ensures the existence of a non-constant morphism $\phi : X_0(N) \to E$ defined over $\mathbb{Q}$. Denote by ϕ_E the morphism, up to sign, which has minimal degree and which sends the cusp $i\infty$ to the neutral point of E. *The modular degree* m_E of E is the degree of ϕ_E. This number is linked to important arithmetic questions such as the abc conjecture [39, 64] and congruences of modular forms [2, 20, 94]. In 2002 Watkins conjectured:

Conjecture 1.1.1 (Watkins [91])**.** *We have that* $2^{r(E)}$ *divides* m_E*, where* $r(E) = \operatorname{rank} E(\mathbb{Q})$.

For instance, the elliptic curve given by the equation $E\colon y^2 = x^3 - x + 1$ has Mordell-Weil rank $r(E) = 1$ and modular degree $m_E = 6$. As of today, the problem remains open. In this thesis, we proved several cases of this conjecture and we investigated a function field analogue.

1.2 Statement of Principal Results

The main strategy to prove that an elliptic curve E satisfies Watkins's conjecture is to give an upper bound R_E for $r(E)$, a lower bound M_E for $\nu_2(m_E)$ and then show that $R_E \leq M_E$.

1.2.1 Different approaches to Watkins's Conjecture

Semistable elliptic curves

In joint work with Pasten [17] we prove Watkins's conjecture for a large family of semistable elliptic curves:

Theorem 1.2.1. *Let E be a semistable elliptic curve over $\mathbb{Q}$ with $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z}$. If the number of primes of non-split multiplicative reduction for E is odd, or if there is no prime of split multiplicative reduction, then Watkins's conjecture holds for E.*

The proof of this theorem has two main ingredients: Firstly, results of Dummingan and Krishnamoorthy [31] provide suitable lower bounds for the 2-adic valuation of the modular degree. Secondly, with Pasten we prove a descent upper bound for the rank, which is of independent interest.

Proposition 1.2.2 (Rank bound)**.** *Let E be an elliptic curve defined over $\mathbb{Q}$ with $E(\mathbb{Q})[2] \neq (0)$. Let α and μ be the number of primes of additive and multiplicative reduction of E, respectively. Then*

$$r(E) \leq 2\alpha + \mu - 1.$$

These bounds, unfortunately, do not match and a further ingredient is necessary: results of Monsky that prove cases of the parity conjecture under a finiteness assumption on Shafarevich-Tate groups. To get an unconditional result, part of the problem is to control these Shafarevich-Tate groups.

Quadratic Twists

In 2021, Esparza-Lozano and Pasten in [34] proved that if E is an elliptic curve defined over $\mathbb{Q}$ of conductor N (minimal conductor among all its quadratic twists) with non-trivial rational 2-torsion, then its quadratic twist $E^{(D)}$ by a quadratic fundamental discriminant D satisfies Watkins's conjecture, whenever the number of the distinct prime divisors of D is big enough. We specialize this process in elliptic curves with prime power conductor, and we obtain that Watkins's conjecture holds unconditionally for $E^{(D)}$ [15].

Theorem 1.2.3. *Let E be an elliptic curve with non-trivial rational 2-torsion. Assume that E is a quadratic twist of an elliptic curve with prime power conductor. Then E satisfies Watkins's conjecture.*

To prove this Theorem, we listed the elliptic curves with prime power conductor, up to quadratic twist, and non-trivial rational 2-torsion. Then, we obtained an upper bound for $\nu_2(m_E)$ by computing the Manin constant c_E and the minimal discriminant of the quadratic twists $\Delta_{E^{(D)}}$, and giving an upper bound for the 2-adic valuation of the norm of f_E (the

associated newform to E) via the Petterson inner product. The upper bound must be carefully computed to match the lower bound given by Proposition 1.2.2.

Quartic Twists

Since the elliptic curve $y^2 = x^3 - x$ has Complex Multiplication by $\mathbb{Z}[i]$ one can do quartic twists on it. However, the method we use to prove Theorem 1.2.3 seems not useful for quartic twists, since one is led to find a lower bound of the 2-adic valuation of an infinite product. *The congruence number* δ_E of E is the largest integer such that there is a modular form $g = \sum_{n=1}^{\infty} b_n q^n \in S_2(\Gamma_0(N))$ such that g and $f_E = \sum_{n=1}^{\infty} a_n q^n$ are orthogonal with respect to the Petersson inner product, and $a_n \equiv b_n \pmod{\delta_E}$ for all n. It is known that $m_E \mid \delta_E$, and it is conjectured in [2] that $\nu_2(\delta_E/m_E) \leq \frac{1}{2}\nu_2(N)$. In view of this conjecture, it is useful to find an alternative method that provides a lower bound of $\nu_2(\delta_E)$ [15].

Theorem 1.2.4. *Let d be an odd square-free integer and D any divisor of d. For the elliptic curve $E^{(D)} : y^2 = x^3 - dD^2x$ we have that*

$$2\left\lfloor \frac{\omega(d)+1}{2} \right\rfloor + 1 \leq \nu_2(\delta_E),$$

where $\omega(d)$ is the number of distinct prime divisors of d.

1.2.2 Watkins's conjecture for elliptic curves over function fields

Let k be a finite field of characteristic $p > 3$, write $A = k[T]$ for the polynomial ring, and let $K = k(T)$ be its fraction field. Let ∞ denote the place of K attached to $1/T$. Let E be a non-isotrivial (the j-invariant is not in k) elliptic curve defined over K. Under the assumption that E has split multiplicative reduction at ∞, there is an analogue to the Modularity Theorem (cf. Theorem 2.2.13). Namely, if E is non-isotrivial, has split multiplicative reduction at ∞, and conductor ideal $\mathfrak{n}$, there is a non-constant map $\phi_E : X_0(\mathfrak{n}) \to E$, where $X_0(\mathfrak{n})$ is the corresponding Drinfeld modular curve. Thus, from now on we say that E is modular if it is non-isotrivial and has split multiplicative reduction at ∞. Given a modular elliptic curve E over K, we say that it satisfies Watkins's conjecture if $\mathrm{rank}(E(K)) \leq \nu_2(m_E)$, where m_E is the minimal degree of a modular parametrization $\phi_E : X_0(\mathfrak{n}) \to E$.

The strategy that we will use in this section is the same as the previous section: giving an upper bound for the Mordell-Weil-Rank, giving a lower bound for $\nu_2(m_E)$, and comparing them. Nevertheless, in the case of elliptic curves over function fields of positive characteristic, there are other kinds of bounds for $\mathrm{rank}(E(K))$.

We prove a potential version of Watkins's conjecture [14], using Atkin-Lehner involutions, for semistable elliptic curves over K (see [31] and [17] for other applications of Atkin-Lehner involutions in the context of Watkins's conjecture).

Theorem 1.2.5. *Let E be a modular semistable elliptic curve defined over K with conductor $\mathfrak{n}_E = (n)\infty$. Let k' be a finite field containing the splitting field of n over k, then Watkins's conjecture holds for $E' = E \times_{\operatorname{Spec} K} \operatorname{Spec} K'$, where $K' := k'(T)$.*

On the other hand, it is not known whether the Mordell-Weil rank of elliptic curves over $\mathbb{Q}$ is unbounded or not. Over K we know that the rank is unbounded thanks to the work of Shafarevitch and Tate [84] in the isotrivial case, and to Ulmer [86] and Griffon [45] in the non-isotrivial case. The next result [14] proves Watkins's conjecture for one of the families given by Ulmer, thus, we prove this conjecture for elliptic curves over K with arbitrarily large rank.

Theorem 1.2.6. *Let p be a prime and n be a positive integer, such that $6 \mid p^n + 1$. The elliptic curve*

$$E : y^2 + T^d xy = x^3 - 1,$$

where $d = (p^n + 1)/6$ defined over $\mathbb{F}_q(T)$, satisfies Watkins's conjecture.

Using the results of Papikian [67] on $L(\operatorname{Sym}^2 f, 2)$ over function fields, when f is an automorphic cusp forms (for a definition see Subsection 2.1.2), we can prove an analogue [14] to the results of [34]. In the following, we write $\omega_K(g)$ for the number of distinct irreducible factors of a polynomial g in A.

Theorem 1.2.7. *Let E be an elliptic curve over K with minimal conductor among its quadratic twists. Let its conductor be $\mathfrak{n}\infty = (n_1^2 n_2)\infty$, where n_1, n_2 are square-free coprime polynomials. Assume that E has non-trivial K-rational 2-torsion. Let g be a monic square-free polynomial of even degree such that $gcd(n_1, g) = 1$, and $\omega_K(g) \geq 2\omega_K(\mathfrak{n}) - \nu_2(m_E)$. Then Watkins's conjecture holds for $E^{(g)}$.*

The condition that g has even degree is necessary to guarantee that $E^{(g)}$ is modular. If we put some conditions on E (analogue to Theorem 1.2.1), we can prove [14] that Watkins's conjecture holds for every quadratic twist:

Corollary 1.2.8. *Assume that E is a semistable modular elliptic curve over K. Then, we have that $E^{(g)}$ satisfies Watkins's conjecture whenever $\omega_K(g) \geq 3$. Furthermore, if every prime dividing $\mathfrak{n}$ has non-split multiplicative reduction and $E(K)[2] \cong \mathbb{Z}/2\mathbb{Z}$, then $E^{(g)}$ satisfies Watkins's conjecture for every square-free polynomial $g \in A$ of even degree.*

1.3 Overview of Chapters

A brief outline of the contents of each chapter is as follows.

In chapter 2, we present the preliminaries of the Drinfeld setting to state the Modularity theorem for elliptic curves over function fields of positive characteristic. Furthermore, we show a joint work with Hector Pasten about an upper bound of the Mordell-Weil rank for elliptic curves over $\mathbb{Q}$ and we present the classification of elliptic curves with prime power conductor given by Mulholland [63].

Chapter 3 is a compendium of some approaches to Watkins's conjecture. This chapter is divided into three main sections: the first one where we prove that every quadratic twist of an elliptic curve with non-trial rational 2-torsion and prime power conductor satisfies the conjecture of Watkins. In the second section, we give a lower bound for the 2-adic valuation of the congruence number for quartic twists of $E : y^2 = x^3 - x$. In the last section, we present a joint work with Hector Pasten where we prove that semistable elliptic curves satisfy Watkins's conjecture, under some conditions in their reduction.

In chapter 4, we state and prove several cases of a potential analogue of Watkins's conjecture for elliptic curves over $\mathbb{F}_q(T)$. This chapter is divided into two sections. The first section is about some results for semistable elliptic curves. In particular, we prove that a family of elliptic curves with unbound rank satisfies this conjecture. In section 2, we show that Watkins's conjecture holds for quadratic twists under some geometric conditions.

Finally, in appendix A, we report on joint work with Hector Pasten on generalizing the classical method of Chabauty and Coleman from the case of curves to surfaces in abelian varieties. We will simply state the results and describe the techniques; for detailed proofs see [16].

Chapter 2

Preparatory Results

2.1 Drinfeld Setting

This section aims to define the associated invariants to state an analogue of Watkins's conjecture for function fields of positive characteristic. Let A be the polynomial ring $\mathbb{F}_q[T]$, where $\mathbb{F}_q$ denotes the finite field with q elements, and let K be its field of fractions. Write K_∞ for the completion of K at T^{-1}, and let $\mathcal{O}_\infty$ be its ring of integers. Let $\mathbb{C}_\infty$ denote the completion of an algebraic closure of K_∞.

2.1.1 Drinfeld Modular Curves

We denote by Ω the Drinfeld upper half plane $\mathbb{C}_\infty - K_\infty$. Notice that $GL(2, K_\infty)$ acts on Ω by fractional linear transformations. In particular, so does the Hecke congruence subgroup attached to an ideal $\mathfrak{n}$ of A

$$\Gamma_0(\mathfrak{n}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, A) \colon c \equiv 0 \ (\text{mod } \mathfrak{n}) \right\}.$$

The compactification of the quotient space $\Gamma_0(\mathfrak{n})\backslash\Omega$ by the finitely many cusps $\Gamma_0(\mathfrak{n})\backslash\mathbb{P}^1(K)$ is the Drinfeld modular curve. We denoted it by $X_0(\mathfrak{n})$.

2.1.2 Automorphic Cusp Forms and Hecke Operators

We define an analogue of the cuspidal Hecke newforms over $\mathbb{C}$. Another way to understand Ω is the Bruhat-Tits tree $\mathcal{T}$ of $PGL(2, K_\infty)$, whose oriented edges, denoted by $E(\mathcal{T})$, are in correspondence with the cosets of $GL(2, K_\infty)/K_\infty^\times \cdot \mathcal{J}$ (see Section 4.2 [43]), where

$$\mathcal{J} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL(2, \mathcal{O}_\infty) \colon c \equiv 0 \ (\text{mod } T^{-1}) \right\}.$$

This correspondence gives an action of $GL(2, K_\infty)$ on the real-valued functions on the oriented edges of $\mathcal{T}$ by left-multiplying the argument. Let $\underline{H}_!(\Gamma_0(\mathfrak{n}), \mathbb{R})$ be the finite-dimensional $\mathbb{R}$-space of real-valued, alternating *($f(e) + f(\overline{e}) = 0$ for all oriented edge e, where $\overline{e}$ is the edge in reverse direction of e)*, harmonic *($\sum f(e) = 0$ for all vertex v, where the sum runs over all oriented edges with origin v)*, and $\Gamma_0(\mathfrak{n})$-invariant functions on the oriented edges of $\mathcal{T}$ having finite support modulo $\Gamma_0(\mathfrak{n})$. A function $f \in \underline{H}_!(\Gamma_0(\mathfrak{n}), \mathbb{R})$ is called automorphic cusp forms of level $\mathfrak{n}$ (of Jacquet–Langlands–Drinfeld type).

The space $\underline{H}_!(\Gamma_0(\mathfrak{n}), \mathbb{R})$ is equipped with a Petersson scalar product defined by

$$\int_{E(\Gamma_0(\mathfrak{n})\backslash\mathcal{T})} f(e) \cdot g(e) d\mu(e),$$

where $E(\Gamma_0(\mathfrak{n}) \setminus \mathcal{T})$ denotes the oriented edges of the quotient of $\mathcal{T}$ via the action of $\Gamma_0(N)$, and $\mu(e)$ is the Haar measure on the discrete set $E(\Gamma_0(\mathfrak{n}) \setminus \mathcal{T})$ given by

$$\frac{q-1}{2\#\mathrm{Stab}_{\Gamma_0(\mathfrak{n})}(e)},$$

where $\mathrm{Stab}_{\Gamma_0(\mathfrak{n})}(e)$ is the stabilizer of $e \in E(\mathcal{T})$ (see Section 4.8 Gekeler *op. cit.*).

For each divisor $\mathfrak{d} = (d)$ of $\mathfrak{n}$, let $i_\mathfrak{d}$ be the map

$$i_\mathfrak{d} \colon (\underline{H}_!(\Gamma_0(\mathfrak{n}/\mathfrak{d}), \mathbb{R}))^2 \longrightarrow \underline{H}_!(\Gamma_0(\mathfrak{n}), \mathbb{R}),$$

given by

$$i_\mathfrak{d}(f, g)(e) = f(e) + g\left(\begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix} \cdot e\right),$$

for every oriented edge e. The subspace of oldforms at level $\mathfrak{n}$ is

$$\underline{H}_!^{old}(\Gamma_0(\mathfrak{n}), \mathbb{R}) = \sum_{\mathfrak{p}|\mathfrak{n}} i_\mathfrak{p}((\underline{H}_!(\Gamma_0(\mathfrak{n}/\mathfrak{p}), \mathbb{R}))^2),$$

where the sum runs over the prime divisors of $\mathfrak{n}$. The orthogonal complement of the oldforms with respect to the Petersson-norm is denoted by $\underline{H}_!^{new}(\Gamma_0(\mathfrak{n}), \mathbb{R})$.

One also can define a Hecke operator $T_\mathfrak{m}$ for any nonzero ideal $\mathfrak{m}$. For example, when $\mathfrak{m}$ is relatively prime to $\mathfrak{n}$ is defined by

$$T_\mathfrak{m} f(e) = \sum f\left(\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \cdot e\right),$$

where the sum runs over $a, b, d \in A$ such that a, d are monic, $\mathfrak{m} = (ad)$, and $\deg(b) < \deg(d)$, see Section 4.9 Gekeler *op. cit.* for a general definition. Finally, a *newform* is a normalized (with respect to the Petersson-norm) automorphic cusp forms f in $\underline{H}_!^{new}(\Gamma_0(\mathfrak{n}), \mathbb{R})$ and an eigenform for all Hecke operators.

Atkin-Lehner involutions

For any ideal $\mathfrak{m} = (m)$, such that $\mathfrak{m} \mid \mathfrak{n} = (n)$ and $\mathfrak{m}$ and $\mathfrak{n}/\mathfrak{m}$ are relatively prime ideals, there is an Atkin-Lehner involution $W_{\mathfrak{m}}$. This involution acts on $\underline{H}_!(\Gamma_0(\mathfrak{n}), \mathbb{R})$ as follows

$$W_{\mathfrak{m}} f(e) = f\left(\begin{pmatrix} ma & b \\ nc & md \end{pmatrix} \cdot e\right),$$

where $a, b, c, d \in A$ and $m^2ab - nbc = \gamma m$ for some $\gamma \in k^\times$. We denote by $\mathcal{W}(\mathfrak{n})$ the 2-elementary abelian group of all Atkin-Lehner involutions. Let f be a primitive newform; since f is primitive, it is determined by its eigenvalues up to sign. By Lemma 11 from [4] the Hecke operators commute with the Atkin-Lehner involutions, hence $W_{\mathfrak{p}}^{(\mathfrak{n})} f$ and f have the same Hecke eigenvalues. By Lemma 1.2, from [74], $\underline{H}_!^{new}(\Gamma_0(\mathfrak{n}), \mathbb{R})$ is stable under the Atkin-Lehner involutions and, consequently, we have that $W_{\mathfrak{p}} f = \pm f$.

2.2 Elliptic curves

This section is divided into three main parts. In the first one, we will show a general theory that is constructed over elliptic curves over global fields. In the second part, we will treat the special case of elliptic curves defined over $\mathbb{Q}$, as well as in the last subsection we will study the case of elliptic curves over $\mathbb{F}_q(T)$. In the latter case, we will denote the conductor of E by $\mathfrak{n}_E$ and the finite part of $\mathfrak{n}_E$ is denoted by $\mathfrak{n}_0$.

2.2.1 Generalities of elliptic curves over Global fields

In this section, K denotes $\mathbb{Q}$ or $\mathbb{F}_q(T)$, and A denotes $\mathbb{Z}$ or $\mathbb{F}_q[T]$, respectively. We let E be an elliptic curve defined over K. Assume that E has an affine model:

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6. \tag{2.1}$$

where $a_i \in K$. For this cubic equation, define the usual Weierstrass invariants:

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \quad b_4 = a_1a_3 + 2a_4, \quad b_6 = a_3^2 + 4a_6, \\ b_8 &= a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2, \\ c_4 &= b_2^2 - 24b_4, \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6, \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \\ j_E &= c_4^3\Delta^{-1}. \end{aligned} \tag{2.2}$$

Let us recall that $\Delta \neq 0$, since our elliptic curve is nonsingular.

L-functions

We define the set $\mathcal{I}_K$ as follows: (i) when $K = \mathbb{Q}$, $\mathcal{I}_K = \{n \in \mathbb{Z} \colon n \geq 1\}$, or (b) when $K = \mathbb{F}_q(T)$, $\mathcal{I}_K$ is the set of effective divisors on $\mathbb{P}^1_K$.

There is an attached L-function to an elliptic curve with conductor $\mathfrak{n}_E$, which has an Euler product expansion

$$L(E,s) = \sum_{n \in \mathcal{I}_K} \frac{a_n}{|n|^s} = \prod_{\mathfrak{p}} \left(1 - \frac{\alpha_{\mathfrak{p}}}{|\mathfrak{p}|^s}\right)^{-1} \left(1 - \frac{\beta_{\mathfrak{p}}}{|\mathfrak{p}|^s}\right)^{-1},$$

where $\alpha_{\mathfrak{p}}, \beta_{\mathfrak{p}}$ are defined as follows:

(1) if E has good reduction at $\mathfrak{p}$, we have that $\alpha_{\mathfrak{p}} + \beta_{\mathfrak{p}} = a_{\mathfrak{p}} \coloneqq |\mathfrak{p}| + 1 - \#E(\mathbb{F}_{\mathfrak{p}})$ and $\alpha_{\mathfrak{p}}\beta_{\mathfrak{p}} = |\mathfrak{p}|$,

(2) if E has multiplicative reduction at $\mathfrak{p}$, we have that $\alpha_{\mathfrak{p}} = 0$ and $\beta_{\mathfrak{p}} = \pm 1$ (depending on whether the reduction is split or is non-split), and finally

(3) if E has additive reduction at $\mathfrak{p}$, then $\alpha_{\mathfrak{p}}$ and $\beta_{\mathfrak{p}}$ are both zero.

Remark 2.2.1. Due to results of Grothendieck [46] and Deligne [27], when $K = \mathbb{F}_q(T)$, we have that $L(E,s) = L(f_E,s)$, where f_E is the newform attached to E (see Remark 2.2.14 for a definition of f_E), and $L(E,s)$ is a polynomial in the variable q^{-s} of degree $\deg(\mathfrak{n}_E) - 4$, where $\mathfrak{n}_E$ is the conductor of E.

Example 2.2.2. Let E be the elliptic curve over $\mathbb{F}_3(T)$ given by the equation

$$E/\mathbb{F}_3(T) : Y^2 = X^3 + (T^4 + 2T^2)X + (T^3 + 2T),$$

which has discriminant $\Delta_E = 2T^{12} + T^6 \neq 0$ and conductor $\mathfrak{n}_E = (T)^6(T+1)^3(T+2)^3$. In this case, we have

$$L(E,s) = 6561 \cdot 3^{-8s} - 729 \cdot 3^{-6s} - 9 \cdot 3^{-2s} + 1.$$

Over the newform f_E we define the L-function attached to its symmetric square $L(\mathrm{Sym}^2 f_E, s)$ with the following local factors:

$$L_{\mathfrak{p}}(\mathrm{Sym}^2 f_E, s) = \begin{cases} 1, & \text{if } \mathfrak{p} \text{ has add. red.} \\ \left(1 - \frac{1}{|\mathfrak{p}|^s}\right)^{-1}, & \text{if } \mathfrak{p} \text{ has mult. red.} \\ \left(1 - \frac{\alpha_{\mathfrak{p}}^2}{|\mathfrak{p}|^s}\right)^{-1} \left(1 - \frac{\alpha_{\mathfrak{p}}\overline{\alpha_{\mathfrak{p}}}}{|\mathfrak{p}|^s}\right)^{-1} \left(1 - \frac{\overline{\alpha_{\mathfrak{p}}}^2}{|\mathfrak{p}|^s}\right)^{-1} & \text{otherwise.} \end{cases}$$

Remark 2.2.3. For $K = \mathbb{F}_q(T)$, when E is semistable (Proposition 5.4 from [67]) $L(\mathrm{Sym}^2 f_E, s)$ is a polynomial in the variable q^{-s} of degree $2\deg(\mathfrak{n}_0) - 4$, where $\mathfrak{n}_0$ is the finite part of the conductor of E.

Example 2.2.4. Let E be the elliptic curve over $\mathbb{F}_3(T)$ given by the equation

$$E/\mathbb{F}_3(T) : Y^2 = X^3 + T^2X^2 + X,$$

which has discriminant $\Delta = T^4 - 1 \neq 0$ and conductor $\mathfrak{n}_E = (T^2+1)(T+1)(T-1)\infty$. In this case, we have

$$L(\mathrm{Sym}^2 f_E, s) = 729 \cdot 3^{-4s} + 6 \cdot 3^{-2s} + 1.$$

Selmer groups

One of the effective methods to compute the Mordell-Weil rank is the 2-descent method. To define this method we must introduce the Selmer and Shafarevich-Tate groups.

Before starting, let us fix some notation. We denote by G_K the absolute Galois group $\mathrm{Gal}(K^{sep}/K)$. Denote by M_K the set of places of K. For each place $\nu \in M_K$ we fix an extension of ν to K^{sep}, which allows us to fix an embedding $K^{sep} \subset K_\nu^{sep}$ and a decomposition group $G_\nu \subset G_K$.

Let E and E' be elliptic curves defined over K connected by an isogeny $\theta : E \to E'$ defined over K. There exists an exact sequence of of G_K-modules

$$0 \longrightarrow E[\theta] \longrightarrow E \xrightarrow{\theta} E' \longrightarrow 0\ ,$$

where $E[\theta]$ denotes the kernel of ϕ. Taking local and global Galois cohomology (see Section X.4 in [78]) one can obtain

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E'(K)/\theta(E(K)) & \xrightarrow{\delta} & H^1(G_K, E[\theta]) & \longrightarrow & H^1(G_K, E)[\theta] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \prod_\nu E'(K_\nu)/\theta(E(K_\nu)) & \xrightarrow{\delta} & \prod_\nu H^1(G_\nu, E[\theta]) & \longrightarrow & \prod_\nu H^1(G_\nu, E)[\theta] & \longrightarrow & 0.
\end{array}$$

Now, we can define the Selmer and Shafarevich-Tate groups.

Definition 2.2.5. Let $\theta : E \to E'$ be an isogeny. The *θ-Selmer group of E* is the subgroup of $H^1(G_K, E[\theta])$ defined by

$$Sel_\theta(E) = \ker \left\{ H^1(G_K, E[\theta]) \to \prod_{\nu \in M_K} H^1(G_\nu, E) \right\}.$$

The Shafarevich-Tate group of E is the subgroup of $H^1(G_K, E)$ defined by

$$Ш(E) = \ker \left\{ H^1(G_K, E) \to \prod_{\nu \in M_K} H^1(G_\nu, E) \right\}.$$

Using these two groups in the particular case that ϕ is a 2-isogeny, one can obtain an upper bound for $\dim_{\mathbb{F}_2} E(K)/2E(K)$, which immediately gives an upper bound for the Mordell-Weil rank.

Bounds for 2-isogeny Selmer groups

For an elliptic curve E over K with a 2-isogeny $\theta : E \to E'$ defined over K and dual isogeny $\theta' : E' \to E$, we let $s(E,\theta) = \dim_{\mathbb{F}_2} \mathrm{Sel}_\theta(E)$ and $s'(E,\theta) = s(E',\theta')$. Here, $\mathrm{Sel}_\theta(E)$ is the 2-isogeny Selmer group. From Section 3.6 of [79], for $K = \mathbb{Q}$ and Chapter 4 of [72] for $K = \mathbb{F}_q(T)$ one deduces

$$\operatorname{rank} E(K) + 2 \leq s(E,\theta) + s'(E,\theta). \tag{2.3}$$

Let $\omega(n)$ be the number of different prime factors of n over A. The following result is Lemma 2.1 in [3], keeping track of the contribution of the place $v = 2$ (in the case $K = \mathbb{Q}$) in the relevant Selmer groups.

Lemma 2.2.6. *Let E be an elliptic curve over K admitting a Weierstrass equation*

$$y^2 = x^3 + ax^2 + bx, \quad \text{with } a, b \in A.$$

Let $\theta : E \to E'$ be the map obtained by taking the quotient by the 2-torsion point $(0,0)$. We have

$$s(E,\theta) + s'(E,\theta) \leq \omega(b) + \omega(a^2 - 4b) + \kappa, \tag{2.4}$$

where $\kappa = 1$ when $K = \mathbb{Q}$, or $\kappa = 2$ when $K = \mathbb{F}_q(T)$.

Furthermore, in the case $K = \mathbb{Q}$, let us define the affine curves

$$\begin{aligned} C^{(1)} :&\quad 2W^2 = 4U^4 - 4aU^2 + (a^2 - 4b) \\ C^{(2)} :&\quad 2W^2 = 4U^4 + 2aU^2 + b. \end{aligned}$$

Suppose that a is even and $C^{(1)}(\mathbb{Q}_2) = \emptyset$, or that b is even and $C^{(2)}(\mathbb{Q}_2) = \emptyset$. Then

$$s(E,\theta) + s'(E,\theta) \leq \omega(b) + \omega(a^2 - 4b). \tag{2.5}$$

The last assertion is not explicitly made in the statement of Lemma 2.1 [3], but it follows from its proof, by noticing that $C^{(1)}$ and $C^{(2)}$ are affine open sets of the homogeneous spaces C_2 and C_2' in the notation of *loc. cit.* Basically, the last assertion says that if the appropriate homogeneous spaces have no $\mathbb{Q}_2$-points, then we get an additional constraint on the corresponding Selmer groups. See also Section X.4 in [78].

2.2.2 Elliptic Curves defined over $\mathbb{Q}$

Bounds for the Mordell-Weil Rank

The following Theorem is a joint work with Hector Pasten [17].

Theorem 2.2.7. *Let E be an elliptic curve over $\mathbb{Q}$ admitting a 2-isogeny $\theta : E \to E'$ over $\mathbb{Q}$. Let α and μ be the number of places of additive and multiplicative reduction of E, respectively. Then $s(E,\theta)+s'(E,\theta) \leq 2\alpha+\mu+1$. In particular,* $\operatorname{rank} E(\mathbb{Q}) \leq 2\alpha+\mu-1$.

Proof. Consider a minimal Weierstrass equation for E over $\mathbb{Z}$ of the form

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, \tag{2.6}$$

with $\Delta \neq 0$. The change of variables $X = z/4$, $Y = y/8 - a_1z/8 - a_3/2$ transforms (2.6) into

$$y^2 = z^3 + b_2z^2 + 8b_4z + 16b_6 \tag{2.7}$$

where

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

Let $\gamma \in \mathbb{Q}$ be a root of the previous cubic which comes from the rational 2-torsion point in $\ker(\theta)$. Then, $\gamma \in \mathbb{Z}$ and the change of variables $z = x + \gamma$ turns (2.7) into

$$y^2 = x^3 + Ax^2 + Bx \tag{2.8}$$

where

$$A = 3\gamma + b_2 \quad \text{and} \quad B = 3\gamma^2 + 2b_2\gamma + 8b_4. \tag{2.9}$$

Let Δ_E be the discriminant of the minimal model (2.6) and let Δ be the discriminant of the model (2.7). We note that (2.8) has the same discriminant Δ. Then $\Delta = 2^{12}\Delta_E$ by the standard transformation formulas and $\Delta = 16B^2(A^2 - 4B)$ by (2.8). In particular, the models (2.7) and (2.8) are minimal at each $p > 2$. This implies that for $p > 2$ we have that p divides neither, one, or both of B and $A^2 - 4B$ if and only if E has good, multiplicative, or additive reduction at p respectively. Hence, the following bounds hold when E has bad reduction at $p = 2$:

- If E has additive reduction at $p = 2$ then $\omega(B) + \omega(A^2 - 4B) \leq \mu + 2\alpha$.
- If E has multiplicative reduction at $p = 2$, then b_2 is odd (cf. Notation (3.1) Ch. 3 and Remark (7.2) Ch. 5 in [49]). Thus, by (2.9) we see that A and B have opposite parity. This gives $\omega(B) + \omega(A^2 - 4B) = \mu + 2\alpha$.

On the other hand, when E has good reduction at $p = 2$, a_1 or a_3 in (2.6) is odd, for otherwise, one directly checks that $(X, Y) = (a_4, a_4 + a_2a_4 + a_4 + a_6)$ is a singular point. By considerations on Newton polygons as in Section 2 of [75], the fact that the cubic in (2.7) is reducible (γ is a root) shows that a_1 is odd; for otherwise, a_1 is even and a_3 is odd, given that the Newton polygon of the right-hand side of (2.7) is the segment joining $(0, 4)$ and $(3, 0)$ which has no other integer points and Dumas's irreducibility criterion (cf. the Corollary in p.55 of [69]) would give that the right-hand side of (2.7) is irreducible.

Hence, when E has good reduction at $p = 2$ we have that $b_2 \equiv 1 \bmod 4$. Thus, (2.9) implies that A and B have opposite parity, which gives $\omega(B) + \omega(A^2 - 4B) = \mu + 2\alpha + 1$.

In order to conclude, let us apply Lemma 2.2.6 to (2.8). The only remaining point is to show that in the case of good reduction at $p = 2$ the additional requirement on the curves $C^{(i)}$ is satisfied. For this, from now on we assume good reduction at $p = 2$; in particular, $b_2 \equiv 1 \bmod 4$.

Note that γ is odd or divisible by 4, for otherwise, we could write $\gamma = 2\delta$ with δ odd, then (2.7) would imply $0 = 2\delta^3 + b_2\delta^2 + 4b_4\delta + 4b_6$ which is impossible as b_2 is odd.

If γ is odd, then A is even and B is odd. Since $v_2(B^2(A^2 - 4B)) = v_2(2^8\Delta_E) = 8$ we deduce

$$A \equiv 2 \bmod 4,\ B \equiv 1 \bmod 8 \text{ and } A^2 - 4B \equiv 0 \bmod 256. \tag{2.10}$$

If $4|\gamma$ then (2.9) shows that A is odd and B even. Hence, $2v_2(B) = v_2(B^2(A^2 - 4B)) = 8$. Furthermore, we recall that $b_2 \equiv 1 \bmod 4$ and $A = 3\gamma + b_2$. Hence

$$A \equiv 1 \bmod 4 \text{ and } v_2(B) = 4. \tag{2.11}$$

Let us now analyze the $\mathbb{Q}_2$-points of the curves $C^{(1)}$ and $C^{(2)}$.

First, if A is odd and B is even (i.e. $4|\gamma$), let us show that $C^{(2)}(\mathbb{Q}_2)$ is empty. For the sake of contradiction, assume that $C^{(2)}(\mathbb{Q}_2) \neq \emptyset$. That implies that there are $u, w \in \mathbb{Q}_2$ such that

$$2w^2 = 4u^4 + 2Au^2 + 16k, \tag{2.12}$$

where $B = 16k$ with k odd (cf. (2.11)). Notice that $v_2(4u^4) = 4v_2(u) + 2$, $v_2(2Au^2) = 2v_2(u)+1$ and $v_2(16k) = 4$. In particular, all of these valuations are different. Consequently, we have that

$$2v_2(w) + 1 = v_2(2w^2) = \min\{4v_2(u) + 2, 2v_2(u) + 1, 4\}.$$

Since $2v_2(w)+1$ is odd, we get $2v_2(w)+1 = 2v_2(u)+1$. That shows not only that $v_2(w) = v_2(u)$, but also that $2v_2(u) + 1 < \min\{4v_2(u) + 2, 4\}$, which implies that $v_2(u) \in \{0, 1\}$. Then:

- If $v_2(w) = v_2(u) = 0$, since 1 is the only invertible square modulo 8, from (2.12) we get $2A \equiv 2w^2 - 4u^4 \equiv 6 \bmod 8\mathbb{Z}_2$, which is not possible by (2.11).

- If $v_2(w) = v_2(u) = 1$, then there exist $s, t \in \mathbb{Z}_2^\times$ such that $w = 2s$ and $u = 2t$. Then equation (2.12) yields $s^2 = 8t^4 + At^2 + 2k$. Since k is odd and $A \equiv 1 \bmod 4$, we deduce $1 \equiv 1 + 2 \bmod 4\mathbb{Z}_2$; a contradiction.

Finally, if A is even and B is odd (i.e. γ is odd), we have to show that $C^{(1)}(\mathbb{Q}_2)$ is empty. The standard equation for E' is $Y^2 = X^3 - 2AX^2 + (A^2 - 4B)X$ which, upon the substitution $X = 4x$, $Y = 8y$, becomes $y^2 = x^3 - Ax^2/2 + (A^2 - 4B)x/16$. Since E' has good reduction at $p = 2$ (it is isogenous to E) by (2.10) we see that the same analysis of the case $4|\gamma$ for E applies to the last equation for E'. This shows that the curve $C'^{(2)} : 2W^2 = 4U^4 - AU^2 + (A^2 - 4B)/16$ (which is the analogue of $C^{(2)}$ for E') has no $\mathbb{Q}_2$-points. The change of variables $W = w/4$, $U = u/2$ transforms the equation for $C'^{(2)}$ into the equation for $C^{(1)}$, hence $C^{(1)}(\mathbb{Q}_2) = \emptyset$. □

Now, let us recall that the quadratic twist of an elliptic curve E by a non-zero integer d, denoted by $E^{(D)}$, is defined as an elliptic curve which is isomorphic to E over $\mathbb{Q}(\sqrt{D})$ but not over $\mathbb{Q}$. We assume that D is a fundamental quadratic twist. By Proposition 4.3.2 in [22], we know that the Weierstrass equation for $E^{(D)}$ is:

$$y^2+a_1xy+a_3y = x^3+\left(a_2d + a_1^2\frac{d-1}{2}\right)x^2+\left(a_4d^2 + a_1a_3\frac{d^2-1}{2}\right)x+\left(a_6d^3 + a_3^2\frac{d^3-1}{4}\right).$$

Corollary 2.2.8. *Let E be an elliptic curve with non-trivial rational 2-torsion and prime power conductor $N = p^\alpha$ and let $E^{(D)}$ its quadratic twist by D. Then, we have*

$$\operatorname{rank}(E^{(D)}(\mathbb{Q})) \leq 2\omega(D) + 1 - 2\nu_p(D).$$

Even sharper, if E is the elliptic curve given by the equation $y^2 = x^3 - x$ (32.a3 in the LMFDB label), we have

$$\operatorname{rank}(E^{(D)}(\mathbb{Q})) \leq \omega(2D) + \omega(D) - 1.$$

Proof. We know that $E^{(D)}[2] \cong E[2]$ as Galois modules, then $E^{(D)}$ also has non-trivial rational 2-torsion. Consequently, we can apply Theorem 2.2.7. Notice that the bad primes of $E^{(D)}$ are the ones that divide D and also the prime p, therefore, we have:

$$\begin{aligned}\operatorname{rank}(E^{(D)}(\mathbb{Q})) &\leq 2\omega(pD) - 1 \leq 2(\omega(D) + (1 - \nu_p(D))) - 1\\ &= 2\omega(D) + 1 - 2\nu_p(D).\end{aligned}$$

For $E : y^2 = x^3 - x$ its quadratic twist by D is $E^{(D)} : y^2 = x^3 - D^2x$. Equations (2.3) and (2.4) imply

$$\begin{aligned}\operatorname{rank}(E(\mathbb{Q})) &\leq \omega(4D^2) + \omega(-D^2) - 1\\ &\leq \omega(2D) + \omega(D) - 1,\end{aligned} \tag{2.13}$$

which ends the proof. □

Remark 2.2.9. Note that we can also apply the inequality (2.13) to $y^2 = x^3 - dx$ for any integer d and, again, we obtain that $\operatorname{rank}(E(\mathbb{Q})) \leq \omega(2d) + \omega(d) - 1$.

Modular degree of quadratic twists

Lemma 3.1 in [34] gives an equation that relates the modular degree of an elliptic curve E with the one of the quadratic twist $E^{(D)}$ by D. We denote by N and $N^{(D)}$ the conductors of E and $E^{(D)}$, respectively. Before showing this equation, we have to define some invariants which appear on it.

Petersson Norm: Let $S_2(\Gamma_0(N))$ be the space of weight 2 cuspidal holomorphic modular forms; over this space, we have an inner product that allows us to define the following norm.

Definition 2.2.10. The Petersson norm of $f \in S_2(\Gamma_0(N))$ is defined by

$$\|f\|_N = \left(\int_{\Gamma_0(N)\backslash \mathfrak{h}} |f(z)|^2 dx \wedge dy \right)^{1/2}, \qquad z = x + iy \text{ and } y > 0.$$

Observation 2.2.11. Although this definition depends on the level N, we know that if $N \mid M$ and $f \in S_2(\Gamma_0(N))$, then $f \in S_2(\Gamma_0(M))$ and $\|f\|_M^2 = [\Gamma_0(N) : \Gamma_0(M)]\|f\|_N^2$.

Manin Constant: Let E be an elliptic curve defined over $\mathbb{Q}$ of conductor N and let ω_E be its Néron differential. We have that $\phi_E^* \omega_E$ is a regular differential on $X_0(N)$, which implies the following formula:

$$\phi_E^* \omega_E = 2\pi i c_E f_E(z) dz$$

where c_E is a rational number (due to Proposition 2 from [33] c_E is an integer) uniquely defined up to sign and f_E denotes the Hecke newform attached to E. We called c_E the Manin constant.

Now, we can show the mentioned equation given by Lemma 3.1 in *loc. cit.*

$$\frac{m_{E^{(D)}}}{c_{E^{(D)}}^2} = \frac{m_E}{c_E^2} \times \frac{\|f_{E^{(D)}}\|_{N^{(D)}}^2}{\|f_E\|_N^2} \left| \frac{\Delta_{E^{(D)}}}{\Delta_E} \right|^{1/6}, \tag{2.14}$$

where Δ_E denotes the global minimal discriminant of E. Equation (2.14) implies the following Lemma:

Lemma 2.2.12. *Let E be an elliptic curve and $E^{(D)}$ its quadratic twist by D. Then*

$$\nu_2(m_{E^{(D)}}) \geq \nu_2\left(\frac{m_E}{c_E^2}\right) + \nu_2\left(\frac{\|f_{E^{(D)}}\|_{N^{(D)}}^2}{\|f_E\|_N^2}\right) + \frac{1}{6}\nu_2\left(\frac{\Delta_{E^{(D)}}}{\Delta_E}\right). \tag{2.15}$$

Elliptic curves with rational 2-torsion and prime power conductor

The aim of Section 3.1 is to prove that every quadratic twist of an elliptic curve with prime power conductor satisfies Watkins's conjecture. In this direction, we have to classify all the elliptic curves defined over $\mathbb{Q}$ with nontrivial 2-torsion and conductor a power of a prime. For this classification, we take into account that $[a_1, a_2, a_3, a_4, a_6]$ denotes the elliptic curve

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

with $\Delta \neq 0$. We begin with the elliptic curves with prime conductor. Setzer [75] proved that for $p \neq 17$ there exists an elliptic curve with prime conductor p and non-trivial rational 2-torsion if and only if $p = u^2 + 64$ for some integer u, in which case there are two nonisomorphic elliptic curves with conductor p. The minimal models of these elliptic curves are

LMFDB label	Weierstrass coefficients	Δ
$p.a1$	$[1, (u-1)/4, 0, -1, 0]$	p
$p.a2$	$[1, (u-1)/4, 0, 4, u]$	$-p^2$

Table 2.1: Elliptic curves with prime conductor $p > 17$ and rational 2-torsion

A 2-isogeny connects these two elliptic curves. Moreover, the work of Mestre & Oesterlé [61] implies that the curve $p.a2$ is $X_0(p)$-optimal (an elliptic curve E is called $X_0(N)$-optimal if it has the minimal modular degree m_E in its isogeny class). For $p = 17$, Setzer *loc. cit.* shows that there are four nonisomorphic elliptic curves

LMFDB label	Weierstrass coefficients	m_E	c_E	Δ
$17.a1$	$[1, -1, 1, -91, -310]$	4	2	17
$17.a2$	$[1, -1, 1, -6, -4]$	2	2	17^2
$17.a3$	$[1, -1, 1, -1, -14]$	1	1	-17^4
$17.a4$	$[1, -1, 1, -1, 0]$	4	4	17

Table 2.2: Elliptic curves with conductor 17

On the other hand, Mulholland [63] proved that for $p > 3$ the elliptic curves with nontrivial 2-torsion and conductor p^2 are the quadratic twist of the elliptic curves in Tables 2.1 and 2.2 by p, together with the ones with conductor 49 listed below

LMFDB label	Weierstrass coefficients	m_E	c_E	Δ
$49.a1$	$[1,-1,0,-1822,30393]$	14	1	7^9
$49.a2$	$[1,-1,0,-107,552]$	7	1	7^9
$49.a3$	$[1,-1,0,-37,-78]$	2	1	7^3
$49.a4$	$[1,-1,0,-2,-1]$	1	1	7^2

Table 2.3: Elliptic curves with conductor 49

Using the database [57], we can classify the elliptic curves with non-trivial rational 2-torsion and conductor a power of 2 or 3. We noticed that there are no elliptic curves with non-trivial rational 2-torsion of conductor 3^m for any integer m, thus we only list the ones with conductor 2^m with $m \in \{5,6,7,8\}$.

The following table shows the elliptic curves with conductor 2^5

LMFDB label	Weierstrass coefficients	m_E	c_E	Δ
$32.a1$	$[0,0,0,-11,-14]$	4	2	2^9
$32.a2$	$[0,0,0,-11,14]$	4	2	2^9
$32.a3$	$[0,0,0,-1,0]$	2	2	2^6
$32.a4$	$[0,0,0,4,0]$	1	1	-2^{12}

Table 2.4: Elliptic curves with conductor 32

Meanwhile, the elliptic curves of conductor 2^6 are the quadratic twists of the previous ones by 2. Finally, the elliptic curves with conductor 2^7 are listed in the following table

LMFDB label	Weierstrass coefficients	m_E	c_E	Δ
$128.a1$	$[0,1,0,-9,7]$	8	1	2^{13}
$128.a2$	$[0,1,0,1,1]$	4	1	-2^8
$128.b1$	$[0,1,0,-2,-2]$	16	2	2^7
$128.b2$	$[0,1,0,3,-5]$	8	1	-2^{14}
$128.c1$	$[0,-1,0,-9,-7]$	8	1	2^{13}
$128.c2$	$[0,-1,0,1,-1]$	4	1	-2^8
$128.d1$	$[0,-1,0,-2,2]$	16	2	2^7
$128.d2$	$[0,-1,0,3,5]$	8	1	-2^{14}

Table 2.5: Elliptic curves with conductor 128

and again the elliptic curves of conductor 2^8 are their quadratic twists by 2.

2.2.3 Elliptic Curves defined over $\mathbb{F}_q(T)$

We say that an elliptic curve E defined over $\mathbb{F}_q(T)$ is *non-isotrivial* when $j_E \notin \mathbb{F}_q$. Since we assume that $\mathrm{char}(k) > 3$ the conductor of E is cubefree. Denote it by $\mathfrak{n}_E$ and its finite part by $\mathfrak{n}$. In particular, $\mathfrak{n}_E = \mathfrak{n} \cdot \infty^i$, where $i \in \{0, 1, 2\}$.

When E has split multiplicative reduction at ∞, due to Drinfeld's reciprocity law (Proposition 10.3 [29]) and the fact that E is automorphic (Theorem 9.8 in [27]), there is an analogue of the modularity Theorem over $\mathbb{Q}$ (see Section 8 of [43] for a detailed proof):

Theorem 2.2.13 (Modularity Theorem)**.** *Let E be an elliptic curve over K of conductor $\mathfrak{n}_E = \mathfrak{n}_0 \cdot \infty$ having split multiplicative reduction at ∞. Then, there is a non-constant morphism $X_0(\mathfrak{n}_0) \to E$ defined over K.*

Remark 2.2.14. This Theorem gives a bijection between primitive newforms f (i.e., f is a newform such that $f \notin n\underline{H}_!^{new}(\Gamma_0(\mathfrak{n}_0), \mathbb{Z})$ for $n > 1$) with integer eigenvalues and isogeny classes of modular elliptic curves over K with conductor $\mathfrak{n}_0 \cdot \infty$. Furthermore, if E is a modular elliptic curve and f_E is its attached primitive newform, f_E is an eigenform of every Atkin-Lehner involution.

Upper Bounds for the Rank of the Mordell-Weil Group

The following is a geometric bound for the Mordell-Weil rank due to Tate [83]:

$$\mathrm{rank}(E(K)) \leq \mathrm{ord}_{s=1} L(E, s) \leq \deg(\mathfrak{n}_E) - 4, \tag{2.16}$$

the last inequality comes from Remark 2.2.1. See [87] for detailed proof.

Example 2.2.15. Let E be the elliptic curve defined over $\mathbb{F}_{31}(T)$ given by the equation

$$E/\mathbb{F}_{31}(T) : Y^2 = X^3 + (6T + 1)X^2 + (3T + 6)X,$$

with discriminant $\Delta_E = 7T^4 + 28T^3 + 2T^2 + 20T + 20$. Since $L(E, s) = -961 \cdot 31^{-2s} + 1$, we have

$$\mathrm{rank}(E(K)) \leq \mathrm{ord}_{s=1}(-31 \cdot 31^{-s} + 1) = 1.$$

Since the element $(15, 30)$ has infinite order, we obtain that $\mathrm{rank}(E(K)) = 1$.

On the other hand, if the elliptic curve E has a non-trivial K-rational 2-torsion, we can give an upper bound for its Mordell-Weil rank in terms of $\omega_K(\mathfrak{n}_0)$, the number of distinct primes that divide $\mathfrak{n}_0$ in A.

First of all, notice that the change of variables $X = z/4$, $Y = y/8 - a_1 z/8 - a_3/2$ transforms

$$Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6. \tag{2.17}$$

into

$$y^2 = z^3 + b_2 z^2 + 8b_4 z + 16b_6. \tag{2.18}$$

Let $\gamma \in K$ be a root of the previous cubic, attached to a non-trivial K-rational 2-torsion point. Then $\gamma \in A$ and the change of variables $z = x + \gamma$ turns (2.7) into

$$y^2 = x^3 + ax^2 + bx, \tag{2.19}$$

where

$$a = 3\gamma + b_2 \quad \text{and} \quad b = 3\gamma^2 + 2b_2\gamma + 8b_4.$$

Let Δ_E be the discriminant of the minimal model (2.17) and let Δ be the discriminant of (2.19). Notice that $\Delta = 2^{12}\Delta_E$ by the standard transformation formulas. Thus, (2.19) is a minimal model of E and then Lemma 2.2.6 implies:

Proposition 2.2.16. *Let E be an elliptic curve with non-trivial K-rational 2-torsion and Weierstrass minimal model $y^2 = x^3 + ax^2 + bx$, then:*

$$\operatorname{rank}(E(K)) \leq \omega_K(a^2 - 4b) + \omega_K(b).$$

Consequently, if α (resp. μ) is the number of finite primes of additive (resp. multiplicative) bad reduction of E/K, then:

$$\operatorname{rank}(E(K)) \leq \mu + 2\alpha.$$

Example 2.2.17. Let E be the elliptic curve defined over $\mathbb{F}_{31}(T)$ given by the equation

$$E/\mathbb{F}_{31}(T) : Y^2 = X^3 + (T^4 + 1)X^2 + 6X,$$

with discriminant $\Delta_E = 18T^8 + 5T^4 + 20 \neq 0$. Its conductor is $\mathfrak{n}_E = (T^4 + 11T^2 + 15)(T^4 + 20T^2 + 15) \cdot \infty$. Proposition 2.2.16 gives the inequality $\operatorname{rank}(E(\mathbb{F}_{31}(T))) \leq 2$, while $\deg(\mathfrak{n}_E) - 4 = 5$. Thus, in this case, the bound in Proposition 2.2.16 is sharper than inequality 2.16.

Modular Degree

Let E be a modular elliptic curve defined over K. Let $X_0(\mathfrak{n})$ be the Drinfeld modular curve parametrizing $\phi_E \colon X_0(\mathfrak{n}) \to E$ where ϕ_E is non-trivial and of minimal possible degree. *The modular degree* m_E is the degree of ϕ_E. The following Lemma relates the 2-adic valuations of m_E and $L(\operatorname{Sym}^2 f, 2)$.

Lemma 2.2.18. *Let E be a modular elliptic curve defined over K. Then we have that*

$$\nu_2(m_E) = \nu_2(L(\operatorname{Sym}^2 f, 2)) - \nu_2(val_\infty(j_E)).$$

Proof. Main Theorem in [67] states that

$$m_E = \frac{q^{\deg \mathfrak{n}_E}}{-val_\infty(j_E)} L(\mathrm{Sym}^2 f, 2), \tag{2.20}$$

where $q = \#k$. In *loc. cit.*, E is assumed to be semistable to have that $L(\mathrm{Sym}^2 f, 2) = L(\mathrm{Sym}^2 E, 2)$. However, for our purposes, this is not necessary and (2.20) is a consequence of equations (18) and (26) in *loc. cit.* which do not need the semistability of E. By taking 2-adic valuations we obtain

$$\nu_2(m_E) = \nu_2(q^{\deg \mathfrak{n}_E - 2}) + \nu_2(L(\mathrm{Sym}^2 f, 2)) - \nu_2(val_\infty(j_E)),$$

which yields the desired result. □

Example 2.2.19. Consider the elliptic curve defined over $\mathbb{F}_3(T)$ by the equation

$$E : Y^2 = X^3 + T^2X^2 + X,$$

with discriminant $\Delta = T^4 - 1 \neq 0$. We have that $j_E = T^{12}/(T^4 - 1)$, and as a consequence $val_\infty(j_E) = 8$. More precisely,

$$L(\mathrm{Sym}^2 f, s) = 729 \cdot 3^{-4s} + 6 \cdot 3^{-2s} + 1,$$

then $L(\mathrm{Sym}^2 f, 2) = 32/27$, so $\nu_2(m_E) = 5 - 3 = 2$.

Chapter 3

Different approaches to Watkins's conjecture

3.1 Watkins's conjecture for quadratic twists of elliptic curves with prime power conductor

3.1.1 Lower bounds for some 2-adic valuations

Theorem 2.2.7 gives an upper bound for the rank of an elliptic curve with non-trivial 2-torsion. To give a lower bound for the modular degree we will use Lemma 2.2.12, hence, this section aims to give lower bounds for the 2-adic valuation of the invariants in this Lemma.

Minimal discriminant

This subsection aims to find a lower bound for

$$\nu_2\left(\left(\frac{\Delta_{E^{(D)}}}{\Delta_E}\right)^{1/6}\right) = \frac{1}{6}\nu_2\left(\frac{\Delta_{E^{(D)}}}{\Delta_E}\right), \tag{3.1}$$

where E has prime power conductor and Δ_E denotes the minimal discriminant of E.

Definition 3.1.1. Let p be a prime. The p-adic signature of an elliptic curve E is the triple $(\nu_p(c_4(E)), \nu_p(c_6(E)), \nu_p(\Delta_E))$, where c_4, c_6 are the usual Weierstrass invariants (2.2).

Pal [66] classifies the valuation (3.1) in terms of the 2-adic signature of E. To begin with, we compute the 2-adic signature of an elliptic curve with odd discriminant and non-trivial rational 2-torsion.

Lemma 3.1.2. *Let E be an elliptic curve with non-trivial rational 2-torsion and odd discriminant. Then, the 2-adic signature of E is $(0,0,0)$.*

Proof. Assume that the minimal model of E is of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Since E has good reduction at 2, then either a_1 or a_3 must be odd. Furthermore, due to the fact that $E[2] \neq (0)$, there exists $x_0 \in \mathbb{Q}$ such that

$$x_0^3 + b_2x_0^2 + 8b_4x_0 + 16b_6 = 0, \tag{3.2}$$

where b_2, b_4, and b_6 are the usual Weierstrass invariants (2.2). We notice that a_1 is odd, otherwise, $\nu_2(b_2) = \nu_2(a_1^2 + 4a_2) \geq 2$, $\nu_2(b_4) = \nu_2(a_1a_3 + 2a_4) \geq 1$ and a_3 must be odd, hence, $b_6 = a_3^2 + 4a_6$ is odd too. Consequently, the Newton polygon (as it is noticed in Section 2 of [75]) attached to (3.2) is a line with slope $-4/3$, so, by Dumas's irreducibility criterion (cf. the Corollary in p.55 of [69]) this polynomial has no rational solutions, which is a contradiction. Hence, b_2 is odd and, therefore, $c_4 = b_2^2 - 24b_4$ and $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$ are odd too. □

Proposition 2.4 in [66] classifies the minimal discriminant of a quadratic twist of an elliptic curve E from the 2-adic signature of E. Let us define $D^* = D$ when $2 \nmid D$, and $D^* = D/4$ when $2 \mid D$. Lemma 3.1.2 and Proposition 2.4.2 *loc. cit.* for elliptic curves with 2-adic signature $(0,0,0)$ imply the following result:

Corollary 3.1.3. *Let E be an elliptic curve with non-trivial rational 2-torsion and odd discriminant. Then we have*

$$\frac{1}{6}\nu_2\left(\frac{\Delta_{E^{(D)}}}{\Delta_E}\right) = \begin{cases} 0 & \text{if } D^* \equiv 1 \pmod 4 \\ 2 & \text{if } D^* \equiv -1 \pmod 4 \\ 3 & \text{if } 2 \mid D^*. \end{cases}$$

Now, let us list the 2-adic valuation of the elliptic curves with conductor 2^5 and 2^7.

LMFDB label	$(c_4(E), c_6(E))$	2-adic signature
$32.a1$	$(528, 12096)$	$(4, 6, 9)$
$32.a2$	$(528, -12096)$	$(4, 6, 9)$
$32.a3$	$(48, 0)$	$(4, \infty, 6)$
$32.a4$	$(-192, 0)$	$(6, \infty, 12)$
$128.a1$	$(448, -8704)$	$(6, 9, 13)$
$128.a2$	$(-32, -640)$	$(5, 7, 8)$
$128.b1$	$(112, 1088)$	$(4, 6, 7)$
$128.b2$	$(-128, 5120)$	$(7, 10, 14)$
$128.c1$	$(448, 3392)$	$(6, 6, 13)$
$128.c2$	$(-32, 1088)$	$(5, 6, 8)$
$128.d1$	$(112, -2368)$	$(4, 6, 7)$
$128.d2$	$(-128, -3520)$	$(7, 6, 14)$

Table 3.1: 2*-adic signature*

Again, applying Proposition 2.4.2 in *loc. cit.*, we have the following Lemma

Lemma 3.1.4. *Let E be an elliptic curve with conductor 2^5 or 2^7. Then we have*

$$\frac{1}{6}\nu_2\left(\frac{\Delta_{E^{(D)}}}{\Delta_E}\right) \geq -\nu_2(D).$$

Petersson norms

Now we want to relate the 2-adic valuation of the Petersson norms of $f_{E^{(D)}}$ and f_E. Let us define $D^* = D$ when $2 \nmid D$, and $D^* = D/4$ when $2 \mid D$

Proposition 3.1.5. *Let E be an elliptic curve with non-trivial rational 2-torsion and minimal conductor N among all its quadratic twists and let D be a quadratic fundamental discriminant.*

(I) Assume that N is a power of an odd prime and, if $N = p^2$, we only consider D such that $p \nmid D$. Then, we have

$$\nu_2\left(\frac{\|f_{E^{(D)}}\|^2_{N^{(D)}}}{\|f_E\|^2_N}\right) \geq 3\omega(D).$$

(II) Furthermore, if E is $17.a4$ in Table 2.2 we have

$$\nu_2\left(\frac{\|f_{E^{(D)}}\|^2_{N^{(D)}}}{\|f_E\|^2_N}\right) \geq 4\omega(D).$$

(III) If N is 2^5 or 2^7 we have

$$\nu_2\left(\frac{\|f_{E^{(D)}}\|^2_{N^{(D)}}}{\|f_E\|^2_N}\right) \geq 3\omega(D) - 2\nu_2(D^*).$$

(IV) Furthermore, if E is $32.a3$ in Table 2.4 we have

$$\nu_2\left(\frac{\|f_{E^{(D)}}\|^2_{N^{(D)}}}{\|f_E\|^2_N}\right) \geq 4\omega(D) - 3\nu_2(D^*).$$

Proof. Before starting, let us fix some notation. For a prime number q we define $V(q) = (q-1)(q+1-a_q)(q+1+a_q)$ and $U(q) = (q-1)(q+1)$, where a_q is the q-th Fourier coefficient of f_E. Finally, we define $U_2 = 2(3-a_2)(3+a_2)$.

Assume that N is a power of an odd prime p. Since $p \mid D$ only if $N = p$, then according to the notation of Delaunay in [25], $D_1 = p$. Thus, Theorem 1 in *loc. cit.* tells us:

$$\nu_2\left(\frac{\|f_{E^{(D)}}\|^2_{N^{(D)}}}{\|f_E\|^2_N}\right) \geq \nu_p(D)\nu_2(U(p)) + \nu_2(D^*)\nu_2(U_2) + \sum_{\substack{q\mid D\\ q\neq 2,p}} \nu_2(V(q)).$$

In view of the fact that $E(\mathbb{Q})[2]$ reduces injectively into $E(\mathbb{F}_q)$ for $q \notin \{2,p\}$, we have that $q+1 \equiv a_q(E) \pmod 2$, in particular, $\nu_2(V(q)) \geq 3$. Furthermore, the LMFDB database [57] tells us that $2 \mid 3-a_2, 3+a_2$ for elliptic curves with conductor 17 or 49 and an inspection of the reduction modulo 2 of $p.a1$ and $p.a2$ for $p > 17$ shows that $2 \mid \#E(\mathbb{F}_2)$, which shows that $\nu_2(U_2) \geq 3$. Finally, it is clear that $\nu_2(U(p)) \geq 3$, then

$$\nu_2\left(\frac{\|f_{E^{(D)}}\|^2_{N^{(D)}}}{\|f_E\|^2_N}\right) \geq 3(\nu_p(D) + \nu_2(D^*) + \sum_{\substack{q\mid D\\ q\neq 2,p}} 1) \geq 3\omega(D),$$

which proves (I).

To prove (II), we notice that $\#E(\mathbb{Q})[4] = 4$ and, due to the fact that $E(\mathbb{Q})[4]$ reduces injectively into $E(\mathbb{F}_q)$ for $q \notin \{2,p\}$, we have that $q+1 \equiv a_q(E) \pmod 4$, in particular, $\nu_2(V(q)) \geq 4$. We also know from the LMFDB database [57] that $a_2 = -1$, then $\nu_2(U_2) = 4$ and $\nu_2(U(17)) = 5$. Putting all together we obtain

$$\nu_2\left(\frac{\|f_{E^{(D)}}\|^2_{N^{(D)}}}{\|f_E\|^2_N}\right) \geq 4(\nu_p(D) + \nu_2(D^*) + \sum_{\substack{q\mid D\\ q\neq 2,p}} 1) \geq 4\omega(D).$$

For (III), we note that for N equal to 2^5 or 2^7 Theorem 1 in *loc. cit.* says that

$$\nu_2\left(\frac{\|f_{E^{(D)}}\|^2_{N^{(D)}}}{\|f_E\|^2_N}\right) = \nu_2(D^*) + \sum_{\substack{q\mid D\\ q\neq 2}} \nu_2(V(q)).$$

As we saw before $\nu_2(V(q)) \geq 3$ for $q \neq 2$, then

$$\nu_2\left(\frac{\|f_{E^{(D)}}\|^2_{N^{(D)}}}{\|f_E\|^2_N}\right) \geq \nu_2(D) + 3(\omega(D) - \nu_2(D^*)) = 3\omega(D) - 2\nu_2(D^*).$$

Finally, to prove (IV), we only need to notice that for the curve $32.a3$ its 2-torsion is rational, then $\nu_2(V(q)) \geq 4$ for $q \neq 2$, which ends the proof. □

Remark 3.1.6. Notice that if D is prime and $D \equiv 1 \pmod 4$ and relatively prime to N we can improve the bounds given in (I) and (II), since $\nu_2(V(D))$ is higher. In this cases, we have that $\nu_2(\|f_{E^{(D)}}\|^2_{N^{(D)}}/\|f_E\|^2_N) \geq 4$ if N is a power of an odd prime, and $\nu_2(\|f_{E^{(D)}}\|^2_{N^{(D)}}/\|f_E\|^2_N) \geq 5$ if E is $17.a4$.

Manin constant

Now, we compute c_E of the elliptic curves E in Table 2.1.

Proposition 3.1.7. *Let E be an elliptic curve $X_0(N)$-optimal with odd square-free conductor N and let E' be an elliptic curve connected with E by a 2 isogeny $\theta : E \to E'$. Then, we have that $c_E = 1$ and $c_{E'} \in \{1, 2\}$.*

Proof. By Corollary 4.2 in [60], c_E must be a power of 2 and Theorem A in [1] says that if $p \mid c_E$ then $p \mid N$, which implies that $c_E = 1$. Now, let $\mathcal{E}$ and $\mathcal{E}'$ be the Néron models of E and E' and let ω, ω' be their respective Néron differentials. Since θ and $\theta^\vee$ define morphisms $\theta^* : H^0(\mathcal{E}', \Omega^1_{\mathcal{E}'/\mathbb{Z}}) \to H^0(\mathcal{E}, \Omega^1_{\mathcal{E}/\mathbb{Z}})$ and $(\theta^\vee)^* : H^0(\mathcal{E}, \Omega^1_{\mathcal{E}/\mathbb{Z}}) \to H^0(\mathcal{E}', \Omega^1_{\mathcal{E}'/\mathbb{Z}})$, then there are $a, b \in \mathbb{Z}$ such that $\theta^*\omega' = a\omega$ and $(\theta^\vee)^*\omega = b\omega'$. Due to the optimality of ϕ_E we have that $\phi_{E'} = \theta \circ \phi_E$, which implies that

$$\phi^*_{E'}\omega' = \phi^*_E\theta^*\omega' = a\phi^*_E\omega = 2\pi i a f_E(z)dz,$$

hence, $c_{E'} = a$. On the other hand, we have that $a \mid 2$ since

$$ab\omega = \theta^*(\theta^\vee)^*\omega = [2]^*\omega = 2\omega,$$

which ends the proof. □

Corollary 3.1.8. *Let E be an elliptic curve with non-trivial rational 2-torsion and prime conductor $p > 17$. Then $\nu_2(m_E/c_E^2) \geq -1$.*

Proof. We denote by $E_{p,1}$ and $E_{p,2}$ to $p.a1$ and $p.a2$ in Table 2.1, respectively. As we discussed before, there is a 2-isogeny θ between these two curves and the work of [61] shows that $E_{p,2}$ is $X_0(p)$-optimal. Because of Proposition 3.1.7 $c_{E_{p,1}} \in \{1, 2\}$ and $c_{E_{p,2}} = 1$, in particular, $\nu_2(m_{E_{p,2}}/c^2_{E_{p,2}}) \geq 0$. Since $\phi_{E_{p,1}} = \theta \circ \phi_{E_{p,2}}$, we have that $m_{E_{p,1}} = 2m_{E_{p,2}}$, therefore $\nu_2(m_{E_{p,1}}) \geq 1$ and consequently

$$\nu_2(m_{E_{p,1}}/c^2_{E_{p,1}}) \geq \nu_2(m_{E_{p,1}}) - 2 \geq -1,$$

which gives the desired result. □

3.1.2 Quadratic twists of elliptic curves with prime power conductor

Before proving Theorem 1.2.3, we need the following Definition and Proposition.

Definition 3.1.9. Let E be an elliptic curve defined over $\mathbb{Q}$ and $f_E = \sum_{i=1}^{\infty} b_n q^n \in S_2(\Gamma_0(N))$ be its Hecke newform. The congruence number δ_E of E is the largest integer such that there is a modular form $g = \sum_{i=1}^{\infty} b_n q^n \in S_2(\Gamma_0(N))$, with $b_n \in \mathbb{Z}$, such that g and f_E are orthogonal with respect to the Petersson inner product and $a_n \equiv b_n \pmod{\delta_E}$ for all n.

Remark 3.1.10. There are some relations between the modular degree and the congruent number, the most relevant is $m_E \mid \delta_E$, whenever E is $X_0(N)$-optimal [20].

Proposition 3.1.11. *Watkins's conjecture holds for every elliptic curve E of prime power conductor and non-trivial rational 2-torsion.*

Proof. Watkins's conjecture is known for elliptic curves of conductor $N < 10000$, in particular, this includes all the elliptic curves with conductor a power of 2. Then, we assume that the conductor is odd. By Corollary 2.2.8, $\mathrm{rank}(E(\mathbb{Q})) \leq 1$, so, it is enough to prove that if m_E is odd, $\mathrm{rank}(E(\mathbb{Q})) = 0$. Theorem 2.2 in [2] says that if a prime p divides the ratio δ_E/m_E, then $p^2 \mid N$, consequently, δ_E is odd. Finally, Theorem 1.1 in [52, 53] implies that $\mathrm{rank}(E(\mathbb{Q})) = 0$. □

Proof of Theorem 1.2.3. Note that the quadratic twists of $E^{(D)}$ are E itself, or quadratic twists of E. Because of Proposition 3.1.11 it is enough to prove the Theorem for elliptic curves with conductor 2^5, 2^6, 17, 49 and p of the form $u^2 + 64$ for some integer u.

When E has conductor $N = 49$, $E^{(7)}$ has conductor $N^{(7)} = 49$ and non-trivial rational 2-torsion. Notice that if $7 \nmid D'$, $E^{(7D')} = (E^{(7)})^{(D')}$, so, we can assume that $7 \nmid D$ and then we can use Proposition 3.1.5.(I) freely.

To begin with, we assume that N is odd and E is different to $17.a4$. By Corollary 3.1.8 and Section 2.2.2, we have that $\nu_2(m_E/c_E^2) \geq -1$. Applying Corollary 3.1.3 and Proposition 3.1.5.(I) to Lemma 2.2.12, (2.15) turns into

$$\nu_2(m_{E^{(D)}}) \geq -1 + 3\omega(D).$$

In the case of $17.a4$, we have that $\nu_2(m_E/c_E^2) = -2$ and therefore applying Proposition 3.1.5.(II) and Corollary 3.1.3 to Lemma 2.2.12 we obtain

$$\nu_2(m_{E^{(D)}}) \geq -2 + 4\omega(D).$$

Meanwhile, Lemma 2.2.8 implies that $\mathrm{rank}(E(\mathbb{Q})) \leq 2\omega(D) + 1$, hence in both cases Watkins's conjecture holds for $\omega(D) \geq 2$.

Now, assume D is a prime number. Proposition 3.1.11 proves the case $D \mid N$. Given Lemma 2.2.8, we only have to prove that $\nu_2(m_{E^{(D)}}) \geq 3$, then Remark 3.1.6 proves the case $D \equiv 1 \pmod 4$. For $D = 2$ or $D \equiv -1 \pmod 4$, Corollary 3.1.3 implies that $(1/6)\nu_2\left(\Delta_{E^{(D)}}/\Delta_E\right) \geq 2$, then for E different that $17.a4$ we have $\nu_2(m_{E^{(D)}}) \geq -1+3+2 = 4$ and when E is $17.a4$ we obtain $\nu_2(m_{E^{(D)}}) \geq -2+4+2 = 4$.

Now, suppose that E has conductor 2^5 or 2^7, and different to $32.a3$, in which case $\nu_2(m_E/c_E^2) \geq 0$. As a consequence, Proposition 3.1.5.(III) and Lemma 3.1.4 applied to Lemma 2.2.12 imply

$$\nu_2(m_{E^{(D)}}) \geq 3\omega(D) - 3\nu_2(D^*),$$

and Lemma 2.2.8 says that $\mathrm{rank}(E(\mathbb{Q})) \leq 2\omega(D) + 1 - 2\nu_2(D)$ and, therefore, Watkins's conjecture holds for $\omega(D) \geq 1 + \nu_2(D^*)$. Thus, the only missing case is $D = 2$, which is covered by Proposition 3.1.11.

Finally, for E equal to $32.a3$ we have that $\nu_2(m_E/c_E^2) = -1$. In this situation, Lemma 2.2.8 tells us that

$$\mathrm{rank}(E(\mathbb{Q})) \leq 2\omega(D) - \nu_2(D^*).$$

On the other hand, applying again Proposition 3.1.5.(IV) and Lemma 3.1.4 to Lemma 2.2.12 we obtain

$$\nu_2(m_{E^{(D)}}) \geq -1 + 4\omega(D) - 4\nu_2(D^*),$$

and we notice that the inequality $2\omega(D) - \nu_2(D^*) \leq -1 + 4\omega(D) - 4\nu_2(D^*)$ is equivalent to

$$\omega(D) \geq \frac{1 + 3\nu_2(D^*)}{2}.$$

Then, the only missing case is $D^* = 2$, which again is covered by Proposition 3.1.11. □

Example 3.1.12. Theorem 1.2.3 gives a different approach to prove that Watkins's conjecture holds for elliptic curves with bad additive reduction at 2, non-trivial rational 2-torsion, and at most two odd primes of bad reduction.

(a) Consider the elliptic curve $E : y^2 = x^3 - x$. Watkins's conjecture holds for its quadratic twists $E^{(p)} : y^2 = x^3 - p^2x$ and $E^{(pq)} : y^2 = x^3 - (pq)^2x$.

(b) Let E be the elliptic curve $y^2 + xy = x^3 - x^2 - x$, then the quadratic twists $E^{(-4)} : y^2 = x^3 - 19x + 18$ and $E^{(-8)} : y^2 = x^3 - 76x + 144$ satisfy Watkins's conjecture.

Finally, Theorem 1.2.3 has the following consequence:

Corollary 3.1.13. *Watkins's conjecture holds for all congruent curves* $E^{(D)} : y^2 = x^3 - D^2x$.

3.2 Congruence Number of $y^2 = x^3 - dx$

The main objective of this section is to prove the Theorem 1.2.4

Theorem 2.8 from [93] shows that the elliptic curves of the form $y^2 = x^3 - Dx$ have even congruence number, whenever $\omega(D) \geq 1$. The goal of this section is to give a lower bound for $\nu_2(\delta_E)$. First of all, let $p_1, \ldots, p_m$ be a list of distinct odd primes and define $d = p_1 \cdots p_m$. Let D be a divisor of d. Now, consider the elliptic curves $E : y^2 = x^3 - dx$ and $E^{(D)} : y^2 = x^3 - dD^2x$. Finally, denote by f and $f^{(D)}$ their associated Hecke newforms. Since $E^{(D)}$ is a quadratic twist by D of E, then we have that

$$a_q(f^{(D)}) = \left(\frac{D}{q}\right) a_q(f),$$

for every prime number q. Before proving Theorem 1.2.4 we need the following two Lemmas.

Lemma 3.2.1. *Let n be a positive integer relatively prime to d and $q_1^{\alpha_1} \cdots q_s^{\alpha_s}$ its prime factorization. Then $a_n(f^{(D)}) = \gamma_n(D) a_n(f)$, where*

$$\gamma_n(D) = \left(\frac{D}{q_1}\right)^{\alpha_1} \cdots \left(\frac{D}{q_s}\right)^{\alpha_s}.$$

Proof. Since $\gamma_{nm}(D) = \gamma_n(D)\gamma_m(D)$, it is enough to show this assertion for powers of primes. We prove it by induction (taking into account $a_1(f) = 1$ and $a_q(f) = \left(\frac{d}{p}\right) a_q(g)$) as follows

$$\begin{aligned} a_{q^{n+1}}(f^{(D)}) &= a_q(f^{(D)}) a_{q^n}(f^{(D)}) - p a_{q^{n-1}}(f^{(D)}) \\ &= \left(\frac{D}{q}\right) a_q(f) \left(\frac{D}{q}\right)^n a_{q^n}(f) - p \left(\frac{D}{q}\right)^{n-1} a_{q^{n-1}}(f) \\ &= \left(\frac{D}{q}\right)^{n+1} a_{q^{n+1}}(f), \end{aligned} \tag{3.3}$$

which gives the desired result. □

Lemma 3.2.2. *Let m be an odd integer and q be a prime such that $q \nmid d$. If $\left(\frac{d}{q}\right) = 1$ then $a_{q^m}(f) \equiv 0$ (mod 2) and if $\left(\frac{d}{q}\right) = -1$ then $a_{q^m}(f) \equiv 0$ (mod 4).*

Proof. We know that E is a quartic twist of $E_1 : y^2 = x^3 - x$ by d. By section 3.2 [24] if E_1 corresponds to the automorphic form $\chi \oplus \overline{\chi}$ (where χ is a Grossencharacter), then E corresponds to the automorphic form $\chi\psi \oplus \overline{\chi}\overline{\psi}$, where $\psi = \left(\frac{\cdot}{d}\right)_4$.

First of all, if $q \equiv 3 \pmod 4$ we have $a_q(E) = 0$ since the image is antidiagonal. By induction on (3.3) we obtain that $a_{q^m}(E) = 0$ for m an odd integer.

Finally, assume that $q \equiv 1 \pmod 4$. We have that if $\left(\frac{d}{q}\right) = 1$ then $a_q(f) = \pm a_q(g)$, where g is the Hecke eigenform attached to E_1, thus, $a_q(f) \equiv 0 \pmod 2$. On the other hand, if $\left(\frac{d}{q}\right) = -1$ then $(a_q(f)/2)^2 + (a_q(g)/2)^2 = p$, so, $a_q(f) \equiv 0 \pmod 4$. By induction on (3.3), we get the desired result. □

Proof of Theorem 1.2.4. We define $n_1 = p_1^{\nu_{p_1}(n)} \cdots p_m^{\nu_{p_m}(n)}$ and $n_2 = n/n_1$. Notice that $(n_2, d) = 1$. By Table I in [48] $N = N^{(D)}$ for every divisor D of d, then it is enough to prove that

$$a_n(\sum_{D|d}(-1)^{\omega(D)} f^{(D)}) \equiv 0 \pmod{2^{m+\epsilon}},$$

where $\epsilon = 1$ if m is even and $\epsilon = 2$ if m is odd. Assume $n_2 = q_1^{\alpha_1} \cdots q_s^{\alpha_s}$, then by Lemma 3.2.1 we have that $a_{n_2}(f^{(D)}) = \gamma_{n_2}(D) a_{n_2}(f)$. We claim that

$$a_n(\sum_{D|d}(-1)^{\omega(D)} f^{(D)}) = \begin{cases} 2^m a_n(f) & \text{if } \gamma_{n_2}(p) = -1 \text{ for all } p \mid d \\ 0 & \text{otherwise.} \end{cases}$$

Before proving the claim, notice that if $p \mid d$, we have that $a_p(f) = a_p(f^{(D)}) = 0$, hence $a_{n_1}(f) = a_{n_1}(f^{(D)})$ for every divisor D of d, as a consequence

$$a_n(\sum_{D|d} f^{(D)}) = a_{n_1}(f) a_{n_2}(\sum_{D|d} f^{(D)}).$$

To begin with, assume that for some $p \mid d$, $\gamma_{n_2}(p) = -1$. Since $\gamma_n(DD') = \gamma_n(D)\gamma_n(D')$, we obtain

$$\begin{aligned} a_n(\sum_{D|d} f^{(D)}) &= a_{n_1}(f) \sum_{\substack{D|d \\ p\nmid D}} (-1)^{\omega(D)} a_{n_2}(f^{(D)}) + a_{n_1}(f) \sum_{\substack{D|d \\ p|D}} (-1)^{\omega(D)-1} a_{n_2}(f^{(D/p)}) \\ &= 2a_{n_1}(f) \sum_{D|(d/p)} a_{n_2}(f^{(D)}). \end{aligned} \tag{3.4}$$

Without loss of generality, assume that t is an integer such that $t \leq m$ and for $i \leq t$ we have $\gamma_{n_2}(p_i) = -1$, and for $i > t$ we have $\gamma_{n_2}(p_i) = 1$. Denote by $d_1 = p_1 \cdots p_t$, then applying equation (3.4) recursively, if $t < m$ we have that

$$a_n(\sum_{D|d} f^{(D)}) = 2^t a_{n_1}(f) \sum_{D|(d/d_1)} a_{n_2}(f^{(D)}) = 2^t a_n(f) \sum_{D|(d/d_1)} (-1)^{\omega(D)} = 0,$$

meanwhile if $t = m$, we obtain that $a_n(\sum_{D|d} f^{(D)}) = 2^m a_n(f)$.

Finally, if $\gamma_{n_2}(p) = -1$ for all $p \mid d$, we have that $\gamma_{q_i}(p)^{\alpha_i} = -1$ for some $1 \leq i \leq s$, in particular, α_i is odd, then because of Lemma 3.2.2 we obtain that $a_n(f)$ is even. Even better, if $\omega(d)$ is odd, $\gamma_{n_2}(d) = -1$, then there exists $1 \leq i \leq s$, such that $\gamma_{q_i}(d)^{\alpha_i} = -1$. Therefore, α_i is odd and $\left(\frac{d}{q_i}\right) = \gamma_{q_i}(d) = -1$, applying Lemma 3.2.2 we obtain that $4 \mid a_n(f)$, so

$$a_n(\sum_{D|d}(-1)^{\omega(D)} f^{(D)}) \equiv 0 \pmod{2^{m+\epsilon}},$$

which proves the desired result. □

Theorem 1.2.4 allows us to prove that for some elliptic curves $\operatorname{rank}(E(\mathbb{Q})) \leq \nu_2(\delta_E)$, which goes in the direction of Watkins's conjecture since $m_E \mid \delta_E$ as we said before.

Corollary 3.2.3. *Let p be an odd prime. Then, for E an elliptic curve $y^2 = x^3 - px$ or $y^2 = x^3 - p^3x$, we have that* $\operatorname{rank}(E(\mathbb{Q})) < \nu_2(\delta_E)$.

Proof. By Remark 2.2.9, $\operatorname{rank}(E(\mathbb{Q})) \leq 2$ when E is equal to $y^2 = x^3 - px$ or $y^2 = x^3 - p^3x$ for p a prime number. On the other hand, Theorem 1.2.4 says that $3 \leq \nu_2(\delta_E)$ in both cases, as a consequence, $\operatorname{rank}(E(\mathbb{Q})) < \nu_2(\delta_E)$. □

3.3 Watkins's conjecture for elliptic curves with non-split multiplicative reduction

This section is in joint work with Hector Pasten [17]. In this section we let E be a semistable elliptic curve over $\mathbb{Q}$; so, N is square-free and $\mu = \omega(N)$. Let $f \in S_2(\Gamma_0(N))$ be its associated newform. Let $\operatorname{Sel}_2(E)$ be the 2-Selmer group of E.

Lemma 3.3.1. *Assume $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z}$. Then we have* $\operatorname{rank} E(\mathbb{Q}) \leq \mu - 1$. *If equality holds, then* $Ш(E)[2] = (0)$.

Proof. By Theorem 2.2.7 we have $\operatorname{rank} E(\mathbb{Q}) \leq \mu - 1$. Now, assume that $\operatorname{rank} E(\mathbb{Q}) = \mu - 1$. Then, $\dim_{\mathbb{F}_2} E(\mathbb{Q})/2E(\mathbb{Q}) \leq \mu$. By the exact sequence

$$(0) \to E(\mathbb{Q})/2E(\mathbb{Q}) \to \operatorname{Sel}_2(E) \to Ш(E)[2] \to (0),$$

it suffices to prove $\dim_{\mathbb{F}_2} \operatorname{Sel}_2(E) \leq \mu$. Let $\theta : E \to E'$ be the 2-isogeny with kernel $E(\mathbb{Q})[2]$ and let $\theta' : E' \to E$ be its dual. Consider the exact sequence from Lemma 6.1 of [73]:

$$(0) \to E'(\mathbb{Q})[\theta']/\theta(E(\mathbb{Q})[2]) \to \operatorname{Sel}_\theta(E) \to \operatorname{Sel}_2(E) \to \operatorname{Sel}_{\theta'}(E').$$

The assumption $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z}$ gives that $\theta(E(\mathbb{Q})[2]) = (0)$ and that 2 divides $\#E'(\mathbb{Q})[\theta']$. From this we deduce $\dim_{\mathbb{F}_2} \operatorname{Sel}_2(E) \leq s(E,\theta) + s'(E,\theta) - 1$. We conclude by Theorem 2.2.7. □

For each $d|N$ there is the Atkin-Lehner involution W_d on $X_0(N)$. They form a group $W \simeq (\mathbb{Z}/2\mathbb{Z})^\mu$. For every $d|N$ we have $W_d(f) = \pm f$. Let $w_d(f) \in \{-1, 1\}$ be defined by $W_d(f) = w_d(f) \cdot f$. These eigenvalues satisfy $\prod_{p|N} w_p(f) = w_N(f) = -\epsilon(f)$, where $\epsilon(f)$ is the sign of the functional equation of $L(f, s)$. In [4] it is shown that $-w_p(f) = a_p(f)$, the p-th Fourier coefficient of f. Thus:

$$w_p(f) = \begin{cases} 1 & \text{if } E \text{ has non-split multiplicative reduction at } p, \\ -1 & \text{if } E \text{ has split multiplicative reduction at } p. \end{cases}$$

The rule $W_d \mapsto w_d$ defines a morphism $\rho : W \to \{-1, 1\}$. Let $W' = \ker(\rho)$. A morphism $W' \to E(\mathbb{Q})[2]$ is constructed in Proposition 2.1 from [31] with kernel denoted by W''. They prove that $\#W''$ divides m_E and that $\dim_{\mathbb{F}_2} W'' \geq \mu - \dim_{\mathbb{F}_2}(W/W') - \dim_{\mathbb{F}_2} E(\mathbb{Q})[2]$. We get:

Lemma 3.3.2. *Assume $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z}$. If $w_p = 1$ for all $p|N$, then $v_2(m_E) \geq \mu - 1$. On the other hand, if $w_p = -1$ for some $p|N$, then $v_2(m_E) \geq \mu - 2$.*

With these lemmas at hand, we can prove Theorem 1.2.1.

Proof of Theorem 1.2.1. Let us assume that E is a semistable elliptic curve of conductor N and modular degree m_E with $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z}$.

If E has no place of split multiplicative reduction, then the first part of Lemma 3.3.2 gives $v_2(m_E) \geq \mu - 1$, while Lemma 3.3.1 gives $\operatorname{rank}(E) \leq \mu - 1$.

So, we may assume that E has an odd number of places of non-split multiplicative reduction. By the second part of Lemma 3.3.2, it suffices to show that $\operatorname{rank}(E) \leq \mu - 2$. If $Ш(E)[2]$ is non-trivial, then, Lemma 3.3.1 gives $\operatorname{rank}(E) \leq \mu - 2$ and we are done. So, let us assume that $Ш(E)[2]$ is trivial. Then $Ш(E)[2^\infty] = (0)$ and by results of Monsky [62] the parity conjecture holds for E: we get $\epsilon(f) = (-1)^{\operatorname{rank} E(\mathbb{Q})}$.

Write $N = N^+N^-$ where N^+ is the product of the primes of split multiplicative reduction for E and N^- is the product for non-split multiplicative reduction. Then $\omega(N^+)$ and $\mu = \omega(N^+) + \omega(N^-)$ have opposite parity, while $\epsilon(f)$ and $(-1)^{\omega(N^+)} = \prod_{p|N} w_p(f)$ have opposite sign. This means that $\operatorname{rank}(E)$ and μ have the same parity. Therefore, the bound $\operatorname{rank}(E) \leq \mu - 1$ from Lemma 3.3.1 is strict and we get $\operatorname{rank}(E) \leq \mu - 2$. □

Chapter 4

Watkins's Conjecture for Elliptic Curves over Function Fields

4.1 Watkins's conjecture for Semistable elliptic curves

The following Proposition gives a lower bound of $\nu_2(m_E)$ in terms of $\omega_K(\mathfrak{n})$.

Proposition 4.1.1. *Let E be a modular elliptic curve with conductor $\mathfrak{n}_E = \mathfrak{n}\infty$. Let f_E be the primitive newform attached to E. Over this newform, we define $\mathcal{W}' = \{W \in \mathcal{W}(\mathfrak{n})\colon W(f_E) = f_E\}$ and $\kappa \coloneqq \dim_{\mathbb{F}_2}(\mathcal{W}(\mathfrak{n})/\mathcal{W}') + \dim_{\mathbb{F}_2}(E(K)[2])$. Then $\omega_K(\mathfrak{n}) - \kappa \leq \nu_2(m_E)$.*

Proof. Proposition 10.3 from [29] gives the following isomorphism

$$\Phi\colon H^1(X_0(\mathfrak{n}) \otimes K_\infty^{sep}, \mathbb{Q}_\ell) \cong \underline{H}_!(\Gamma_0(\mathfrak{n}), \mathbb{Q}_\ell) \otimes \mathrm{sp},$$

where sp is the two-dimensional special ℓ-adic representation of $\mathrm{Gal}(K_\infty^{sep}/K_\infty)$. Furthermore, by Remark 4.13.2 [43] this isomorphism is compatible with the action of the Atkin-Lehner involutions.

Since $H^1(X_0(\mathfrak{n}) \otimes K_\infty^{sep}, \mathbb{Q}_\ell)$ is the dual of $V_\ell(J_0(\mathfrak{n}))$, we have that if $\pi : J_0(\mathfrak{n}) \to E$ is the projection, then, $\pi([W(D)]) = \pi([D])$ for every divisor D of degree 0 over $X_0(\mathfrak{n})$ whenever $W \in \mathcal{W}'$ (due to the compatibility of Φ with the action of W, we have that $\Phi f \circ W = \Phi(Wf)$, thus, if $Wf = f$ we have $\pi \circ W = \Phi f \circ W = \Phi(Wf) = \Phi(f) = \pi$). By Remark 2.2.14, $\mathcal{W}'$ has at most index 2 in $\mathcal{W}(\mathfrak{n})$. Now, as in Proposition 2.1 in [31], we construct a homomorphism $\theta : \mathcal{W}' \to E(K)[2]$. First of all, we fix a K-rational point $x_0 \in X_0(\mathfrak{n})$ (for example a cusp), then, for $W \in \mathcal{W}'$ we define $\theta(W) = \pi([W(x_0) - (x_0)])$. Notice that $\theta(W) \in E(K)[2]$, since $x_0 \in X_0(\mathfrak{n})(K)$ and

$$\theta(W) = \pi([W(x_0) - (x_0)]) = \pi([W(W(x_0) - (x_0))]) = -\pi([W(x_0) - (x_0)]) = -\theta(W).$$

Now, define $\mathcal{W}'' = \ker\theta$. We define $\mathcal{X} = X_0(\mathfrak{n})/\mathcal{W}''$ and consider the quotient map $\psi : X_0(\mathfrak{n}) \to \mathcal{X}$ which is also defined over K. The Jacobian of $\mathcal{X}$ is denoted by $\mathcal{J}$. We can define $\iota : X_0(\mathfrak{n}) \to J_0(\mathfrak{n})$ based on x_0, and $\iota' : \mathcal{X} \to \mathcal{J}$ based on $\psi(x_0)$, so we obtain a commutative diagram

$$\begin{array}{ccc} X_0(\mathfrak{n}) & \xrightarrow{\quad\iota\quad} & J_0(\mathfrak{n}) \\ {\scriptstyle\psi}\downarrow & & \downarrow{\scriptstyle\psi_*} \\ \mathcal{X} & \xrightarrow{\quad\iota'\quad} & \mathcal{J}. \end{array}$$

Since $\pi([W(x_0) - x_0]) = 0$ for $W \in \mathcal{W}''$, we have that $\pi \circ \iota(W(x)) = \pi \circ \iota(x)$ for all $x \in X_0(\mathfrak{n})$, in particular, $\pi \circ \iota$ factors through $\mathcal{X}$. Since the image of ι generates to $J_0(\mathfrak{n})$ as a group, there exists $\pi' : \mathcal{J} \to E$ such that $\pi = \pi' \circ \psi_*$, then,

$$[m_E] = \pi \circ \pi^\vee = (\pi' \circ \psi_*) \circ (\psi^* \circ \pi'^\vee) = \pi' \circ [\deg(\psi)] \circ \pi'^\vee = [\#\mathcal{W}''] \circ (\pi' \circ \pi'^\vee).$$

Since the degree of $[i]$ (multiplication by i) is $i \cdot i^*$ or $(i^*)^2$ where i^* denotes the p-free part of i, then, $\#\mathcal{W}'' \mid m_E$, since $p \neq 2$. □

Example 4.1.2. Consider the elliptic curve defined over $\mathbb{F}_3(T)$ by the equation

$$E : Y^2 = X^3 + T^2X^2 + X.$$

This curve has conductor $\mathfrak{n}_E = (T^2+1)(T+1)(T-1)\infty$, and also $E(\mathbb{F}_3(T)) \cong \mathbb{Z}/2\mathbb{Z}$. By Proposition 5.7 from [74] we have that $\mathcal{W}'' = \langle W_{(T-1)(T^2+1)}, W_{(T+1)(T^2+1)} \rangle$, therefore Proposition 4.1.1 tells us that $\nu_2(m_E) \geq \nu_2(\#\mathcal{W}'') \geq 2$. More precisely, from Example 2.2.19 we know that $\nu_2(m_E) = 2$, which implies that the bound in Proposition 4.1.1 is optimal.

Proposition 4.1.1 and Tate's geometric bound (2.16) allow us to prove Theorem 1.2.5.

Proof of Theorem 1.2.5. Recall that $E' = E \times_{\operatorname{Spec} K} \operatorname{Spec} K'$. Since the conductor of E' is also $\mathfrak{n}_E = (n)\infty$, then, by Tate's geometric bound (2.16) $\operatorname{rank}(E'(K')) \leq \deg(n) - 4$. On the other hand, we know that $\omega_{K'}((n)) = \deg(n)$ because k' contains the splitting field of n. Furthermore, since $\dim_{\mathbb{F}_2}([\mathcal{W}(\mathfrak{n}) : \mathcal{W}']) \leq 1$, by Remark 2.2.14, we have that $\kappa \leq 3$, then, by Proposition 4.1.1 we have that

$$\nu_2(m_{E'}) \geq \omega_K((n)) - 3 = \deg(n) - 3 = \deg(\mathfrak{n}_E) - 4 \geq \operatorname{rank}(E'(k'(T))),$$

which yields the desired result. □

Ulmer [86] exhibits a closed formula for the rank of a family of elliptic curves. Proposition 4.1.1 together with this formula allows us to show Watkins's conjecture for this family.

Proof of Theorem 1.2.6. First of all, we notice that $E(\overline{\mathbb{F}_p}(T))[2] = (0)$, since the polynomial $4x^3 + T^{2d}x - 4$ does not have a solution over $\overline{\mathbb{F}_p}(T)$. Notice that E is the change of base point of $\mathbb{P}^1$ given by $[0:1] \mapsto \infty$ of

$$E' : y^2 + xy = x^3 - T^m,$$

where $m = p^n + 1$. Theorem 1.5 in [86] shows that $\mathfrak{n}_{E'} = T(1 - 2^4 3^3 T^m)$, consequently, $\mathfrak{n}_E = (T^m - 2^4 3^3)\infty$. We claim that $f(T) = T^m - 2^4 3^3$ always has a root in $\mathbb{F}_{p^2}$. Let $\alpha \in \mathbb{F}_{p^2}$ such that $\alpha^2 = 3$ and notice that if $\alpha \in \mathbb{F}_p$, then $2^2 3\alpha$ is a root of f. If $\alpha \notin \mathbb{F}_p$, since $6 \mid p^n - 1$ we have that $p \equiv -1 (\text{mod } 3)$, then $p \equiv 1 (\text{mod } 4)$ by the law of quadratic reciprocity. This implies that $2^2 3\alpha$ or $2^2 3\alpha\beta$ is a root of f, where $\beta^2 = -1$. Consequently, there is a bijection between the prime divisors of even degree of $T^m - 1$ and $f(T)$.

By definition, $T^m - 1$ factors over $\mathbb{F}_p[T]$ as follows:

$$T^m - 1 = \prod_{e|m} \Phi_e(T),$$

where $\Phi_n(T)$ is the n^{th}-cyclotomic polynomial. Thus, the number of prime divisors over $\mathbb{F}_q[T]$ of $f(T)$ is

$$\omega_{\mathbb{F}_q(T)}(\mathfrak{n}_E) = \sum_{e|m} \frac{\phi(e)}{o_e(q)} - \begin{cases} 0 & \text{if } T^m - 2^4 3^3 \text{ has a solution in } \mathbb{F}_q \\ 1 & \text{otherwise} \end{cases},$$

where $\phi(e)$ is the cardinality of $(\mathbb{Z}/e\mathbb{Z})^\times$ and $o_e(q)$ is the order of q in $(\mathbb{Z}/e\mathbb{Z})^\times$. On the other hand, we know that $\text{rank}(E(\mathbb{F}_p(T))) = \text{rank}(E'(\mathbb{F}_p(T)))$. Theorem 1.5 in [86] states a closed expression for $\text{rank}(E'(\mathbb{F}_q(T)))$

$$\sum_{\substack{e|m \\ e\nmid 6}} \frac{\phi(e)}{o_e(q)} + \begin{cases} 2 & \text{if } 3 \mid q-1 \\ 1 & \text{otherwise} \end{cases} + \begin{cases} 1 & \text{if } 4 \mid q-1 \\ 0 & \text{otherwise} \end{cases}.$$

Since there are 4 divisors of 6 we obtain

$$\sum_{e|m} \frac{\phi(e)}{o_e(q)} \geq \sum_{\substack{e|m \\ e\nmid 6}} \frac{\phi(e)}{o_e(q)} + 4$$

Furthermore, if $3 \mid q - 1$ then q is a square since $p \equiv -1 (\text{mod } 3)$; which implies that $T^m - 2^4 3^3$ has a solution in $\mathbb{F}_q$. Hence, Proposition 4.1.1 implies that

$$\nu_2(m_E) \geq \omega_{\mathbb{F}_q(T)}(\mathfrak{n}_E) - 1 = \sum_{e|m} \frac{\phi(e)}{o_e(q)} - 1 \geq \sum_{\substack{e|m \\ e\nmid 6}} \frac{\phi(e)}{o_e(q)} + 3 \geq \text{rank}(E(\mathbb{F}_q(T))).$$

Finally, if $3 \nmid q-1$, we obtain

$$\nu_2(m_E) \geq \omega_{\mathbb{F}_q(T)}(\mathfrak{n}_E) - 1 \geq \sum_{e|m} \frac{\phi(e)}{o_e(q)} - 2 \geq \sum_{\substack{e|m \\ e\nmid 6}} \frac{\phi(e)}{o_e(q)} + 2 \geq \operatorname{rank}(E(\mathbb{F}_q(T))),$$

which gives the desired result. □

4.2 Watkins's Conjecture for Quadratic Twists

Let E be a modular elliptic curve with conductor $\mathfrak{n}_E$, since $\operatorname{char}(k) > 3$ there exist square-free coprime polynomials $n_1, n_2 \in A$ such that $\mathfrak{n}_E = (n_1^2 n_2)\infty$. Let $g \in A$ be a monic square-free polynomial, with $(n_1, g) = 1$, we define the quadratic twist $E^{(g)}$ of E by g as follows

$$E^{(g)} \colon y^2 = x^3 + Agx^2 + Bg^2x.$$

We assume that $\deg(g)$ is even to ensure that $E^{(g)}$ is modular. To see that, notice that if the change of variables $x \mapsto T^{2n}x$ and $y \mapsto T^{3n}y$ makes E a minimal T^{-1}-integral model, then the change $x \mapsto T^{2(n+m)}x$ and $y \mapsto T^{3(n+m)}y$ makes $E^{(g)}$ a minimal T^{-1}-integral model, where $\deg(g) = 2m$; since g is a monic polynomial, both reductions modulo T^{-1} are the same. Note that the conductor $\mathfrak{n}_E^{(g)}$ of $E^{(g)}$ is equal to $\mathfrak{n}_E(g^2/d)$, where $d = \gcd(n_2, g)$. The attached Drinfeld newform to $E^{(g)}$ is denoted by $f^{(g)}$.

The following lemma gives an upper bound for the Mordell-Weil rank of $E^{(g)}$.

Lemma 4.2.1. *With the notation above, we have that*

$$\operatorname{rank}(E^{(g)}(K)) \leq \omega_K(n_2) + 2(\omega_K(n_1) + \omega_K(g)).$$

Proof. First of all, we notice that $E^{(g)}$ has multiplicative reduction at $\mathfrak{p}$ if $\mathfrak{p} \mid n_2/d$, $E^{(g)}$ has additive reduction at $\mathfrak{p}$ if $\mathfrak{p} \mid n_1 g$ and otherwise $E^{(g)}$ has good reduction at $\mathfrak{p}$. Then by Proposition 2.2.16 we obtain that

$$\operatorname{rank}(E^{(g)}(K)) \leq \omega_K(n_2/d) + 2(\omega_K(n_1) + \omega_k(g)),$$

since $\omega_K(n_2/d) \geq \omega_K(n_2)$ we obtain the desired result. □

To find a lower bound for $\nu_2(m_{E^{(g)}})$ we need to relate $L(\operatorname{Sym}^2 f^{(g)}, 2)$ and $L(\operatorname{Sym}^2 f, 2)$, so, we can use Lemma 2.2.18 and the fact that $j_E = j_{E^{(g)}}$ (since this two elliptic curves are isomorphic in a quadratic extension of K), but before, we need the following lemma:

Lemma 4.2.2. *Let $\mathfrak{p}$ be a prime ideal of A and let $\left(\frac{\cdot}{\mathfrak{p}}\right) : \mathbb{F}_{\mathfrak{p}} \to \{-1, 0, 1\}$ be the extended Legendre symbol. Then*

$$a_{\mathfrak{p}}(E^{(g)}) = \left(\frac{g}{\mathfrak{p}}\right) a_{\mathfrak{p}}(E).$$

Proof. If $E^{(g)}$ has additive reduction at $\mathfrak{p}$, we have that $\mathfrak{p} \mid n_1$ or $\mathfrak{p} \mid g$, then $a_{\mathfrak{p}}(E^{(g)}) = 0$ and there is nothing to prove. On the other hand, assume that $E^{(g)}$ has multiplicative reduction at $\mathfrak{p}$. By Lemma 2.2 in [23] E has split multiplicative reduction at $\mathfrak{p}$ if and only if $\left(\frac{-c_6(E)}{\mathfrak{p}}\right) = 1$, as a consequence, this quantity is equal to $a_{\mathfrak{p}}(E)$. Furthermore, since $c_6(E^{(g)}) = g^3 c_6(E)$, we have

$$a_{\mathfrak{p}}(E^{(g)}) = \left(\frac{-c_6(E^{(g)})}{\mathfrak{p}}\right) = \left(\frac{-g^3 c_6(E)}{\mathfrak{p}}\right) = \left(\frac{g}{\mathfrak{p}}\right) a_{\mathfrak{p}}(E).$$

Finally, assume that $\mathfrak{p} \nmid \mathfrak{n}^{(g)}$. Define $M = \{x \in \mathbb{F}_{\mathfrak{p}} \colon x^3 + Ax^2 + B \neq 0\}$. Consequently, we obtain

$$\begin{aligned}
\#E^{(g)}_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}}) &= |\mathfrak{p}| + 1 + \sum_{x \in M} \left(\frac{x^3 + Agx^2 + Bg^2x}{\mathfrak{p}}\right) \\
&= |\mathfrak{p}| + 1 + \sum_{x \in M} \left(\frac{g^3(x^3 + Ax^2 + Bx)}{\mathfrak{p}}\right) \\
&= |\mathfrak{p}| + 1 + \left(\frac{g}{\mathfrak{p}}\right) \sum_{x \in M} \left(\frac{x^3 + Ax^2 + Bx}{\mathfrak{p}}\right) \\
&= |\mathfrak{p}| + 1 - \left(\frac{g}{\mathfrak{p}}\right) a_{\mathfrak{p}}(E^{(g)}),
\end{aligned}$$

by recalling the definition of $a_{\mathfrak{p}}(E)$ we get the desired result. □

Proposition 4.2.3. *Let E be a modular elliptic curve with conductor $\mathfrak{n}_E$ and associated primitive newform f. Assume that E' is a quadratic twist of E, with conductor $\mathfrak{n}'_E$ and associated primitive newform f', such that $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{n}_E) \leq \mathrm{ord}_{\mathfrak{p}}(\mathfrak{n}'_E)$ for all $\mathfrak{p}$. Thus, there exist n_1, n_2, d, g square-free monic polynomials with $1 = \gcd(n_1, g)$, and $d = \gcd(n_2, g)$ such that $\mathfrak{n}_E = (n_1^2 n_2)\infty$ and $\mathfrak{n}'_E = \mathfrak{n}_E g^2/d$. Then, one has*

$$L(\mathrm{Sym}^2 f', 2) = L(\mathrm{Sym}^2 f, 2) \frac{|d|}{|g|^3} \prod_{\mathfrak{p} \mid d} (|\mathfrak{p}|^2 - 1) \prod_{\mathfrak{p} \mid g/d} \left((|\mathfrak{p}| + 1)^2 - a_{\mathfrak{p}}(E)^2\right) (|\mathfrak{p}| - 1).$$

Proof. By Lemma 4.2.2 we have that when $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{n}) = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{n}')$ the local factors are equal, i.e. $L_{\mathfrak{p}}(\mathrm{Sym}^2 f', 2) = L_{\mathfrak{p}}(\mathrm{Sym}^2 f, 2)$. If $\mathfrak{p} \mid d$, we have that

$$L_{\mathfrak{p}}(\mathrm{Sym}^2 f', s) = L_{\mathfrak{p}}(\mathrm{Sym}^2 f, s)(1 - |\mathfrak{p}|^{-s}),$$

thus, at $s = 2$ we obtain

$$L_{\mathfrak{p}}(\mathrm{Sym}^2 f', 2) = L_{\mathfrak{p}}(\mathrm{Sym}^2 f, 2)\frac{1}{|\mathfrak{p}|^2}(|\mathfrak{p}|^2 - 1).$$

Finally, assume that $\mathfrak{p} \mid (g/d)$. The local factors are related as follows

$$L_{\mathfrak{p}}(\mathrm{Sym}^2 f', s) = L_{\mathfrak{p}}(\mathrm{Sym}^2 f, s)\left(1 - \alpha_{\mathfrak{p}}^2|\mathfrak{p}|^{-s}\right)\left(1 - \overline{\alpha_{\mathfrak{p}}}^2|\mathfrak{p}|^{-s}\right)\left(1 - |\mathfrak{p}|^{1-s}\right),$$

therefore at $s = 2$ we obtain

$$L_{\mathfrak{p}}(\mathrm{Sym}^2 f', 2) = L_{\mathfrak{p}}(\mathrm{Sym}^2 f, 2)\frac{1}{|\mathfrak{p}|^3}\left((|\mathfrak{p}| + 1)^2 - a_{\mathfrak{p}}(E)^2\right)(|\mathfrak{p}| - 1),$$

putting all together, we achieve the desired result. □

Now, we can prove Theorem 1.2.7

Proof of Theorem 1.2.7. Since E and $E^{(g)}$ are isomorphic over $\mathbb{C}_\infty$, we have that $j_E = j_{E^{(g)}}$. Thus, by Lemma 2.2.18 we obtain

$$\nu_2(m_{E^{(g)}}) = \nu_2(m_E) + \nu_2(L(\mathrm{Sym}^2 f^{(g)}, 2)) - \nu_2(L(\mathrm{Sym}^2 f, 2)).$$

On the other hand, Proposition 4.2.3 implies that

$$\nu_2\left(\frac{L(\mathrm{Sym}^2 f^{(g)}, 2)}{L(\mathrm{Sym}^2 f, 2)}\right) = \sum_{\mathfrak{p}|d}\nu_2(|\mathfrak{p}|^2 - 1) + \sum_{\mathfrak{p}|g/d}\nu_2\left(((|\mathfrak{p}| + 1)^2 - a_{\mathfrak{p}}(E)^2)(|\mathfrak{p}| - 1)\right).$$

We know that $|\mathfrak{p}|^2 - 1 \equiv 0 \pmod 8$ and $|\mathfrak{p}| - 1 \equiv 0 \pmod 2$. As $E(K)[2]$ is non-trivial and it maps injectively into $E_{\mathfrak{p}}(\mathbb{F}_{\mathfrak{p}})$ for every prime $\mathfrak{p} \nmid \mathfrak{n}\infty$, then, $|\mathfrak{p}| + 1 - a_{\mathfrak{p}}(E) \equiv 0 \pmod 2$, which implies $(|\mathfrak{p}| + 1)^2 - a_{\mathfrak{p}}(E)^2 \equiv 0 \pmod 4$. As a consequence

$$\nu_2(L(\mathrm{Sym}^2 f^{(g)}, 2)) - \nu_2(L(\mathrm{Sym}^2 f, 2)) \geq 3\omega_K(g).$$

Putting all together, we achieve the result.

$$\nu_2(m_{E^{(g)}}) \geq \nu_2(m_E) + 3\omega_K(g). \tag{4.1}$$

By Proposition 2.2.16 we know that $\mathrm{rank}(E^{(g)}) \leq 2(\omega_K(\mathfrak{n}) + \omega_K(g))$. By our assumptions on g we obtain that

$$\nu_2(m_E) + 3\omega_K(g) \geq 2(\omega_K(\mathfrak{n}) + \omega_K(g)),$$

consequently, $\mathrm{rank}(E^{(g)}) \leq \nu_2(m_{E^{(g)}})$. □

Corollary 4.2.4. *Assume that E is a semistable modular elliptic curve over K. Then, we have that $E^{(g)}$ satisfies Watkins's conjecture whenever $\omega_K(g) \geq 3$. Furthermore, if every prime dividing $\mathfrak{n}$ has non-split multiplicative reduction and $E(K)[2] \cong \mathbb{Z}/2\mathbb{Z}$ we have that $E^{(g)}$ satisfies Watkins's conjecture for every square-free polynomial $g \in A$ of even degree.*

Proof. By Proposition 4.1.1 we have that $\nu_2(m_E) \geq \omega_K(\mathfrak{n}) - 3$. Since E is semistable, $\mathfrak{n}$ is square-free, consequently, Lemma 4.2.1 implies that $\operatorname{rank}(E^{(g)}) \leq \omega_K(\mathfrak{n}) + 2\omega_K(g)$. Using equation (4.1), we have

$$\nu_2(m_{E^{(g)}}) \geq \nu_2(m_E) + 3\omega_K(g) \geq \omega_K(\mathfrak{n}) - 3 + 3\omega_K(g) \geq \omega_K(g) - 3 + \operatorname{rank}(E^{(g)}), \quad (4.2)$$

hence, Watkins's conjecture holds for $E^{(g)}$, whenever $\omega_K(d) \geq 3$. Furthermore, if a prime ideal $\mathfrak{p}$ divides $\mathfrak{n}$ and has non-split multiplicative reduction, by Theorem 3 in [4] $W_{\mathfrak{p}} f = f$, consequently, $\mathcal{W} = \mathcal{W}'$. Therefore, if every prime $\mathfrak{p}$ which divides $\mathfrak{n}$ has non-split multiplicative reduction and $E(K)[2] \cong \mathbb{Z}/2\mathbb{Z}$ Proposition 4.1.1 implies that $\nu_2(m_E) \geq \omega_K(\mathfrak{n}) - 1$. Thus, equation (4.2) turns into

$$\nu_2(m_{E^{(g)}}) \geq \omega_K(g) - 1 + \operatorname{rank}(E^{(g)}),$$

accordingly, Watkins's Conjecture holds for quadratic twists by every square-free polynomial g of even degree. □

Appendix A

A Chabauty-Coleman bound for surfaces: work report

In this appendix, we describe joint work with Hector Pasten [16] on generalizing the classical Chabauty-Coleman bound from the case of curves to the case of surfaces. While this is not directly related to the main part of the thesis, it is a report on a relevant part of the work I did as a Ph.D. student at PUC. We will simply state the results and describe the techniques; a detailed exposition of the proofs can be found in [16].

We thank Fabien Pazuki for suggesting to include this section.

A.1 The Chabauty-Coleman bound

Let C be a smooth, geometrically irreducible, projective curve of genus $g \geq 2$ defined over a number field F, with Jacobian J. In the direction of Mordell's conjecture, Chabauty [18] proved in 1941 that if $\operatorname{rank} J(F) \leq g-1$, then the set $C(F)$ of F-rational points of C is finite. Let us recall the main ideas for $F = \mathbb{Q}$: After embedding C into J, one has $C(\mathbb{Q}) \subseteq C(\mathbb{Q}_p) \cap \Gamma$ where p is an auxiliary prime and Γ is the p-adic closure of $J(\mathbb{Q})$ in $J(\mathbb{Q}_p)$. Then $\dim \Gamma \leq \operatorname{rank} J(\mathbb{Q}) < g = \dim J(\mathbb{Q}_p)$ which leads to the finiteness of $C(\mathbb{Q}_p) \cap \Gamma$ because $C(\mathbb{Q}_p)$ is not contained in a lower dimensional p-adic analytic subgroup of $J(\mathbb{Q}_p)$.

Coleman [21] proved in 1985 a celebrated explicit version of Chabauty's theorem, which we recall over $\mathbb{Q}$: with the same conditions, if $p > 2g$ is a prime of good reduction for C, then

$$\#C(\mathbb{Q}) \leq \#C'(\mathbb{F}_p) + 2g - 2 \tag{A.1}$$

where C' is the reduction of C modulo p. While Chabauty's finiteness result was superseded by Faltings's proof of Mordell's conjecture [35], the method of Chabauty and Coleman has

led to a number of striking developments: explicit determination of the rational points on suitable curves (see [59] for an introduction and references), improvements on (A.1) such as [50, 58, 59, 81], progress towards the Caporaso–Harris–Mazur conjecture [51, 82], and explicit versions of Kim's non-abelian approach [54] such as [5–9, 32].

A.2 Beyond curves

Despite all these remarkable developments over the last few decades, the problem of proving a version of (A.1) for the rational points of a higher dimensional variety X contained in an abelian variety A has remained out of reach. Our main results provide such an extension of (A.1) when X is a hyperbolic surface contained in an abelian variety A of dimension $n \geq 3$, both defined over a number field F, under the assumption $\operatorname{rank} A(F) \leq 1$. Although we work over number fields (see Sections 9 and 10 [16]), let us keep the discussion over $\mathbb{Q}$ in this introduction to simplify the exposition. Our results, when applicable, will imply

$$\#X(\mathbb{Q}) \leq \#X'(\mathbb{F}_p) + 4p \cdot c_1^2(X) \tag{A.2}$$

where $c_1^2(X)$ is the first Chern number of the surface X (the self-intersection of a canonical divisor), p is a prime of good reduction satisfying some technical assumptions, and X' is the reduction of X modulo p. The coefficient $4p$ in (A.2) is in fact a simplification of a slightly more complicated expression that gives a better estimate. See Theorem A.3.1 and Remark A.3.3.

We observe that Coleman's bound (A.1) can be written as

$$\#C(\mathbb{Q}) \leq \#C'(\mathbb{F}_p) + c_1(C)$$

where $c_1(C) = 2g - 2$ is the first Chern number of C, i.e. the degree of a canonical divisor. Also, we recall that hyperbolic projective curves are precisely those of genus $g \geq 2$. We hope that these remarks clarify the analogy between our results for surfaces and Coleman's bound for curves.

Although the *shape* of our bound (A.2) is analogous to (A.1), the methods of proof are quite different. Let X be a subvariety of an abelian variety A over $\mathbb{Q}$. Let Γ be the p-adic closure of the group $A(\mathbb{Q})$ in $A(\mathbb{Q}_p)$. Then $X(\mathbb{Q})$ is contained in $\Gamma \cap X(\mathbb{Q}_p)$ and one tries to bound the latter.

In the case of curves ($X = C$ embedded in $A = J$) Coleman used his theory of p-adic integration to construct p-adic analytic functions on $C(\mathbb{Q}_p)$ that vanish on $C(\mathbb{Q}_p) \cap \Gamma$ and then he bounded the number of zeros of the relevant one-variable p-adic power series on residue disks.

On the other hand, when $d = \dim X > 1$, the analogous approach using p-adic analytic functions on $X(\mathbb{Q}_p)$ quickly encounters difficulties. Such functions are locally given by

power series in d variables. To get finiteness of $\Gamma \cap X(\mathbb{Q}_p)$ one needs to consider at least d different p-adic analytic functions on $X(\mathbb{Q}_p)$ whose zero sets (usually, p-adic analytic sets of dimension $d-1$) meet properly, and then there is the problem of giving an upper bound for the number of common zeros. So far, this approach has not succeeded in proving a version of (A.1) other than in the case of curves.

We take a different route instead. When $\operatorname{rank} A(\mathbb{Q}) = 1$ we can give a p-adic analytic parametrization of Γ by power series in one variable. Upon composing with suitably chosen local equations for the surface X in A and working on residue disks, the problem of bounding $\#\Gamma \cap X(\mathbb{Q}_p)$ is reduced to bounding the number of zeros of a certain power series $h(z) = \sum_j c_j z^j \in \mathbb{Q}_p[[z]]$ on a disk. The key difficulty in doing so (and in the whole approach) it so prove the existence of a small N such that $|c_N| \geq 1$. We achieve this by developing a method based on overdetermined ω-integrality, which in our case is essentially a study of overdetermined systems of differential equations in positive characteristic.

Prior to our work, the efforts on extending (A.1) to the higher dimensional setting have focused on the special case when $A = J$ is the Jacobian of a curve C and $X = W_d$ is the image in J of the d-th symmetric power of C via the addition map. Klassen [55] obtained some partial results for the varieties W_d, later improved by Siksek [77]. Although Siksek's work does not give an explicit bound for $\#W_d(\mathbb{Q})$ such as (A.1), it gives a practical method that in many cases computes the set of rational points of W_d. Park [68] used tropical geometry to obtain a weak analogue of (A.1) for W_d (at least if $\operatorname{rank} J(\mathbb{Q}) \leq 1$), but the result turns out to be conditional on an unproved technical assumption as explained in [47]. Uniform extensions of Park's result are studied in [88] for W_2, but these are also conditional due to the same issue discussed in [47].

A.3 Results

As usual, K_X denotes a canonical divisor of a smooth projective variety X. We recall that X is said to be of general type if K_X is big. For every field F, we choose an algebraic closure and denote it by F^{alg}. The following Theorem is also proved over any number field; see Theorem 9.1 in *loc. cit.*

Theorem A.3.1 (Main result, case over $\mathbb{Q}_p$)**.** *Let p be a prime. Let X be a smooth, geometrically irreducible, projective surface contained in an abelian variety A of dimension $n \geq 3$, both defined over $\mathbb{Q}_p$ and having good reduction. Let X' and A' be the corresponding reductions modulo p. Let $G \leq A(\mathbb{Q}_p)$ be a finitely generated group with $\operatorname{rank} G \leq 1$ and let Γ be its p-adic closure in $A(\mathbb{Q}_p)$. Suppose that either of the following conditions holds:*

(i) We have $n = 3$, X is of general type, X' contains no elliptic curves over $\mathbb{F}_p^{\mathrm{alg}}$, and $p > (128/9)c_1^2(X)^2$;

(ii) The abelian variety A' is simple over $\mathbb{F}_p^{\mathrm{alg}}$, $p > 3c_1^2(X) + 2$, and there is an ample divisor H on A such that

$$p > \frac{n! \cdot (3\deg(H^2.X) + \deg(H.K_X))^n}{n^n \cdot \deg(H^n)}.$$

Then $X(\mathbb{Q}_p) \cap \Gamma$ is finite and we have

$$\#X(\mathbb{Q}_p) \cap \Gamma \leq \#X'(\mathbb{F}_p) + \frac{p-1}{p-2} \cdot \left(p + 4p^{1/2} + 3\right) \cdot c_1^2(X). \tag{A.3}$$

Remark A.3.2. By the Riemann Hypothesis for surfaces over finite fields [26] we have the estimate $|\#X'(\mathbb{F}_p) - (p^2+1)| \leq b_3 p^{3/2} + b_2 p + b_1 p^{1/2}$ where b_j is the j-th Betti number of $X(\mathbb{C})$. In particular, one can use $\#X'(\mathbb{F}_p) \leq p^2 + b_3 p^{3/2} + b_2 p + b_1 p^{1/2} + 1$ in (A.3) to get a more uniform bound.

Remark A.3.3. When Theorem A.3.1 applies, $p \geq 7$ and (A.3) implies $\#X(\mathbb{Q}_p) \cap \Gamma < \#X'(\mathbb{F}_p) + 4p \cdot c_1^2(X)$. Also, Remark A.3.2 shows that $\#X'(\mathbb{F}_p)$ is roughly of size p^2, say, for large p and fixed Betti numbers of X. In this way, $\#X'(\mathbb{F}_p)$ can be seen as the main term in the upper bound (A.3).

The following two results on rational points of surfaces are deduced from Theorem A.3.1 by base change to $\mathbb{Q}_p$ and choosing G as the group of $\mathbb{Q}$-rational points of the corresponding abelian variety. We also obtain similar results over any number field, not just $\mathbb{Q}$; see Section 10.1 in *loc. cit.*

Theorem A.3.4. *Let X be a smooth, geometrically irreducible, projective surface of general type contained in an abelian threefold A, both defined over $\mathbb{Q}$. Let $p > (128/9) \cdot c_1^2(X)^2$ be a prime of good reduction for X and A, and let X' be the reduction of X modulo p. If $\operatorname{rank} A(\mathbb{Q}) \leq 1$ and X' contains no elliptic curves over $\mathbb{F}_p^{\mathrm{alg}}$, then $X(\mathbb{Q})$ is finite and*

$$\#X(\mathbb{Q}) \leq \#X'(\mathbb{F}_p) + \frac{p-1}{p-2} \cdot \left(p + 4p^{1/2} + 3\right) \cdot c_1^2(X).$$

Remark A.3.5. A compact complex manifold M is *hyperbolic* if every holomorphic map $f\colon \mathbb{C} \to M$ is constant. If a complex projective surface is hyperbolic, then it is of general type. So, in Theorem A.3.4 we may require that $X(\mathbb{C})$ be hyperbolic instead of requiring general type —depending on the application, this might be easier to check. In fact, there is no loss of generality in doing so: under the assumptions of Theorem A.3.4, the surface X contains no elliptic curves over $\mathbb{Q}^{\mathrm{alg}}$, hence, over $\mathbb{C}$ (by specialization). Furthermore, X is not an abelian surface because it is of general type. Since $X \subseteq A$, a result of Green (Theorem 1 in [44]) implies that $X(\mathbb{C})$ is hyperbolic.

Theorem A.3.6. *Let X be a smooth, geometrically irreducible, projective surface contained in an abelian variety A of dimension $n \geq 3$, both defined over $\mathbb{Q}$. Let H be an ample divisor on A and let p be a prime of good reduction for X and A satisfying*

$$p > \max\left\{3c_1^2(X) + 2, \frac{n! \cdot (3\deg(H^2.X) + \deg(H.K_X))^n}{n^n \cdot \deg(H^n)}\right\}.$$

Let X' and A' be the corresponding reductions modulo p of X and A. If $\operatorname{rank} A(\mathbb{Q}) \leq 1$ and A' is simple over $\mathbb{F}_p^{\mathrm{alg}}$, then $X(\mathbb{Q})$ is finite and

$$\#X(\mathbb{Q}) \leq \#X'(\mathbb{F}_p) + \frac{p-1}{p-2} \cdot \left(p + 4p^{1/2} + 3\right) \cdot c_1^2(X).$$

Remark A.3.7. Since A' is geometrically simple, so is A. Thus, $X(\mathbb{C})$ is hyperbolic by Theorem 1 in [44] as it was in Theorem A.3.4 (see Remark A.3.5). Deep conjectures by Bombieri and Lang predict that if V is a smooth projective variety over $\mathbb{Q}$ such that $V(\mathbb{C})$ is hyperbolic, then $V(\mathbb{Q})$ is finite. For curves this is Faltings's theorem since hyperbolic projective curves are precisely those of genus $g \geq 2$. When V is contained in an abelian variety and $V(\mathbb{C})$ is hyperbolic, finiteness of $V(\mathbb{Q})$ was proved by Faltings [36] extending methods of Vojta [89]. Hence, hyperbolicity of $X(\mathbb{C})$ is natural in our context.

Remark A.3.8. It is expected that the rank of abelian varieties over $\mathbb{Q}$ of a fixed positive dimension is 0 or 1 a positive proportion of the time each —ordering the abelian varieties, for instance, by (Faltings or Theta) height— and this is proved for elliptic curves [10, 11]. Thus, one can expect that the rank assumption in Theorems A.3.4 and A.3.6 is often satisfied in examples.

Remark A.3.9. For a variety X contained in an abelian variety A over $\mathbb{Q}$, heuristically, one sees that the limit of applicability of an analogue of Chabauty's classical approach should be $\dim X + \dim \Gamma \leq \dim A$ where Γ is the p-adic closure of $A(\mathbb{Q})$ in $A(\mathbb{Q}_p)$. In our results in the case $\dim A = 3$, this limit rank condition is in fact reached.

A simple case where our results are applicable is given by the following.

Corollary A.3.10. *Let A be an abelian threefold over $\mathbb{Q}$ with $\operatorname{rank} A(\mathbb{Q}) \leq 1$ and $\operatorname{End}(A_{\mathbb{C}}) = \mathbb{Z}$. There is a set of primes $\mathcal{P}$ of density 1 in the primes such that the following holds:*

Let X be a smooth, geometrically irreducible, projective surface defined over $\mathbb{Q}$ and contained in A, and let $p \in \mathcal{P}$ be a prime of good reduction for X with $p > (128/9) \cdot c_1^2(X)^2$. Let X' be the reduction of X modulo p. Then

$$\#X(\mathbb{Q}) \leq \#X'(\mathbb{F}_p) + \frac{p-1}{p-2} \cdot \left(p + 4p^{1/2} + 3\right) \cdot c_1^2(X).$$

This is deduced from Theorem A.3.4 and results of Chavdarov [19] on absolutely simple reduction of abelian varieties. Chavdarov's results together with Theorem A.3.6 imply analogous corollaries when $\dim A \geq 3$ is odd.

Remark A.3.11. Given $n \geq 1$, a general abelian variety B over $\mathbb{C}$ of dimension n satisfies $\mathrm{End}(B) \simeq \mathbb{Z}$. In view of Remark A.3.8, abelian threefolds satisfying the conditions in Corollary A.3.10 should be rather common. And in fact, they are easy to find; the Jacobian of the genus 3 hyperelliptic curve $y^2 = x^7 - x - 1$ is such an example with Mordell–Weil rank 1.

Remark A.3.12. For any abelian threefold as in Corollary A.3.10, our bounds for the number of rational points apply to *any* smooth surface contained in A, e.g. by embedding A in a projective space and intersecting with a general hyperplane (by Bertini's theorem). This gives plenty of examples.

For a curve C over a field, we let $C^{(n)}$ be its n-th symmetric power. If C is defined over $\mathbb{Q}$, the $\mathbb{Q}$-rational points of $C^{(2)}$ are in bijection with Galois orbits of quadratic points and unordered pairs of $\mathbb{Q}$-rational points. If C is a hyperelliptic curve over $\mathbb{Q}$, then we certainly have that $C^{(2)}(\mathbb{Q})$ is infinite. As a direct application of our results, we can bound $\#C^{(2)}(\mathbb{Q})$ for non-hyperelliptic curves whose Jacobian has rank 0 or 1, under some conditions on the reduction type at p.

Corollary A.3.13. *Let C be a smooth, geometrically irreducible, projective curve over $\mathbb{Q}$ of genus $g \geq 3$ which is not hyperelliptic over $\mathbb{Q}^{\mathrm{alg}}$ and such that its Jacobian J has $\mathrm{rank}\, J(\mathbb{Q}) \leq 1$. Let $p > (8g-10)^g$ be a prime of good reduction for C. Let C' and J' denote the reduction of C and J modulo p respectively. Suppose that C' is not hyperelliptic over $\mathbb{F}_p^{\mathrm{alg}}$ and that J' is geometrically simple. Then $C^{(2)}(\mathbb{Q})$ is finite and*

$$\#C^{(2)}(\mathbb{Q}) \leq \#(C')^{(2)}(\mathbb{F}_p) + \frac{p-1}{p-2} \cdot \left(p + 4p^{1/2} + 3\right) \cdot (4g-9)(g-1).$$

This is directly obtained from Theorem A.3.6 after some computations in intersection theory. Regarding the hyperelliptic case, let us remark that one can get a bound for the number of "unexpected" quadratic points by applying our results to the image of $C^{(2)}$ in the Jacobian of C (this observation was pointed out to us by one of the referees.)

In a similar fashion, we will prove the following strengthening of Corollary A.3.13 for curves of genus 3, by applying Theorem A.3.4 instead.

Corollary A.3.14. *Let C be a smooth, geometrically irreducible, projective curve over $\mathbb{Q}$ of genus 3 which is not hyperelliptic over $\mathbb{Q}^{\mathrm{alg}}$ and such that its Jacobian J has $\mathrm{rank}\, J(\mathbb{Q}) \leq 1$. Let $p \geq 521$ be a prime of good reduction for C and denote by C' the reduction of C modulo p. Suppose that C' is not hyperelliptic over $\mathbb{F}_p^{\mathrm{alg}}$ and that $(C')^{(2)}$ does not contain elliptic curves over $\mathbb{F}_p^{\mathrm{alg}}$. Then $C^{(2)}(\mathbb{Q})$ is finite and*

$$\#C^{(2)}(\mathbb{Q}) \leq \#(C')^{(2)}(\mathbb{F}_p) + 6 \cdot \frac{p-1}{p-2} \cdot \left(p + 4p^{1/2} + 3\right) < \#(C')^{(2)}(\mathbb{F}_p) + 7.1 \cdot p.$$

Finally, we mention that the finiteness aspect of Theorem A.3.1 (and more generally, Theorem 1.2.1) does not follow from Faltings's theorem for subvarieties of abelian varieties [36], as Γ is not a finite rank group when $\operatorname{rank} G = 1$. Regarding bounds for the number of rational points, the Diophantine approximation methods of Vojta [89] and Faltings [36, 37] led to explicit bounds such as [70, 71] for subvarieties of abelian varieties over number fields, outside the special set. However, as it is the case for the classical Chabauty–Coleman method on curves compared to Diophantine approximation bounds, our p-adic approach for surfaces leads to sharper estimates when it applies.

A.4 Sketch of the method: overdetermined ω-integrality

To simplify the notation, let us focus on the case $\dim A = 3$ since the key features already appear here. Furthermore, enlarging G we may assume that $\operatorname{rank} G = 1$.

First we note that, at least heuristically, the Chabauty–Coleman p-adic approach has a chance to succeed since $\dim X + \dim \Gamma = 2 + 1 = \dim A$.

Consider the reduction map $\mathrm{red}\colon A(\mathbb{Q}_p) \to A'(\mathbb{F}_p)$ and for each $x \in A'(\mathbb{F}_p)$ let $U_x = \mathrm{red}^{-1}(x) \subseteq A(\mathbb{Q}_p)$ be the corresponding residue disk. We want to bound $\#\Gamma \cap X(\mathbb{Q}_p) \cap U_x$ and then add these upper bounds as x varies in $X'(\mathbb{F}_p)$. Let us parametrize $\Gamma \cap U_x$ by a p-adic analytic map $\gamma\colon p\mathbb{Z}_p \to U_x \subseteq A(\mathbb{Q}_p)$. If f is a local equation for X in U_x, then $\#\Gamma \cap X(\mathbb{Q}_p) \cap U_x$ is the number of zeros of the one-variable p-adic analytic function $h = f \circ \gamma$ on $p\mathbb{Z}_p$. We remark that the idea of parametrizing Γ can be traced back to work of Flynn [38] and it has been successful in computing the rational points of curves in particular examples, although it has not previously led to general bounds such as (A.1).

Writing $h(z) = c_1 z + c_2 z^2 + \ldots \in \mathbb{Q}_p[[z]]$, the number of zeros can be estimated *provided* that we have some information on the size of the coefficients c_j. Namely, we need:

(I) a good upper bound for $|c_j|$ for all j, and

(II) some small N such that $|c_N|$ is not too small, say, $|c_N| \geq 1$.

To achieve (I) we perform the construction of the p-adic analytic map γ very carefully. We develop a completely explicit theory of 1-parameter p-adic analytic subgroups and, with some care in the choice of the local equation f, this allows us to prove the desired upper bound. The key difficulty in the whole argument, however, is (II). We take a somewhat indirect approach.

Consider the morphism of p-adic analytic groups $\mathrm{Log}\colon A(\mathbb{Q}_p) \to \mathrm{Lie}(A(\mathbb{Q}_p)) \simeq H^0(A, \Omega^1_{A/\mathbb{Q}_p})^\vee$ constructed by Coleman integration or by classical theory of p-adic Lie groups. As $\operatorname{rank} G = 1$, $\mathrm{Log}(\Gamma)$ is contained in a line of $\mathrm{Lie}(A(\mathbb{Q}_p))$ which determines a hyperplane $\mathcal{H} \subseteq H^0(A, \Omega^1_{A/\mathbb{Q}_p})$. We choose $\omega_1, \omega_2 \in \mathcal{H}$ so that they reduce to independent differentials ω_1', ω_2' on A', which we restrict to differentials u_1, u_2 on X'. For

$x \in X'(\mathbb{F}_p)$ let $m(x)$ be the supremum of all integers m such that there is a closed immersion $\phi_m \colon \operatorname{Spec} \mathbb{F}_p^{\mathrm{alg}}[z]/(z^{m+1}) \to X'$ supported at x which is ω-integral for both $\omega = u_1, u_2$. Roughly speaking, ω-integrality for a differential ω means that the morphism ϕ_m solves the differential equation determined by ω.

If u_1 and u_2 are independent over the function field of X', then the maps ϕ_m in the definition of $m(x)$ are jet solutions to an *overdetermined system of differential equations*. So, one expects $m(x)$ to be finite and bounded in terms of u_1 and u_2. This is indeed correct, but it is far from obvious. Theorem 4.4 in *loc. cit.* gives such a bound in terms of the geometry of the divisor D of the 2-form $u_1 \wedge u_2$.

Bounding $m(x)$ turns out to be crucial, since we show in Lemma 9.16 in *loc. cit.* that $N \leq m(x) + 1$ with N as in (II). Together with the zero estimates and our upper bounds for $|c_j|$ (see (I) above) we obtain the following key estimate:

$$\#\Gamma \cap X(\mathbb{Q}_p) \cap U_x \leq 1 + m(x) \cdot \frac{p-1}{p-2}. \tag{A.4}$$

Finally, the geometric bound for $m(x)$ is applied to (A.4), and then added over $x \in X'(\mathbb{F}_p)$. When x is not in the support of $D = \operatorname{div}(u_1 \wedge u_2)$ we show $m(x) = 0$, thus, $\#\Gamma \cap X(\mathbb{Q}_p) \cap U_x \leq 1$. The contribution for x in the support of D is more complicated and it corresponds to counting $\mathbb{F}_p$-points in the support of D with suitable weights. The divisor D can be non-reduced and highly singular, so this counting problem does not directly follow from Weil's estimates for points in curves over finite fields. We address this problem by studying certain modified Zeta functions (see Section 3.5 in *loc. cit.*), which allows us to conclude the argument.

We make heavy use of ω-integrality for schemes over rings or over fields of positive characteristic. Thus, classical analytic considerations on ω-integrality are not enough, and we need purely algebraic methods. Fortunately such a study was carried out by Garcia-Fritz [40–42] over $\mathbb{C}$ in the context of her generalization of Vojta's explicit version of Bogomolov's approach to quasi-hyperbolicity, see [28, 90]. These algebraic methods easily extend to an arbitrary base.

There is a major technical difficulty which is not present in previous works around the Chabauty–Coleman method. Namely, at various points of the argument we need to restrict differential forms to subvarieties of abelian varieties in a way that preserves non-triviality. For example, while ω_1' and ω_2' are independent on A', is is not clear whether $u_1 \wedge u_2$ is not the zero form on X', and this is necessary even to define the divisor $D = \operatorname{div}(u_1 \wedge u_2)$. Part of the difficulties are due to the fact that X does not have a particularly convenient presentation that allows for explicit computations with differentials, unlike the case of symmetric powers of curves. The required non-vanishing results for restriction of forms are not difficult to obtain in characteristic zero by analytic means, but we need them in positive characteristic. This is achieved in Section 5 in *loc. cit.* by means of intersection theory.

Bibliography

[1] Abbes, A., & Ullmo, E. (1996). *A propos de la conjecture de Manin pour les courbes elliptiques modulaires*. Compositio Mathematica, 103(3), 269-286.

[2] Agashe, A., Ribet, K. A., & Stein, W. A. (2012). *The modular degree, congruence primes, and multiplicity one*. In Number theory, analysis and geometry (pp. 19-49). Springer, Boston, MA.

[3] Aguirre, J., Lozano-Robledo, Á., & Peral, J. C. (2008). *Elliptic curves of maximal rank*. In Proceedings of the Segunda Jornada de Teoría de Números (pp. 1-28).

[4] Atkin, A., & Lehner, J. (1970). *Hecke operators on* $\Gamma_0(m)$. Mathematische Annalen, 185(2), 134-160.

[5] Balakrishnan, J., Besser, A. & Müller, J. (2017). *Computing integral points on hyperelliptic curves using quadratic Chabauty*. Mathematics of Computation, 86(305) 1403-1434.

[6] Balakrishnan, J. & Dogra, N. (2018). *Quadratic Chabauty and rational points, I:* p*-adic heights*. Duke Math. J. 167(11), 1981-2038.

[7] Balakrishnan, J. & Dogra, N. (2019). *An effective Chabauty-Kim theorem*. Compositio Math. 155, 1057-1075.

[8] Balakrishnan, J. & Dogra, N. (2020). *Quadratic Chabauty and rational points II: Generalised height functions on Selmer varieties*. Int. Math. Res. Not. doi:10.1093/imrn/rnz362

[9] Balakrishnan, J., Dogra, N., Müller, J., Tuitman, J. & Vonk, J. (2019). *Explicit Chabauty–Kim for the split Cartan modular curve of level 13*. Ann. Math., 189(3), 885-944.

[10] Bhargava, M. & Shankar, A. (2015). *Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0*. Ann. Math., 181, 587-621.

[11] Bhargava, M. & Skinner, C. (2014). *A positive proportion of elliptic curves over Q have rank one*. Journal of the Ramanujan Mathematical Society, 29(2), 221-242.

[12] Breuil, C. Conrad, B., Diamond, F. & Taylor, R. (2001). *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*. Journal of the American Mathematical Society, pages 843-939.

[13] Calegari, F. & Emerton, M. (2009). *Elliptic curves of odd modular degree*. Israel Journal of Mathematics, 169(1):417-444.

[14] Caro, J. (2022). *Watkins's conjecture for elliptic curves over function fields.* arXiv preprint arXiv:2203.10932.

[15] Caro, J. (2022). *Watkins's conjecture for quadratic twists of Elliptic Curves with Prime Power Conductor.* arXiv preprint arXiv:2206.10008.

[16] Caro, J. & Pasten, H. (2021). *A Chabauty-Coleman bound for surfaces.* arXiv preprint arXiv:2102.01055.

[17] Caro, J., & Pasten, H. (2022). *Watkins's conjecture for elliptic curves with non-split multiplicative reduction*. Proceedings of the American Mathematical Society. Volume 150, Number 8, August 2022, Pages 3245-3251.

[18] Chabauty C., (1941). *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*. C. R. Acad. Sci. Paris 212, 882-885.

[19] Chavdarov, N. (1997). *The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy*. Duke Math. J. 87, no. 1, 151-180.

[20] Cojocaru, A., & Kani, E. (2004). *The modular degree and the congruence number of a weight 2 cusp form.* Acta Arithmetica-Warszawa-., 114, 159-167.

[21] Coleman, R. (1985). *Effective Chabauty*. Duke Math. J. 52, no. 3, 765-770.

[22] Connell, I. (1999). *Elliptic curve handbook*. McGill University.

[23] Conrad, B., Conrad, K. & Helfgott, H. (2005). *Root numbers and ranks in positive characteristic.* Advances in Mathematics, 198(2): 684–731.

[24] Cremona, J., & Pacetti, A. (2019). *On elliptic curves of prime power conductor over imaginary quadratic fields with class number 1.* Proceedings of the London Mathematical Society, 118(5), 1245-1276.

[25] Delaunay, C. (2003). *Computing modular degrees using L-functions*. Journal de théorie des nombres de Bordeaux, 15(3), 673-682.

[26] Deligne, P. (1974). *La conjecture de Weil: I*. Publications Mathématiques de l'IHÉS. 43: 273-307.

[27] Deligne, P. (1973). *Les constantes des éqations fonctionnelles des fonctions L*, 501–597. Lecture Notes in Math., Vol. 349.

[28] Deschamps, M. (1978). *Courbes de genre géométrique borné sur une surface de type général (d'après F. A. Bogomolov)*. Séminaire Bourbaki 30e année, 1977/78, Lecture Notes in Mathematics 710, Springer, No. 519.

[29] Drinfel'd, V. G. (1974). *Elliptic modules.* Mathematics of the USSR-Sbornik, 23(4), 561.

[30] Dummigan, N. (2006). *On a conjecture of Watkins.* J. Théor. Nombres Bordeaux 18, no. 2, 345-355.

[31] Dummigan, N. & Krishnamoorthy, S. (2013). *Powers of 2 in modular degrees of modular abelian varieties*. Journal of Number Theory, 133(2):501–522.

[32] Edixhoven, B. & Lido, G. (2019). *Geometric quadratic Chabauty*. Preprint, v3 in arXiv: 1910.10752.

[33] Edixhoven, B. (1991). *On the Manin constants of modular elliptic curves*. In Arithmetic algebraic geometry (pp. 25-39). Birkhäuser, Boston, MA.

[34] Esparza-Lozano, J. & Pasten, H. (2021). *A conjecture of Watkins for quadratic twists.* Proceedings of the American Mathematical Society, 149(6): 2381–2385.

[35] Faltings, G. (1983). *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*. (German) [Finiteness theorems for abelian varieties over number fields] Invent. Math. 73, no. 3, 349-366.

[36] Faltings, G. (1991). *Diophantine approximation on abelian varieties*. Ann. Math., 133, 549-576.

[37] Faltings, G. (1994). *The general case of S. Lang's conjecture*. Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991). Perspect. Math. 15. Academic Press. San Diego, p. 175-182

[38] Flynn, E. (1997). *A flexible method for applying Chabauty's theorem*. Compositio Math. 105, no. 1, 79-94.

[39] Frey, G. (1989). *Links between solutions of $A-B=C$ and elliptic curves*. In Number theory (pp. 31-62). Springer, Berlin, Heidelberg.

[40] Garcia-Fritz, N. (2015). *Curves of low genus on surfaces and applications to Diophantine problems*. PhD Thesis, Queen's University.

[41] Garcia-Fritz, N. (2018). *Sequences of powers with second differences equal to two and hyperbolicity*. Trans. Am. Math. Soc. 370(5), 3441-3466.

[42] Garcia-Fritz, N. (2018). *Quadratic sequences of powers and Mohanty's conjecture*. International Journal of Number Theory 14.02, 479-507.

[43] Gekeler, E. & Reversat, A. (1996). *Jacobians of Drinfeld Modular Curves* J.Reine Angew. Math. 476, 27-93.

[44] Green, M. (1978). *Holomorphic Maps to Complex Tori*. American Journal of Mathematics, 100(3), 615-620.

[45] Griffon, R. (2018). *A new family of elliptic curves with unbounded rank.* Moscow Mathematical Journal, Volume 20, Issue 2, pp. 343-374.

[46] Grothendieck, A. (1964) *Formule de Lefschetz et rationalité des fonctions L,* Sém. Bourbaki 279.

[47] Gunther, J. & Morrow, J. (2017). *Irrational points on random hyperelliptic curves*. Preprint, v3 in arXiv:1709.02041

[48] Hadano, T. (1975). *Conductor of elliptic curves with complex multiplication and elliptic curves of prime conductor*. Proceedings of the Japan Academy, 51(2), 92-95.

[49] Husemoller, D. (2004). *Elliptic curves*. Second edition. With appendices by Otto Forster, Ruth Lawrence and Stefan Theisen. Graduate Texts in Mathematics, 111. Springer-Verlag, New York, xxii+487 pp.

[50] Katz, E. & Zureick-Brown, D. (2013). *The Chabauty-Coleman bound at a prime of bad reduction and Clifford bounds for geometric rank functions*. Compos. Math. 149, no. 11, 1818-1838.

[51] Katz, E., Rabinoff, J. & Zureick-Brown, D. (2016). *Uniform bounds for the number of rational points on curves of small Mordell-Weil rank*. Duke Math. J., 165(16), 3189-3240.

[52] Kazalicki, M., & Kohen, D. (2018). *On a special case of Watkins' conjecture*. Proceedings of the American Mathematical Society, 146(2), 541-545.

[53] Kazalicki, M., & Kohen, D. Corrigendum (2019). *On a special case of Watkins' conjecture*. Proceedings of the American Mathematical Society, 147(10):4563-4563.

[54] Kim, M. (2005). *The motivic fundamental group of* $\mathbf{P}^1 \setminus \{0, 1, \infty\}$ *and the theorem of Siegel*. Inventiones Mathematicae, 161, 629-656.

[55] Klassen, M. (1993). *Algebraic points of low degree on curves of low rank*. Thesis, University of Arizona.

[56] Koblitz, N. I. (2012). *Introduction to elliptic curves and modular forms* (Vol. 97). Springer Science & Business Media.

[57] LMFDB Collaboration. (2021). *L-functions and modular forms database*. `www.lmfdb.org`.

[58] Lorenzini, D. & Tucker, T. (2002). *Thue equations and the method of Chabauty-Coleman*. Invent. Math. 148, 47-77.

[59] McCallum, W. & Poonen, B. (2012). *The method of Chabauty and Coleman*. Explicit methods in number theory; rational points and diophantine equations, Panoramas et Synthèses 36, Société Math. de France, 99-117.

[60] Mazur, B., & Goldfeld, D. (1978). *Rational isogenies of prime degree*. Inventiones mathematicae, 44(2), 129-162.

[61] Mestre, J. F., & Oesterlé, J. (1989). *Courbes de Weil semi-stables de discriminant une puissance m-ième*. Journal für die reine und angewandte Mathematik (Crelles Journal), 1989(400), 173-184.

[62] Monsky, P. (1996). *Generalizing the Birch-Stephens theorem. I. Modular curves.* Math. Z. 221, no. 3, 415-420.

[63] Mulholland, J. T. (2006). *Elliptic curves with rational* 2*-torsion and related ternary Diophantine equations* (Vol. 67, No. 12).

[64] Murty, R. (1999). *Bounds for congruence primes*. Automorphic forms, automorphic representations, and arithmetic (Fort Worth, TX, 1996), 177-192, Proc. Sympos. Pure Math., 66, Part 1, Amer. Math. Soc., Providence, RI.

[65] Pál, A. (2010). *The Manin constant of elliptic curves over function fields.* Algebra & Number Theory, 4(5), 509-545.

[66] Pal, V. (2012). *Periods of quadratic twists of elliptic curves*. Proceedings of the American Mathematical Society, 140(5), 1513-1525.

[67] Papikian, M. (2002). *On the degree of modular parametrizations over function fields.* Journal of Number Theory, 97(2): 317–349.

[68] Park, J. (2016). *Effective Chabauty for symmetric powers of curves*. Preprint, v1 in arXiv:1504.05544

[69] Prasolov, V. V. (2004). *Polynomials* (Vol. 11). Springer Science & Business Media.

[70] Rémond, G. (2000). *Décompte dans une conjecture de Lang.* Inventiones Mathematicae, 142 (3), 513-545.

[71] Rémond, G. (2002). *Sur les sous-variétés des tores*. Compositio Mathematica 134.3, 337-366.

[72] Roberts, D. (2007). *Explicit decent on elliptic curves over function fields.* PhD thesis, University of Nottingham.

[73] Schaefer, E. & Stoll, M. (2004). *How to do p-descent on an elliptic curve.* Transactions of the American Mathematical Society, 356(3): 1209–1231.

[74] Schweizer, A. (1998). *Involutory elliptic curves over $\mathbb{F}_q(T)$*. Journal de théorie des nombres de Bordeaux, 10(1), 107-123

[75] Setzer, B. (1975). *Elliptic curves of prime conductor*. Journal of the London Mathematical Society, 2(3), 367-378.

[76] Shioda, T. (1992). *Some remarks on elliptic curves over function fields*. Astérisque, 209(12):99–114.

[77] Siksek, S. (2009). *Chabauty for symmetric powers of curves*. Algebra & Number Theory, 3(2), 209-236.

[78] Silverman, J. H. (2009). *The arithmetic of elliptic curves* volume 106. Springer Science & Business Media.

[79] Silverman, J. & Tate, J. (2015). *Rational points on elliptic curves*. Second edition. Undergraduate Texts in Mathematics. Springer, Cham. xxii+332 pp. ISBN: 978-3-319-18587-3; 978-3-319-18588-0.

[80] Stein, W. & Watkins, M. (2004). *Modular parametrizations of Neumann-Setzer elliptic curves*. International Mathematics Research Notices, 2004(27), 1395-1405.

[81] Stoll, M. (2006). *Independence of rational points on twists of a given curve*. Compositio Math. 142, 1201-1214

[82] Stoll, M. (2019). *Uniform bounds for the number of rational points on hyperelliptic curves of small Mordell-Weil rank*. Journal of the European Mathematical Society, 21(3), 923-956.

[83] Tate, J. (1965). *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*. Séminaire Bourbaki, 9(306), 415-440.

[84] Tate, J., & Shafarevich, I. R. (1967). *The rank of elliptic curves.* In Doklady Akademii Nauk (Vol. 175, No. 4, pp. 770-773). Russian Academy of Sciences.

[85] Taylor, R., & Wiles, A. (1995). *Ring-theoretic properties of certain Hecke algebras*. Annals of Mathematics, 141(3), 553-572.

[86] Ulmer, D. (2002). *Elliptic curves with large rank over function fields*. Annals of Mathematics, pages 295–315.

[87] Ulmer, D. (2011). *Park City lectures on elliptic curves over function fields.* Preprint, v1 in arXiv:1101.1939.

[88] Vemulapalli, S. & Wang, D. (2017). *Uniform bounds for the number of rational points on symmetric squares of curves with low Mordell-Weil rank*. Preprint, v3 in arXiv:1708.07057

[89] Vojta, P. (1991). *Siegel's theorem in the compact case*. Annals of Mathematics, 133(3), 509-548.

[90] Vojta, P. (2000). *Diagonal quadratic forms and Hilbert's tenth problem*. Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999), 261-274, Contemp. Math., 270, Amer. Math. Soc., Providence, RI.

[91] Watkins, M. (2002). *Computing the modular degree of an elliptic curve*. Experimental Mathematics, 11(4), 487-502.

[92] Wiles, A. (1995). *Modular elliptic curves and Fermat's last theorem*. Annals of mathematics, 141(3), 443-551.

[93] Yazdani, S. (2011). *Modular abelian varieties of odd modular degree*. Algebra & Number Theory, 5(1), 37-62.

[94] D. Zagier, (1985). *Modular parametrizations of elliptic curves*. Canad. Math. Bull. 28, no. 3, 372-384.