ON TWISTS OF TUPLES OF HYPERELLIPTIC CURVES

by
BEYZA MEVLÜDE AMIR

Submitted to the Graduate School of Engineering and Natural Sciences
in partial fulfilment of
the requirements for the degree of Master of Science

Sabancı University
June 2025

ON TWISTS OF TUPLES OF HYPERELLIPTIC CURVES

Approved by:

Assoc. Prof. Mohammad Sadek .....
(Thesis Supervisor)

Assoc. Prof. Kağan Kurşungöz .....

Assoc. Prof. Mücahit Akbıyık .....

Date of Approval: June 11, 2025

ABSTRACT

ON TWISTS OF TUPLES OF HYPERELLIPTIC CURVES

BEYZA MEVLUDE AMIR

Mathematics, Master Thesis, June 2025

Thesis Supervisor: Assoc. Prof. Mohammad Sadek

Keywords: elliptic curves, hyperelliptic curves, rational points, high-rank twists, quadratic twist

We investigate families of hyperelliptic curves whose Jacobians possess positive Mordell-Weil rank over $\mathbb{Q}$. Given a square-free polynomial $f(x) \in \mathbb{Q}[x]$ of degree at least 3 and fixed odd integers $m_1, m_2, m_3 \geq 3$, we construct parametric families of non-square rational values D such that the Jacobians of the twisted curves $C : Dy^2 = f(x)$ and $C_i : y^2 = Dx^{m_i} + a_i$ for $i = 1, 2, 3$, attain positive Mordell-Weil rank over $\mathbb{Q}(u, v_1, v_2, v_3)$. Our approach involves solving a Diophantine system reducible to finding rational points on certain elliptic curves defined by intersections of quadratic surfaces. Exploiting explicit rational parametrizations and leveraging Silverman's specialization theorem, we demonstrate the existence of infinite-order points on these Jacobians. This yields rational functions D that simultaneously induce high-rank twists across the considered families of curves.

ÖZET

HIPERELIPTIK EĞRI DIZILERININ BÜKMELERI ÜZERINE

BEYZA MEVLÜDE AMIR

Matematik, Yüksek Lisans Tezi, Haziran 2025

Tez Danışmanı: Assoc. Prof. Mohammad Sadek

Anahtar Kelimeler: eliptik eğriler, hipereliptik eğriler, rasyonel noktalar, yüksek mertebeli bükmeler, kareklik bükme

Bu çalışmada, Jacobian'ları $\mathbb{Q}$ üzerinde pozitif Mordell-Weil rankına sahip olan hipereliptik eğriler ailesi incelenmektedir. Derecesi en az 3 olan karekök içermeyen bir $f(x) \in \mathbb{Q}[x]$ polinomu ve $m_1, m_2, m_3 \geq 3$ olmak üzere tek pozitif tamsayılar verildiğinde, eğriler $C : Dy^2 = f(x)$ ve $C_i : y^2 = Dx^{m_i} + a_i$ (i = 1, 2, 3) biçiminde tanımlanan twist'lerin Jacobian'larının $\mathbb{Q}(u, v_1, v_2, v_3)$ üzerinde pozitif Mordell-Weil rankına sahip olmasını sağlayan kare olmayan rasyonel D değerlerinin parametrik bir ailesi oluşturulmaktadır. Yaklaşımımız, bazı kuadratik yüzeylerin kesişiminden oluşan eliptik eğriler üzerinde rasyonel noktaların bulunmasına indirgenebilen bir Diofantin sistemin çözümüne dayanmaktadır. Açık rasyonel parametrelendirmeler ve Silverman'ın specialization teoremi kullanılarak bu Jacobian'larda sonsuz mertebeli noktaların varlığı gösterilmektedir. Bu yöntemle, ele alınan eğri ailelerinde aynı anda yüksek rütbeli twist'ler oluşturan rasyonel fonksiyonlar D elde edilmektedir.

ACKNOWLEDGEMENTS

First and foremost, I would like to express my deepest gratitude to my thesis advisor, Dr. Mohammad Sadek, for his invaluable guidance, continuous support, and insightful feedback throughout the course of my research. His expertise and encouragement were instrumental in the successful completion of this thesis.

I would also like to sincerely thank the members of my thesis jury, Dr. Kağan Kurşungöz and Dr. Mücahit Akbıyık, for their time, thoughtful comments, and valuable suggestions that greatly enriched this work.

On a personal note, I am profoundly grateful to my beloved husband, Oussama Amir, for his unwavering love, patience, and encouragement. His support has been a constant source of strength. I also extend my heartfelt thanks to my dear son, Driss Kaan, whose presence brought joy and motivation throughout this journey.

I am especially thankful to my parents for their unconditional love and belief in me. In particular, I would like to express my deep appreciation to my mother, whose strength, sacrifices, and constant encouragement have inspired me every step of the way.

This achievement would not have been possible without the support and love of all these incredible individuals. I am truly grateful.

To my beloved son, Kaan.
You made every challenge worth it.

TABLE OF CONTENTS

Introduction

Beginning with foundational work [7], Kuwata and Wang demonstrated the existence of a polynomial $D \in \mathbb{Z}[t]$ such that the quadratic twists $E_{i,D}$ of each curve E_i (for $i = 1, 2$) by D have positive rank. However, their method does not apply in the special case where both curves share the same exceptional j-invariant, that is, when $j(E_1) = j(E_2) = j$, with $j = 0$ or $j = 1728$. Later on Ulas gave results for same question which asks for positive rank of twists of pairs of elliptic curves with j-invariant 0 or 1728 for both elliptic curves. In subsequent papers, by elaborating on the types of twists and curves, research advances toward developing explicit families of twists, quarks, m-twists and $2m$-twists, that ensure positive rank in the Jacobians of these curves over rational function fields.

In 2010, Ulas explores the arithmetic properties of higher-order twists, specifically sextic and quartic twists, of pairs of elliptic curves over the rational numbers $\mathbb{Q}$ in [15]. The paper proves that for any pair of elliptic curves E_1, E_2 with $j(E_1) = j(E_2) = 0$, namely,

$$E_1 : y^2 = x^3 + a \quad \text{and} \quad E_2 : y^2 = x^3 + b,$$

one can find a polynomial $D \in \mathbb{Z}[u, v, w, t]$ such that the sextic twists of both curves by D, given by

$$E_{1,D} : y^2 = x^3 + aD \quad \text{and} \quad E_{2,D} : y^2 = x^3 + bD$$

have rank at least 2 over $\mathbb{Q}(u, v, w, t)$.

The method involves constructing two rational points of infinite order on each twisted elliptic curve. To establish that these points are independent, the authors show that the action of the automorphisms of the function field on these points is different. Consequently, they conclude that the Mordell–Weil rank of each twisted curve is at least 2.

This paper [14] by Maciej Ulas studies systems of Diophantine equations involving polynomial expressions such as $h(x, y) = y^n - x^m$, and investigates the existence of infinite families of rational parametric solutions. These are then applied to construct superelliptic curves with Jacobians of positive rank over rational function fields [4].

This paper extends results on quadratic, sextic, and quartic twists of elliptic curves to hyperelliptic curves of the form

$$y^2 = x^n + a.$$

The authors prove that for given nonzero rational numbers a, b and an integer $n \geq 3$, there exists a polynomial $d(t) \in \mathbb{Q}[t]$ such that the Jacobian varieties of the hyperelliptic curves:

$$C_1 : y^2 = x^n + ad(t), \quad C_2 : y^2 = x^n + bd(t)$$

both have positive rank over $\mathbb{Q}(t)$. The results generalize analogous findings for pairs of elliptic curves. Following the development of the concept of twists for pairs of curves, subsequent research advanced this framework by extending the same concept to triples of curves instead of pairs.

In 2013, Ulas considered triples of elliptic curves [16], whereas in 2014, Jędrzejak and Ulas extended the same concept to investigate the existence of the function D for Jacobians of twists applied to hyperelliptic curves [3]. The theorems discussed in [16] investigate the existence of a rational function $D(u, v, w) \in Q(u, v, w)$ such that, when used as a common twisting parameter, it simultaneously induces nontrivial quadratic, cubic, or sextic twists of three different elliptic curves, each of which then attains positive Mordell–Weil rank over the function field $Q(u, v, w)$. This work generalizes and deepens earlier results by Kuwata and Wang, providing broader classes of elliptic curves and twist types. The three primary cases explored differ based on the twist types applied and on whether the elliptic curves involved possess general or special j-invariants.

In the first major theorem, the authors consider three elliptic curves E_1, E_2, E_3 where E_1 has an arbitrary j-invariant, while E_2 and E_3 are of the special form $y^2 = x^3 + b$, having $j = 0$. The goal is to construct a rational function $D_{2,3,3}(u, v, w)$ such that E_1 undergoes a quadratic twist and both E_2 and E_3 undergo cubic twists by the same parameter D, resulting in all three twisted curves having positive rank. To achieve this, the authors construct rational solutions to a system equating the twist expressions for each curve. They parametrically define values for x_i and y_i in terms of u, v, w, and derive the twist factor D in terms of these parameters. Then, they construct explicit rational points on the twisted curves and verify these points are of infinite order, ensuring the twists have positive rank.

A generalization of this is offered in a second theorem, where E_2 and E_3 undergo sextic twists instead of cubic twists. These twists are algebraically more complex and demand more sophisticated parametrizations but remain tractable using similar methods. Here, the twist factor $D_{2,6,6}(u, v, w)$ is defined such that the same elliptic curve E_1 undergoes a quadratic twist, and the other two curves are sextically twisted, still resulting in positive ranks. The proof strategy follows that of the previous

theorem but accounts for the more intricate algebra of sextic twists.

The third main theorem focuses on the case where all three curves have $j = 0$, making higher-order twists possible for each. In this symmetric setup, two curves receive cubic twists, and the third a sextic twist. The twist factor $D_{3,3,6}(u, v, w)$ is again explicitly constructed, and rational points are demonstrated on each twisted curve. Because all curves are now of the form $y^2 = x^3 + a$, with $a \in \mathbb{Z} \setminus \{0\}$, the symmetry simplifies the system of equations involved and facilitates a unified treatment of the twist parameter across all three curves. This scenario is especially powerful as it utilizes the full flexibility of elliptic curves with $j = 0$, which admit multiple nontrivial twisting operations.

Each of these theorems guarantees the existence of infinitely many values $d \in \mathbb{Q}$ such that twisting all three curves simultaneously by d yields positive rank. Corollaries also consider variations involving only two curves, where similar rational functions lead to one curve achieving rank at least two.

Extending these results beyond elliptic curves, the authors reference a related 2014 work with Jędrzejak, which generalizes the method to hyperelliptic and superelliptic curves. In that context, instead of studying the Mordell–Weil group of an elliptic curve, the focus shifts to the Jacobian of a hyperelliptic curve. They prove that rational functions can be constructed that simultaneously twist multiple such curves, ensuring that their Jacobians also acquire positive rank over $Q(u, v, w)$. The approach is conceptually similar: establish a system of algebraic equalities corresponding to the twist conditions and parameterize its rational solutions to derive a twisting function and corresponding rational points.

Extending from triples to quadruples of hyperelliptic curves, we demonstrate the existence of a rational function D such that each corresponding twist admits a Jacobian of positive Mordell-Weil rank.

In our thesis, we study the simultaneous twisting of a hyperelliptic curve $C : y^2 = f(x)$, with $f \in \mathbb{Q}[x]$ square-free of degree at least 3, and three higher-degree hyperelliptic curves $C_i : y^2 = x^{m_i} + a_i$, where $m_1, m_2, m_3 \geq 3$ are fixed odd integers. We establish the existence of a non-square rational parameter D such that the quadratic twist $C_D : Dy^2 = f(x)$ and the m_i-twists $C_{i,D} : y^2 = Dx^{m_i} + a_i$ all have Jacobians of positive Mordell-Weil rank over the rational function field $\mathbb{Q}(u, v_1, v_2, v_3)$.

Our main result (Theorem 3.1.1) proves that these twists admit rational points of infinite order, thereby showing that the Mordell-Weil ranks of their Jacobians are strictly positive. This is achieved by reducing the problem to finding rational points on a parametrized elliptic curve defined by the intersection of two quadratic

surfaces in $\mathbb{P}^3$, and applying Silverman's specialization theorem to deduce abound on the rank.

Furthermore, in Theorem 3.1.2, we show that in the symmetric case $m_1 = m_2 = m_3 = m$, and $a_1 = a_2 = a_3 = a \in \mathbb{Q}^\times$, the Jacobian of the m-twist of $y^2 = x^m + a$ by D has Mordell-Weil rank at least 3.

1. PRELIMINARIES

1.1 Varieties

1.1.1 Affine Varieties

Definition 1.1.1. *An affine space of dimension n over a field K, denoted as $\mathbb{A}^n = \mathbb{A}^n(\bar{K})$, is a set of points that can be described using coordinates from the field K, namely,*

$$\mathbb{A}^n = \mathbb{A}^n(\bar{K}) = \{P = (x_1, ..., x_n) : x_i \in \bar{K}\}$$

where $\bar{K}$ is an algebraic closure of K. In the same way, the set of $K-$rational points of $\mathbb{A}^n$ is the set

$$\mathbb{A}^n(K) = \{P = (x_1, ..., x_n) \in \mathbb{A}^n : x_i \in K\}.$$

We set $K[X] := K[X_1, \cdots, X_n]$ for any field K.

Given an ideal $I \subseteq K[X]$, the set V_I is the subset of $\mathbb{A}^n$ defined by I,

$$V_I = \{P \in \mathbb{A}^n : f(P) = 0 \text{ for all } f \in I\}.$$

Definition 1.1.2. *A set of the form V_I is called an algebraic set. If V is an algebraic set, the ideal of V, denoted by $I(V)$, is defined as*

$$I(V) = \{f \in \bar{K}[X] : f(P) = 0 \text{ for all } P \in V\}.$$

If the ideal $I(V)$ can be generated by polynomials in $K[X]$, then V is said to be defined over K, denoted by V/K.

Example 1. *We consider the set V of points of $\mathbb{A}^2$ defined as follows*

$$V = \{(x, y) \in \mathbb{A}^2 \mid x^2 + y^2 - 2 = 0\}$$

Since V is defined as the zero set of a polynomial, it is an algebraic set and the ideal of V given by

$$I(V) = (x^2 + y^2 - 2)$$

is a principal ideal.

Definition 1.1.3. *An affine algebraic set V is an affine variety if $I(V)$ is a prime ideal in $\bar{K}[X]$.*

If V is defined over K, it is not enough to check that $I(V/K)$ is prime in $K[X]$ because the primality may change when considering the ideal over the algebraic closure $\bar{K}$. Thus, the primality of the ideal $I(V/K)$ must be verified in $\bar{K}[X]$ because the behavior of the ideal can differ between $K[X]$ and $\bar{K}[X]$. This can be seen as whether the algebraic set is irreducible or not.

Example 2. *In Example 1, the ideal $I(V)$ is the principal ideal generated by an irreducible polynomial over $\mathbb{C}$. It follows that the ideal $I(V)$ is prime in $\mathbb{C}[x, y]$. Since $I(V)$ is a prime ideal, V is an algebraic variety.*

Definition 1.1.4. *The algebraic set V is irreducible if it cannot be expressed as the union of two proper algebraic subsets.*

Example 3. *Consider the algebraic set*

$$V = \{x^2 + y^2 - 1 = 0\}$$

in $\mathbb{A}^2$. This represents the unit circle. This set is irreducible because it cannot be split into two smaller algebraic sets, and any proper subset of the circle would not satisfy the equation.

Example 4. *Consider the algebraic set V in the affine plane $\mathbb{A}^2$ defined by the equation:*

$$V = V(XY) = \{(x, y) \in \mathbb{A}^2 \mid xy = 0\}.$$

This set consists of the union of the two coordinate axes $(X = 0)$ and $(Y = 0)$. So, V is reducible and it is not a variety.

Definition 1.1.5. *The dimension of a variety V is transcendence degree of $\bar{K}(V)$ over $\bar{K}$ and denoted by $dim(V)$.*

1.1.2 Projective Varieties

Definition 1.1.6. *A projective n-space over a field K is the set of points*

$$[x_0, x_1, .., x_n]$$

where x_i's are homogeneous coordinates and at least one of x_i is non-zero. Every point $[x_0, x_1, .., x_n]$ is an equivalence class with the equivalence relation

$$(x_0, x_1, .., x_n) \sim (y_0, y_1, .., y_n)$$

if there exists a $\lambda \in \bar{K}^*$ such that $x_i = \lambda y_i$ for all i, where $(x_0, x_1, ..x_n) \in \mathbb{A}^{n+1}$. Projective n-space is denoted by $\mathbb{P}^n$.

Definition 1.1.7. *If a polynomial $f \in \bar{K}[X]$ of degree d satisfies*

$$f(\lambda X_0, \lambda X_1, .., \lambda X_n) = \lambda^d f(X_0, X_1, .., X_n) \quad \text{for all} \quad \lambda \in \bar{K}$$

then it is called a homogeneous polynomial.

Example 5. *Consider the polynomial*

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

This polynomial is not homogeneous because if we scale x, y, and z by a factor t, we get

$$f(tx, ty, tz) = (tx)^3 + (ty)^2(tz) + (ty)(tz)^2 + 2(tx) + ty$$

since $t^3 \cdot f(x, y, z) \neq f(tx, ty, tz)$, it follows that $f(x, y, z)$ is not homogeneous.

We can homogenize this polynomial by introducing a new variable w and modifying each term by multiplying it by an appropriate power of w. We will define the homogenized function $f^*(x, y, z, w)$ by

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

In general the homogenization of a polynomial $f \in \bar{K}[x_1, \cdots, x_n]$ of degree d is defined by $f^*(x_1, \cdots, x_n, x_{n+1}) = x_{n+1}^d f(x_1/x_{n+1}, x_2/x_{n+1}, \cdots x_n/x_{n+1})$.

A homogeneous ideal I is an ideal generated by homogeneous polynomials. We define V_I to be the set of points of $\mathbb{P}^n$ which are zeros of polynomials of the homogeneous ideal I. Given a homogeneous ideal I, the set V_I is the subset of $\mathbb{P}^n$ defined by I, i.e.,

$$V_I = \{P \in \mathbb{P}^n : f(P) = 0 \text{ for all homogeneous } f \in I\}.$$

Definition 1.1.8. *A set of the form V_I is called a projective algebraic set. If V is an algebraic set, we define the ideal of V, denoted by $I(V)$, as follows*

$$I(V) = \{f \in \bar{K}[X] : f(P) = 0 \text{ for all } P \in V\}.$$

If the ideal $I(V)$ can be generated by polynomials in $K[X]$, the algebraic set V is said to be defined over K, denoted by V/K.

Definition 1.1.9. *A projective variety is a projective algebraic set whose homogeneous ideal $I(V)$ is a prime ideal in $\bar{K}[X]$.*

Definition 1.1.10. *The dimension of a projective variety V/K is the dimension of $V \cap \mathbb{A}^n$.*

1.1.3 Algebraic Curves

Throughout the thesis, by a curve we mean the following:

Definition 1.1.11. *An affine algebraic curve over a field K is a one-dimensional algebraic variety, i.e., a set of points in $\mathbb{A}^2(K)$ which satisfies a polynomial in two variables*

$$F(x, y) = 0.$$

This affine algebraic curve can be extended to a projective algebraic curve by homogenizing the polynomial. Now a projective curve will be a set of points in $\mathbb{P}^2(K)$ defined by an equation of the form

$$F^*(x, y, z) = 0$$

where F^* is a homogenization of the polynomial F.

Definition 1.1.12. *For an algebraic curve C defined over a field K, given by a polynomial equation $F(x, y) = 0$, the curve is smooth at a point P if at least one of the partial derivatives*

$$\frac{\partial F}{\partial x} \quad or \quad \frac{\partial F}{\partial y}$$

is nonzero at P. The curve is called a non-singular curve if it is smooth everywhere.

Example 6. *Consider an algebraic curve given by the equation:*

$$E : y^2 = x^3 + 3x,$$

This is an affine equation that describes an elliptic curve in $\mathbb{A}^2$. To embed this

curve in the projective space $\mathbb{P}^2$, we introduce homogeneous coordinates $[x : y : z]$ and rewrite the equation as:

$$E : y^2z = x^3 + 3xz^2.$$

This equation defines a projective variety in $\mathbb{P}^2$, meaning it is a solution set of homogeneous polynomials. Since it is irreducible, it qualifies as a variety. This projective elliptic curve remains a smooth, irreducible algebraic variety in $\mathbb{P}^2$, making it a projective variety.

Definition 1.1.13. *Two algebraic curves C_1 and C_2 over a field K are said to be isomorphic if there exists a bijective morphism*

$$\varphi : C_1 \to C_2$$

such that both φ and its inverse φ^{-1} are regular maps.
This means C_1 and C_2 have the same algebraic structure, and can be transformed into one another via an algebraic change of coordinates.
In particular, isomorphic curves have the same genus and are indistinguishable from the point of view of algebraic geometry.

Example 7. *Consider the curve:*

$$E_1 : y^2 = x^3 - x, \quad E_2 : y^2 = x^3 - 4x.$$

Defining the map as follows,

$$\varphi : E_1 \to E_2, \quad (x, y) \mapsto (2x, 2\sqrt{2}y).$$

We verify that this is a morphism between the two curves:

Substitute $x' = 2x$, $y' = 2\sqrt{2}y$ into the equation of E_2:

$$y'^2 = (2\sqrt{2}y)^2 = 8y^2, \quad x'^3 - 4x' = (2x)^3 - 4(2x) = 8x^3 - 8x = 8(x^3 - x).$$

So:

$$y'^2 = 8y^2 = 8(x^3 - x) = x'^3 - 4x'.$$

Hence, $(x', y') = \varphi(x, y) \in E_2$, and the map is valid.

The inverse map is:

$$\varphi^{-1}(x, y) = \left(\frac{x}{2}, \frac{y}{2\sqrt{2}}\right),$$

which maps points on E_2 back to E_1. Therefore, $E_1 \cong E_2$ over $\mathbb{C}$.

One of the important result in algebraic geometry is Bézout's Theorem because it establishes a deep connection between the geometry of algebraic curves and the algebraic properties of their defining equations.

Theorem 1.1.1 (Bézout's Theorem)**.** *Let C_1 and C_2 be two projective algebraic curves in $\mathbb{P}^2$ given by homogeneous polynomials of degrees d_1 and d_2, respectively. Then the total number of intersection points of C_1 and C_2, counted with multiplicities, is given by*

$$d_1 \cdot d_2.$$

One of the fundamental theorems in algebraic geometry is Riemann-Roch Theorem which provides a way to compute the dimension of the space of meromorphic functions (or sections of line bundles) on a curve, and it has deep implications in both geometry and topology. Before presenting the theorem, we will first define the concepts of genus, divisors, and the degree of a divisor.

Definition 1.1.14. *Let C be a smooth projective algebraic curve over a field K. A divisor D on C is a formal sum of points:*

$$D = \sum_{P \in C} n_P P, \quad n_P \in \mathbb{Z},$$

where all but finitely many n_P are zero.

The degree of the divisor D is defined as:

$$\deg(D) = \sum_{P \in C} n_P.$$

Definition 1.1.15. *Let C be a smooth projective algebraic curve. The group of divisors on C, denoted* $\mathrm{Div}(C)$*, is defined as:*

$$\mathrm{Div}(C) = \left\{ \sum_{P \in C} n_P \cdot P \,\middle|\, n_P \in \mathbb{Z}, \text{ and } n_P = 0 \text{ for all but finitely many } P \right\}$$

The group of degree zero divisors on C is the subgroup:

$$\mathrm{Div}^0(C) = \{D \in \mathrm{Div}(C) \,|\, \deg(D) = 0\}$$

Definition 1.1.16. *A rational function $f \in K(X)^\times$ defines a principal divisor:*

$$\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f) \cdot P$$

The set of all such divisors forms the subgroup of principal divisors:

$$\mathrm{Prin}(C) = \left\{ \mathrm{div}(f) \mid f \in K(X)^{\times} \right\} \subseteq \mathrm{Div}^0(C)$$

Definition 1.1.17. *Given a divisor D, the associated space of rational functions is:*

$$L(D) = \{ f \in K(X)^{\times} \mid Div(f) + D \geq 0 \} \cup \{0\}.$$

The dimension of $L(D)$ is denoted by $\ell(D)$.

Definition 1.1.18. *The genus g of a curve C is an invariant given by:*

$$g = \dim H^1(C, \mathcal{O}_C).$$

Definition 1.1.19. *A canonical divisor W on a curve C is a divisor associated with a differential form on C. That is, if ω is a nonzero meromorphic differential on C, then the divisor of ω is given by:*

$$div(\omega) = \sum_{P \in C} v_P(\omega) P,$$

where $v_P(\omega)$ is the order of ω at P. The canonical divisor W is any divisor linearly equivalent to $div(\omega)$.

*The **degree** of a canonical divisor satisfies:*

$$\deg(W) = 2g - 2,$$

where g is the genus of the curve.

Theorem 1.1.2 (Riemann-Roch Theorem)**.** *Let W be a canonical divisor of a smooth projective algebraic curve C of genus g. For each divisor D on C*

$$\ell(D) - \ell(W - D) = \deg(D) - g + 1.$$

1.2 Elliptic curves

Elliptic curves play a fundamental role in algebraic geometry, number theory, and cryptography. A key property that makes elliptic curves so powerful in these fields is their natural group structure, which arises from a geometric construction based on the Weierstrass equation. This part introduces the definition of an elliptic curve and develops the algebraic structure that turns it into a group.

Definition 1.2.1. *An elliptic curve is a non-singular, projective algebraic curve of genus one, with a specified point at infinity. Let E be an elliptic curve defined over a field K with Weierstrass equation of the form*

$$E: \quad y^2 = x^3 + Ax + B \tag{1.1}$$

where $A, B \in K$ and the discriminant, $\Delta = 4A^3 + 27B^2 \neq 0$.

Here, we need to clarify how we have used the specific form of the elliptic curve equation. An elliptic curve E over a field K is expressed in its general Weierstrass form using non-homogeneous coordinates x and y as:

$$E: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2a_4x + a_6$$

where $a_1, ..., a_6 \in K$ and with a point at infinity $\mathcal{O} = [0, 1, 0]$. We can simplify the general form of the Weierstrass equation if characteristic of $\bar{K}$ is not 2, by completing the square. The substitution by $1/2(y - a_1x - a_3)$ for y gives an equation of the form

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

where $b_2 = a_1^2 + 4a_4$, $b_4 = 2a_4 + a_1a_3$ and $b_6 = a_3^2 + 4a_6$, with extra restriction, if $char(\bar{K}) \neq 2, 3$, then the substitution

$$(x, y) \longmapsto (\frac{x - 3b^2}{36}, \frac{y}{108})$$

gives an equation simpler,

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

and in the equation (1.1) $A = -27c_4$ and $B = -54c_6$ where $c_4 = b_2^2 - 24b_4$ and $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$. Consequently, if characteristic of K is not 2 or 3 the elliptic curve has a Weierstrass equation of the form appearing in equation (1.1).

Let E and E' be two elliptic curves defined by the Weierstrass equations $y^2 = x^3 + Ax + B$ and $y'^2 = x'^3 + A'x' + B'$, respectively. Then E and E' are said to be isomorphic if $x = u^2x'$ and $y = u^3y'$ for some non-zero u. In that case, we can see that $A = u^4A'$, $B = u^6B'$ and $\Delta = u^{12}\Delta'$.

Definition 1.2.2. *Let E be an elliptic curve with Weierstrass equation of the form*

$$E : y^2 = x^3 + Ax + B$$

and the discriminant as follows

$$\Delta = -16(4A^3 + 27B^2) \neq 0$$

the j-invariant is given by

$$j(E) = -1728\frac{(4A)^3}{\Delta}.$$

Two elliptic curves E_1 and E_2 defined over K are isomorphic over $\bar{K}$ if and only if they have the same j-invariant, i.e.,

$$j(E_1) = j(E_2) \quad \Longleftrightarrow \quad E_1 \cong E_2.$$

1.2.1 The Group structure of an Elliptic Curve

An elliptic curve E defined by a Weierstrass equation in the projective plane $\mathbb{P}^2$ contains a distinguished point at infinity, denoted by $\mathcal{O}$, which will serve as the identity element in the group structure. The fundamental idea behind the group law is that a line intersecting E at three points defines a well-defined binary operation which will be called the composition law. Specifically, given two points P and Q on E, the third intersection point of the line passing through them determines their sum under this operation.

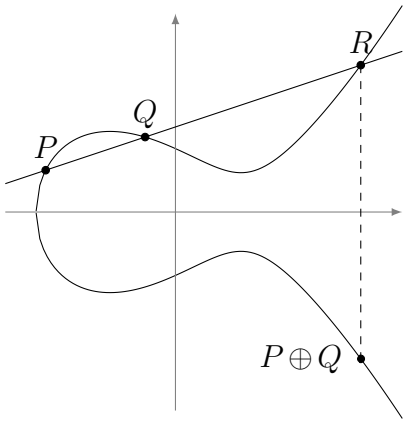

Figure 1: $y^2 = x^3 + Px + Q, \quad P, Q \in \mathbb{Q}$.

Definition 1.2.3. ***Composition Law*** *The composition law is a binary operation on the set of points of elliptic and hyperelliptic curves. Given two points P and Q on the curve, let L be the line passing through P and Q (or the tangent line at P if $P = Q$). The line L intersects the curve at a third point R. The composition law defines $P \oplus Q$ as the reflection of R across the x-axis and let $R = (x, y)$, then its reflection across the x-axis is given by $-R = (x, -y)$,*

$$P \oplus Q = -R = (x, -y).$$

With the following properties of the composition law, an elliptic curve E is an abelian group with identity element $\mathcal{O}$ (the point at infinity).

Properties of the Composition Law:

- For any two points P, Q on an elliptic curve E, their composition $P \oplus Q$ is also a point on E, ensuring that the set of points on the elliptic curve is closed under the composition law.
- The associativity property holds for the composition law, meaning that for any three points $P, Q, R \in E$,

$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R).$$

- The identity element in the composition law of an elliptic curve is an unique point, which is the point at infinity $\mathcal{O}$. For all $P \in E$,

$$P \oplus \mathcal{O} = \mathcal{O} \oplus P = P$$

- Every point on the elliptic curve has a unique inverse element, if $P = (x, y) \in E$,

then the inverse of P is $-P = (x, -y)$,

$$P \oplus -P = -P \oplus P = \mathcal{O}.$$

geometrically the inverse of P reflecting P across the x-axis.

- The composition law is commutative, meaning that for any two points $P, Q \in E$,

$$P \oplus Q = Q \oplus P.$$

Definition 1.2.4. *If the curve E is defined over a field K, then the set of K-rational points*

$$E(K) = \{(x, y) \in K^2 \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\}$$

forms a subgroup of E under the composition law. The group $E(K)$ is called the Mordell-Weil group of E.

Definition 1.2.5. *The torsion subgroup of $E(K)$, denoted by $E_{tors}(K)$, consists of all points in $E(K)$ that have finite order under the group law. $E_{tors}(K)$ is the union of $n-$torsion subgroups, denoted by $E[n]$, where $n \geq 1$ is a positive integer, namely*

$$E[n] = \{P \in E(K) : [n]P = \mathcal{O}\}$$

where $\mathcal{O}$ is the identity element. The torsion group $E_{tors}(K)$ is a finite group.

Definition 1.2.6. *Let $P = (x, y)$ be a point on an elliptic curve E defined over K. We say that P has finite order n if $nP = \mathcal{O}$, where $\mathcal{O}$ is the identity element of the group. In this case, we call P an n-torsion point. The set of all such points is denoted $E[n]$.*

To determine the coordinates of n-torsion points, we use the division polynomials of E. For an elliptic curve given by $E : y^2 = x^3 + ax + b$, the first few division polynomials are:

$$\begin{aligned}
&\psi_1 = 1,\\
&\psi_2 = 2y,\\
&\psi_3 = 3x^4 + 6ax^2 + 12bx - a^2,\\
&\psi_4 = 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3),
\end{aligned}$$

and recursively for $m \geq 2$,

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3,$$
$$\psi_{2m} = \frac{\psi_m}{2y}\left(\psi_{m+2}\psi_{2m-1} - \psi_{m-2}\psi_{2m+1}\right).$$

These polynomials lie in $\mathbb{Z}[x, y, a, b]$, and a point $P = (x, y)$ is an n-torsion point if and only if $\psi_n(x, y) = 0$.

The complete classification of torsion subgroups over arbitrary number fields is still ongoing. However, L. Merel proved the following boundedness result:

Theorem 1.2.1 ([9], Merel)**.** *For every integer $d \geq 1$, there exists a constant $N(d)$ such that for all number fields K with $[K : \mathbb{Q}] = d$, and for all elliptic curves E/K,*

$$\#E(K)_{tors} \leq N(d).$$

Theorem 1.2.2 ([8], Mazur)**.** *If E is defined over $\mathbb{Q}$, then $E(\mathbb{Q})_{tors}$ is isomorphic to one of:*

- $\mathbb{Z}/m\mathbb{Z}$*, where* $1 \leq m \leq 10$ *or* $m = 12$*,*
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$*, where* $1 \leq m \leq 4$*.*

Theorem 1.2.3 ([5], M. A. Kenku, F. Momose)**.** *If E is defined over a quadratic field K, then $E(K)_{tors}$ is isomorphic to one of the following 26 groups:*

- $\mathbb{Z}/m\mathbb{Z}$*, where* $1 \leq m \leq 18$*,* $m \neq 17$*,*
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$*, where* $1 \leq m \leq 6$*,*
- $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3m\mathbb{Z}$*, where* $m = 1, 2$*,*
- $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$*.*

Theorem 1.2.4 ([2], Derickx, Etropoloski, Morrow, Zuerick-Brown and Van Hoeij)**.** *Let E be an elliptic curve defined over a* cubic number field *K. Then the torsion subgroup $E(K)_{\text{tors}}$ is isomorphic to one of the following 27 groups:*

- $\mathbb{Z}/m\mathbb{Z}$ *for* $m = 1, 2, \ldots, 18, 20, 21$*,*
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$ *for* $1 \leq m \leq 7$*.*

Theorem 1.2.5 (Mordell-Weil Theorem)**.** *Let E be an elliptic curve defined over a number field K and let $E(K)$ be the Mordeil-Weil group. Then $E(K)$ is a finitely generated abelian group. In particular,*

$$E(K) \cong \mathbb{Z}^r \oplus E_{tors}(K)$$

for some non-negative integer r, called the rank of the elliptic curve.

Example 8. *Consider the elliptic curve E defined over $\mathbb{Q}$ given by the equation:*

$$E : y^2 = x^3 - x.$$

all rational points of $E(\mathbb{Q})$ come from its finite torsion subgroup. The torsion subgroup of E consists only of 2-torsion points, i.e.,

$$E(\mathbb{Q}) = E_{tors}(\mathbb{Q}) = E[2](\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

which consists of the points

$$E[2](\mathbb{Q}) = \{\mathcal{O}, (0,0), (1,0), (-1,0)\}.$$

Since there are no points of infinite order in $E(\mathbb{Q})$, the rank of $E(\mathbb{Q})$ is 0.

Example 9. *An elliptic curve with positive rank has at least one rational point of infinite order in its Mordell–Weil group. Consider the elliptic curve:*

$$E : y^2 = x^3 - x + 1.$$

This curve has rank 1. In fact, $E(\mathbb{Q}) \cong \mathbb{Z}$. The Mordell-Weil group $E(\mathbb{Q})$ is generated by the point $(1,1)$.

1.2.2 Twists of an Elliptic Curve

In what follows, we define a twist of an algebraic smooth curve.

Definition 1.2.7. *Let C be a smooth projective curve defined over a field K. A twist of C is a smooth projective curve C' such that there exists an isomorphism:*

$$\varphi : C' \to C$$

defined over an algebraic closure $\bar{K}$ of K, but not necessarily over K itself. Two twists are considered equivalent if they are isomorphic over K.

Definition 1.2.8. *Let E be an elliptic curve over a field K, a twist of E is another elliptic curve E' over K that is isomorphic to E over an algebraic extension of K, but not isomorphic over K itself.*

If is known that if two elliptic curves E and E' defined over K are isomorphic over

$\bar{K}$, then E and E' have the same j-invariant. In particular, an elliptic curve and any of its twists possess the same j-invariant.

Quadratic Twist: Let $D \in K^*$ and E be an elliptic curve with j-invariant $j(E) \neq 1728, 0$, given in its general Weierstrass form:

$$E : y^2 = x^3 + Ax + B.$$

The quadratic twist of E by D is defined by the equation

$$E^D : y^2 = x^3 + D^2Ax + D^3B$$

For elliptic curves with special form of the j-invariant $j(E) = 1728$, in particular $B = 0$, a quadratic twist of E is given by

$$E^D : y^2 = x^3 + DAx.$$

For the special form of E with $j(E) = 0$, in particular $A = 0$, a quadratic twist of E is given by

$$E^D : y^2 = x^3 + DB.$$

These quadratic twists define elliptic curves that are isomorphic over the field $K(\sqrt{D})$.

Example 10. *Consider the elliptic curve*

$$E : y^2 = x^3 - x.$$

The quadratic twist by D is given by

$$E^D : y^2 = x^3 - Dx.$$

For example, if $D = -1$, the corresponding twist is

$$E^{-1} : y^2 = x^3 + x.$$

This curve is isomorphic to E over $\mathbb{Q}(i)$, but not over $\mathbb{Q}$.

Definition 1.2.9. *Let E be an elliptic curve defined over the complex numbers $\mathbb{C}$. The set of all holomorphic endomorphisms of E, denoted* $\mathrm{End}(E)$*, forms a ring under pointwise addition and composition.*

In general, $\mathrm{End}(E) \cong \mathbb{Z}$*, consisting only of the integer multiplication maps. However,*

if

$$\mathrm{End}(E) \supsetneq \mathbb{Z},$$

then E is said to have complex multiplication *(CM). More precisely, E has complex multiplication if*

$$\mathrm{End}(E) \cong \mathcal{O}_K,$$

where $\mathcal{O}_K$ is an order in an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-d})$ for some square-free positive integer d.

In this case, the endomorphism ring of E contains not only the integer multiplications but also additional endomorphisms corresponding to elements of $\mathcal{O}_K$, the ring of integers in the field K.

Elliptic curves with complex multiplication play a central role in the theory of modular forms, class field theory, and explicit class field constructions

1.2.3 Hyperelliptic curves

A hyperelliptic curve is a generalization of an elliptic curve with genus greater than or equal to 2. An elliptic curve allows us to define a natural group structure. When we move to hyperelliptic curves, we are dealing with curves of genus ≥ 2. Unlike elliptic curves, the points on a hyperelliptic curve do not form a group under a similar geometric addition law. Instead, we consider a higher-dimensional algebraic object called the Jacobian variety of the curve, denoted as J(C), where C is the hyperelliptic curve.

Definition 1.2.10. *A Hyperelliptic Curve over a field K is a smooth, projective, algebraic curve of the form*

$$C : y^2 = f(x)$$

where $f(x)$ is a square-free polynomial degree of $2g+1$ or $2g+2$ with no repeated roots, ensuring smoothness.

The genus of a hyperelliptic curve defined by $y^2 = f(x)$ is given by $\lfloor (\deg f - 1)/2 \rfloor$.

Definition 1.2.11 (Jacobian Variety)**.** *Let H be a hyperelliptic curve of genus $g \geq 1$, defined over a field K. The Jacobian variety of H, denoted by* $\mathrm{Jac}(H)$*, is an abelian variety of dimension g defined over K, which parametrizes degree-zero divisor classes on H.*

Formally, it is given by

$$\mathrm{Jac}(H) := \mathrm{Pic}^0(H) = \mathrm{Div}^0(H)/\mathrm{Prin}(H) = \frac{\{\textit{divisors of degree } 0\}}{\textit{linear equivalence}}.$$

The group $\mathrm{Jac}(H)(K)$ *of* K*-rational points of the Jacobian carries a natural abelian group structure and plays a central role in arithmetic geometry.*

One may define quadratic twists of a hyperelliptic curve in a similar fashion to quadratic twists of elliptic curves.

Definition 1.2.12. *Let* H *be a hyperelliptic curve defined over a field* K *of characteristic different from 2, given by*

$$H : y^2 = f(x),$$

where $f(x) \in K[x]$ *is a square-free polynomial of degree at least 3.*

Let $D \in K^\times \setminus (K^\times)^2$ *be a non-square in* K*. The quadratic twist of the curve* H *by* D *is the curve*

$$H^D : y^2 = D \cdot f(x).$$

The curves H *and* H^D *are not isomorphic over* K*, but they become isomorphic over the quadratic extension field* $K(\sqrt{D})$*.*

Definition 1.2.13. *Let* H *be a Hyperelliptic Curve defined over a field* K*,*

$$H : y^2 = x^m + a$$

where m *is an odd integer equal or greater than* 3 *and* $a \in K$*.* H_m^D *is* D*th* m*-twist of* H *given by*

$$H_m^D : y^2 = Dx^m + a$$

In this case, the curves H *and its* m*-twist* H_m^D *are isomorphic over the extension field* $\mathbb{Q}(\sqrt[m]{D})$*, where* $D \in \mathbb{Q}^\times$ *is such that the exponent of at least one prime in its prime factorization is relatively prime to* m*.*

Example 11. *Let* $m = 5$*,* $a = 1$*, and* $D = 3$*. Then the original curve is*

$$H : y^2 = x^5 + 1,$$

and the 5*-twist by* $D = 3$ *is given by*

$$H_5^{(3)} : y^2 = 3x^5 + 1.$$

Definition 1.2.14. *Let* H *be a Hyperelliptic Curve defined over a field* K*,*

$$H : y^2 = x^m + a$$

where m is an odd integer equal or greater than 3 and $a \in K$. H_{2m}^D is Dth $2m$-twist of H given by

$$H_{2m}^D : y^2 = x^m + Da$$

the curve H and its $2m$-twist H_{2m} are isomorphic over the field $K(\sqrt[2m]{D})$, provided that the rational number D has at least one prime factor whose exponent is not divisible by $2m$.

Example 12. *Consider the hyperelliptic curve H defined over $\mathbb{Q}$:*

$$H : y^2 = x^5 + 1,$$

where $m = 5$ and $a = 1$.

Let $D = 3$. The $2m$-twist of the curve H by D is defined as:

$$H_{10}^{(3)} : y^2 = x^5 + aD = x^5 + 3.$$

The curves H and $H_{10}^{(3)}$ are isomorphic over the field $\mathbb{Q}(\sqrt[10]{3})$.

1.3 Elliptic Surfaces

1.3.1 Elliptic Curves over Function Fields

Let K be a number field and V be an algebraic variety defined over K. The function field of V, denoted by $K(V)$, is the field of rational functions on V

$$K(V) = \{f/g : f, g \in K[V], g \neq 0\}$$

where $K[V]$ is the coordinate ring of V.

Given an elliptic curve E over the function field $K(V)$, one can specialize E at points $t \in V$ to obtain elliptic curves E_t over K. This specialization process ensures that, for almost all values of t, the resulting curve preserves the essential properties of E.

A fundamental result in this context states that the Mordell–Weil theorem applies to function fields, implying that the group of rational points $E(K(V))$ is finitely generated.

Definition 1.3.1. *(specialization of E) Let V be a variety over a number field K, and consider an elliptic curve E defined over the function field $K(V)$ by the Weierstrass equation*

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

where the coefficients $a_1, \ldots, a_6$ are rational functions in $K(V)$. For almost all points $t \in V$, these functions take well-defined values, allowing us to define a specialization of E at t as the elliptic curve

$$E_t : y^2 + a_1(t)xy + a_3(t)y = x^3 + a_2(t)x^2 + a_4(t)x + a_6(t),$$

which is now an elliptic curve over K.

If $P = (x, y) \in E(K(V))$, meaning x and y are rational functions in $K(V)$, then for almost all t, these functions specialize to give a point

$$P_t = (x(t), y(t)) \in E_t(K).$$

Definition 1.3.2. *(specialization homomorphism) Given an elliptic curve E defined over a function field $K(V)$, the specialization homomorphism is defined by*

$$\sigma_t : E(K(V)) \to E_t(K),$$

$$(x, y) \mapsto (x(t), y(t))$$

which maps a point on $E(K(V))$ to its specialization on $E_t(K)$. This map is a group homomorphism.

The idea that an elliptic surface can be understood as a family of elliptic curves parameterized by a single variable. As an example, consider the following family

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

with rational functions $A(T), B(T) \in K(T)$. More generally, one can fix a non-singular projective curve C/K and consider the Weierstrass equation

$$E : y^2 = x^3 + Ax + B$$

for some $A, B \in K(C)$ with $4A^3 + 27B^2 \neq 0$. Then for almost all points $t \in C(\bar{K})$

evaluating A and B at t yields an elliptic curve

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

Rather than evaluating the functions A and B at specific points of the curve C, we treat the parameter t as a variable, on equal footing with x and y. Accordingly, we consider the subvariety of $\mathbb{P}^2 \times C$ of dimension two determined by

$$\mathcal{E} = \left\{([X,Y,Z],t) \in \mathbb{P}^2 \times C : Y^2Z = X^3 + A(t)XZ^2 + B(t)Z^3\right\}.$$

$\mathcal{E}$ is a surface derived from a family of elliptic curves.

Theorem 1.3.1 ([12], Silverman's Specialization Theorem)**.** *Consider a non-split elliptic surface $\mathcal{E} \to C$ defined over a number field K, where C is a non-singular projective curve. Let $\delta \in \mathrm{Div}(C)$ be a divisor on C whose degree is positive. Then there exists a constant $c > 0$ such that the specialization map*

$$\sigma_t : E(K) \longrightarrow \mathcal{E}_t(\bar{K})$$

is injective for all points $t \in C(\bar{K})$ satisfying the height condition $h_\delta(t) \leq c$.

In other words, the set of points t for which the map σ_t fails to be injective is a set of bounded height. In particular, the map

$$\sigma_t : E(K) \to \mathcal{E}_t(\bar{K})$$

is injective for all but finitely many points $t \in C(K)$.

Example 13. *Consider the elliptic curve defined over the function field $\mathbb{Q}(t)$ by the Weierstrass equation:*

$$E_t : y^2 = x^3 + (t^2 - 1)x + t.$$

Here, the coefficients are rational functions in t, so E_t is an elliptic curve defined over the function field $\mathbb{Q}(t)$.

Now, let's specialize this curve at $t = 1$. By substituting $t = 1$ into the equation, we get the specialized elliptic curve over $\mathbb{Q}$:

$$E_1 : y^2 = x^3 + (1^2 - 1)x + 1 = x^3 + 1.$$

Thus, the elliptic curve E_1 defined over $\mathbb{Q}$ is:

$$E_1 : y^2 = x^3 + 1.$$

This is a well-known elliptic curve, commonly referred to as the elliptic curve with the equation $y^2 = x^3 + 1$. *The point* $(0, 1)$ *is a rational point on* E_1.

2. TWISTS OF TUPLES OF ELLIPTIC AND HYPERELLIPTIC CURVES

2.1 VARIATIONS ON TWISTS OF ELLIPTIC CURVES

The main theorems investigate the existence of a rational function $D(u, v, w) \in \mathbb{Q}(u, v, w)$ such that the specific twists of three elliptic curves have a positive rank over the field $\mathbb{Q}(u, v, w)$. The main distinction among the theorems lies in the types of twists and assumptions about the curves.

The first theorem considers a general setup of the problem. The authors consider a quadratic twist of an elliptic curve with arbitrary j-invariant and a cubic twists of two other elliptic curves with $j = 0$. This serves as a natural extension of earlier results by Kuwata and Wang. Another result advances this framework by replacing cubic twists with sextic twists, which are algebraically more intricate and require more sophisticated parametrization but still apply to any choice of such elliptic curves. Finally, assuming $j = 0$ for all elliptic curves, the authors introduce a more symmetric treatment involving two cubic twists and one sextic twist. This case leverages the special properties of elliptic curves with $j = 0$, allowing all curves to admit higher twists and yielding a more unified algebraic system.

Let us introduce the polynomial $f(x) = x^3 + mx + a$. Curves with non-zero j-invariant (i.e., $m \neq 0$) typically only admit quadratic twists. Curves with $j = 0$ (i.e., $m = 0$) admit higher-degree twists like cubic and sextic twists. In order to construct the desired rational functions that define the twists, we must find parametric solutions to the following sets of equations:

Case (1): One Quadratic Twist and Two Sextic Twists

Consider the following elliptic curves:

$$E_1 : y^2 = x^3 + mx + a, \quad E_2 : y^2 = x^3 + b, \quad E_3 : y^2 = x^3 + c,$$

where $m, a, b, c \in \mathbb{Q}$. When twisting E_1 quadratically and E_2, E_3 cubically by a common parameter $D_{2,3,3}$, we require:

$$D_{2,3,3} = \frac{f(x_1)}{y_1^2} = \frac{y_2^2 - b}{x_2^3} = \frac{y_3^2 - c}{x_3^3},$$

where $f(x) = x^3 + mx + a$.

Case (2): One Quadratic Twist and Two Sextic Twists

Using the same elliptic curves:

$$E_1 : y^2 = x^3 + mx + a, \quad E_2 : y^2 = x^3 + b, \quad E_3 : y^2 = x^3 + c,$$

a quadratic twist is applied to E_1, and sextic twists to E_2 and E_3. The twisting parameter $D_{2,6,6}$ must satisfy:

$$D_{2,6,6} = \frac{f(x_1)}{y_1^2} = \frac{y_2^2 - x_2^3}{b} = \frac{y_3^2 - x_3^3}{c}.$$

Case (3): Two Cubic Twists and One Sextic Twist

Assume $m = 0$, so the elliptic curves become:

$$E_1 : y^2 = x^3 + a, \quad E_2 : y^2 = x^3 + b, \quad E_3 : y^2 = x^3 + c.$$

Here, we apply cubic twists to E_1 and E_2, and a sextic twist to E_3. The condition on the common twisting parameter $D_{3,3,6}$ is:

$$D_{3,3,6} = \frac{y_1^2 - a}{x_1^3} = \frac{y_2^2 - b}{x_2^3} = \frac{y_3^2 - x_3^3}{c}.$$

Each system ensures that a single rational function D simultaneously serves as the twist factor for all three curves, matching the respective type of twist—quadratic, cubic, or sextic—assigned to each.

Quadratic Twist and Two Cubic Twists

Theorem 2.1.1 ([16], Theorem 2.1)**.** *Let $m,a,b,c \in \mathbb{Z}$, and consider the elliptic curves:*

$$E_1 : y^2 = x^3 + mx + a,$$
$$E_2 : y^2 = x^3 + b,$$
$$E_3 : y^2 = x^3 + c,$$

with $bc \neq 0$ and $4m^3 + 27a^2 \neq 0$. Then there exists a rational function

$$D_{2,3,3}(u,v,w) \in \mathbb{Q}(u,v,w)$$

such that, the quadratic twist of E_1 by $D_{2,3,3}$, the cubic twists of E_2 and E_3 by $D_{2,3,3}$, each have positive rank over the field $\mathbb{Q}(u,v,w)$.

Proof. To find a rational function $D_{2,3,3}(u,v,w)$ such that the quadratic twist of the elliptic curve E_1 and the cubic twists of E_2 and E_3 all have positive rank, they begin with the system:

$$\frac{f(x_1)}{y_1^2} = \frac{y_2^2 - b}{x_2^3} = \frac{y_3^2 - c}{x_3^3},$$

where $f(x) = x^3 + mx + a$. We require that $x_i y_i \neq 0$ for $i = 1,2,3$, and $f(x_1)(y_2^2 - b)(y_3^2 - c) \neq 0$.

They make the rational substitutions:

$$x_1 = u, \quad x_2 = \frac{1}{v^2 T}, \quad x_3 = \frac{1}{T}, \quad y_1 = \frac{1}{T}, \quad y_2 = p, \quad y_3 = q,$$

with parameters $u,v \in \mathbb{Q}$, and unknowns p,q,T. Substituting these into the system yields:

$$T^2 f(u) = v^6 T^3 (p^2 - b) = T^3 (q^2 - c).$$

Solving, we get the equivalent system:

$$T = \frac{f(u)}{v^6(p^2 - b)}, \qquad v^6(p^2 - b) = q^2 - c.$$

The second equation defines a genus-zero curve C_1 over $\mathbb{Q}(v)$ with a rational point at infinity $[p : q : r] = [1 : v^3 : 0]$. Parameterizing C_1 via standard methods gives:

$$p = \frac{(b + w^2)v^6 - c}{2wv^6}, \quad q = \frac{(b - w^2)v^6 - c}{2wv^3},$$

where $w \in \mathbb{Q}$ is a free parameter.

Using this, we obtain:

$$T(u,v,w) = \frac{4w^2v^6f(u)}{v^{12}w^4 - 2v^6(bv^6+c)w^2 + (bv^6-c)^2}.$$

Then, they define the desired twist parameter:

$$D_{2,3,3}(u,v,w) = f(u)\cdot T(u,v,w)^2.$$

Now, they construct rational points on the twisted curves:

$$P_1 = \left(uf(u)T^2, f(u)^2T^3\right)$$

lies on the quadratic twist of E_1 by $D_{2,3,3}$, and

$$P_2 = \left(\frac{1}{v^2}f(u)T, f(u)pT^2\right), \quad P_3 = \left(f(u)T, f(u)qT^2\right)$$

lie on the cubic twists of E_2 and E_3, respectively.

Since $x_iy_i \neq 0$ and $D_{2,3,3}$ is not a sixth power, the twists are not isomorphic to curves over $\mathbb{Q}$. Thus, each point P_i is of infinite order, so the associated twists have positive rank over $\mathbb{Q}(u,v,w)$. □

The following 3 corollaries are derived from the results established by M. Ulas([16], Corollary 2.2, 2.4, 2.5);

For elliptic curves of the form $E_1 : y^2 = x^3 + mx + a$, $E_2 : y^2 = x^3 + b$, and $E_3 : y^2 = x^3 + c$, it is established that there exist infinitely many rational numbers $d \in \mathbb{Q}$ such that the quadratic twist of E_1 by d, and the cubic twists of E_2 and E_3 by d, all possess positive Mordell–Weil rank. Additionally, in the case involving only two curves, one can construct a rational function $D_{2,3}(u,v,w)$ such that the quadratic twist of E_1 by $D_{2,3}$ has positive rank, and the cubic twist of E_2 by $D_{2,3}$ attains rank at least two. As a consequence, the set of such twisting parameters $d \in \mathbb{Q}$ is infinite.

Quadratic Twist and Two Sextic Twists

Theorem 2.1.2 ([16], Theorem 3.1)**.** *Let $m,a,b,c \in \mathbb{Z}$, and consider the elliptic curves:*

$$E_1 : y^2 = x^3 + mx + a,$$
$$E_2 : y^2 = x^3 + b,$$
$$E_3 : y^2 = x^3 + c,$$

with $bc \neq 0$ *and* $4m^3 + 27a^2 \neq 0$. *Then there exists a rational function*

$$D_{2,6,6}(u, v, w) \in \mathbb{Q}(u, v, w)$$

such that, the quadratic twist of E_1 *by* $D_{2,6,6}$*, the sextic twists of* E_2 *and* E_3 *by* $D_{2,6,6}$*, each have positive rank over the field* $\mathbb{Q}(u, v, w)$.

Proof. The strategy is the same as in Theorem 2.1.1, with the only difference being that we now employ sextic twists instead of cubic twists. □

Two Cubic Twists and a Sextic Twist

Theorem 2.1.3 ([16], Theorem 4.1)**.** *Let* $a, b, c \in \mathbb{Z} \setminus \{0\}$*, and consider the elliptic curves:*

$$E_1 : y^2 = x^3 + a,$$
$$E_2 : y^2 = x^3 + b,$$
$$E_3 : y^2 = x^3 + c.$$

Then there exists a rational function

$$D_{3,3,6}(u, v, w) \in \mathbb{Q}(u, v, w)$$

such that, the cubic twists of E_1 *and* E_2 *by* $D_{3,3,6}$*, the sextic twist of* E_3 *by* $D_{3,3,6}$*, each have positive rank over the field* $\mathbb{Q}(u, v, w)$.

Proof. The proof proceeds by the same method as in the earlier case. By constructing a rational parametric solution to the relevant system and verifying that the resulting points have infinite order, the desired conclusion is obtained. □

2.2 VARIATIONS ON TWISTS OF HYPERELLIPTIC CURVES

The paper [3] by Jędrzejak and Ulas can be viewed as a natural and significant generalization of Ulas's earlier work [16] on elliptic curves. While the paper [16] focused on constructing rational functions that induce simultaneous twists of multiple elliptic curves with positive rank, the paper [3] extends this idea to hyperelliptic and superelliptic curves. Using similar parametric techniques, the authors demonstrate that Jacobians of these higher-genus twisted curves also have

positive rank.

Theorem 2.2.1 ([3], Theorem 2.1)**.** *Let $f \in \mathbb{Q}[x]$ be a square-free polynomial of degree at least 3, and let $m \in \mathbb{N}$ be odd. Then there exists a rational function $D_{2,m,m} \in \mathbb{Q}(u,v,w)$ such that the quadratic twist of the curve $C_1 : y^2 = f(x)$, and the m-twists of the curves $C_2 : y^2 = x^m + b$, $C_3 : y^2 = x^m + c$, all have Jacobians of positive rank over $\mathbb{Q}(u,v,w)$.*

Proof. Let $m = 2n+1$ with $n \in \mathbb{N}$. Consider the system:

$$\frac{f(x_1)}{y_1^2} = \frac{y_2^2 - b}{x_2^m} = \frac{y_3^2 - c}{x_3^m}.$$

To find rational solutions x_i, y_i, we make the substitutions:

$$x_1 = u, \quad x_2 = \frac{1}{v^2 T}, \quad x_3 = \frac{1}{T^n}, \quad y_1 = \frac{1}{T}, \quad y_2 = p, \quad y_3 = q.$$

This reduces the system to:

$$T = \frac{f(u)}{v^{2m}(p^2 - b)}, \quad v^{2m}(p^2 - b) = q^2 - c.$$

The second equation defines a genus zero curve C over $\mathbb{Q}(v)$, with a known rational point at infinity. A rational parametrization of this curve is:

$$p = \frac{(b + w^2)v^{2m} - c}{2wv^{2m}}, \quad q = \frac{(b - w^2)v^{2m} - c}{2wv^m}.$$

Substituting into the expression for T, we get:

$$T(u,v,w) = \frac{4w^2 v^{2m} f(u)}{v^{4m} w^4 - 2v^{2m}(bv^{2m} + c)w^2 + (bv^{2m} - c)^2}.$$

Hence, define:

$$D_{2,m,m}(u,v,w) = f(u) \cdot T(u,v,w)^{m-1}.$$

Now define the points:

$$P_1 = \left(u, \frac{1}{T(u,v,w)^n}\right), \quad P_2 = \left(v^{-2} f(u) T^{m-2}, f(u)^n p T^{n(m-1)}\right),$$

$$P_3 = \left(f(u) T^{m-2}, f(u)^n q T^{n(m-1)}\right).$$

These lie respectively on:

$$C_1' : D_{2,m,m}(u,v,w)y^2 = f(x), \quad C_2' : y^2 = x^m + bD_{2,m,m}(u,v,w),$$

$$C_3' : y^2 = x^m + cD_{2,m,m}(u,v,w).$$

Let J_i be the Jacobians of the curves C_i'. Define divisors $D_i = (P_i) - (\infty)$. Since P_1 is non-constant and C_1' is a non-constant quadratic twist, it follows that D_1 is of infinite order in $J_1(\mathbb{Q}(u,v,w))$.

For D_2, D_3, we apply [[4], Proposition 2.1] which ensures that a divisor $(P) - (\infty)$ is of infinite order in the Jacobian of a hyperelliptic curve if P is non-constant with $y \neq 0$. Thus D_2, D_3 are also of infinite order, completing the proof. □

As a consequence of the main twisting constructions, the authors establish several results concerning the ranks of Jacobians of simultaneously twisted hyperelliptic curves. Specifically, for suitable odd integers m and square-free polynomials $f(x) \in \mathbb{Q}[x]$, they show that there exists a rational function $D_{2,m} \in \mathbb{Q}(u,v,w)$ such that the quadratic twist of the curve $C_1 : y^2 = f(x)$ and the m-twist of the curve $C_2 : y^2 = x^m + b$ both have Jacobians of positive rank, with the latter achieving Jacobians of m-twist of the curve $C_2 : y^2 = x^m + b$ rank at least two. Moreover, for the triple $C_1 : y^2 = f(x)$, $C_2 : y^2 = x^m + b$, $C_3 : y^2 = x^m + c$, there exist infinitely many rational numbers $d \in \mathbb{Q}$ such that the quadratic twist of C_1 by d, and the m-twists of C_2 and C_3 by d, yield Jacobians of positive rank. In particular, the set of such d for which the Jacobian of the quadratic twist of C_1 has positive rank and the Jacobian of the m-twist of C_2 has rank at least two is infinite.

Theorem 2.2.2 ([3], Theorem 3.1)**.** *Let $f \in \mathbb{Q}[x]$ be square-free, and let $m \in \mathbb{N}$ be odd. Then there exists a rational function $D_{2,2m,2m} \in \mathbb{Q}(u,v,w)$ such that the quadratic twist of $C_1 : y^2 = f(x)$, and the $2m$-twists of the curves $C_2 : y^2 = x^m + b$, $C_3 : y^2 = x^m + c$, have Jacobians of positive rank over $\mathbb{Q}(u,v,w)$.*

Proof. The proof follows the same reasoning as in the previous cases. □

Theorem 2.2.3 ([3], Theorem 4.1)**.** *Let $f \in \mathbb{Q}[x]$ be square-free, and let $m \in \mathbb{N}$ be odd. Then there exists a rational function $D_{m,m,2m} \in \mathbb{Q}(u,v,w)$ such that the m-twists of the curves $C_1 : y^2 = f(x)$, $C_2 : y^2 = x^m + b$, and the $2m$-twist of the curve $C_3 : y^2 = x^m + c$, have Jacobians of positive rank over $\mathbb{Q}(u,v,w)$.*

Proof. The proof follows the same steps as in the previous proofs, with the same structure and reasoning applied to this case. □

The next result will be shifting our attention to specific families of superelliptic curves, primarily those defined by the equation

$$C_{m,a}: \quad y^p = x^m(x+a),$$

where p is a prime number and $m \in \mathbb{N}$ with $0 < m < p$, assumed without loss of generality. These curves admit an automorphism given by $(x, y) \mapsto (x, \zeta_p y)$, where ζ_p is a primitive p-th root of unity. The Jacobian $J_{m,a}$ of $C_{m,a}$, defined over $K := \mathbb{Q}(\zeta_p)$, has complex multiplication by $\mathbb{Z}[\zeta_p]$, and the genus of $C_{m,a}$ is $(p-1)/2$.

For any nonzero integer $D \in \mathbb{Z} \setminus \{0\}$ that is not a p-th power, we may consider the p-twist of $C_{m,a}$, denoted $C_{m,a,D}$, given by the equation

$$C_{m,a,D}: \quad Dy^p = x^m(x+a).$$

We are interested in finding values of $D \in \mathbb{Z}$ such that the simultaneous p-twists of $C_{m,a}$ and $C_{m,b}$ by D both admit rational points. As we will show in the following lemma, this is a relatively straightforward problem. A more subtle and interesting question involves the computation of the *torsion subgroup* of the Jacobian $J_{m,a}$ associated with $C_{m,a}$. Understanding the torsion subgroup is crucial for proving that certain divisors have infinite order in $J_{m,a}$. In fact, the analysis of the torsion part of $J_{m,a}$ will constitute the main focus of this section.

We begin by constructing such a function D, which will serve our purpose.

Lemma 2.2.4 ([3], Lemma 5.1)**.** *Let m and p be integers such that $0 < m < p$ and p is an odd prime. Let $a, b \in \mathbb{Z} \setminus \{0\}$. Then there exists a rational function $D_{p,p}(u, v, w, t) \in \mathbb{Q}(u, v, w, t)$ such that the p-twists of the curves*

$$C_1 : y^p = x^m(x+a), \quad C_2 : y^p = x^m(x+b)$$

by $D_{p,p}$ both have rational points. In particular, the Jacobians $J(C_1^{(p)})$ and $J(C_2^{(p)})$ have positive rank over $\mathbb{Q}(u, v, w, t)$.

Proof. To prove the first part of our lemma, we introduce the following substitutions:

$$x_1 = uT, \quad y_1 = vT, \quad x_2 = wT, \quad y_2 = tT,$$

where T needs to be determined, and u, v, w, t are rational parameters. After making these substitutions and performing some simple algebraic manipulations, we are left with a linear equation in the variable T, which takes the form:

$$um(uT + a) = vp(wT + b) = tp.$$

From this, we obtain an expression for T:

$$T = T(u, v, w, t) = \frac{bvpwm - aumtp}{um + 1tp - vpwm + 1}.$$

Summarizing our reasoning, we observe that if

$$D = D(u, v, w, t) = Tm - p \cdot um(uT + a) \cdot vp,$$

then the superelliptic curves $Dyp = xm(x + a)$ and $Dyp = xm(x + b)$ contain $Q(u, v, w, t)$-rational points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, respectively, where x_i and y_i are given by (14) and the expression for T is provided above.

Next, we apply a similar approach to prove the second part of our lemma. Suppose $\gcd(p, m + n) = 1$, so there exist $\alpha, \beta \in \mathbb{N}^+$ such that

$$p\alpha - (m + n)\beta = 1.$$

In order to solve the equation from the statement of our result, we introduce the substitutions:

$$x_1 = uT^\alpha, \quad y_1 = wT^\beta, \quad x_2 = vT^\alpha, \quad y_2 = tT^\beta,$$

where T again needs to be determined, and u, v, w, t are rational parameters.

After these substitutions and some algebraic manipulation, we are left with a linear equation in the variable T of the form:

$$wpT - um + n = aum = tpT - vm + n = bvm.$$

From this, we obtain an expression for T:

$$T = T(u, v, w, t) = \frac{umvm(bun - avn)}{bvmwp - aumtp}.$$

Summarizing our reasoning, we observe that if

$$D = T^\beta nwpT - um + n \cdot aun,$$

then the superelliptic curves $yp = xm(xn + aD)$ and $yp = xm(xn + bD)$ contain $Q(u, v, w, t)$-rational points $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, respectively, where x_i and y_i are given by (16) and the expression for T is provided above.

□

Proposition 1 ([3], Proposition 5.3)**.** *We have*

$$\mathbb{Z}/p\mathbb{Z} \subset J_{m,a}(\mathbb{Q})_{\text{tors}} \subset \mathbb{Z}/2p\mathbb{Z}.$$

Proposition 2 ([3], Proposition 5.6)**.** *If $a \in \mathbb{Z}$ is an odd integer and $p \neq 7$, then the Jacobian $J_{m,a}(\mathbb{Q})$ has no point of order 2.*

Theorem 2.2.5 ([3], Theorem 5.9)**.** *Let $a, b \in \mathbb{Z} \setminus \{0\}$ be odd integers, and let p be an odd prime such that $p \neq 7$. Suppose $0 < m < p-1$. Then there exists a rational function $D_{p,p} \in \mathbb{Q}(u,v,w,t)$ such that the p-twists of the superelliptic curves*

$$C_1 : y^p = x^m(x+a), \quad C_2 : y^p = x^m(x+b)$$

have Jacobians of positive rank over $\mathbb{Q}(u,v,w,t)$.

Proof. Let $D_{p,p} := D(u,v,w,t)$, where D is defined by the expression (15), which was derived in the first part of Lemma 5.1. In the next step, we utilize the results from Propositions 5.3 and 5.6, which provide insight into the structure of $Q(u,v,w,t)$-rational divisors. Specifically, we identify two divisors: $D_1 = (P_1) - (\infty)$ and $D_2 = (P_2) - (\infty)$. Here, P_1 and P_2 are points whose coordinates are given by expression (14). These points are of significant interest because they have infinite order in the Jacobians of the p-twists of the curves C_1 and C_2, respectively, when taken with respect to $D_{p,p}$.

The fact that P_1 and P_2 have infinite order in the Jacobian of these twists suggests an important algebraic property, namely that they are not torsion points, but rather elements with infinite order. This key observation, which follows from the application of the results from Lemmas and Propositions, implies that the divisors D_1 and D_2 are rational with respect to the field $Q(u,v,w,t)$, and the behavior of these divisors in relation to the Jacobians of the curves is crucial for the theorem's conclusion.

Thus, by confirming that the points P_1 and P_2 are of infinite order in the Jacobians of the p-twists of C_1 and C_2, we have shown that the divisors D_1 and D_2 satisfy the necessary conditions for rationality. This ultimately leads to the establishment of the theorem, completing the proof.

□

3. ON TWISTS OF TUPLES OF HYPERELLIPTIC CURVES

3.1 A Quadratic Twist and Three Higher Degree Twists

Let $f(x) \in \mathbb{Q}[x]$ be a square-free polynomial of degree at least 3. Fix odd integers $m_1, m_2, m_3 \geq 3$. We are investigating the existence of non-square rational numbers D such that the Jacobians of the (hyperelliptic) curves

$$C : Dy^2 = f(x), \quad C_1 : y^2 = Dx^{m_1} + a, \quad C_2 : y^2 = Dx^{m_2} + b, \quad C_3 : y^2 = Dx^{m_3} + c$$

are of positive Mordell-Weil rank over $\mathbb{Q}$.

We set $M = \mathrm{lcm}(m_1, m_2, m_3)$, and $M_i = M/m_i$, for $i = 1, 2, 3$. The rational number D can be found by solving the following system of equations:

$$\frac{y_1^2 - a}{x_1^{m_1}} = \frac{y_2^2 - b}{x_2^{m_2}} = \frac{y_3^2 - c}{x_3^{m_3}} = \frac{f(x_4)}{y_4^2}.$$

We require that

$$x_1 x_2 x_3 (y_1^2 - a)(y_2^2 - b)(y_3^2 - c) y_4 f(x_4) \neq 0.$$

We now define a parametric family of solutions:

$$x_1 = \frac{1}{v_1^2 T^{M_1}}, \quad x_2 = \frac{1}{v_2^2 T^{M_2}}, \quad x_3 = \frac{1}{v_3^2 T^{M_3}}, \quad x_4 = u,$$

$$y_1 = p, \quad y_2 = q, \quad y_3 = r, \quad y_4 = \frac{1}{T^{(M-1)/2}}.$$

Then:

$$T = \frac{f(u)}{v_3^{2m_3}(r^2-c)}, \quad v_1^{2m_1}(p^2-a) = v_2^{2m_2}(q^2-b) = v_3^{2m_3}(r^2-c).$$

Geometrically, the second equation defines an intersection $C_{a,b,c}$ of two quadratic surfaces in $\mathbb{P}^3$ over $\mathbb{Q}(v_1, v_2, v_3)$. Since

$$[p : q : r : s] = [\pm v_2^{m_2} v_3^{m_3} : \pm v_1^{m_1} v_3^{m_3} : \pm v_1^{m_1} v_2^{m_2} : 0]$$

are rational points on $C_{a,b,c}$, it follows that $C_{a,b,c}$ is an elliptic curve over $\mathbb{Q}(v_1, v_2, v_3)$. These points form a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Now assume a, b, c are non-zero rational squares. After a transformation, the curve $C_{a,b,c}$ becomes:

$$x^2 - T_1^2 = y^2 - T_2^2 = z^2 - T_3^2,$$

where $T_1 = av_1^{m_1}$, $T_2 = bv_2^{m_2}$, $T_3 = cv_3^{m_3}$.

Proposition 3. *Let C_{T_1,T_2,T_3} be the elliptic curve defined by*

$$x^2 - T_1^2 = y^2 - T_2^2 = z^2 - T_3^2$$

over $\mathbb{Q}(T_1, T_2, T_3)$. Then C_{T_1,T_2,T_3} has positive Mordell-Weil rank over $\mathbb{Q}(T_1, T_2, T_3)$. In particular, for all but a thin set of $(t_1, t_2, t_3) \in \mathbb{Q}^3$, the specialized curve C_{t_1,t_2,t_3} has positive rank over $\mathbb{Q}$.

Proof. The point $[T_1 : T_2 : T_3 : 1] \in C_{T_1,T_2,T_3}(\mathbb{Q}(T_1, T_2, T_3))$ specializes to a point of infinite order when $[1 : 1 : 1 : 0]$ is the identity. By Silverman's specialization theorem [[13],§20, Theorem 20.1], the result follows. □

Now, doubling the point $P := [a : b : c : 1] \in C_{a^2,b^2,c^2}(\mathbb{Q}(v_1, v_2, v_3))$ yields:

$$2P = [w_1 : w_2 : w_3 : 1],$$

where

$$w_1 = \frac{a^2b^2v_1^{2m_1}v_2^{2m_2} + a^2c^2v_1^{2m_1}v_3^{2m_3} - b^2c^2v_2^{2m_2}v_3^{2m_3}}{2abcv_1^{m_1}v_2^{m_2}v_3^{m_3}},$$

$$w_2 = \frac{a^2b^2v_1^{2m_1}v_2^{2m_2} - a^2c^2v_1^{2m_1}v_3^{2m_3} + b^2c^2v_2^{2m_2}v_3^{2m_3}}{2abcv_1^{m_1}v_2^{m_2}v_3^{m_3}},$$

$$w_3 = \frac{-a^2b^2v_1^{2m_1}v_2^{2m_2} + a^2c^2v_1^{2m_1}v_3^{2m_3} + b^2c^2v_2^{2m_2}v_3^{2m_3}}{2abcv_1^{m_1}v_2^{m_2}v_3^{m_3}}.$$

We now define:

$$T = \frac{f(u)}{v_3^{2m_3}(w_3^2 - c^2)}, \quad D = (w_1^2 - a^2)v_1^{2m_1}T^M.$$

We consider the twists:

$$C : Dy^2 = f(x), \quad C_1 : y^2 = Dx^{m_1} + a^2, \quad C_2 : y^2 = Dx^{m_2} + b^2, \quad C_3 : y^2 = Dx^{m_3} + c^2.$$

The points $P_i := (x_i, y_i) = \left(\frac{1}{v_i^2 T^{M_i}}, w_i\right)$ are $\mathbb{Q}(v_1, v_2, v_3)$-rational points on C_i, $i = 1, 2, 3$, whereas $P := (x_4, y_4) = \left(u, \frac{1}{T^{(M-1)/2}}\right)$ is a $\mathbb{Q}(u, v_1, v_2, v_3)$-rational point on C.

Theorem 3.1.1. *Let $f \in \mathbb{Q}[x]$ be a square-free polynomial of degree at least 3. Let $m_1, m_2, m_3 \geq 3$ be odd integers. We consider the hyperelliptic curves*

$$E : y^2 = f(x), \quad E_1 : y^2 = x^{m_1} + a^2, \quad E_2 : y^2 = x^{m_2} + b^2, \quad E_3 : y^2 = x^{m_3} + c^2.$$

Then there exists a rational function $D_{2,m_1,m_2,m_3} \in \mathbb{Q}(u, v_1, v_2, v_3)$ such that the Jacobian of the quadratic twist of E and the Jacobians of the m_i-twists of E_i have positive Mordell-Weil rank.

Proof. Let C and C_i for $i = 1, 2, 3$, be the quadratic twists of the elliptic curve E and its respective twists E_i, as previously described. Let P and P_i for $i = 1, 2, 3$, denote the corresponding rational points on C and C_i, respectively.

Define J and J_i to be the Jacobians of the curves C and C_i, respectively. Consider the rational divisor $D = (P) - (\infty)$ on C, and for each $i = 1, 2, 3$, let $D_i = (P_i) - (\infty)$ be the corresponding divisors on C_i.

Since C is a non-constant quadratic twist of the constant elliptic curve E, the divisor D determines a rational point of infinite order in the Jacobian $J(\mathbb{Q}(u, v_1, v_2, v_3))$.

Moreover, by [[4],Proposition 2.1], each divisor D_i gives rise to a rational point of infinite order in $J_i(\mathbb{Q}(u, v_1, v_2, v_3))$, due to the fact that the points P_i have non-constant coordinates and non-zero y-coordinates. □

Theorem 3.1.2. *Let $m := m_1 = m_2 = m_3$ and $a = b = c$. Then the Jacobian of the quadratic twist of $y^2 = f(x)$ by $D_{2,m}$ has positive Mordell-Weil rank, and the Jacobian of the m-twist of $y^2 = x^m + a^2$ by $D_{2,m}$ has Mordell-Weil rank at least 3.*

Proof. In Theorem 3.1.1, we consider the specialization $a = b = c$ and $m := m_1 = m_2 = m_3$. Choosing the triple $(p, q, r) = (w_1, w_2, w_3)$ as defined previously, we obtain

three rational points

$$P_i = \left(\frac{1}{v_i^2}, w_i\right) \in E'(\mathbb{Q}), \quad i = 1, 2, 3,$$

where E' is the elliptic curve defined by $y^2 = Dx^m + a$.

Let $K = \mathbb{Q}(u, v_1, v_2, v_3)$, and define automorphisms $\varphi_i : K \to K$, for $i = 1, 2, 3$, by

$$\varphi_i(u) = u, \quad \varphi_i(v_i) = -v_i, \quad \varphi_i(v_j) = v_j \quad \text{for } j \neq i.$$

Since φ_i fixes both T and D, it induces an automorphism Φ_i on the curve E' and its Jacobian J. Specifically, the automorphism acts on the points as:

$$\Phi_i(P_i) = P_i, \quad \Phi_i(P_j) = \left(\frac{1}{v_j^2}, -w_j\right), \quad j \neq i.$$

Define the divisors $D_i := (P_i) - (\infty)$ on E', for $i = 1, 2, 3$. From the argument in Theorem 3.1.1, each divisor D_i corresponds to a rational point of infinite order in J.

Furthermore, the induced automorphisms satisfy:

$$\Phi_i(D_i) = D_i, \quad \Phi_i(D_j) \sim -D_j, \quad j \neq i.$$

Suppose that there exist integers $\alpha, \beta, \gamma \in \mathbb{Z}$ such that

$$\alpha D_1 + \beta D_2 + \gamma D_3 \sim 0.$$

Applying Φ_1, we obtain:

$$\alpha D_1 - \beta D_2 - \gamma D_3 \sim 0.$$

Adding the two relations yields:

$$2\alpha D_1 \sim 0 \quad \Rightarrow \quad \alpha = 0.$$

Applying the same reasoning using Φ_2 and Φ_3, we conclude $\beta = \gamma = 0$. Thus, the divisors D_1, D_2, D_3 are linearly independent. □

3.2 A Quadratic Twist and Three Twists of Even Degrees

Let $f(x) \in \mathbb{Q}[x]$ be a square-free polynomial of degree at least 3. Fix odd integers $m_1, m_2, m_3 \geq 3$. We are investigating the existence of non-square rational numbers D such that the Jacobians of the curves

$$H : Dy^2 = f(x), \quad H_1 : y^2 = x^{m_1} + aD, \quad H_2 : y^2 = x^{m_2} + bD, \quad H_3 : y^2 = x^{m_3} + cD$$

are of positive Mordell-Weil rank over $\mathbb{Q}$.

We define $M = \mathrm{lcm}(m_1, m_2, m_3)$, and $M_i = M/m_i$ for $i = 1, 2, 3$. We solve the system:

$$\frac{y_1^2 - x_1^{m_1}}{a} = \frac{y_2^2 - x_2^{m_2}}{b} = \frac{y_3^2 - x_3^{m_3}}{c} = \frac{f(x_4)}{y_4^2}.$$

We require:

$$x_i y_i f(x_4)(y_1^2 - x_1^{m_1})(y_2^2 - x_2^{m_2})(y_3^2 - x_3^{m_3}) \neq 0.$$

Parametrize:

$$x_1 = v_1^2 T^{M_1}, \quad x_2 = v_2^2 T^{M_2}, \quad x_3 = v_3^2 T^{M_3}, \quad x_4 = u,$$

$$y_1 = pT^{(M-1)/2}, \quad y_2 = qT^{(M-1)/2}, \quad y_3 = rT^{(M-1)/2}, \quad y_4 = \frac{1}{T^{(M-1)/2}}.$$

Then:

$$T = \frac{p^2 - af(u)}{v_1^{2m_1}} = \frac{q^2 - bf(u)}{v_2^{2m_2}} = \frac{r^2 - cf(u)}{v_3^{2m_3}}.$$

Hence, we consider rational points on the curve:

$$v_2^{2m_2} v_3^{2m_3}(p^2 - af(u)) = v_1^{2m_1} v_3^{2m_3}(q^2 - bf(u)) = v_1^{2m_1} v_2^{2m_2}(r^2 - cf(u)).$$

This is the intersection $H_{a,b,c}$ of two quadratics in $\mathbb{P}^3$ over $\mathbb{Q}(v_1, v_2, v_3)$, and the curve possesses rational points:

$$[p : q : r : s] = [\pm v_1^{m_1} : \pm v_2^{m_2} : \pm v_3^{m_3} : 0],$$

implying that $H_{a,b,c}$ is an elliptic curve.

Theorem 3.2.1. *Let E be an elliptic curve defined by $y^2 = f(x)$, where $f \in \mathbb{Q}[x]$ has degree 3 or 4 and positive Mordell-Weil rank. Let $m_1, m_2, m_3 \geq 3$ be odd integers.*

Consider the hyperelliptic curves

$$E_1 : y^2 = x^{m_1} + a^2, \quad E_2 : y^2 = x^{m_2} + b^2, \quad E_3 : y^2 = x^{m_3} + c^2.$$

Then there exists a rational function $D_{2,2m_1,2m_2,2m_3} \in \mathbb{Q}(v_1, v_2, v_3)$ such that the quadratic twist of E and the Jacobians of the $2m_i$-twists of E_i by $D_{2,2m_1,2m_2,2m_3}$ have positive Mordell-Weil rank.

Proof. Choose $u \in \mathbb{Q}$ such that $(u, y_u) \in E(\mathbb{Q})$ has infinite order. Let $T_1 = av_2^{m_2}v_3^{m_3}y_u, T_2 = bv_1^{m_1}v_3^{m_3}y_u, T_3 = cv_1^{m_1}v_2^{m_2}y_u$.

Then the elliptic curve:

$$x^2 - T_1^2 = y^2 - T_2^2 = z^2 - T_3^2$$

has positive rank over $\mathbb{Q}(T_1, T_2, T_3)$ by Proposition 3. The rest follows as in Theorem 3.1.1. □

Remark. Doubling the point $[ay_u : by_u : cy_u : 1] \in H_{a^2,b^2,c^2}(\mathbb{Q}(v_1, v_2, v_3))$ yields:

$$[w_1 : w_2 : w_3 : 1],$$

where

$$w_1 = \frac{a^2b^2v_3^{2m_3}y_u + a^2c^2v_2^{2m_2}y_u - b^2c^2v_1^{2m_1}y_u}{2abcv_2^{m_2}v_3^{m_3}},$$

$$w_2 = \frac{a^2b^2v_3^{2m_3}y_u - a^2c^2v_2^{2m_2}y_u + b^2c^2v_1^{2m_1}y_u}{2abcv_1^{m_1}v_3^{m_3}},$$

$$w_3 = \frac{-a^2b^2v_3^{2m_3}y_u + a^2c^2v_2^{2m_2}y_u + b^2c^2v_1^{2m_1}y_u}{2abcv_1^{m_1}v_2^{m_2}}.$$

This leads to the following result.

Theorem 3.2.2. *Let E be an elliptic curve defined by $y^2 = f(x)$, where $f \in \mathbb{Q}[x]$ has degree 3 or 4 and positive Mordell-Weil rank. Let $m \geq 3$ be an odd integer. Consider $E' : y^2 = x^m + a^2$, with $a \in \mathbb{Q} \setminus \{0\}$. Then there exists a rational function $D_{2,2m} \in \mathbb{Q}(v_1, v_2, v_3)$ such that the quadratic twist of E and the Jacobian of the $2m$-twist of E' by $D_{2,2m}$ have Mordell-Weil rank at least 3.*

Proof. Set $m := m_1 = m_2 = m_3$ and $a = b = c$ in Theorem 3.2.1. Define rational points $P_i := (v_i^2, w_i T^{(m-1)/2})$ on E' of infinite order. The automorphisms $\varphi_i : v_i \mapsto -v_i$ show the divisors $D_i := (P_i) - (\infty)$ are linearly independent. □

3.3 One Even Degree Twist and Three Odd Degree Twists

Consider the curves:

$$y^2 = x^{m_1} + a, \quad y^2 = x^{m_2} + b, \quad y^2 = x^{m_3} + c, \quad y^2 = x^{m_4} + d,$$

where $a, b, c, d \in \mathbb{Q} \setminus \{0\}$ and $m_i \geq 3$ are odd integers.

We seek a rational function D such that the Jacobians of the following twists have positive Mordell-Weil rank:

$$y^2 = Dx^{m_1} + a, \quad y^2 = Dx^{m_2} + b, \quad y^2 = Dx^{m_3} + c, \quad y^2 = x^{m_4} + dD.$$

Solve:

$$\frac{y_1^2 - a}{x_1^{m_1}} = \frac{y_2^2 - b}{x_2^{m_2}} = \frac{y_3^2 - c}{x_3^{m_3}} = \frac{y_4^2 - x_4^{m_4}}{d},$$

with non-degenerate conditions on x_i, y_i.

Let $M = \operatorname{lcm}(m_1, m_2, m_3, m_4)$, and define:

$$x_1 = \frac{1}{v_1^2 T^{M_1}}, \quad x_2 = \frac{1}{v_2^2 T^{M_2}}, \quad x_3 = \frac{1}{v_3^2 T^{M_3}}, \quad x_4 = v_4^2 T^{m_4},$$

$$y_1 = p, \quad y_2 = q, \quad y_3 = r, \quad y_4 = u T^{(M-1)/2},$$

where u, v_1, v_2, v_3, v_4 are rational parameters.

We get:

$$T = \frac{u^2}{v_4^{2m_4}} + \frac{d(r^2 - c)}{v_3^{2m_3}}, \quad v_1^{2m_1}(p^2 - a) = v_2^{2m_2}(q^2 - b) = v_3^{2m_3}(r^2 - c).$$

Theorem 3.3.1. *Let $m_1, m_2, m_3, m_4 \geq 3$ be odd integers, and $a, b, c, d \in \mathbb{Q} \setminus \{0\}$. Then there exists a rational function*

$$D_{m_1, m_2, m_3, 2m_4} \in \mathbb{Q}(u, v_1, v_2, v_3)$$

such that the Jacobians of the m_i-twists of $y^2 = x^{m_i} + \alpha_i$ for $i = 1, 2, 3$, and the $2m_4$-twist of $y^2 = x^{m_4} + d$ by $D_{m_1, m_2, m_3, 2m_4}$, all have positive Mordell-Weil rank.

Proof. From Proposition 3, the curve

$$v_1^{2m_1}(p^2 - a^2) = v_2^{2m_2}(q^2 - b^2) = v_3^{2m_3}(r^2 - c^2)$$

has positive Mordell-Weil rank over $\mathbb{Q}(u, v_1, v_2, v_3)$. The result follows by analogous reasoning to Theorems 3.1.1 and 3.2.1. □

BIBLIOGRAPHY

[1] M. Alaa and M. Sadek. High rank quadratic twists of pairs of elliptic curves. *Journal of Number Theory*, 174:436–444, 2017.

[2] M. Derickx, A. Etropolski, M. van Hoeij, J. Morrow, and D. Zureick-Brown. Sporadic cubic torsion. *Algebra and Number Theory*, 15:1837–1864, 2021. doi: 10.2140/ant.2021.15.1837.

[3] T. Jędrzejak and M. Ulas. Variations on twists of tuples of hyperelliptic curves and related results. *Journal of Number Theory*, 137:222–240, 2014. doi: 10.1016/j.jnt.2013.11.011.

[4] T. Jędrzejak, J. Top, and M. Ulas. Tuples of hyperelliptic curves $y^2 = x^n + a$. *Acta Arithmetica*, 150(2):105–113, 2011. doi: 10.4064/aa150-2-1. URL http://eudml.org/doc/279521.

[5] M. A. Kenku and F. Momose. Torsion points on elliptic curves defined over quadratic fields. *Nagoya Mathematical Journal*, 109:125–149, March 1988. doi: 10.1017/s0027763000002816.

[6] M. Kuwata. Quadratic twists of an elliptic curve and maps from a hyperelliptic curve. *Mathematical Journal of Okayama University*, 47(1):85–98, 2005.

[7] M. Kuwata and L. Wang. Topology of rational points on isotrivial elliptic surfaces. *International Mathematics Research Notices*, (4):113–123, 1993.

[8] B. Mazur. Modular curves and the eisenstein ideal. *Publications Mathématiques de l'IHÉS*, 47(1):33–186, 1977. doi: 10.1007/bf02684339.

[9] L. Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Inventiones Mathematicae*, 124:437–449, 1996. doi: 10.1007/s002220050059.

[10] M. Sadek. On quadratic twists of hyperelliptic curves. *Rocky Mountain Journal of Mathematics*, 44:1015–1026, 2014.

[11] M. Sadek. Minimal regular models of quadratic twists of genus two curves. *Acta Arithmetica*, 183:317–337, 2018.

[12] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, 1994. ISBN 978-0-387-94328-9. doi: 10.1007/978-1-4612-0851-8.

[13] J. H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, 2 edition, 2009. ISBN 978-0-387-09494-6. doi: 10.1007/978-0-387-09494-6.

[14] M. Ulas. On certain diophantine systems with infinitely many parametric solutions and applications. *Acta Arithmetica*, 145(3):305–313, 2010. URL http://eudml.org/doc/279371.

[15] M. Ulas. Variations on higher twists of pairs of elliptic curves. *International Journal of Number Theory*, 6(5):1183–1189, 2010. URL https://doi.org/10.1142/S1793042110003472.

[16] M. Ulas. Variations on twists of elliptic curves. *Rocky Mountain Journal of Mathematics*, 43(2):645–660, 2013.