WATKINS’ CONJECTURE FOR ELLIPTIC CURVES OVER FUNCTION FIELDS

JERSON CARO

Abstract. In 2002 Watkins conjectured that given an elliptic curve defined over \( \mathbb{Q} \), its Mordell-Weil rank is at most the 2-adic valuation of its modular degree. We consider the analogous problem over function fields of positive characteristic, and we prove it in several cases. More precisely, every modular semi-stable 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 the analogue of Watkins’ conjecture. Furthermore, for a well-known family of elliptic curves with unbounded rank due to Ulmer, we prove the analogue of Watkins’ conjecture.

1. INTRODUCTION

Let \( \mathcal{E} \) be an elliptic curve over \( \mathbb{Q} \) of conductor \( N \). The modular degree \( m_\mathcal{E} \) of \( \mathcal{E} \) is the minimum degree of all modular parametrizations \( \phi : X_0(N) \to \mathcal{E} \) over \( \mathbb{Q} \). The modularity Theorem \([24, 20, 2]\) implies that it is well-defined. In 2002 Watkins \([23]\) conjectured that for every elliptic curve \( \mathcal{E} \) over \( \mathbb{Q} \) we have \( r \leq \nu_2(m_\mathcal{E}) \), where \( \nu_2 \) denotes the 2-adic valuation and \( r := \text{rank}_{\mathbb{Z}}(\mathcal{E}(\mathbb{Q})) \).

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 \( \infty \) denote the place of \( K \) associated with \( 1/T \). Let \( E \) be a non-isotrivial (see Section 2.3 for the definition) elliptic curve defined over \( K \). Under the assumption that \( E \) has split multiplicative reduction at \( \infty \), there is an analogue to the modularity Theorem cf. Theorem 2.1. Namely, if \( E \) is non-isotrivial and has split multiplicative reduction at \( \infty \) and conductor ideal \( n \), then there is a non-constant map \( \phi_E : X_0(n) \to E \), where \( X_0(n) \) 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 \( \infty \). Given a modular elliptic curve \( E \) over \( K \), we say that it satisfies Watkins’ conjecture if \( \text{rank}_\mathbb{Z}(E(K)) \leq \nu_2(m_\mathcal{E}) \), where \( m_\mathcal{E} \) is the minimal degree of a modular parametrization \( \phi_E \).

Using Atkin-Lehner involutions we prove a potential version of Watkins’ conjecture for semi-stable elliptic curves over \( K \) (see \([7]\) and \([3]\) for other applications of Atkin-Lehner involutions in the context of Watkins’ conjecture).

**Theorem 1.1.** Let \( E \) be a modular semi-stable elliptic curve defined over \( K \) with conductor \( n_E = (n)^\infty \). Let \( k' \) be a finite field containing the splitting field of \( n \) over \( k \), then Watkins’ conjecture holds for \( E' = E \times_{\text{Spec}K} \text{Spec}K' \), where \( K' := k'(T) \).

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 \([19]\) in the isotrivial case and Ulmer \([21]\) in the non-isotrivial case. The next result proves Watkins’ conjecture for one of the families given by Ulmer, thus, we obtain Watkins’ conjecture for elliptic curves over \( K \) with arbitrarily large rank.

**Theorem 1.2.** Let \( p \) be a prime and \( n \) be a positive integer, such that \( 6 \mid p^n + 1 \). The elliptic curve \( E : y^2 + T^dxy = x^3 - 1 \) where \( d = (p^n + 1)/6 \) defined over \( \mathbb{F}_q(T) \), satisfies Watkins’ conjecture.
On the other hand, Esparza-Lozano and Pasten [8] prove that, over \( \mathbb{Q} \), the quadratic twist \( E(D) \) of \( E \) by \( D \) satisfies Watkins’ conjecture whenever the number of distinct prime divisor of \( D \) is big enough. Using results of Papikian [13] on \( L(\text{Sym}^2 f, 2) \) over function fields, when \( f \) is a Drinfeld modular form, we can prove an analogue over function fields. In the following we write \( \omega_K(g) \) for the number of distinct irreducible factors of a polynomial \( g \) in \( A \).

**Theorem 1.3.** 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 a 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 \( \omega_K(g) \geq 2 \omega_K(n) - \nu_2(m_E) \), then Watkins’ conjecture holds for \( E(g) \).

The condition that \( g \) has even degree is necessary to guarantee that \( E(g) \) is modular (cf. Section 4). The previous Theorem will be used to deduce the following:

**Corollary 1.4.** Assume that \( E \) is a semi-stable modular elliptic curve over \( K \). Then we have that \( E(g) \) satisfies Watkins’ 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’ conjecture for every square-free polynomial \( g \in A \) of even degree.

## 2. Preliminaries

The idea of this section is to define the associated invariants to Watkins’ conjecture over function fields. Write \( K_\infty \) for the completion of \( K \) at \( T^{-1} \), and let \( \mathcal{O}_\infty \) be its ring of integers. Let \( C_\infty \) denote the completion of an algebraic closure of \( K_\infty \).

### 2.1. Drinfeld Modular Curves.** We denote by \( \Omega \) the Drinfeld upper half plane \( C_\infty - K_\infty \). Notice that \( GL(2, K_\infty) \) acts on \( \Omega \) by fractional linear transformations, in particular, so does the Hecke congruence subgroup associated with an ideal \( \mathfrak{n} \) of \( A \)

\[
\Gamma_0(\mathfrak{n}) = \left\{ g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G : a, b, c, d \in \mathbb{F}_q[T], c \equiv 0 \pmod{\mathfrak{n}}, \det(g) \in \mathcal{O}_\infty \right\}.
\]

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 \( X_0(\mathfrak{n}) \).

### 2.2. Drinfeld Modular Forms and Hecke Operators.** In this section, we define an analogue of the cuspidal Hecke newforms over \( C \). Another way to understand \( \Omega \) is the Bruhat-Tits tree \( T \) of \( PGL(2, K_\infty) \), whose oriented edges are in correspondence with the cosets of \( GL(2, K_\infty)/K_\infty \cdot \mathcal{J} \) (see Section 4.2 [9]), where

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

This correspondence gives an action of \( GL(2, K_\infty) \) on the real-valued functions on the oriented edges of \( T \) by left-multiplying the argument. Let \( H^1(\Gamma_0(\mathfrak{n}), \mathbb{R}) \) be the finite-dimensional \( \mathbb{R} \)-space of real-valued, alternating, harmonic and \( \Gamma_0(\mathfrak{n}) \)-invariant functions on the oriented edges of \( T \) having finite support modulo \( \Gamma_0(\mathfrak{n}) \).

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

\[
i_\mathfrak{d} : (H^1(\Gamma_0(\mathfrak{n}/\mathfrak{d}), \mathbb{R}))^2 \longrightarrow H^1(\Gamma_0(\mathfrak{n}), \mathbb{R})
\]

given by

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

2
for every oriented edge $e$. The subspace of oldforms at level $n$ is
\[
H^\text{old}_{\ell}(\Gamma_0(n), \mathbb{R}) = \sum_{p | n} \mathbb{Z}_p((H_{\ell}(\Gamma_0(n/p), \mathbb{R}))^2).
\]

Denote by $H^\text{new}_{\ell}(\Gamma_0(n), \mathbb{R})$ to the orthogonal complement of the oldforms with respect to the Petersson-norm (see Section 4.8 Gekeler op. cit.) defined over $H_{\ell}(\Gamma_0(n), \mathbb{R})$.

For any nonzero ideal $m$ there is a Hecke operator $T_m$, for example, for $m$ relatively prime to $n$ is defined by
\[
T_m f(e) = \sum f \left( \left( \frac{a}{b} \right) \cdot e \right),
\]
where the sum runs over $a, b, d \in A$ such that $a, d$ are monic, $m = (ad)$, and $\deg(b) < \deg(d)$, see Section 4.9 Gekeler op. cit. for a general definition. Finally, a newform is a normalized Drinfeld modular form $f \in H^\text{new}_{\ell}(\Gamma_0(n), \mathbb{R})$, and an eigenform for all Hecke operators.

2.3. **Elliptic curves.** Let $E$ be an elliptic curve defined over $K$. Assume that $E$ has an affine model
\[
Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6.
\]
where $a_i \in K$. For this cubic equation, define the usual Weierstrass invariants:
\[
\begin{align*}
    b_2 &= a_1^2 + 4a_2, & b_4 &= a_1 a_3 + 2a_4, & b_6 &= a_3^2 + 4a_6, \\
    b_8 &= a_1^2 a_6 - a_1 a_3 a_4 + 4a_2 a_6 + a_2 a_3^2 - a_4, \\
    c_4 &= b_2^2 - 24b_4, & c_6 &= -b_2^3 + 36b_2 b_4 - 216b_6, \\
    \Delta &= -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6, \\
    j_E &= c_4^3 \Delta^{-1}.
\end{align*}
\]

We say that $E$ is **non-isotrivial** when $j_E \notin k$. Since we assume that $\text{char}(k) > 3$ the conductor of $E$ is cubefree. Denote it by $n_E$ and by $n$ its finite part, in particular, $n_E = n_0 \cdot \infty$, where $i \in \{0, 1, 2\}$. When $E$ has split multiplicative reduction at $\infty$, due to Drinfeld’s reciprocity law (Proposition 10.3 [6]) and the fact that $E$ is automorphic (Theorem 9.8 in [5]), there is an analogue of the modularity Theorem over $\mathbb{Q}$:

**Theorem 2.1** (Modularity Theorem). Let $E$ be an elliptic curve over $K$ of conductor $n_E = n_0 \cdot \infty$ having split multiplicative reduction at $\infty$. There is a non-constant morphism $X_0(n) \to E$ defined over $K$.

**Remark 2.2.** This Theorem gives a bijection between primitive newforms $f$ (i.e., $f$ is a newform such that $f \notin nH^\text{new}_{\ell}(\Gamma_0(n), \mathbb{Z})$ for $n > 1$) with integer eigenvalues and isogeny classes of modular elliptic curves over $K$ with conductor $n_0 \cdot \infty$.

2.3.1. **$L$-functions.** There is an attached $L$-function to an elliptic curve with conductor $n_E$, which has an Euler product expansion
\[
L(E, s) = \sum_{n \text{ pos. div.}} \frac{a_n}{|n|^s} = \prod_{p} \left( 1 - \frac{\alpha_p}{|p|^s} \right)^{-1} \left( 1 - \frac{\beta_p}{|p|^s} \right)^{-1},
\]
where $\alpha_p, \beta_p$ are defined as follows: (1) if $p \nmid n_E$, $\alpha_p + \beta_p = a_p := |p| + 1 - #E(F_p)$ and $\alpha_p \beta_p = |p|$, (2) if $p \mid n_E$, $\alpha_p = 0$ and $\beta_p = \pm 1$, and (3) if $p^2 \mid n_E$, $\alpha_p = \beta_p = 0$.

Due to results of Grothendieck [10] and Deligne [5] $L(E, s) = L(f_E, s)$, where $f_E$ is the newform associated to $E$, and $L(E, s)$ is a polynomial in the variable $q^{-s}$ of degree $\deg(n) - 4$. 


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

\[
L_p(\text{Sym}^2 f_E, s) = \begin{cases} 
1, & \text{if } p^2 \mid n_E, \\
\left(1 - \frac{1}{p^2}\right)^{-1}, & \text{if } p \mid n_E, \\
\left(1 - \frac{\alpha^2}{|p|^s}\right)^{-1} \left(1 - \frac{\alpha}{|p|^s}\right)^{-1} \left(1 - \frac{\alpha^*}{|p|^s}\right)^{-1}, & \text{if } p \nmid n_E.
\end{cases}
\]

When \( E \) is semi-stable Proposition 5.4 from [12] implies that \( L(\text{Sym}^2 f_E, s) \) is a polynomial in the variable \( q^{-s} \) of degree \( 2 \deg(n_E) - 4 \).

2.3.2. Upper Bounds for the Rank of the Mordell-Weil Group. The following is a geometric bound for the Mordell-Weil rank due to Tate [15]

\[
\text{rank}_{\mathbb{Z}}(E(K)) \leq \text{ord}_{s=1} L(E, s) \leq \deg(n_E) - 4.
\] (2)

See [22] for detailed proof. In addition, 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 \( \omega_K(n) \), the number of distinct primes that divide \( n \) in \( A \).

First of all, notice that the change of variables \( X = z/4, \ Y = y/8 - a_4 z/8 - a_3/2 \) transforms (1) into

\[
y^2 = z^3 + b_2 z^2 + 8 b_4 z + 16 b_6.
\] (3)

Let \( \gamma \in K \) be a root of the previous cubic, associated to a non-trivial \( K \)-rational 2-torsion point. Then \( \gamma \in A \) and the change of variables \( z = x + \gamma \) turns (3) into

\[
y^2 = x^3 + A x^2 + B x
\] (4)

where

\[
A = 3 \gamma + b_2 \quad \text{and} \quad B = 3 \gamma^2 + 2 b_2 \gamma + 8 b_4.
\]

Let \( \Delta_{\text{min}} \) be the discriminant of the minimal model (1) and let \( \Delta \) be the discriminant of (4). Notice that \( \Delta = 2^{12} \Delta_{\text{min}} \) by the standard transformation formulas, thus, (4) is a minimal model of \( E \). Now, recall the usual exact sequence related to a 2-descent,

\[
0 \longrightarrow \frac{E(K)}{2E(K)} \longrightarrow \text{Sel}_2(E/K) \longrightarrow \text{III}(E/K)[2] \longrightarrow 0.
\] (5)

Furthermore, consider the exact sequence from Lemma 6.1 of [15]

\[
0 \longrightarrow \frac{E'(K)[\theta]}{\phi[E(K)[2]]} \longrightarrow \text{Sel}^\theta(E/K) \longrightarrow \text{Sel}_2(E/K) \longrightarrow \text{Sel}^\theta(E'/K).
\] (6)

These two exact sequences imply that \( \text{rank}_{\mathbb{Z}}(E(K)) + 2 \leq s(E, \theta) + s'(E, \theta) \), where \( s(E, \theta) = \dim_{\mathbb{F}_2}(\text{Sel}^\theta(E/K)) \) and \( s'(E, \theta) = \dim_{\mathbb{F}_2}(\text{Sel}^\theta(E'/K)) \). In addition, there is a correspondence between Selmer groups and homogeneous spaces (see Chapter 4 from [14]), which shows that \( s(E, \theta) \leq \omega_K(A^2 - 4B) + 1 \) and \( s'(E, \theta) \leq \omega_K(B) + 1 \). Thus, we have the following proposition:

**Proposition 2.3.** Let \( E \) be an elliptic curve with \( K \)-rational 2-torsion and Weierstrass minimal model \( y^2 = x^3 + A x^2 + B x \), then:

\[
\text{rank}_{\mathbb{Z}}(E(K)) \leq \omega_K(A^2 - 4B) + \omega_K(B),
\]

consequently, if \( \alpha \) (resp. \( \mu \)) is the number of primes of additive (resp. multiplicative) bad reduction of \( E/K \). Then:

\[
\text{rank}_{\mathbb{Z}}(E(K)) \leq \mu + 2\alpha.
\]
2.3.3. **Modular Degree.** Let $E$ be a modular elliptic curve defined over $K$. Let $X_0(n)$ be the Drinfeld modular curve parametrizing $\phi_E: X_0(n) \to E$ where $\phi_E$ is non-trivial and of minimal possible degree. The modular degree $m_E$ is the degree of $\phi_E$. The following Lemma relates the 2-adic valuations of $m_E$ and $L(\text{Sym}^2 f, 2)$.

**Lemma 2.4.** Let $E$ be a modular elliptic curve with conductor $n\infty$. Then we have that
\[
\nu_2(m_E) = \nu_2(L(\text{Sym}^2 f, 2)) - \nu_2(\text{val}_\infty(j_E)).
\]

**Proof.** Proposition 1.3 in [13] states that
\[
m_E = \frac{q^{\deg n-2}(c_E)^2}{-\text{val}_\infty(j_E)}L(\text{Sym}^2 f, 2),
\]
where $c_E$ is the Manin constant and $q = \#E$. By taking 2-adic valuations we obtain
\[
\nu_2(m_E) = \nu_2(q^{\deg n-2}(c_E)^2) + \nu_2(L(\text{Sym}^2 f, 2)) - \nu_2(\text{val}_\infty(j_E)),
\]
and by Proposition 1.2 from [11] $c_E$ is a power of $q$ which yields the desired result. \qed

3. **WATKINS’ CONJECTURE FOR SEMI-STABLE ELLIPTIC CURVES**

For any ideal $\mathfrak{m} = (m)$, such that $\mathfrak{m} | n = (n)$, and $\mathfrak{m}$ and $n/\mathfrak{m}$ are relatively primes, there is an Atkin-Lehner involution $W_{\mathfrak{m}}$. This involution acts on $H_0(\Gamma_0(n), \mathbb{R})$ as follows
\[
W_{\mathfrak{m}} f(e) = f\left( \left( \begin{array}{cc} ma & b \\ nc & md \end{array} \right) \cdot e \right),
\]
where $a, b, c, d \in A$ and $m^2ab - nbc = \gamma m$ for some $\gamma \in k^\times$. We denote by $W(n)$ 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 [1] the Hecke operators commute with the Atkin-Lehner involutions, hence $W_p(n)f$ and $f$ have the same Hecke eigenvalues. By Lemma 1.2 from [16] $H_1^{\text{new}}(\Gamma_0(n), \mathbb{R})$ is stable under the Atkin-Lehner involutions, and consequently, we have that $W_p f = \pm f$.

**Remark 3.1.** Let $E$ be a modular elliptic curve, and $f_E$ be its attached primitive newform, then $f_E$ is an eigenform of every Atkin-Lehner involution.

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

**Proposition 3.2.** Let $E$ be an elliptic curve with conductor $n_E = n\infty$. Let $f_E$ be the primitive newform associated to $E$. Over this newform, we define $W' = \{ W \in W : W(f_E) = f_E \}$, and $\kappa := \dim\mathbb{F}_2(\mathbb{W}((n)) : W') + \dim\mathbb{F}_2(E(K)[2])$. Then $\omega_K(n) - \kappa \leq \nu_2(m_E)$.

**Proof.** Proposition 10.3 from [6] gives the following isomorphism
\[
H^1(X_0(n) \otimes K^{\text{sep}}_\infty, \mathbb{Q}_\ell) \cong H_0(\Gamma_0(n), \mathbb{Q}_\ell) \otimes \text{sp},
\]
where sp is the two-dimensional special $\ell$-adic representation of $\text{Gal}(K^{\text{sep}}_\infty/K_\infty)$. Furthermore, this isomorphism is compatible with the action of the Atkin-Lehner involutions.

Since $H^1(X_0(n) \otimes K^{\text{sep}}_\infty, \mathbb{Q}_\ell)$ is the dual of $V_i(J_0(n))$, we have that if $\pi: J_0(n) \to E$ is the projection, then $\pi((W(D)) = \pi([D])$ for every divisor $D$ of degree 0 over $X_0(n)$ whenever $W \in W'$. By Remark 3.1 $W'$ has at most index 2 in $W(n)$. Now, as in Proposition 2.1 in [7] we construct a homomorphism $\theta: W' \to E(K)[2]$. First of all, we fix a $K$-rational point $x_0 \in X_0(n)$, then for $W \in W'$ we define $\theta(W) = \pi([W(x_0) - (x_0)])$. Notice that $\theta(W) \in E(K)[2]$, since $x_0 \in X_0(n)(K)$ 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 \( W'' = \ker \theta \). Let \( \mathcal{X} = X_0(n)/W'' \), and denote by \( \psi : X_0(n) \to \mathcal{X} \) that is also defined over \( K \) and by \( \mathcal{J} \) the Jacobian of \( \mathcal{X} \). We can define \( i : X_0(n) \to J_0(n) \) based on \( x_0 \), and \( i' : \mathcal{X} \to \mathcal{J} \) based on \( \psi(x_0) \), so we obtain a commutative diagram

\[
\begin{array}{ccc}
X_0(n) & \xrightarrow{i} & J_0(n) \\
\downarrow \psi & & \downarrow \psi_* \\
\mathcal{X} & \xrightarrow{i'} & \mathcal{J}.
\end{array}
\]

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

\[
[m_E] = \pi \circ \pi' = (\pi' \circ \psi_*) \circ (\psi \circ \pi') = \pi' \circ [\deg(\psi)] \circ \pi = \deg(\psi) \circ \pi = [\#W''] \circ (\pi' \circ \pi').
\]

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 \( \#W'' | m_E \), since \( p \neq 2 \).

\[\Box\]

The previous Proposition and Tate’s geometric bound (2) allow us to prove Theorem 1.1.

**Proof of Theorem 1.1.** Recall that \( E' = E \times_{\text{Spec} K} \text{Spec} K' \). Since the conductor of \( E' \) is also \( n_E = (n)\infty \), then by Tate’s geometric bound (2) \( \text{rank}(E'(K')) \leq \deg(n) - 4 \). On the other hand, we know that \( \omega_{K'}((n)) = \deg(n) \) because \( k' \) contains the splitting field of \( n \). Furthermore, since \( \text{dim}_{E'}([W(n) : W]) \leq 1 \), by Remark 3.1 we have \( \kappa \leq 3 \), then by Proposition 3.2 we have that

\[
\nu_2(m_{E'}) \geq \omega_K((n)) - 3 = \deg(n) - 3 = \deg(n_E) - 4 \geq \text{rank}(E'(k'(T))),
\]

which yields the desired result.

\[\Box\]

Ulmer [21] exhibits a closed formula for the rank of a family of elliptic curves. Proposition 3.2 together with this formula allow us to show Watkins’ conjecture for this family.

**Proof of Theorem 1.2.** First of all, we notice that \( E(\overline{\mathbb{F}_p}(T))[2] = (0) \), since the polynomial \( 4x^3 + T^24x - 4 \) does not have 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 [21] shows that \( n_{E'} = T(1 - 2^{33}3^{T^m}) \), then in particular \( n_E = (T^m - 2^{33}3^{T^m})\infty \). We claim that \( f(T) = T^m - 2^{33}3^m \) 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 \( \alpha \in \mathbb{F}_p \), \( 2^33^m \) is a root of \( f \). If \( \alpha \notin \mathbb{F}_p \), since \( 6 | n^p - 1 \) we have that \( p \equiv -1 \mod 3 \), then \( p \equiv 1 \mod 4 \) by the law of quadratic reciprocity. This implies that \( 2^33^m \) or \( 2^33^m \beta \) is a root of \( f \), where \( \beta^2 = -1 \). Consequently, there is a bijection between the prime divisors of \( T^m - 1 \) and \( f(T) \).

By definition, \( T^m - 1 \) factors over \( \overline{\mathbb{F}}_p[T] \) 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

\[
\omega_{\mathbb{F}_q(T)}(n_E) = \sum_{e|m} \phi(e) - \begin{cases} 0 & \text{if } T^m - 2^{33}3^m \text{ has solution in } \mathbb{F}_q, \\ 1 & \text{otherwise}. \end{cases}
\]

6
where $\phi(e)$ is the cardinality of $(\mathbb{Z}/e\mathbb{Z})^\times$ and $\omega_e(q)$ 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 [21] states a closed expression for $\text{rank}(E'(\mathbb{F}_q(T)))$

$$\sum_{e|m \atop e \not| 6} \frac{\phi(e)}{\omega_e(q)} + \begin{cases} 2 & \text{if } 3 \mid q - 1 \\ 1 & \text{otherwise} \\ 0 & \text{otherwise} \end{cases}.$$

Since there are 4 divisors of 6 we obtain

$$\sum_{e|m \atop e \not| 6} \frac{\phi(e)}{\omega_e(q)} \geq \sum_{e|m \atop e \not| 6} \frac{\phi(e)}{\omega_e(q)} + 4.$$

Furthermore, if $3 \mid q - 1$ then $q$ is a square since $p \equiv -1 \pmod{3}$; which implies that $T^m - 2^43^3$ has solution in $\mathbb{F}_q$.

Hence, Proposition 3.2 implies that

$$\nu_2(m_E) \geq \omega_{\mathbb{F}_q(T)}(n_E) - 1 = \sum_{e|m \atop e \not| 6} \frac{\phi(e)}{\omega_e(q)} - 1 \geq \sum_{e|m \atop e \not| 6} \frac{\phi(e)}{\omega_e(q)} + 3 \geq \text{rank}(E(\mathbb{F}_q(T))).$$

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

$$\nu_2(m_E) \geq \omega_{\mathbb{F}_q(T)}(n_E) - 1 \geq \sum_{e|m \atop e \not| 6} \frac{\phi(e)}{\omega_e(q)} - 2 \geq \sum_{e|m \atop e \not| 6} \frac{\phi(e)}{\omega_e(q)} + 2 \geq \text{rank}(E(\mathbb{F}_q(T))),$$

which gives the desired result. 

4. Watkins’ Conjecture for Quadratic Twists

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

$$E^{(g)}: y^2 = x^3 + Ax^2 + Bg^2x.$$

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 $n_E^{(g)}$ of $E^{(g)}$ is equal to $n_E(g^2/d)$, where $d = \gcd(n_2, g)$. We denote by $f^{(g)}$ to the associated Drinfeld newform to $E^{(g)}$.

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

**Lemma 4.1.** With the notation above, we have that

$$\text{rank}_\mathbb{Z}(E^{(g)}(K)) \leq \omega_K(n_2) + 2(\omega_K(n_1) + \omega_K(g)).$$

**Proof.** First of all, we notice that $E^{(g)}$ has multiplicative reduction at $p$ if $p \mid n_2/d$, $E^{(g)}$ has additive reduction at $p$ if $p \mid n_1g$, and otherwise $E^{(g)}$ has good reduction at $p$. Then by Proposition 2.3 we obtain that

$$\text{rank}_\mathbb{Z}(E^{(g)}(K)) \leq \omega_K(n_2/d) + 2(\omega_K(n_1) + \omega_K(g)),$$

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 $L(\text{Sym}^2 f^{(g)}, 2)$ and $L(\text{Sym}^2 f, 2)$, so, we can use Lemma [2.4] 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. Let $p$ be a prime ideal of $A$ and let $\left( \frac{p}{p} \right) : \mathbb{F}_p \to \{-1, 0, 1\}$ be the extended Legendre symbol. Then

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

Proof. If $E^{(g)}$ has additive reduction at $p$, we have that $p | n_1$ or $p | g$, then $a_p(E^{(g)}) = 0$ and there is nothing to prove. On the other hand, assume that $E^{(g)}$ has multiplicative reduction at $p$. By Lemma 2.2 in [4] $E$ has split multiplicative reduction at $p$ if and only if $(\frac{-c_0(E)}{p}) = 1$, as a consequence, this quantity is equal to $a_p(E)$. Furthermore, since $c_0(E^{(g)}) = g^3c_0(E)$, we have

$$a_p(E^{(g)}) = \left( \frac{-c_0(E^{(g)})}{p} \right) = \left( \frac{-g^3c_0(E)}{p} \right) = \left( \frac{g}{p} \right) a_p(E).$$

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

$$\#E_p^{(g)}(\mathbb{F}_p) = |p| - 1 + \sum_{x \in M} \left( \frac{x^3 + Ax^2 + B}{p} \right)$$

$$= |p| - 1 + \sum_{x \in M} \left( \frac{g^3(x^3 + Ax^2 + B)}{p} \right)$$

$$= |p| - 1 + \left( \frac{g}{p} \right) \sum_{x \in M} \left( \frac{x^3 + Ax^2 + B}{p} \right)$$

by recalling the definition of $a_p(E)$ we get the desired result. 

□

Proposition 4.3. Let $E$ be a modular elliptic curve with conductor $n_E$ and associated primitive newform $f$. Assume that $E'$ is a quadratic twist of $E$, with conductor $n'_E$ and associated primitive newform $f'$, such that $\text{ord}_p(n_E) \leq \text{ord}_p(n'_E)$ for all $p$. 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 $n_E = (n_1^2n_2)\infty$ and $n'_E = n_Eg^2/d$. Then one has

$$L(\text{Sym}^2 f', 2) = L(\text{Sym}^2 f, 2) \frac{|d|}{|g|^3} \prod_{p|d} (|p|^2 - 1) \prod_{p|g/d} ((|p| + 1)^2 - a_p(E^2)) (|p| - 1).$$

Proof. By Lemma 4.2 we have that when $\text{ord}_p(n) = \text{ord}_p(n')$ the local factors are equal, i.e. $L_p(\text{Sym}^2 f', 2) = L_p(\text{Sym}^2 f, 2)$. If $p | d$, we have that

$$L_p(\text{Sym}^2 f', s) = L_p(\text{Sym}^2 f, s)(1 - |p|^{-s}),$$

thus, at $s = 2$ we obtain

$$L_p(\text{Sym}^2 f', 2) = L_p(\text{Sym}^2 f, 2) \frac{1}{|p|^2}(|p|^2 - 1).$$

Finally, assume that $p | (g/d)$. The local factors are related as follows

$$L_p(\text{Sym}^2 f', s) = L_p(\text{Sym}^2 f, s) \left( 1 - a_p^2|p|^{-s} \right) \left( 1 - \frac{a_p^2}{|p|} |p|^{-s} \right) (|p| - 1)^{-s},$$
We know that helpful remarks. I was supported by ANID Doctorado Nacional 21190304.

On the other hand, Proposition 4.3 implies that Lemma 2.4 we obtain

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

Putting all together, we achieve the desired result. \( \Box \)

**Proof of Theorem 1.3.** Since \( E \) and \( E^{(g)} \) are isomorphic over \( \mathbb{C}_\infty \), we have that \( j_E = j_{E^{(g)}} \), thus by Lemma 2.4 we obtain

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

On the other hand, Proposition 4.3 implies that \( \nu_2(L(\text{Sym}^2 f^{(g)}, 2)/L(\text{Sym}^2 f, 2)) = \sum_{p \mid d} \nu_2(|p|^2 - 1) + \sum_{p \nmid g/d} \nu_2\left(\left(|p| + 1\right)^2 - a_p(E)^2\right)(|p| - 1)\right). \]

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

\[ \nu_2(L(\text{Sym}^2 f^{(g)}, 2)) - \nu_2(L(\text{Sym}^2 f, 2)) \geq 3\omega_K(g). \]

Putting all together, we achieve the result.

\[ \nu_2(m_{E^{(g)}}) \geq \nu_2(m_E) + 3\omega_K(g). \]

By Proposition 2.3 we know that \( \text{rank}(E^{(g)}) \leq 2(\omega_K(n) + \omega_K(g)) \). By our assumptions on \( g \) we obtain that

\[ \nu_2(m_E) + 3\omega_K(g) \geq 2(\omega_K(n) + \omega_K(g)), \]

consequently, \( \text{rank}(E^{(g)}) \leq \nu_2(m_{E^{(g)}}) \). \( \Box \)

**Proof of Corollary 1.4.** By Proposition 3.2 we have that \( \nu_2(m_E) \geq \omega_K(n) - 3 \). Since \( E \) is semi-stable, \( n \) is square-free, consequently, Lemma 4.1 implies that \( \text{rank}(E^{(g)}) \leq \omega_K(n) + 2\omega_K(g) \). Using the equation (7), we have

\[ \nu_2(m_{E^{(g)}}) \geq \nu_2(m_E) + 3\omega_K(g) \geq \omega_K(n) - 3 + 3\omega_K(g) \geq \omega_K(g) - 3 + \text{rank}(E^{(g)}), \]

hence Watkins’ conjecture holds for \( E^{(g)} \), whenever \( \omega_K(d) \geq 3 \). Furthermore, if a prime ideal \( p \) divides \( n \) and has non-split multiplicative reduction, by Theorem 3 in [1] \( W_p f = f \), consequently, \( \mathcal{W} = \mathcal{W}' \). Therefore, if every prime \( p \) which divides \( n \) has non-split multiplicative reduction and \( E(K)[2] \cong \mathbb{Z}/2\mathbb{Z} \) Proposition 3.2 implies that \( \nu_2(m_E) \geq \omega_K(n) - 1 \), thus, equation (8) turns into

\[ \nu_2(m_{E^{(g)}}) \geq \omega_K(g) - 1 + \text{rank}(E^{(g)}), \]

accordingly, Watkins’ Conjecture holds for every square-free polynomial \( g \) of even degree. \( \Box \)

**Acknowledgements**

I want to thank Professor Hector Pasten for suggesting this problem to me and for numerous helpful remarks. I was supported by ANID Doctorado Nacional 21190304.
References

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

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

[3] Jerson Caro and Héctor Pastén. *Watkins’s conjecture for elliptic curves with non-split multiplicative reduction*. Preprint, 2021.

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

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

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

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

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

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

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

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

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

[13] Papikian, M. (2007) *Analogue of the degree conjecture over function fields*. Transactions of the American Mathematical Society, 359(7): 3483–3503.

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

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

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

[17] Shioda, T. (1992) *Some remarks on elliptic curves over function fields*. Astérisque, 209(12):90–114.

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

[19] 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.

[20] Taylor, R. and Wiles, A. *Ring-theoretic properties of certain hecke algebras*. Annals of Mathematics, pages 553–572, 1995.

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

[22] Ulmer, D. (2011). *Park City lectures on elliptic curves over function fields*. arXiv preprint [arXiv:1101.1939]

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

[24] Wiles, A. *Modular elliptic curves and Fermat’s last theorem*. Annals of Mathematics, pages 443–551, 1995.

[25] Yazdani, S. *Modular abelian varieties of odd modular degree*. Algebra and Number Theory, 5(1): 37–62, 2011.

Email address: jocaro@uc.cl

Facultad de Matemáticas, Pontificia Universidad Católica de Chile, Campus San Joaquín, Avenida Vicuña Mackenna 4860, Santiago, Chile.