DIVISIBILITY OF RATIONAL POINTS ON ELLIPTIC CURVES AND ARITHMETIC PROGRESSIONS IN POLYNOMIAL DYNAMICAL SYSTEMS

by
TUĞBA YESİN ELSHEIKH

Submitted to the Graduate School of Social Sciences
in partial fulfilment of
the requirements for the degree of Doctor of Philosophy

Sabancı University
June 2023

DIVISIBILITY OF RATIONAL POINTS ON ELLIPTIC CURVES AND ARITHMETIC PROGRESSIONS IN POLYNOMIAL DYNAMICAL SYSTEMS

Approved by:

Assoc. Prof. Dr. Mohammad Sadek .....
(Dissertation Supervisor)

Asst. Prof. Dr. Nurdagül Anbar Meidl .....

Assoc. Prof. Dr. Kağan Kurşungöz .....

Prof. Dr. Andrej Dujella .....

Prof. Dr. Gökhan Soydan .....

Date of Approval: June 20, 2023

ABSTRACT

DIVISIBILITY OF RATIONAL POINTS ON ELLIPTIC CURVES AND ARITHMETIC PROGRESSIONS IN POLYNOMIAL DYNAMICAL SYSTEMS

TUĞBA YESİN ELSHEIKH

MATHEMATİCS Ph.D DISSERTATION, JUNE 2023

Dissertation Supervisor: Assoc. Prof. Dr. Mohammad Sadek

Keywords: elliptic curves, quartic models, divisibility-by-2, Diophantine quintuples, dynamical systems, polynomial orbits, arithmetic progressions

Let K be a number field and E be an elliptic curve described by the Weierstrass equation over K. As a result of 2-descent Theorem on elliptic curves, a criterion for the divisibility-by-2 of a rational point on E is obtained previously. This divisibility criterion has been used to study rational $D(q)$-m-tuples. In this thesis, we investigate smooth genus one curves C described by a quartic polynomial equation over the rational field $\mathbb{Q}$ together with $P \in C(\mathbb{Q})$. We give an analogous divisibility-by-2 criterion for rational points in $C(\mathbb{Q})$. We also show how this criterion might be used to study extensions of rational $D(q)$-quadruples to quintuples.

The existence of consecutive squares in arithmetic progression is a classical problem. Fermat claimed that there does not exist an arithmetic progression of four rational squares; and Euler proved this claim. In this thesis, we give a dynamical analogue of Fermat's Squares Theorem. More precisely, given a polynomial $f(x)$ and a rational point a, we ask how many consecutive squares can be there in the orbit $\{a, f(a), f^2(a), \ldots, f^n(a), \ldots\}$? In fact, we give explicit constructions of quadratic polynomials with orbits containing three consecutive squares. Finally, we investigate the question of covering the latter orbit using finitely many arithmetic progressions. We establish a connection between the answer to the latter question and the existence of primitive divisors in the orbit.

ÖZET

ELİPTİK EĞRİLER ÜZERİNDEKİ RASYONEL NOKTALARIN BÖLÜNEBİLİRLİĞİ VE POLİNOMSAL DİNAMİK SİSTEMLERDE ARİTMETİK DİZİLER

TUĞBA YESİN ELSHEIKH

PROGRAM ADI DOKTORA TEZİ, HAZİRAN 2023

Tez Danışmanı: Doç. Dr. Mohammad Sadek

Anahtar Kelimeler: eliptik eğriler, dördüncü dereceden modeller, 2 ile bölünebilme, Diophantine beşlileri, dinamik sistemler, polinom yörüngeleri, aritmetik diziler

K bir sayı cismi ve E Weierstrass denklemi ile K üzerinde tanımlanan bir eliptik eğri olsun. Eliptik eğrilerdeki 2-indirgeme teoreminin bir sonucu olarak, E üzerindeki rasyonel bir noktanın 2'ye bölünebilirliği için bir kriter daha önceki çalışmalarda verilmiştir. Bu bölünebilirlik kriteri, rasyonel $D(q)-m$'lilerini incelemek için kullanılmıştır. Bu tez çalışmasında, düzgün, cinsi 1 olan, $\mathbb{Q}$ rasyonel cismi üzerinde dördüncü dereceden bir polinom denklemiyle tanımlanan ve $P \in C(\mathbb{Q})$ özelliğini sağlayan C eğrileri araştırılmıştır. $C(\mathbb{Q})$'daki rasyonel noktalar için benzer bir 2'ye bölünebilirlik kriteri verilmiştir. Ayrıca, bu kriterin rasyonel $D(q)$-dörtlülerin beşlilere genişletilmelerini incelemek için nasıl kullanılabileceği de gösterilmiştir.

Aritmetik dizide ardışık karelerin varlığı klasik bir problemdir. Fermat, dört rasyonel karenin bir aritmetik dizi oluşturmadığını iddia etmiş; ve bu iddia Euler tarafından ispatlanmıştır. Bu tezde, Fermat'nın Kareler Teoremi'nin dinamik bir benzeri verilmiştir. Daha kesin olarak, bir $f(x)$ polinomu ve a rasyonel sayısı verildiğinde, $\{a, f(a), f^2(a), \ldots, f^n(a), \ldots\}$ yörüngesinde kaç ardışık kare olabileceği sorusu ele alınmıştır. Aslında, ardışık üç kare içeren yörüngelere sahip ikinci dereceden polinomların kesin yapıları verilmiştir. Son olarak, sonlu sayıda aritmetik dizi kullanarak yukarıda verilen yörüngeyi örtüp örtmediği araştırılmıştır. Yukarıdaki sorunun cevabı ile yörüngedeki ilkel bölenlerin varlığı arasında bir bağlantı kurulmuştur.

ACKNOWLEDGEMENTS

First of all, I would like to express my sincere and deepest gratitude to my thesis advisor Assoc. Prof. Dr. Mohammad Sadek for his motivation, guidance, encouragement, and extensive knowledge. He has been motivating me all the time to do my best. His contributions to my academic experience and my personality have been enormous. I am really honored and consider myself more than lucky to work with Assoc. Prof. Dr. Mohammad Sadek.

I would like to thank my jury members, Asst. Prof. Nurdagül Anbar Meidl, Assoc. Prof. Dr. Kağan Kurşungöz, Prof. Dr. Andrej Dujella, Prof. Dr. Gökhan Soydan for reviewing my Ph.D. thesis and for their valuable comments.

I would like to give the biggest thanks to my precious husband, Mohamed Wafik. I am very lucky to have him. He has been the one who understands and values my work, encourages me at every step, stands by my side, and lifts me up every time I fell into pessimism during this work. I am certain that the difficult long roads waiting for us after the doctorate will be much easier and more enjoyable together.

Many thanks to my friend and my sister, Melike Efe, for her constant encouragement, and for the great companionship she gave me throughout fourteen years. She is the person who helped me overcome not only academic difficulties but also every challenge I faced in life. I would like to thank her again for playing the most important role in completing this work.

I would like to thank each member of the Mathematics Program of Sabancı University for providing a warm atmosphere, which always made me feel at home. I would also like to thank Dr. Nermine El Sissi and Nagwa El Hefnaoui for their priceless support. I would especially like to thank my dear friend Tekgül Kalaycı. She has always been with me throughout my master's and doctorate education at Sabancı University. I'm grateful for her invaluable friendship and continuous support.

Last but not least, I am deeply grateful to my family, who has continuously supported me throughout my life unconditionally. Their support and their prayers got me to this point. I feel their endless love, patience, and understanding in every second of my life.

Finally, I gratefully acknowledge the support provided by TÜBİTAK 1001 programme, project number 120F308.

To my family

TABLE OF CONTENTS

1. INTRODUCTION

Let E be an elliptic curve over a number field K. The Mordell-Weil Theorem asserts that the abelian group of rational points $E(K)$ is finitely generated. In particular, there are finitely many points $P_1,...,P_n$ in $E(K)$ such that any $P \in E(K)$ can be written as a linear combination $m_1P_1 + \cdots + m_nP_n$ for some integers $m_1, \cdots, m_n$. During the course of the proof of the latter theorem, one proves the weak Mordell-Weil Theorem which states that the abelian group $E(K)/2E(K)$ is finite.

In order to show that $E(K)/2E(K)$ is finite, one needs to pass from a point $P \in E(K)$ to a point $Q \in E$ such that $2Q = P$. This process is called the 2-descent on elliptic curves. The following theorem is known as the 2-descent Theorem and gives a necessary and sufficient condition such that $Q \in E(K)$, see [49, Chapter IV], [43, Chapter 6], [64, Chapter VIII], or [2] for a criterion of the divisibility of rational points by powers of 2.

Theorem 1.1 (2-descent Theorem) *Let E be an elliptic curve over a field K of characteristic not equal to 2 or 3. Suppose E is given by*

$$E : y^2 = (x-\alpha)(x-\beta)(x-\gamma)$$

with distinct elements $\alpha, \beta, \gamma \in K$. For $(x_2, y_2) \in E(K)$, there exists $(x_1, y_1) \in E(K)$ with $2(x_1, y_1) = (x_2, y_2)$, in other words, (x_2, y_2) is divisible by 2 in $E(K)$ if and only if $x_2 - \alpha, x_2 - \beta, x_2 - \gamma$ are squares in K.

The following quartic equation

$$y^2 = (a_1x + b_1)(a_2x + b_2)(a_3x + b_3)(a_4x + b_4), \qquad a_i, b_i \in K,$$

where b_i/a_i are distinct in K, describes a genus one curve C. Fixing a rational point $P \in C(K)$ to serve as the identity element of the group law, one may look for a similar criterion for the divisibility-by-2 on the elliptic curve (C, P). In Chapter 3, we obtain a similar condition that depends on P, more precisely, a point $Q \in C(\mathbb{Q})$ is twice a rational point if and only if the values of certain degree-2 polynomials

evaluated at the x-coordinate of Q are all squares in $\mathbb{Q}$. More precisely, we prove the following theorem.

Theorem 1.2 *Let C be a smooth genus 1 curve over $\mathbb{Q}$ defined by an equation of the form*

$$y^2 = (a_1x+b_1)(a_2x+b_2)(a_3x+b_3)(a_4x+b_4), \qquad \text{where } a_i \in \mathbb{Q}^\times, b_i \in \mathbb{Q}.$$

Let $(x_0,y_0) \in C(\mathbb{Q})$ be such that $x_0 \neq -b_i/a_i$, $i=1,2,3,4$. We set $\phi : C \longrightarrow E := J(C)$ to be a $\mathbb{Q}$-birational isomorphism with $\phi((x_0,y_0)) = O_E$. For $Q \in C(\mathbb{Q})$, one has $Q \in 2C(\mathbb{Q})$ if and only if $f_i(x_0)\, f_j(x_0)\, f_i(x(Q)) f_j(x(Q)) \in \mathbb{Q}^2$ for all $i,j \in \{1,2,3,4\}$ where $f_i(x) = a_ix + b_i$.

Consequently, we show how to characterize such quartic models of elliptic curves that possess rational 4-torsion points.

A rational $D(q)$-m-tuple is an m-tuple $a_1, \cdots, a_m$ of distinct non-zero rational numbers such that $a_ia_j + q$ is a square for all $1 \leq i < j \leq m$. If $q = 1$, then the latter m-tuple is called a rational Diophantine m-tuple. The divisibility-by-2 on elliptic curves described by Weierstrass equations has been used to study rational $D(q)$-m-tuples. In [17], 2-divisibility on elliptic curves described by Weierstrass equations was used to extend rational Diophantine triples to quadruples. It was also used to show that there are infinitely many rational Diophantine sextuples, see [27]. In [11], it was proved that assuming the Parity Conjecture for the twists of several explicitly given elliptic curves, the density of rational numbers q for which there exist infinitely many rational $D(q)$-quintuples is at least $295026/296010 \approx 99.5\%$.

Rational Diophantine m-tuples have turned out to provide a useful tool to construct elliptic curves with prescribed torsion subgroups and high rank. In [30], rational Diophantine triples have been used to construct elliptic curves over $\mathbb{Q}(u)$ with rank 2 and either torsion subgroup $\mathbb{Z}/8\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. In [24], for each of the groups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$ for $k = 2,4,6,8$, the authors proved the existence of infinitely many rational Diophantine quadruples with the property that the induced elliptic curve has this torsion group. In [16], the so-called regular Diophantine quadruples and quintuples were characterized by elliptic curves. In addition, these characterizations were used to find examples of elliptic curves over $\mathbb{Q}$ with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and with Mordell-Weil rank equal to 8.

Researchers have been investigating $D(q)$-tuples whose elements enjoy certain properties. For example, in [29] the authors prove the existence of infinitely many essentially different $D(q)$-quintuples, where q is an integer, whose elements are squares.

Further, integers that possess the $D(q)$-property for at least two integers q_1, q_2 have been studied. In fact, the authors of [23] proved the existence of infintely many essentially different sets consisting of perfect squares which are simultaneously $D(q_1)$-quadruples and $D(q_2)$-quadruples for distinct nonzero perfect squares q_1 and q_2.

For every rational number q, the authors of [12] found all rational m such that there exists a rational $D(q)$-quadruple $\{a_1, a_2, a_3, a_4\}$ with product $a_1a_2a_3a_4 = m$. Using a certain rational map defined on a specific elliptic curve, the authors show that all such quadruples are identified if a certain rational map defined on the elliptic curve attains rational square values. For this reason, using the divisibility by-2 criterion on elliptic curves described by quartic equations in our work resembles the approach used in the aforementioned paper.

The notion of a strong rational m-tuple was introduced in [22]. Such a tuple is a rational Diophantine m-tuple, $\{a_1, \ldots, a_m\}$, with the additional property that $a_i^2 + 1$ is a rational square for every $i = 1, \ldots, m$. The authors proved that there exist infinitely many strong rational Diophantine triples. A strong rational $D(q)$-m-tuple is a set of non-zero rationals $\{a_1, \ldots, a_m\}$ such that $a_ia_j + q$ is a square for all $i, j = 1, \ldots, m$, including the case $i = j$. The case $q = -1$ was studied in [28] and it was shown that there exist infinitely many strong rational $D(-1)$-triples. In [59], it was proved that there exist infinitely many square-free integers q with the property that there exist infinitely many strong rational $D(q)$-triples.

A natural question to pose is how large a set of rational numbers enjoying the $D(q)$-property, for some $q \in \mathbb{Q}$, can be. For a historical overview of rational $D(q)$-m-tuples, we refer the reader to [19], [20, Sections 14.6 and 16.7] as well as the webpage of Andrej Dujella[11].

Jones initiated the study of polynomial $D(q)$-m-tuples where q itself is a polynomial, see [46, 45]. If we define

$$P_q = \sup\{|S| : S \text{ is a polynomial } D(q)\text{-tuple}\},$$

then $P_q \leq 22$ for all $q \in \mathbb{Z}$, see [15, Theorem 1]. More properties of P_q can be found in [21]. In this thesis, we focus on the case where q is a linear polynomial. Setting

$$L = \sup\{|S| : S \text{ is a polynomial } D(ax+b)\text{-tuple for some } a \neq 0 \text{ and } b\},$$

one can easily observe that $L \geq 4$ by viewing the $D(16x+9)$-quadruple $T = \{x, 16x+$

[11] https://web.math.pmf.unizg.hr/~duje/dtuples.html

$8, 25x+14, 36x+20\}$, see [13]. For upper bounds on L, the reader can consult the papers [26, 25].

We examine the case of polynomial $D(q)$-m-tuples consisting of linear polynomials where q itself is a linear polynomial. If the set S consists only of linear polynomials, then $\sup\{|S|\}$ is 4, see [26]. Hence, the above $D(16x+9)$-quadruple T can not be extended to a polynomial $D(16x+9)$-quintuple using a linear polynomial. In Chapter 4, we use the 2-divisibility criterion on elliptic curves described by quartic models to study the extension of polynomial $D(q)$-quadruples to rational quintuples at infinitely many values of these polynomials. In fact, we show that although T cannot be extended to a polynomial $D(16x+9)$-quintuple, there are infinitely many values for x parametrized by an elliptic curve of positive rank such that T can be extended to a quintuple using a rational function. We also present other polynomial $D(ax+b)$-quadruples with the same property. In particular, we prove the following result.

Theorem 1.3 ([60]) *The polynomial $D(16t+9)$-quadruple $\{t, 16t+8, 225t+14, 36t+20\}$ can be extended to a rational $D(16t+9)$-quintuple for infinitely many $t \in \mathbb{Q}$.*

We remark that the theory of elliptic curves was used to show that there are only finitely many ways of extending a rational $D(q)$-quadruple to a rational $D(q)$-quintuple, see [42]. Our method provides an explicit description of how to extend certain rational $D(q)$-quadruples to rational $D(q)$-quintuples. In [14], an explicit expression for the element extending a rational $D(q)$-quadruple to a rational $D(q)$-quintuple was provided if q is a rational square. This means that if x is chosen such that $16x+9$ is a rational square q^2, then our result together with [14] provides a method of constructing almost rational $D(q^2)$-sextuples, i.e., a tuple $a_1, \cdots, a_6$ of distinct nonzero rational numbers such that $a_i a_j + q^2$ is a square for all $1 \leq i < j \leq 6$ except for $(i,j) = (5,6)$.

In the second part of this thesis, we investigate the existence of consecutive squares in the set of iterations of a rational point under a given polynomial. The existence of three consecutive squares in arithmetic progression is a phenomenon that can be seen in $\mathbb{Q}$. The rationals 1, 5^2, and 7^2 provide such an example. In fact, one can parameterize all such rationals by observing that they satisfy the following equation

$$x_2^2 - x_1^2 = x_3^2 - x_2^2.$$

This means that three rational numbers in arithmetic progression give rise to a rational point $(x_1 : x_2 : x_3)$ on the conic $C : x_1^2 - 2x_2^2 + x_3^2 = 0$. Since the point

$(1:1:1) \in C(\mathbb{Q})$, it follows that $C(\mathbb{Q})$ has infinitely many points. Moreover, one may parametrize these points as follows $(x_1 : x_2 : x_3) = (-p^2 + 2ps + s^2, p^2 + s^2, p^2 + 2ps - s^2)$ for some $p, s \in \mathbb{Q}$.

Fermat claimed that there does not exist an arithmetic progression of four squares over $\mathbb{Q}$. Euler, among others, proved this statement. One sees that the existence of such squares is equivalent to the existence of nontrivial rational points on the intersection of the following two quadric surfaces in $\mathbb{P}^3_{\mathbb{Q}}$

$$\begin{aligned} x_1^2 - 2x_2^2 + x_3^2 &= 0 \\ x_2^2 - 2x_3^2 + x_4^2 &= 0. \end{aligned}$$

The latter intersection describes an elliptic curve E for which $E(\mathbb{Q}) = \{(1 : \pm 1 : \pm 1 : \pm 1)\}$. The points in $E(\mathbb{Q})$ do not give rise to any non-constant rational squares in arithmetic progression.

In [70], it was proved that a uniform upper bound exists on the number of squares in the arithmetic progression over a given number field that depends only on the degree of the field. Moreover, the author proved that this bound is 5 for quadratic fields. In [38], the authors provide several criteria to identify the quadratic number fields over which there is a non-constant arithmetic progression of five squares.

One may ask the aforementioned questions in a different setting, namely within the frame of arithmetic dynamical systems. A dynamical system is a self-map $f : S \longrightarrow S$ on a set S that allows iteration. The m-th iteration of f is defined recursively by $f^0(x) = x$ and $f^m(x) = f(f^{m-1}(x))$ when $m \geq 1$. The *orbit* of a point $P \in S$ under f is given by

$$\mathrm{Orb}_f(P) = \{f^i(P) : i = 0, 1, 2 \ldots\}.$$

In case the map f is fixed, we write $\mathrm{Orb}(P)$. If $\mathrm{Orb}(P)$ is infinite, P is called a wandering point; otherwise, P is called a preperiodic point. A preperiodic point $P \in S$ is said to be *periodic* if there exists an integer $n > 0$ such that $f^n(P) = P$, where n is called the period of P. If n is the smallest such integer, we say that P has the exact period n. The orbit of a periodic point is called a *periodic orbit*.

The question of the existence of K-rational squares in arithmetic progression of length m, $m \geq 2$, over a number field K can be reformulated using dynamical systems as follows. Can we find a linear polynomial $\ell(x) = x + c$, $c \in K^\times$, and $x_0 \in K$ such that $\mathrm{Orb}_\ell(x_0)$ contains m consecutive K-squares? In particular, is there an $x_0 \in \mathbb{Q}$ such that $x_0, \ell(x_0), \ell^2(x_0), \ldots, \ell^{m-1}(x_0)$ are all in K^2?

In this thesis, we are dealing with a higher degree dynamical analogue of Fermat's

Squares Theorem. Namely, given a degree two polynomial $f(x) = x^2 + Ax + B \in K[x]$ and a point $x_0 \in K$, how many consecutive squares can be there in the orbit $\{x_0, f(x_0), f^2(x_0), \ldots, f^n(x_0), \ldots\}$ of x_0? It can be seen that for any irreducible quadratic map $f(x) \in K[x]$, the number of orbits under f that contain at least three consecutive K-rational squares should be finite. This holds because each such square will give rise to a K-rational point on the hyperelliptic curve $C_m : y^2 = f^m(x^2)$ for $m = 0, 1, 2, \ldots$. When $m \geq 2$, the curve C_m is of the genus > 2. By Faltings' theorem, see [33], one then knows that the number of rational points on C_m, $m \geq 2$, must be finite.

In Chapter 5, we give three different constructions of 1-parameter polynomial maps of degree 2 over $\mathbb{Q}$ and rational points that possess three different consecutive squares in their orbit under the iteration of these polynomials. For example, we show that the following result holds.

Theorem 1.4 *For each $\beta \in \mathbb{Q}$, there are infinitely many rational numbers α, γ, and c such that $f_c(\alpha^2) = \beta^2$ and $f_c(\beta^2) = \gamma^2$ where $f_c(x) = x^2 + c$. In particular, one may choose*

$$\begin{aligned}
\alpha &= \frac{\beta^2(3-4\beta^4)^2}{(1+8\beta^2+4\beta^4)^2}, \\
\gamma &= \frac{\beta(-1+24(\beta^2+3\beta^4+4\beta^6+2\beta^8))}{(1+8\beta^2+4\beta^4)^2}, \\
c &= \frac{\beta^2-49\beta^4+400\beta^6+2864\beta^8+7264\beta^{10}+8864\beta^{12}+6400\beta^{14}+2816\beta^{16}+256\beta^{18}-256\beta^{20}}{(1+8\beta^2+4\beta^4)^4}.
\end{aligned}$$

In addition, unlike linear polynomial dynamical systems generated by polynomials of the form $x + c$, $c \in \mathbb{Q}^\times$, there exists at least one polynomial of the form $x^2 + c$, $c \in \mathbb{Q}^\times$, and a point $x_0 \in \mathbb{Q}$ such that $x_0, f(x_0), f^2(x_0)$ and $f^3(x_0)$ are all rational squares.

Finally, assuming a standard conjecture of Poonen on the exact period of periodic points of polynomial maps of degree 2 over $\mathbb{Q}$, we introduce necessary and sufficient conditions under which polynomial maps of the form $x^2 + ax + b \in \mathbb{Q}[x]$ possess periodic orbits containing only rational squares.

In the last part of this thesis, we investigate the intersection of arithmetic progressions with polynomial orbits. More precisely, we examine the intersection of orbits of polynomials of arbitrary degrees with orbits of linear polynomials. In [36, 37], the authors proved that two complex polynomials f and g of degree at least 2 having orbits that intersect in infinitely many points must have a common iteration. Moreover, in [36], it was shown that if f and g are non-monic linear polynomials such

that $\mathrm{Orb}_f(s) \cap \mathrm{Orb}_g(t)$ is infinite, then f and g must have a common iterate. In this thesis, we work on the intersection of polynomial orbits with linear polynomial orbits and we give the following proposition in Chapter 6.

Proposition 1.1 *Let $f(x) \in K[x]$ be of degree at least 2 such that $f(x)$ is not a power of a linear polynomial. Let $g(x) = ax+b \in K[x]$ be such that $\mathrm{Orb}_f(s) \cap \mathrm{Orb}_g^{\pm}(t)$ is infinite for some fixed $s,t \in K$. Then a is a root of unity in $\mathcal{O}_K$.*

In addition, we give the definition of relative density of A, where A is a subset of $\mathbb{Z}$, in the orbit of s under f, $\delta_{f,s}(A)$, and we present some relations between primitive prime divisors of a sequence A and $\delta_{f,s}(A)$. Finally, we use arithmetic progression sequences to cover polynomial orbits and we prove the following theorem.

Theorem 1.5 *Let $f(x)$ be a polynomial in $\mathbb{Z}[x]$ and $t \in \mathbb{Z}$. Let $g_i(x)$, $1 \le i \le k$, be a finite family of monic linear polynomials in $\mathbb{Z}[x]$. The following statements are equivalent.*

i) $\delta_{f,t}\left(\bigcup_{i=1}^{k} \mathrm{Orb}_{g_i}^{\pm}(t)\right) = 1$.

ii) $\delta_{f,t}\left(\mathrm{Orb}_{g_i}^{\pm}(t)\right) = 1$ *for some* i, $1 \le i \le k$.

iii) $\mathrm{Orb}_f(t) \subset \mathrm{Orb}_{g_i}^{\pm}(t)$ *for some* i, $1 \le i \le k$.

where $\mathrm{Orb}_g^{\pm}(a) := \{g^n(a), n \in \mathbb{Z}\}$ the union of both the forward and backward orbits of a point a under the iterations of g.

We say that a family $A = \{A_1, \cdots, A_k\}$ of arithmetic progressions covers a set $S \subseteq \mathbb{Z}$ if $S \subset A_1 \cup \cdots \cup A_k$, and if A covers $\mathbb{Z}$ then it is called a covering system. For example, every integer n satisfies at least one of the congruences

$$n \equiv 0 \mod 2, \quad n \equiv 0 \mod 3, \quad n \equiv 1 \mod 4, \quad n \equiv 1 \mod 6, \quad n \equiv 11 \mod 12.$$

In particular, the above system of congruences is a covering system. Erdős introduced covering systems in 1950, see [32]. In this thesis, we will shed some light on covers of orbits of polynomials with integer coefficients.

Given a polynomial $f \in \mathbb{Z}[x]$, and a wandering point $t \in \mathbb{Z}$, we will show that if A is a cover of $\mathrm{Orb}_f(t)$ such that every congruence in $A = \{A_1, \cdots, A_k\}$ contains t, then A must consists of exactly one congruence, i.e., $k = 1$. This directly implies that if $k \ge 2$ and t is represented by each congruence A_k, then A cannot cover $\mathrm{Orb}_f(t)$. This motivates investigating the relative density $\delta_{f,t}(\bigcup_{i=1}^{k} A_i)$. In particular, a real number that is realized in the form of the latter relative density will be called (f,t,k)-accessible. We will give an explicit description of rational numbers that are (f,t,k)-accessible. In addition, fixing $k \ge 2$, we show that (f,t,k)-accessible numbers

are bounded from above in the interval $(0,1)$. In chapter 6, we give the following theorem.

Theorem 1.6 *Let $f(x) \in \mathbb{Z}[x]$ and $t \in \mathbb{Z}$ be a wandering point for f. Let $m,n \in \mathbb{Z}$ and p_i's are prime in order. If k is an positive integer such that*

$$\delta_k = 1 - \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) < \frac{m}{n},$$

then m/n is not (f,t,k)-accessible. In particular, there does not exist k linear polynomials $g_1(x), \ldots, g_k(x)$ such that

$$\delta_{f,t}\left(\bigcup_{i=1}^{k} \mathrm{Orb}_{g_i}^{\pm}(t)\right) = \frac{m}{n}.$$

2. Preliminaries

In this chapter, we present the definitions, basic facts, and significant results needed for our work. We give a summary of the arithmetic of algebraic curves, and divisors, that will be needed for our study of elliptic curves. We also introduce the notion of the Weiertrass models and the group law of elliptic curves and some classification of rational torsion points on elliptic curves over number fields.

We set the following notation, which will be used throughout this thesis.

K is a perfect field with an algebraic closure $\bar{K}$.

For this chapter, all definitions can be found in [20] and [64] with the change of some notation. We also let m and n denote positive integers.

2.1 Curves

Definition 2.1 *The affine n-space is the set of n-tuples*

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

Similarly, the set of K-rational points of $\mathbb{A}^n$ *is the set*

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

Definition 2.2 *Let I be an ideal of the polynomial ring in n variables* $\bar{K}[X] = \bar{K}[X_1, \ldots, X_n]$. *An (affine) algebraic set is any set of the form*

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

If V is an algebraic set, the ideal of V is given by

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

An algebraic set is defined over K if its ideal $I(V)$ can be generated by polynomials in $K[X]$. If V is defined over K, then the set of K- rational points of V is the set

$$V(K) = V \cap \mathbb{A}^n(K)$$

Definition 2.3 *Projective n-space (over K), denoted by $\mathbb{P}^n$ or $\mathbb{P}^n(\bar{K})$, is the set of all $(n+1)$-tuples*

$$(x_0, \ldots, x_n) \in \mathbb{A}^{n+1}$$

such that at least one x_i is nonzero, modulo the equivalence relation

$$(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n)$$

if there exists a $\lambda \in \bar{K}^*$ such that $x_i = \lambda y_i$ for all i. An equivalence class

$$\{(\lambda x_0, \ldots, \lambda x_n) : \lambda \in \bar{K}^*\},$$

is denoted by $[x_0, \ldots, x_n]$, and the individual $x_0, \ldots, x_n$ are called homogeneous coordinates for the corresponding points in $\mathbb{P}^n$ is the set

$$\mathbb{P}^n(K) = \{[x_0, \ldots, x_n] \in \mathbb{P}^n : \text{ all } x_i \in K\}.$$

Remark 2.1 *Note that if $P = [x_0, \ldots, x_n] \in \mathbb{P}^n(K)$, it does not follow that each $x_i \in K$. However, choosing some i with $x_i \neq 0$, it does follow that $x_j/x_i \in K$ for every j.*

Example 2.1 *Let $\mathbb{F}_{11}$ be a finite field with 11 elements. Let the algebraic set*

$$V : (x^3 + y^2 z)^2 = x^5 z$$

be defined over $\mathbb{P}^2(\mathbb{F}_{11})$. Then one can observed that

$$V(\mathbb{P}^2(\mathbb{F}_{11})) = \{(0:0:1), (1:0:1), (1:3:1), (1:8:1), (3:4:1), (3:7:1), (4:1:1), (4:5:1),$$

$$(4:6:1), (4:10:1), (9:3:1), (9:8:1), (0:1:0)\}.$$

Definition 2.4 *A polynomial $f \in \bar{K}[X_0, \ldots, X_n]$ is homogeneous of degree d if*

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

An ideal $I \subset \bar{K}[X]$ is homogeneous if it is generated by homogeneous polynomials.

Let f be a homogeneous polynomial and let $P \in \mathbb{P}^n$. It makes sense to ask whether $f(P) = 0$, since the answer is independent of the choice of homogeneous coordinates for P. To each homogeneous ideal I we associate a subset of $\mathbb{P}^n$ by the rule

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

Definition 2.5 *A (projective) algebraic set is any set of the form V_I for a homogeneous ideal I. If V is projective algebraic set, the (homogeneous) ideal of V, denoted by $I(V)$, is the ideal of $\bar{K}[X]$ generated by*

$$\{f \in \bar{K}[X] : f \textit{ is homogeneous and } f(P) = 0 \textit{ for all } P \in V\}.$$

Example 2.2 *Let V be the algebraic set in $\mathbb{P}^2$ given by the single equation*

$$X^2 + Y^2 = Z^2.$$

Then for any field K with $char(K) \neq 2$, the set $V(K)$ is isomorphic to $\mathbb{P}^1(K)$, for example by the map

$$\mathbb{P}^1(K) \longrightarrow V(K), \quad [s,t] \to [s^2 - t^2, 2st, s^2 + t^2].$$

Example 2.3 *The algebraic set*

$$V : X^n + Y^n = 1$$

is defined over $\mathbb{Q}$. Fermat's last theorem proven by Andrew Wiles in [67], states that for all $n \geq 3$,

$$V(\mathbb{Q}) = \begin{cases} \{(1,0),(0,1)\} & \textit{if } n \textit{ is odd,} \\ \{(\pm 1,0),(0,\pm 1)\} & \textit{if } n \textit{ is even.} \end{cases}$$

Definition 2.6 *A projective algebraic set is called a (projective) variety if its homogeneous ideal $I(V)$ is a prime ideal in $\bar{K}[X]$.*

Definition 2.7 *An algebraic curve in the affine plane $\mathbb{A}^2$ is defined as the set of*

solutions to a polynomial equation in two variables

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

Let F be a non-constant homogeneous polynomial. We define a projective curve C in the projective plane $\mathbb{P}^2$ to be the set of solutions to a polynomial equation

$$C : F(X,Y,Z) = 0.$$

We also call C an algebraic curve, or sometimes just a curve if it is clear that we are working in $\mathbb{P}^2$. The degree of the curve C is the degree of the polynomial F.

Definition 2.8 *Let P be a point of a curve $C : f(x,y) = 0$. P is called a singular point of the curve if*

$$\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0.$$

If at least one of the partial derivatives does not vanish, then P is called a non-singular point. Moreover, C is called a non-singular curve (or a smooth curve) if every point of C is non-singular.

Let C be a curve defined over K and P be a smooth point on C. It is known that in this case the local ring of C at P, $K[C]_P$ is a discrete valuation ring with valuation given by

$$\mathrm{Ord}_P(f) := \sup\{d \in \mathbb{Z} | f \in M_P^d\}$$

where M_P is the maximal ideal of $K[C]_P$.

Now we can define the order of $f \in K(C)$ at P.

Definition 2.9 *Let C be a curve and $P \in C$ a smooth point. Let $f \in \bar{K}(C)$. The order of f at P is $\mathrm{Ord}_P(f)$. If $\mathrm{Ord}_P(f) > 0$, then f has a zero at P, and if $\mathrm{Ord}_P(f) < 0$, then f has a pole at P. If $\mathrm{Ord}_P(f) \geq 0$, then f is regular (or defined) at P and we can evaluate $f(P)$. Otherwise, f has pole at P and we write $f(P) = \infty$.*

Example 2.4 *Consider the two curves*

$$C_1 : Y^2 = X^3 + X \quad \text{and} \quad C_2 : Y^2 = X^3 + X^2.$$

Let $P = (0,0)$. Then C_1 is smooth at P whereas C_2 is not. The maximal ideal M_P of $\bar{K}[C_1]_P$ has the property that M_P/M_P^2 is generated by Y. For example,

$$\mathrm{Ord}_P(Y) = 1, \quad \mathrm{Ord}_P(X) = 2, \quad \mathrm{Ord}_P(2Y^2 - X) = 2.$$

2.1.1 Divisors

In this thesis, we will deal with smooth curves unless otherwise stated.

Definition 2.10 *The divisor group of a curve C is the free abelian group generated by the points of C. It is denoted by* $\mathrm{Div}(C)$. *Hence a divisor $D \in \mathrm{Div}(C)$ is a formal sum*

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

where $n_P \in \mathbb{Z}$ and $n_P = 0$ for all but finitely many $P \in C$.
The degree of D is defined by

$$degD = \sum_{P \in C} n_P.$$

The divisors of degree 0 *form a subgroup of* $\mathrm{Div}(C)$, *which we denote by*

$$\mathrm{Div}^0(C) = \{D \in \mathrm{Div}(C) : degD = 0\}.$$

Definition 2.11 *A divisor $D \in \mathrm{Div}(C)$ is principal if it is of the form $D = \mathrm{div}(f)$ for some $f \in \bar{K}(C)^*$. Two divisors are linearly equivalent, written $D_1 \sim D_2$, if $D_1 - D_2$ is principal. The divisor class group (or Picard group) of C, denoted by* $\mathrm{Pic}(C)$, *is the quotient of* $\mathrm{Div}(C)$ *by its subgroup of principal divisors.*

Proposition 2.5 *Let C be a smooth curve and let $f \in \bar{K}(C)^*$.*

(a) $\mathrm{div}(f) = 0$ *if and only if $f \in \bar{K}^*$.*

(b) $deg(\mathrm{div}(f)) = 0$.

Definition 2.12 *We define the degree-*0 *part of the divisor class group of C as the quotient of* $\mathrm{Div}^0(C)$ *by the subgroup of principal divisors. We denote this group by* $\mathrm{Pic}^0(C)$.

Example 2.6 *We can observe that every divisor of degree 0 is principal on $\mathbb{P}^1$. Suppose that $D = \sum n_P(P)$ has degree 0. Let $P = [\alpha_P, \beta_P]$ be a point on $\mathbb{P}^1$. We see that D is the divisor of the function*

$$\prod_{P \in \mathbb{P}^1} (\beta_P X - \alpha_P Y)^{n_P}.$$

Note that $\sum n_P = 0$ ensures that this function is in $K(\mathbb{P}^1)$. It follows that the degree map $\deg : \mathrm{Pic}(\mathbb{P}^1) \to \mathbb{Z}$ *is an isomorphism. The converse is also true. i.e., if C is a smooth curve and* $\mathrm{Pic}(C) \cong \mathbb{Z}$, *then C is isomorphic to $\mathbb{P}^1$.*

2.2 Elliptic Curves

Let K be a field. An *elliptic curve* over K is a non-singular cubic projective curve over K with at least one point over K. It has an (affine) equation of the form

$$F(x,y) = ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0 \tag{2.1}$$

where the coefficients $a, b, \ldots, j \in K$, and the non-singularity means that for each point on the curve, considered in the projective plane $\mathbb{P}^2(\bar{K})$ over the algebraic closure of K, at least one partial derivative of F is non-zero.

2.2.1 Weierstrass Equations

The Weierstrass equation for an elliptic curve is written by using non-homogeneous coordinates x and y,

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{2.2}$$

If $a_1, \ldots, a_6 \in K$, then E is said to be defined over K.

One can show that the equation (2.1) can be written in the form of a Weierstrass equation after applying certain birational transformation.

A point at infinity appears naturally if we represent an elliptic curve in a projective plane. A *projective plane* $\mathbb{P}^2(K)$ is obtained by introducing on the set $K^3 - \{(0,0,0)\}$ the equivalence relation $(X,Y,Z) \sim (kX,kY,kZ),\ k \in K, k \neq 0$. By substituting $x = \frac{X}{Z}, y = \frac{Y}{Z}$ in the affine equation (2.2), we obtain the projective equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

If $Z \neq 0$, then the equivalence class of (X,Y,Z) has the representative $(x,y,1)$, so we can identify that class by (x,y). However, there is also an equivalence class which contains points with $Z = 0$. It has the representative $(0:1:0)$ and we identify that class with the point at infinity $\mathcal{O}$.

Also, if $\mathrm{char}(\bar{K}) \neq 2$, then we can simplify the equation by completing the square.

Thus the substitution

$$y \to \frac{1}{2}(y - a_1, x - a_3)$$

gives an equation of the form

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

where

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

We also define quantities

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,$$

$$c_4 = b_2^2 - 24b_4,$$

$$c_6 = -b_2^3 + 36b_2b_4 - 216b_6,$$

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,$$

One easily verifies that they satisfy the relations

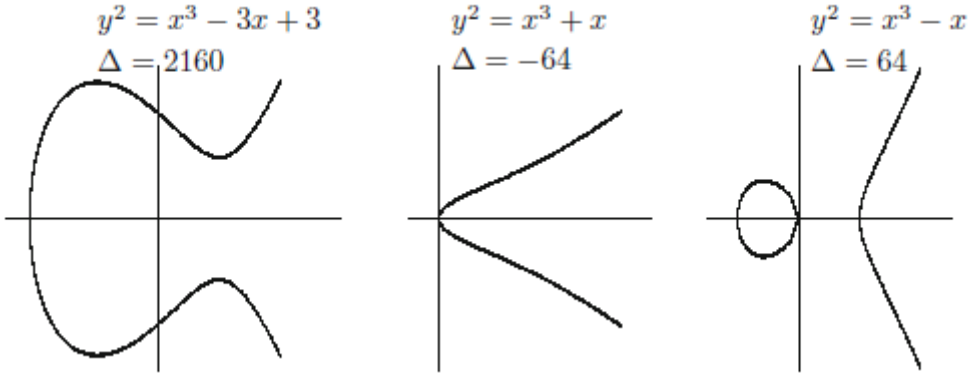
$$4b_8 = b_2b_6 - b_4^2 \quad \text{and} \quad 1728\Delta = c_4^3 - c_6^2.$$

Moreover, if the characteristic of the field K is different from 2 and 3, then this equation can be transformed into the form

$$y^2 = x^3 + ax + b \tag{2.3}$$

which we call the *short Weierstrass equation*. The condition of non-singularity now means that the cubic polynomial $f(x) = x^3 + ax + b$ does not have multiple roots (in the algebraic closure $\bar{K}$), which is equivalent to the condition that the *discriminant* $\Delta = -16(4a^3 + 27b^2)$ is non-zero.

One of the most important properties of elliptic curves is that on the set $E(K)$, of its K-rational points, we can, in a natural way, introduce an operation with which it will become an Abelian group. In order to explain that, let us take that $K = \mathbb{R}$. Then the elliptic curve $E(\mathbb{R})$ (without the point at infinity) can be represented as a subset of the plane. The polynomial $f(x)$ can either have one (if $\Delta < 0$) or three (if $\Delta > 0$) real roots. Depending on that, the graph of the corresponding elliptic curve has one or two components, as is shown in the following figures.



Example 2.7 *Assume that* $char(K) \neq 2$. *Let* $e_1, e_2, e_3 \in \bar{K}$ *be distinct, and consider the curve*

$$C : y^2 = (x - e_1)(x - e_2)(x - e_3).$$

One can check that C *is smooth and that it has a single point at infinity, which we denote* P_∞. *For* $i = 1, 2, 3$, *let* $P_i = (e_i, 0) \in C$. *Then*

$$\mathrm{div}(x - e_i) = 2(P_i) - 2(P_\infty) \quad \textit{and} \quad \mathrm{div}(y) = (P_1) + (P_2) + (P_3) - 3(P_\infty).$$

2.2.2 The Group Law

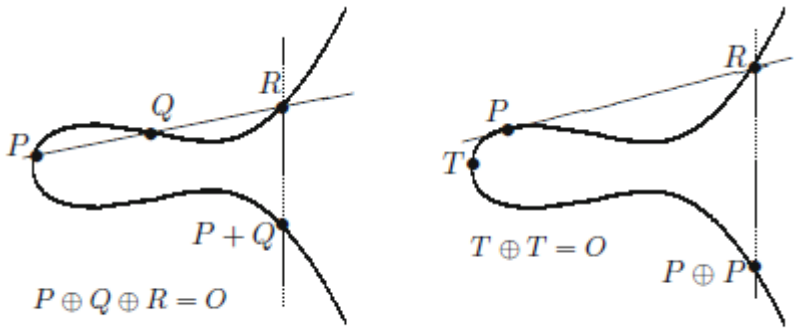
Let E be an elliptic curve given by a Weierstrass equation. Thus $E \subset \mathbb{P}^2$ consists of the points $P = (x, y)$ satisfying the Weierstrass equation, together with the point $\mathcal{O} = [0, 1, 0]$ at infinity. Let $L \subset \mathbb{P}^2$ be a line. Then, since the equation has degree three, the line L intersects E at exactly three points, say P, Q, R. Of course, if L is tangent to E, then P, Q, R need to be distinct. The fact that $L \cap E$, taken with multiplicities, consists of exactly three points is special case of Bezout's theorem [40, I.7.8].

2.2.2.1 Composition Law

Let $P, Q \in E$, let L be the line through P and Q (if $P = Q$, let L be the tangent line to E at P), and let R be the third point of intersection of L with E. Let L' be

the line through R and $\mathcal{O}$. Then L' intersects E at $R, \mathcal{O}$, and a third point. We denote that third point by $P \oplus Q$.

Various instances of the composition law are illustrated in the following figure. We now justify the use of the symbol $\oplus$.



Proposition 2.8 *The composition law has the following properties:*

(a) If a line L intersects E at the (not necessarily distinct) points P, Q, R, then

$$(P \oplus Q) \oplus R = \mathcal{O}.$$

(b) $P \oplus \mathcal{O} = P$ for all $P \in E$.

(c) $P \oplus Q = Q \oplus P$ for all $P, Q \in E$.

(d) Let $P \in E$. There is a point of E, denoted by $\ominus P$, satisfying

$$P \oplus (\ominus P) = \mathcal{O}$$

(e) Let $P, Q, R \in E$. Then

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

.

In other words, the composition law makes E into an abelian group with identity element $\mathcal{O}$. Further:

(f) Suppose that E is defined over K. Then

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

is a subgroup of E.

Notation. From now on, we drop the special symbols $\oplus$ and $\ominus$ and simply write $+$ and $-$ respectively. For $m \in \mathbb{Z}$ and $P \in E$, we let

$$[m]P = \underbrace{P + \cdots + P}_{\text{m terms if m>0}}, \quad [m]P = \underbrace{-P - \cdots - P}_{\text{|m| terms if m<0}}, \quad [0]P = \mathcal{O}.$$

2.2.2.2 Group Law Algorithm

Let E be an elliptic curve by a Weierstrass equation

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

(a) $P_0 = (x_0, y_0)$. Then

$$-P_0 = (x_0, -y_0 - a_1x_0 - a_3).$$

Next, let

$$P_1 + P_2 = P_3 \quad \text{with} \quad P_i = (x_i, y_i) \in E \quad \text{for} \quad i = 1, 2, 3.$$

(b) If $x_1 = x_2$ and $y_1 + y_2 + a_1x_2 + a_3 = 0$, then $P_1 + P_2 = \mathcal{O}$. Otherwise, define λ and ν by the following formulas:

	λ	ν
$x_1 \neq x_2$	$\frac{y_2 - y_1}{x_2 - x_1}$	$\frac{y_1x_2 - y_2x_1}{x_2 - x_1}$
$x_1 = x_2$	$\frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}$	$\frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}$

Then $y = \lambda x + \nu$ is the line through P_1 and P_2, or tangent to E if $P_1 = P_2$.

(c) With notation as in (b), $P_3 = P_1 + P_2$ has coordinates

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2,$$

$$y_3 = -(\lambda + a_1)x_3 - \nu - a_3.$$

(d) As special cases of (c), we have for $P_1 \neq \pm P_2$,

$$x(P_1 + P_2) = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 + a_1\left(\frac{y_2 - y_1}{x_2 - x_1}\right) - a_2 - x_1 - x_2,$$

and the duplication formula for $P=(x,y)\in E$,

$$x([2]P)=\frac{x^4-b_4x^2-2b_6x-b_8}{4x^3+b_2x^2+2b_4x+b_6},$$

where b_2,b_4,b_6,b_8 are the polynomial in the a_i's given above.

Example 2.9 *Let $E/\mathbb{Q}$ be the elliptic curve*

$$E: y^2=x^3+7x+4.$$

A brief inspection reveals some points with integer coordinates,

$$P_1=(0,-2),\ P_2=(\frac{49}{16},\frac{471}{64}).$$

To compute P_1+P_2, we find the line through P_1 and P_2. This is the line

$$y=\frac{599}{196}x-\frac{863}{196},\quad so\quad \lambda=\frac{599}{196}\quad and\quad \nu=-\frac{863}{196}.$$

Next

$$x_3=\lambda^2-x_1-x_2=-\frac{15072}{2401}\quad and\quad y_3=-\lambda x_3-\nu=-\frac{2021734}{117649}.$$

Finally, we find that

$$P_1+P_2=(x_3,y_3)=\left(-\frac{15072}{2401},-\frac{2021734}{117649}\right).$$

2.2.3 Torsion Group

The most celebrated theorem on elliptic curves over number fields is the Mordell-Weil theorem.

Theorem 2.1 (The Mordell-Weil Theorem) *A group $E(K)$ is a finitely generated Abelian group.*

In 1922, this theorem was proved by the British mathematician Louis Joel Mordell (1888-1972), while in 1928, the French mathematician André Weil (1906-1998) generalized it to Abelian varieties over number fields.

The Mordell-Weil theorem states that there is a finite set of rational points

$\{P_1, \ldots, P_k\}$ on E from which all other rational points on E can be obtained by using the secant-tangent construction. Since each finitely generated abelian group is isomorphic to the product of cyclic groups, [31, Chapter 5.2, Theorem 3], we obtain the following consequence of the Mordell-Weil theorem.

Definition 2.13 *Let E be an elliptic curve over K. The subgroup $E(K)_{\text{tor}}$ of $E(K)$ which consists of all points of finite order is called the torsion group of E, and the non-negative integer r is called the rank of E and it is denoted by $rank(E)$ (or more precisely by $\text{rank}(E(K))$).*

Corollary 2.1 *Given an elliptic curve E over K. Then*

$$E(K) \cong E(K)_{\text{tor}} \times \mathbb{Z}^r$$

where r is the rank of $E(K)$.

Definition 2.14 *The subgroup $E(\mathbb{Q})_{\text{tor}}$ of $E(\mathbb{Q})$ which consists of all points of finite order is called the torsion group of E, and the non-negative integer r is called the rank of E and it is denoted by $rank(E)$ (or more precisely by $rank(E(\mathbb{Q}))$).*

The corollary states that there are r rational points $P_1, \ldots, P_r$ of infinite order on curve E such that each rational point P on E can be represented in the form

$$P = T + m_1 P_1 + \cdots + m_r P_r,$$

where T is a point of finite order and $m_1, \ldots, m_r$ are integers. Here $m_1 P_1$ denotes the sum $P_1 + \cdots + P_1$ of m_1 summands, which is often also denoted by $[m_1]P_1$.

The following theorem is Mazur's classification of rational torsion points on elliptic curves defined over $\mathbb{Q}$, see [53] or [64, VIII.7, Theorem 7.5].

Theorem 2.2 (Mazur, [53]) *Let $E/\mathbb{Q}$ be an elliptic curve. Then the torsion subgroup $E_{tor}(\mathbb{Q})$ of $E(\mathbb{Q})$ is isomorphic to one of the following fifteen groups:*

$$\mathbb{Z}/k\mathbb{Z} \quad \text{for } k = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z} \quad \text{for } k = 2, 4, 6, 8.$$

Further, each of these groups occurs as $E_{tor}(\mathbb{Q})$ for some elliptic curve $E/\mathbb{Q}$.

The following theorem gives a complete classification of possible torsion points of elliptic curves over quadratic fields established in [47, 48, 55] after a series of papers.

Theorem 2.3 *Let K be a quadratic field and E an elliptic curve over K. Then the torsion subgroup $E(K)_{tor}$ of $E(K)$ is isomorphic to one of the following 26 groups:*

$$\mathbb{Z}/m\mathbb{Z} \quad \text{for } 1 \leq m \leq 18,\ m \neq 17,$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z} \quad \text{for } 1 \leq m \leq 6,$$

$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3m\mathbb{Z} \quad \text{for } m = 1, 2$$

$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

The following theorem completes the classification of torsion over cubic number fields, see [9].

Theorem 2.4 *Let $K/\mathbb{Q}$ be a cubic extension and E/K be an elliptic curve. Then $E(K)$ is isomorphic to one of the following 26 groups:*

$$\mathbb{Z}/N_1\mathbb{Z} \quad \text{with } N_1 = 1, \ldots, 16, 18, 20, 21,$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N_2\mathbb{Z} \quad \text{with } N_2 = 1, \ldots, 7.$$

There exist finitely many $\bar{\mathbb{Q}}$-isomorphism classes for each torsion subgroup except for $\mathbb{Z}/21\mathbb{Z}$. In this case, we base change of the elliptic curve 162b1 *to $\mathbb{Q}(\zeta_9)^+$ is the unique elliptic curve over a cubic field with $\mathbb{Z}/21\mathbb{Z}$-torsion.*

The following theorem, which is about a complete classification for torsion points of elliptic curves defined over Galois quartic fields, is given in [5].

Theorem 2.5 *Let $E/\mathbb{Q}$ be an elliptic curve, and let K be a quartic Galois extension of $\mathbb{Q}$. Then $E(K)_{tor}$ is isomorphic to one of the following groups:*

$$\mathbb{Z}/N_1\mathbb{Z} \quad \text{for } N_1 = 1, \ldots, 16,\ N_1 \neq 11, 14,$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N_2\mathbb{Z} \quad \text{for } N_2 = 1, \ldots 6, 8,$$

$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3N_3\mathbb{Z} \quad \text{for } N_3 = 1, 2,$$

$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4N_4\mathbb{Z} \quad \text{for } N_4 = 1, 2,$$

$$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z},$$

$$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}.$$

Each of these groups, except for $\mathbb{Z}/15\mathbb{Z}$, appears as the torsion structure over some quartic Galois field for infinitely many (non-isomorphic) elliptic curves defined over $\mathbb{Q}$.

2.3 Dynamical Systems

We start with the definition of a dynamical system. Also, the following definitions can be found in [63] with the change of some notations.

Definition 2.15 *A dynamical system is a set S together with a self-map $f : S \to S$ that allows iterations. The n^{th}-iterate of f is*

$$f^n = \underbrace{f \circ f \circ \cdots \circ f}_{n \text{ times}}.$$

By convention, f^0 is the identity map, i.e., $f^0(x) = x$.

Definition 2.16 *For a given point $x_0 \in S$, the (forward) orbit of x_0 under the map f is the set*

$$\mathrm{Orb}_f(x_0) = \mathrm{Orb}(x_0) \quad = \quad \{f^n(x_0) : n \geq 0\}.$$

Definition 2.17 *The point $x_0 \in S$ is called a periodic point under f, if there exists an integer $n > 0$ such that $f^n(x_0) = x_0$. The orbit of x_0 is called a periodic orbit.*

An integer n such that $f^n(x_0) = x_0$ is called a period of x_0. The smallest such integer n is called the exact period of x_0. We also say that the point x_0 has period type $(0, n)$.

Definition 2.18 *The point $x_0 \in S$ is called a preperiodic point under f, if there exists an integer $m \geq 0$ such that $f^m(x_0)$ is periodic, i.e., x_0 is preperiodic if $\mathrm{Orb}_f(x_0)$ is finite. The orbit of x_0 is called a preperiodic orbit. If $m \neq 0$, then the point x_0 is called a strictly preperiodic point.*

The least such integer m is the tail length of the orbit, whereas the exact period of $f^m(x_0)$ is the eventual period. If the orbit of x_0 has a tail length m and an eventual period n, then we say that s has a period type (m, n).

Definition 2.19 *The sets of periodic and preperiodic points of f in S are denoted by*

$$\begin{aligned} Per(f, S) &= \{x_0 \in S : f^n(x_0) = x_0 \text{ for some } n \geq 1\} \\ PrePer(f, S) &= \{x_0 \in S : f^{n+m}(x_0) = f^m(x_0) \text{ for some } n \geq 1, m > 0\} \\ &= \{x_0 \in S : \mathrm{Orb}_f(x_0) \text{ is finite}\}. \end{aligned}$$

We write $Per(f)$ and $PrePer(f)$ when the set S is fixed.

The following Proposition, which is the classification of quadratic polynomial maps with periodic points of periods 1, 2, or 3, can be found in [56, Theorem 1].

Theorem 2.6 *Let $f(x) = x^2 + c$ with $c \in \mathbb{Q}$. Then*

1) $f(x)$ has a rational point of period 1, i.e., a rational fixed point, if and only if $c = 1/4 - \rho^2$ for some $\rho \in \mathbb{Q}$. In this case, there are exactly two, $1/2 + \rho$ and $1/2 - \rho$, unless $\rho = 0$, in which case they coincide.

2) $f(x)$ has a rational point of period 2 if and only if $c = -3/4 - \sigma^2$ for some $\sigma \in \mathbb{Q}$, $\sigma \neq 0$. In this case, there are exactly two, $-1/2 + \sigma$ and $-1/2 - \sigma$ (and these form a 2-cycle).

3) $f(x)$ has a rational point of period 3 if and only if

$$c = -\frac{\tau^6 + 2\tau^5 + 4\tau^4 + 8\tau^3 + 9\tau^2 + 4\tau + 1}{4\tau^2(\tau+1)^2}$$

for some $\tau \in \mathbb{Q}$, $\tau \neq -1, 0$. In this case, there are exactly three,

$$x_1 = \frac{\tau^3 + 2\tau^2 + \tau + 1}{2\tau(\tau+1)}, \quad x_2 = \frac{\tau^3 - \tau - 1}{2\tau(\tau+1)}, \quad x_3 = -\frac{\tau^3 + 2\tau^2 + 3\tau + 1}{2\tau(\tau+1)}$$

and these are cyclically permuted by $f(x)$.

3. Divisibility by 2 on quartic models of elliptic curves

Chapter 3 and Chapter 4 contain the studies in our published article, [60].

Let C be a smooth genus one curve described by a quartic polynomial equation over the rational field $\mathbb{Q}$ with $P \in C(\mathbb{Q})$. In this chapter, we give an explicit criterion for the divisibility-by-2 of a rational point on the elliptic curve (C, P). This provides an analogue to the classical criterion of the divisibility-by-2 on elliptic curves described by the Weierstrass equations. Finally, we show how to characterize elliptic curves described by quartic polynomial equations that possess rational 4-torsion points.

3.1 Models of elliptic curves

In this section, we introduce the genus one curve models that we are going to use throughout this thesis.

3.1.1 Quartic models

We recall that a *Weierstrass equation* is an equation of the form

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

where the coefficients $a_1, \cdots, a_6$ are lying in a field K. One may associate to such equation the invariants c_4, c_6 and Δ which are polynomials in $a_1, \cdots, a_6$ with integer coefficients satisfying $1728\Delta = c_4^3 - c_6^2$, [64, Chapter III]. If $\Delta \neq 0$, then the Weierstrass equation describes a smooth projective genus one curve with a K-rational

point at infinity on the curve, i.e., an elliptic curve. Two such equations describe the same curve if they are related via a transformation of the form

$$x \mapsto u^2x+r, \qquad y \mapsto u^3y+u^2sx+t$$

for some $u \in K^\times$, $r,s,t \in K$. Therefore, if $\operatorname{char} K \neq 2,3$, a Weierstrass equation can be written as $y^2 = x^3+Ax+B$ for some $A,B \in K$.

Definition 3.1 *A* quartic model *is an equation of the form $y^2+P(x)y=Q(x)$ where P and Q are polynomials of degree 2 and 4, respectively, with coefficients in K.*

If $Q(x)+P(x)^2/4 = ax^4+bx^3+cx^2+dx+e$, then we attach to the quartic model the invariants $c_4 = 2^4I$ and $c_6 = 2^5J$ where

$$\begin{aligned} I &= 12ae-3bd+c^2, \\ J &= 72ace-27ad^2-27b^2e+9bcd-2c^3. \end{aligned}$$

Moreover, the discriminant $\Delta = (c_4^3-c_6^2)/1728$ is 16 times the usual discriminant of a quartic polynomial. We find that c_4, c_6 and Δ are primitive integer coefficient polynomials in the coefficients of P and Q, again satisfying $c_4^3-c_6^2 = 1728\Delta$.

The following Theorem in [8], has properties of c_4, c_6, Δ.

Theorem 3.1 *Let C be a genus 1 curve defined by a quartic model. The following statements hold.*

(i) The polynomials c_4, c_6, Δ are invariants of the curve C.

(ii) A quartic model defines a smooth curve C of genus one (over $\bar{K}$) if and only if $\Delta \neq 0$.

(iii) If $char(K) \neq 2,3$ then c_4 and c_6 generate the ring of invariants. Moreover if $\Delta \neq 0$ then the Jacobian of the curve C has Weierstrass equation

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

If the set of K-rational points $C(K)$ of C is non-empty, then the quartic model describes an elliptic curve. Two such models describe the same curve if they are related via a transformation of the form

$$x \mapsto (a_{11}x+a_{21})/(a_{12}x+a_{22}), \qquad y \mapsto \mu y+rx^2+sx+t$$

where $(a_{ij}) \in \mathrm{GL}_2(K)$, $\mu \in K^\times$, $r,s,t \in K$. It follows that if $\operatorname{char} K \neq 2,3$, then a

quartic model can be written in the form $y^2 = P(x)$ where $P(x)$ is a polynomial of degree 4 with coefficients in K.

3.1.2 Group law on quartic models

Let K be a field. The set of K-rational points on an elliptic curve E defined over K is an abelian group. If the curve is given by a Weierstrass equation, then the group law is described using the chord and tangent process. Given a smooth genus one curve C that possesses a K-rational point and defined by a quartic model, one uses the isomorphism between the curve C and its Jacobian to define the group law on C.

We consider a quartic model $y^2 = f(x)$ where $f(x) \in K[x]$, $\deg f(x) = 4$, and the discriminant of the model is nonzero, or equivalently, $f(x)$ has no multiple roots. This quartic model describes a smooth genus one curve over K. The Jacobian of C will be denoted by E.

The following proposition can be found in [7, Proposition 4.1].

Proposition 3.1 *Let C be a curve over K defined as above. Then C has a K-rational point if and only if the leading coefficient of $f(x)$ is square.*

PROOF: If the leading coefficient of $f(x)$ is square, say a^2, then $(1 : a : 0)$ a K-rational point on C. Conversely, if C has a K-rational point, we may apply a projective transformation to send its x-coordinate to infinity, thereby replacing $f(x)$ by an equivalent quartic whose leading coefficient is a square. □

From now on, we assume that $C(K) \neq \emptyset$. By Proposition 3.1, this allows us to assume that the leading coefficient (or the constant term) of $f(x)$ is a square in K. In this case, if the leading coefficient of $f(x)$ is a square a^2, $a \in K$, we set ∞_+ and ∞_- to be the two rational points at infinity, namely, $(x : y : z) = (1 : a : 0)$ and $(1 : -a : 0)$, respectively.

We fix a point $P \in C(K)$. Let ϕ_P be a K-birational isomorphism between C and E

$$\phi_P : C \longrightarrow E \quad \text{such that} \quad \phi_P(P) = O_E.$$

The map ϕ_P may be used to define an abelian group structure on C as follows

$$Q_1 +_P Q_2 = \phi_P^{-1}(\phi_P(Q_1) + \phi_P(Q_2))$$

with P the identity on $(C, +_P)$.

In particular, we say that $S \in nC(K)$, $n \geq 2$, if $S = \underbrace{Q +_P \cdots +_P Q}_{n-\text{times}}$ for some $Q \in C(K)$. This identifies $nC(K)$ with $nE(K)$.

3.2 2-Divisibility on quartic models

Let K be a perfect field of characteristic different from 2. In this section, we consider quartic models $y^2 = f(x)$ where $f(x)$ is a polynomial of degree 4 with coefficients in K and no multiple roots. We assume moreover that $f(x)$ splits completely in K. In other words, a quartic model will be of the form

$$y^2 = f(x) := (a_1x + b_1)(a_2x + b_2)(a_3x + b_3)(a_4x + b_4),$$

$a_i \in K^\times, b_i \in K$, $(a_ix + b_i)/(a_jx + b_j) \notin K$ for $i \neq j$ and it describes a smooth genus one curve C over K. The existence of the points $Q_i := (-b_i/a_i, 0) \in C(K)$, $1 \leq i \leq 4$, imlies that $C(K) \neq \emptyset$. We notice that $\infty_+, \infty_- \in C(K(\sqrt{a_1a_2a_3a_4}))$. We set $f_i(x) := a_ix + b_i$ and $c_i = -b_i/a_i$, $1 \leq i \leq 4$.

We will always assume the existence of a rational point $(x_0, y_0) \in C(K)$ different from the points Q_i, $1 \leq i \leq 4$. In particular, $|C(K)| > 4$. We fix throughout a K-birational isomorphism $\phi : C \to E := \mathrm{Jac}(C)$ such that $\phi(x_0, y_0) = O_E$.

Now, we define the following rational maps $g_{ij} \in K(E)$, $1 \leq i, j \leq 4$, as follows

$$g_{ij}(P) = f_i(x_0)f_j(x_0)f_i(x(\phi^{-1}(P)))f_j(x(\phi^{-1}(P)))$$

where $x(\phi^{-1}(P))$ is the x-coordinate of $\phi^{-1}(P) \in C(K)$. It is clear that $g_{ij}(O_E) = f_i(x_0)^2 f_j(x_0)^2 \in (K^\times)^2$.

The following two propositions give properties of the maps g_{ij} that we are going to use during the course of the proof of the main theorem of this section. These properties have been proved for other rational maps on different models of elliptic curves, see for example [43, Chapter 6], [49, Chapter IV], and [12].

Proposition 3.2 *Let $[2] : E \to E$ be the multiplication by-2-morphism on E. There exist $h_{ij} \in K(E)$ such that $g_{ij} \circ [2] = h_{ij}^2$ for all i, j.*

PROOF: One can see that $\mathrm{div}(g_{ij}) = 2\phi(Q_i) + 2\phi(Q_j) - 2\phi(\infty_+) - 2\phi(\infty_-)$.

We set $[2]^* : \mathrm{Div}(E) \to \mathrm{Div}(E)$ to be the map $(Q) \mapsto \sum_{P \in [2]^{-1}Q}(Q)$. Let $\tilde{h}_{ij} \in \overline{K}(E)$ be such that

$$\begin{aligned} \mathrm{div}(\tilde{h}_{ij}) &= [2]^*(\phi(Q_i) + \phi(Q_j) - \phi(\infty_+) - \phi(\infty_-)) \\ &= \sum_{T \in E[2]} (M_i + T) + \sum_{T \in E[2]} (M_j + T) - \sum_{T \in E[2]} (N_1 + T) - \sum_{T \in E[2]} (N_2 + T) \end{aligned}$$

where $2M_i = \phi(Q_i),\ 2M_j = \phi(Q_j),\ 2N_1 = \phi(\infty_+),\ 2N_2 = \phi(\infty_-)$. Then we can observe that

$$\mathrm{div}(g_{ij} \circ [2]) = 2\,\mathrm{div}(\tilde{h}_{ij}) = \mathrm{div}(\tilde{h}_{ij}^2).$$

There exists $r \in \overline{K}$ such that $r\tilde{h}_{ij}^2 = g_{ij} \circ [2]$, see for example [35, Theorem 7.8.3]. We define $h_{ij} = \tilde{h}_{ij}\sqrt{r}$.

It is clear that $\tilde{h}_{ij} \in K(E)$ for all i, j. This follows by choosing $\sigma \in \mathrm{Gal}(\overline{K}/K)$ and observing that σ permutes the zeros of $\tilde{h}_{ij}$, and the poles of $\tilde{h}_{ij}$, respectively. More precisely,

$$O_E = (\phi(Q_i))^\sigma - \phi(Q_i) = (2M_i)^\sigma - 2M_i = 2(M_i^\sigma - M_i),$$

hence $M_i^\sigma = M_i + T$ where $T \in E[2]$. Same holds if one replaces M_i with N_i. It is left to show that $r \in (K^\times)^2$. This holds by evaluating both sides of the equality $r\tilde{h}_{ij}^2 = g_{ij} \circ [2]$ at O_E. The statement holds as $g_{ij}(O_E) \in (K^\times)^2$. □

Proposition 3.3 *For any $P, Q \in E(K)$, one has*

$$g_{ij}(P + Q) \equiv g_{ij}(P) g_{ij}(Q) \mod K^2.$$

PROOF: When $i = j$, the statement is straightforward, so we may pick $i \neq j$ and set $g := g_{ij}$. According to Proposition 3.2, we see that $g \circ [2] = h^2$ for some $h \in K(E)$.

Let $P = 2\tilde{P},\ Q = 2\tilde{Q}$. First we will prove

$$\frac{(h(\tilde{P} + \tilde{Q}))^\sigma}{h(\tilde{P} + \tilde{Q})} = \frac{(h(\tilde{P}))^\sigma}{h(\tilde{P})} \frac{(h(\tilde{Q}))^\sigma}{h(\tilde{Q})} \tag{3.1}$$

for every $\sigma \in \mathrm{Gal}(\bar{K}/K)$. Fix $T \in E[2]$, we have $h^2(S + T) = g \circ [2](S + T) = g \circ [2](S) = h^2(S)$ for any $S \in E$, so $\frac{h(S+T)}{h(S)} = \pm 1$. Considering the morphism $E \to \mathbb{P}^1$ induced by the rational map $S \mapsto h(S + T)/h(S)$, one then may assume that it must be a constant map. Since $2\tilde{P} = P \in E(K),\ \ 2\tilde{Q} = Q \in E(K)$, we get $\tilde{P}^\sigma - \tilde{P} \in$

$E[2], \tilde{Q}^\sigma - \tilde{Q} \in E[2]$, $(\tilde{P}+\tilde{Q})^\sigma - (\tilde{P}+\tilde{Q}) \in E[2]$ for every $\sigma \in \mathrm{Gal}(\bar{K}/K)$. Now we have

$$\frac{(h(\tilde{P}))^\sigma}{h(\tilde{P})} = \frac{h(\tilde{P}^\sigma)}{h(\tilde{P})} = \frac{h(\tilde{P}+(\tilde{P}^\sigma - \tilde{P}))}{h(\tilde{P})} = \frac{h(S+(\tilde{P}^\sigma - \tilde{P}))}{h(S)} \quad \text{for any } S \in E$$

Similarly,

$$\frac{(h(\tilde{Q}))^\sigma}{h(\tilde{Q})} = \frac{h(S+(\tilde{Q}^\sigma - \tilde{Q}))}{h(S)}, \quad \text{and } \frac{(h(\tilde{P}+\tilde{Q}))^\sigma}{h(\tilde{P}+\tilde{Q})} = \frac{h(S+(\tilde{P}+\tilde{Q})^\sigma - (\tilde{P}+\tilde{Q}))}{h(S)} \quad \text{for any } S \in E.$$

Therefore,

$$\begin{aligned} \frac{(h(\tilde{P}+\tilde{Q}))^\sigma}{h(\tilde{P}+\tilde{Q})} &= \frac{h(S+(\tilde{P}+\tilde{Q})^\sigma - (\tilde{P}+\tilde{Q}))}{h(S)} = \frac{h(S+(\tilde{P}+\tilde{Q})^\sigma - (\tilde{P}+\tilde{Q}))}{h(S+(\tilde{P})^\sigma - \tilde{P})} \frac{h(S+\tilde{P}^\sigma - \tilde{P})}{h(S)} \\ &= \frac{(h(\tilde{Q}))^\sigma}{h(\tilde{Q})} \frac{(h(\tilde{P}))^\sigma}{h(\tilde{P})} \end{aligned}$$

This gives

$$\frac{h(\tilde{P}+\tilde{Q})}{h(\tilde{P})h(\tilde{Q})} = \frac{(h(\tilde{P}+\tilde{Q}))^\sigma}{(h(\tilde{P}))^\sigma (h(\tilde{Q}))^\sigma} = \left(\frac{h(\tilde{P}+\tilde{Q})}{h(\tilde{P})h(\tilde{Q})}\right)^\sigma$$

for every $\sigma \in \mathrm{Gal}(\bar{K}/K)$. Now we have

$$\frac{h(\tilde{P}+\tilde{Q})}{h(\tilde{P})h(\tilde{Q})} \in K, \text{ i.e., } \quad h^2(\tilde{P}+\tilde{Q}) \equiv h^2(\tilde{P})h^2(\tilde{Q}) \mod K^2.$$

Thus,

$$g(P+Q) = g \circ [2](\tilde{P}+\tilde{Q}) = h^2(\tilde{P}+\tilde{Q}) \equiv h^2(\tilde{P})h^2(\tilde{Q}) = g(P)g(Q) \mod K^2.$$

□

Theorem 3.2 *Let C be a smooth genus 1 curve over $\mathbb{Q}$ defined by an equation of the form*

$$y^2 = (a_1x+b_1)(a_2x+b_2)(a_3x+b_3)(a_4x+b_4), \qquad \text{where } a_i \in \mathbb{Q}^\times, b_i \in \mathbb{Q}.$$

Let $(x_0, y_0) \in C(\mathbb{Q})$ be such that $x_0 \neq -b_i/a_i$, $i = 1,2,3,4$. We set $\phi : C \longrightarrow E := J(C)$ to be a $\mathbb{Q}$-birational isomorphism with $\phi((x_0,y_0)) = O_E$. For $Q \in C(\mathbb{Q})$, one has

$Q \in 2C(\mathbb{Q})$ if and only if $f_i(x_0)\, f_j(x_0)\, f_i(x(Q)) f_j(x(Q)) \in \mathbb{Q}^2$ for all $i,j \in \{1,2,3,4\}$ where $f_i(x) = a_ix + b_i$.

PROOF:The statement that $Q \in 2C(\mathbb{Q})$ implies that $f_i(x_0)\, f_j(x_0)\, f_i(x(Q))f_j(x(Q)) \in \mathbb{Q}^2$ is a direct consequence of Proposition 3.2.

So we assume that $Q \in C(\mathbb{Q})$ is such that $f_i(x_0)\, f_j(x_0)\, f_i(x(Q))f_j(x(Q)) \in \mathbb{Q}^2$. Let $P \in E(\mathbb{Q})$ be such that $\phi^{-1}(P) = Q$. It suffices to show that if $g_{ij}(P) \equiv 1 \mod \mathbb{Q}^2$ for all i, j, then $P \in 2E(\mathbb{Q})$.

Set $[2]^{-1}P = \{R_i : 1 \leq i \leq 4\} \subset E$. Let fix $R \in [2]^{-1}P$. We also set $R_{C,i} = \phi^{-1}(R_i) \in C$, $i = 1, 2, 3, 4$. We recall that $R_i = R + T_i$ for some $T_i \in E[2]$. A simple calculation of the Jacobian E shows that $E(\mathbb{Q})[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, hence all 2-torsion points of E are rational. It follows that $[\mathbb{Q}(x(R_i), y(R_i)) : \mathbb{Q}]$ is fixed for all $i = 1, 2, 3, 4$.

Recall that $g_{ij} \in K(E)$, $1 \leq i, j \leq 4$, is defined as follows

$$g_{ij}(P) = f_i(x_0)f_j(x_0)f_i(x(\phi^{-1}(P)))f_j(x(\phi^{-1}(P)))$$

where $x(\phi^{-1}(P))$ is the x-coordinate of $\phi^{-1}(P) \in C(K)$. By Proposition 3.3, we have

$$g_{ij}(P) = g_{ij}(2R_m) \equiv g_{ij}(R_m)^2 \mod \mathbb{Q}^2, \qquad m = 1, 2, 3, 4.$$

However, one knows that $g_{ij}(P) \in \mathbb{Q}^2$ by assumption. It follows that $g_{ij}(R_m) \in \mathbb{Q}$. Since $g_{ij}(R_m) = f_i(x_0)f_j(x_0)f_i(x(R_{C,m}))f_j(x(R_{C,m}))$, it follows that $[\mathbb{Q}(x(R_{C,m})) : \mathbb{Q}] \leq 2$. Writing $x(R_{C,m}) = A + B\sqrt{D}$ for some $A, B, D \in \mathbb{Q}$, one sees that

$$\frac{g_{12}(R_m)}{f_1(x_0)f_2(x_0)} = (a_1(A + B\sqrt{D}) + b_1)(a_2(A + B\sqrt{D}) + b_2) \in \mathbb{Q}^*.$$

Therefore, either $B = 0$ or $a_1b_2 + 2a_1a_2A + a_2b_1 = 0$. If $B \neq 0$, then $A = \frac{-a_1b_2 - a_2b_1}{2a_1a_2}$. In a similar fashion, since $\frac{g_{13}(R_m)}{f_1(x_0)f_3(x_0)} \in \mathbb{Q}$, one has $A = \frac{-a_1b_3 - a_3b_1}{2a_1a_3}$. One concludes that $\frac{b_2}{a_2} = \frac{b_3}{a_3}$, which contradicts the fact that the points $(-b_i/a_i, 0) \in C$ must be distinct. It follows that $B = 0$, i.e., $x(R_{C,m}) \in \mathbb{Q}$. Since $y(R_{C,m})^2 = f_1(x(R_{C,m}))f_2(x(R_{C,m}))f_3(x(R_{C,m}))f_4(x(R_{C,m}))$, the latter implies that $y(R_{C,m}) \in \mathbb{Q}$ or $y(R_{C,m}) = K\sqrt{D}$ for some $K \in \mathbb{Q}$ and $D \in \mathbb{Q}^*/\mathbb{Q}^{*2}$. In particular, $\mathbb{Q}(R_{C,m}) = \mathbb{Q}(\sqrt{D})$. Since ϕ is a $\mathbb{Q}$-birational isomorphism, it follows that $\mathbb{Q}(R_m) = \mathbb{Q}(\sqrt{D})$. Moreover, from the observation above, all R_m are $\mathbb{Q}$-rational, or all are defined over $\mathbb{Q}(\sqrt{D}) \setminus \mathbb{Q}$.

One knows that since $P \in E(\mathbb{Q})$, it follows that

$$P = P^\sigma = (2R)^\sigma = 2R^\sigma$$

for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. In addition, since $\phi^{-1}(S^\sigma) = (\phi^{-1}(S))^\sigma$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

and $S \in E$. Therefore, we may assume without loss of generality that

$$R_{C,1} = (u_1, u_2\sqrt{D}),\ \ R_{C,2} = (u_1, -u_2\sqrt{D}),\ \ R_{C,3} = (v_1, v_2\sqrt{D})\ \ R_{C,4} = (v_1, -v_2\sqrt{D}),$$

where $u_1, v_1, u_2, v_2 \in \mathbb{Q}$.

We observe that $g_{ij}(R_1)g_{ij}(R_2) \in \mathbb{Q}^2$, we also see that $g_{ij}(R_1)g_{ij}(R_2) \equiv g_{ij}(P+T_1)$ for some $T_1 \in E[2]$ for $i,j \in \{1,2,3,4\}$. In view of Proposition 3.3, we obtain that $g_{ij}(T_1) \in \mathbb{Q}^2$ for $i,j \in \{1,2,3,4\}$. Repeating the argument above for R_3 and R_4, we get that $g_{ij}(T_2)$ for some $T_2 \in E[2]$, $T_2 \neq T_1$. Noticing that $T_2 \pm T_1 \in E[2]$, it follows that $g_{ij}(T) \in \mathbb{Q}^2$ for all $i,j = 1,2,3,4$, and all $T \in E[2]$.

Using the fact that $g_{ij}(T) \in \mathbb{Q}^2$ for all $T \in E[2]$, we may replace the point P in the argument above with a point $T \in E[2]$. In particular, as seen above, this leads to the following: Given $T_i \in E[2]$, $i = 1,2,3,4$, there exists $T_i^j \in E$ such that $2T_i^j = T_i$, $j = 1,2,3,4$, where $T_i^1, T_i^2, T_i^3, T_i^4$ are all in $E(\mathbb{Q})$ or all in $E(\mathbb{Q}(\sqrt{d_i})) \setminus E(\mathbb{Q})$ for some square free integer $d_i \neq 0$. Now since $2(T_i^j \pm T_s^t) \in E[2]$, then this implies that all $T_i^j \in E(K)$, for all $1 \leq i,j \leq 4$, where K is either $\mathbb{Q}(\sqrt{D})$ or $\mathbb{Q}(\sqrt{D}, \sqrt{D'})$ where D and D' are square free integers. The fact that T_i^j cannot be all in $E(\mathbb{Q})$ is due to Theroem 2.2.

Now we rule out the possibility that T_i^j are lying in $E(K)$ where K is either $\mathbb{Q}(\sqrt{D})$ or $\mathbb{Q}(\sqrt{D}, \sqrt{D'})$, hence $R_{C,i}$ should have all lived in $C(\mathbb{Q})$ for $i = 1,2,3,4$. If $K = \mathbb{Q}(\sqrt{D})$, then this means that the torsion part of $E(K)$ contains complete 2-torsion where for each 2-torsion point T_i there are 4 distinct torsion point T_i^j such that $4T_i^j = T_i$. In particular, if an elliptic curve is defined over $E(\mathbb{Q}(\sqrt{D}))$ with a non-cyclic torsion group containing $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, then by the Theorem 2.3 it should be one of the following groups

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}, 1 \leq m \leq 6, \qquad \text{or } \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$

where it can be seen easily that it is impossible for the 2-torsion points to satisfy the aforementioned property.

Now we rule out the possibility that $K = \mathbb{Q}(\sqrt{D}, \sqrt{D'})$. If an elliptic curve is defined over $E(K)$ with a non-cyclic torsion group containing $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, then it should be one of the following groups, see Theorem 2.5,

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}, 1 \leq m \leq 8, \qquad \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4n\mathbb{Z}, n = 1,2, \qquad \text{or } \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}.$$

Again one may check that for neither of these groups all two torsion points are divisible by 4. Hence when $g_{ij}(P) \in \mathbb{Q}^2$, for all $i,j = 1,2,3,4$, then $R_{C,i} \in C(\mathbb{Q})$, in

particular $Q = \phi^{-1}(P) \in 2C(\mathbb{Q})$. $\square$

Remark 3.1 *In Theorem 3.2, if (x_0, y_0) is chosen to be ∞_+, then g_{ij} becomes*

$$g_{ij}(P) = a_i a_j f_i(x(\phi^{-1}(P)))f_j(x(\phi^{-1}(P))).$$

In this case we assume $a_1a_2a_3a_4 \in (K^\times)^2$ to make sure that the points $\infty_\pm$ are in $C(\mathbb{Q})$.

3.3 Examples

Let C be defined over a perfect field K by the following quartic model

$$v^2 = au^4 + bu^3 + cu^2 + du + q^2$$

where $a, b, c, d \in K$ and $q \in K^*$. The birational isomorphism $\phi_1 : C \to E := J(C)$ is defined by

$$x = (2q(v+q) + du)/u^2 \quad \text{and} \quad y = (4q^2(v+q) + 2q(du + cu^2) - d^2u^2/2q)/u^3$$

where E is described by

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

and

$$a_1 = d/q, \quad a_2 = c - d^2/4q^2, \quad a_3 = 2qb, \quad a_4 = -4q^2a, \quad a_6 = a_2a_4,$$

see [6, Chapter 1, Proposition 1.2.1]. The inverse map is given by

$$u = (2q(x+c) - d^2/2q)/y, \qquad v = -q + u(ux - d)/2q.$$

In view of Theorem 3.2, the point (x_0, y_0) is $(0, q)$ as $\phi(0, q) = O_E$.

Example 3.4 *Let C : $v^2 = (u+1)(2u+1)(8u+1)(9u+1)$. We consider the map $\phi_1 : C \to E$ defined above, where*

$$E : \quad y^2 + 20xy + 500y = x^3 + 25x^2 - 576x - 14400.$$

We start with the point $T=(3,140)\in C(\mathbb{Q})$. *Then*

$$\phi_1(T)=(38,42),\quad \textit{and } 2\phi_1(T)=(-2375/144,-29155/1728)\in E(\mathbb{Q}).$$

Now $Q=\phi_1^{-1}(2\phi_1(T))=(-120/119,9889/14161)\in 2C(\mathbb{Q})$. *Setting* $f_1(u)=u+1$, $f_2(u)=2u+1$, $f_3(u)=8u+1$ *and* $f_4(u)=9u+1$, *we see that*

$$f_1\Big(\frac{-120}{119}\Big)=\frac{-1}{119},\quad f_2\Big(\frac{-120}{119}\Big)=\frac{-121}{119},\quad f_3\Big(\frac{-120}{119}\Big)=\frac{-841}{119},\quad f_4\Big(\frac{-120}{119}\Big)=\frac{-981}{119}.$$

Since $f_i(0)=1$ *for* $i=1,2,3,4$, *it follows that*

$$g_{ij}(2\phi_1(T))=f_i\,(-120/119)\,f_j\,(-120/119)\in\mathbb{Q}^2\quad \textit{for all } i,j=1,2,3,4.$$

Example 3.5 *Let* $C:\ v^2=(u+2)(u+5)(u+6)(u+15)$. *Then the transformation* ϕ_1 *gives the elliptic curve*

$$E:\quad y^2+28xy+1680y=x^3+51x^2-3600x-183600.$$

Considering the point $T=(-5/9,1820/81)\in C(\mathbb{Q})$, *we obtain*

$$\phi_1(T)=(8688,-943812),\quad \textit{and } 2\phi_1(T)=(\frac{722192509}{342225},\frac{-26636791574008}{200201625})\in E(\mathbb{Q}).$$

Now the point $\phi_1^{-1}(2\phi_1(T))=(-\frac{982800}{1008361},\frac{43031054907914370}{1016791906321})$ *lies in* $2C(\mathbb{Q})$. *We see that*

$$f_1\Big(-\frac{982800}{1008361}\Big)=\frac{1033922}{1008361},\quad f_2\Big(-\frac{982800}{1008361}\Big)=\frac{4059005}{1008361},$$

$$f_3\Big(-\frac{982800}{1008361}\Big)=\frac{5067366}{1008361},\quad f_4\Big(-\frac{982800}{1008361}\Big)=\frac{14142615}{1008361}$$

where $f_1(u)=u+2$, $f_2(u)=u+5$, $f_3(u)=u+6$ *and* $f_4(u)=u+15$. *Since* $f_1(0)=2$, $f_2(0)=5$, $f_3(0)=6$, $f_4(0)=15$, *we see that*

$$g_{ij}(2\phi_1(T))=f_i(0)f_j(0)f_i(-\frac{982800}{1008361})f_j(-\frac{982800}{1008361})\in\mathbb{Q}^2\quad \textit{for all } i,j.$$

In the following example, we consider a birational map between a quartic model and its jacobian elliptic curve different from the map introduced in the previous two examples. The elliptic curve

$$E: w^2=v^3+Av+B,$$

where $A, B \in K$, is the Jacobian of the elliptic curve defined by the following quartic model

$$C : y^2 = x^4 - 6ax^2 - 8bx + c$$

where $c = -4A - 3a^2$ and $B = b^2 - a^3 - Aa$. We notice that the point $P = (a, b) \in E(K)$ and that ∞_+ and ∞_- map to O_E and P respectively, see [1, §2]. We define a birational isomorphism $\phi_2 : C \to E$ as follows

$$x = \frac{w+b}{v-a}, \quad y = 2v + a - \left(\frac{w+b}{v-a}\right)^2,$$

whereas the inverse map of ϕ_2 is given by

$$v = \frac{1}{2}(x^2 + y - a), \quad w = \frac{1}{2}(x^3 + xy - 3ax - 2b).$$

Example 3.6 *Let $C : y^2 = (x+2)(x+4)(x+8)(x+9)$. Applying the transformation $x \mapsto x - \frac{23}{4}$, $y \mapsto y$, we get the quartic curve*

$$\tilde{C} : y^2 = x^4 - \frac{131}{8}x^2 - \frac{33}{8}x + \frac{12285}{256}.$$

Setting $a = \frac{131}{48}$, $b = \frac{33}{64}$, $A = -\frac{211}{12}$, $B = \frac{754}{27}$, the Jacobian elliptic curve is defined by

$$E : w^2 = v^3 - \frac{211}{12}v + \frac{754}{27}$$

The point $Q = (-5, 6)$ is in $C(\mathbb{Q})$ and $2Q = (-\frac{217}{24}, \frac{715}{576})$. We get

$$f_1\left(-\frac{217}{24}\right) = -\frac{169}{24}, \quad f_2\left(-\frac{217}{24}\right) = -\frac{121}{24}, \quad f_3\left(-\frac{217}{24}\right) = -\frac{25}{24}, \quad f_4\left(-\frac{217}{24}\right) = -\frac{1}{24}$$

where $f_1(x) = x + 2$, $f_2(x) = x + 4$, $f_3(x) = x + 8$ and $f_4(x) = x + 9$. According to Remark 3.1, $a_i = 1$ for all $i = 1, 2, 3, 4$. It follows that

$$g_{ij}(2\phi_1(Q)) = f_i(-217/24) f_j(-217/24) \in \mathbb{Q}^2 \quad \text{for all } i, j.$$

3.4 4-torsion points on quartic models

In [2], it is given a simple proof of the well-known divisibility by 2 conditions for rational points on elliptic curves with rational 2-torsion and the explicit division by 2^n formulas. The following example from the same article gives the necessary and sufficient condition of divisibility by 4.

Example 3.7 *Let K be a field of characteristic different from 2. Let*

$$E : y^2 = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$$

be an elliptic curve over K, where $\alpha_1, \alpha_2, \alpha_3$ are distinct elements of K. Let $P = (x_0, y_0)$ and R be a point of E such that $4R = P$, and let $Q = 2R = (x_1, y_1)$. Some formulas given in [2] give

$$x_1 = x_0 + (r_1r_2 + r_2r_3 + r_3r_1),\ y_1 = -(r_1+r_2)(r_2+r_3)(r_3+r_1),$$

where the square roots

$$r_i = \sqrt{x_0 - \alpha_i},\ i = 1, 2, 3,$$

are chosen in such a way that $r_1r_2r_3 = -y_0$. Further, let

$$r_i^{(1)} = \sqrt{(r_i + r_j)(r_i + r_k)}$$

be square roots that are chosen in such a way that

$$r_1^{(1)}r_2^{(1)}r_3^{(1)} = -y_1 = (r_1+r_2)(r_2+r_3)(r_3+r_1).$$

In light of equations (4) and (7) in [2],

$$x(R) = x_1 + r_1^{(1)}r_2^{(1)} + r_2^{(1)}r_3^{(1)} + r_3^{(1)}r_1^{(1)},$$

$$y(R) = -(r_1^{(1)} + r_2^{(1)})(r_2^{(1)} + r_3^{(1)})(r_3^{(1)} + r_1^{(1)}),$$

which implies that

$$x(R) = x_0 + (r_1r_2 + r_2r_3 + r_3r_1) + r_1^{(1)}r_2^{(1)} + r_2^{(1)}r_3^{(1)} + r_3^{(1)}r_1^{(1)}$$

,

$$y(R) = -(r_1^{(1)} + r_2^{(1)})(r_2^{(1)} + r_3^{(1)})(r_3^{(1)} + r_1^{(1)}).$$

In what follows we give a necessary and sufficient condition for an elliptic curve defined by a quartic model over $\mathbb{Q}$ to possess a 4-torsion point.

Theorem 3.3 *Let C be a smooth genus one curve defined over $\mathbb{Q}$ by*

$$v^2 = (k_1u+1)(k_2u+1)(k_3u+1)(k_4u+1), \qquad k_i \in \mathbb{Q}^\times.$$

Fix the map $\phi_1 : C \to E := J(C)$ defined as in §3.3. Then C has a 4-torsion point defined over $\mathbb{Q}$ if and only if one of the following holds:

i) $(k_1-k_3)(k_2-k_4)$ *and* $(k_1-k_2)(k_3-k_4)$ *are both squares in* $\mathbb{Q}$*; or*

ii) $(k_2-k_3)(k_1-k_4)$ *and* $(k_1-k_2)(k_4-k_3)$ *are both squares in* $\mathbb{Q}$*; or*

iii) $(k_3-k_2)(k_1-k_4)$ *and* $(k_1-k_3)(k_4-k_2)$ *are both squares in* $\mathbb{Q}$*.*

PROOF: The curve $J(C)$ is defined by the Weierstrass equation

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

where $a_1 = k_1+k_2+k_3+k_4,\ a_2 = k_1k_2+k_1k_3+k_2k_3+k_1k_4+k_2k_4+k_3k_4 - \frac{1}{4}(k_1+k_2+k_3+k4)^2,\ a_3 = 2(k_1k_2k_3+k_2k_3k_4+k_1(k_2+k_3)k_4),\ a_4 = -4k_1k_2k_3k_4,\ a_6 = a_2a_4$. Using MAGMA, the 2-torsion points on E are

$$\begin{aligned}
P_1 &= O_E,\\
P_2 &= (-k_1k_4-k_2k_3,\ \tfrac{1}{2}k_1^2k_4 - \tfrac{1}{2}k_1k_2k_3 - \tfrac{1}{2}k_1k_2k_4 - \tfrac{1}{2}k_1k_3k_4 + \tfrac{1}{2}k_1k_4^2 + \tfrac{1}{2}k_2^2k_3 + \tfrac{1}{2}k_2k_3^2 - \tfrac{1}{2}k_2k_3k_4),\\
P_3 &= (-k_1k_3-k_2k_4,\ \tfrac{1}{2}k_1^2k_3 - \tfrac{1}{2}k_1k_2k_3 - \tfrac{1}{2}k_1k_2k_4 + \tfrac{1}{2}k_1k_3^2 - \tfrac{1}{2}k_1k_3k_4 + \tfrac{1}{2}k_2^2k_4 - \tfrac{1}{2}k_2k_3k_4 + \tfrac{1}{2}k_2k_4^2),\\
P_4 &= (-k_1k_2-k_3k_4, \tfrac{1}{2}k_1^2k_2 + \tfrac{1}{2}k_1k_2^2 - \tfrac{1}{2}k_1k_2k_3 - \tfrac{1}{2}k_1k_2k_4 - \tfrac{1}{2}k_1k_3k_4 - \tfrac{1}{2}k_2k_3k_4 + \tfrac{1}{2}k_3^2k_4 + \tfrac{1}{2}k_3k_4^2).
\end{aligned}$$

Then

$$\begin{aligned}
\phi_1^{-1}(P_2) &= ((k_1-k_2-k_3+k_4)/(k_2k_3-k_1k_4), -(((k_1-k_2)(k_1-k_3)(k_2-k_4)(k_3-k_4))/(k_2k_3-k_1k_4)^2)),\\
\phi_1^{-1}(P_3) &= ((-k_1+k_2-k_3+k_4)/(k_1k_3-k_2k_4), ((k_1-k_2)(k_2-k_3)(k_1-k_4)(k_3-k_4))/(k_1k_3-k_2k_4)^2),\\
\phi_1^{-1}(P_4) &= ((-k_1-k_2+k_3+k_4)/(k_1k_2-k_3k_4), ((k_1-k_3)(-k_2+k_3)(k_1-k_4)(k_2-k_4))/(k_1k_2-k_3k_4)^2).
\end{aligned}$$

In view of Theorem 3.2, the point $\phi_1^{-1}(P_2) = (u_2, v_2) \in 2C(\mathbb{Q})$ if and only if $(k_iu_2+1)(k_ju_2+1) \in \mathbb{Q}^2$, where $i,j \in \{1,2,3,4\}$. Now direct substitution yields that the latter conditions are equivalent to $(k_1-k_3)(k_2-k_4)$ and $(k_1-k_2)(k_3-k_4)$ are squares in $\mathbb{Q}$. The other two conditions follow by considering the points $\phi_1^{-1}(P_3)$ and $\phi_1^{-1}(P_4)$. □

As an application of Theorem 3.3, we construct the following example of a 2-parameter family of elliptic curves over $\mathbb{Q}$ described by a quartic equation for which none of the nonsingular fibers has a nontrivial rational torsion point of order 4.

Example 3.8 *Let $C_{s,t}$ be a smooth genus 1 curve over $\mathbb{Q}(s,t)$ defined by*

$$v^2 = \left(\frac{t^2+s^2+ts}{t+s}u+1\right)\left(\frac{-ts}{t+s}u+1\right)(tu+1)(su+1).$$

Setting $k_1 = \frac{t^2+s^2+ts}{t+s}$, $k_2 = \frac{-ts}{t+s}$, one may use Theorem 3.3 to investigate the existence of rational numbers s,t such that $C_{s,t}$ has a torsion point of order 4. Condition (iii) of Theorem 3.3 is the fact that the two expressions $t(2s+t)$ and $s(2t+s)$ are squares in $\mathbb{Q}$. The latter is equivalent to the existence of a rational point on the following intersection of two quadric surfaces in $\mathbb{P}^3$:

$$u^2 = t(2s+1), \qquad v^2 = s(2t+s).$$

In fact, the latter intersection is an elliptic curve that can be described by the Weierstrass equation $y^2 = x^3 - 4x^2 + 16x$ and whose Mordell-Weil group is isomorphic to $\mathbb{Z}/4\mathbb{Z}$ corresponding to the points $(s:t:u:v) = (0:1:\pm 1:0), (1:0:0:\pm 1)$.

Conditions (i) and (ii) of Theorem 3.3 are equivalent to the existence of a rational point on the intersection of the quadric surfaces

$$\begin{aligned} u^2 &= -s(s+2t), \qquad v^2 = -s^2+t^2, \text{ and} \\ u^2 &= -t(t+2s), \qquad v^2 = -t^2+s^2, \end{aligned}$$

respectively. Both intersections are isomorphic to the elliptic curve described by $y^2 = x^3 - x^2 + x$ whose Mordell-Weil group is isomorphic to $\mathbb{Z}/4\mathbb{Z}$ corresponding to the points $(s:t:u:v) = (0:1:0:\pm 1), (1:-1:\pm 1:0)$.

It follows that the curve $C_{s,t}$ does not have a torsion point of order 4 over $\mathbb{Q}$ for any choice of the rational pair s,t with $s,t \neq 0, s \neq \pm t$.

4. Diophantine m-tuples

In this chapter, we present some facts about Diophantine m-tuples. We then employ the criterion for the divisibility-by-2 of a rational point on the elliptic curve (C, P) to investigate the question of extending a rational $D(q)$-quadruple to a quintuple. We give concrete examples to which we can give an affirmative answer. One of these results implies that although the rational $D(16t+9)$-quadruple $\{t, 16t+8, 225t+14, 36t+20\}$ can not be extended to a polynomial $D(16t+9)$-quintuple using a linear polynomial, there are infinitely many rational values of t for which the aforementioned rational $D(16t+9)$-quadruple can be extended to a rational $D(16t+9)$-quintuple. Moreover, these infinitely many values of t are parametrized by the rational points on a certain elliptic curve of positive Mordell-Weil rank.

4.1 What is Diophantine m-tuple?

The Greek mathematician Diophantus of Alexandria first studied the problem of finding four numbers such that the product of any two of them increased by unity is a perfect square. He found a set of four positive rationals with this property:

$$\left\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\right\}$$

$$\frac{1}{16}\cdot\frac{33}{16}+1=(\frac{17}{16})^2,\quad \frac{1}{16}\cdot\frac{17}{4}+1=(\frac{9}{8})^2,\quad \frac{1}{16}\cdot\frac{105}{16}+1=(\frac{19}{16})^2,$$
$$\frac{33}{16}\cdot\frac{17}{4}+1=(\frac{25}{8})^2,\quad \frac{33}{16}\cdot\frac{105}{16}+1=(\frac{61}{16})^2,\quad \frac{17}{4}\cdot\frac{105}{16}+1=(\frac{43}{8})^2.$$

However, the first set of four positive integers with the above property, $\{1, 3, 8, 120\}$, was found by Fermat. Indeed,

$$1\cdot 3+1=2^2,\quad 1\cdot 8+1=3^2,\quad 1\cdot 120+1=11^2,$$

$$3\cdot 8+1=5^2,\quad 3\cdot 120+1=19^2,\quad 8\cdot 120+1=31^2.$$

Definition 4.1 *A set of m positive integers* $\{a_1, a_2, ..., a_m\}$ *is called a Diophantine m-tuple if* $a_i.a_j+1$ *is a perfect square for all* $1 \leq i < j \leq m$.

Definition 4.2 *A set of m non-zero rationals* $\{a_1, a_2, ..., a_m\}$ *is called a Rational Diophantine m-tuple if* $a_i.a_j+1$ *is a perfect square for all* $1 \leq i < j \leq m$.

4.1.1 Diophantine triple and quadruple

Any Diophantine pair $\{a, b\}$ can be extended to a Diophantine triple, e.g. by adding $a+b+2r$ to the set, where $a.b+1=r^2$. For instance, $\{2, 12\}$ can be extended to Diophantine triple $\{2, 12, 24\}$. Also, any Diophantine triple $\{a, b, c\}$ can be extended to a Diophantine quadruple. Namely, let $a.b+1=r^2$, $b.c+1=s^2$, $c.a+1=t^2$, where r, s, t are positive integers. Then for $d_{\pm}=a+b+c+2abc\pm 2rst$, the set $\{a, b, c, d_{\pm}\}$ is a Diophantine quadruple. For instance, $\{4, 12, 30\}$ can be extended to Diophantine quadruple $\{4, 12, 30, 5852\}$ with $5852=d_+$. Quadruples of this form are called **regular**.

It is natural to ask how large these sets, i.e. (rational) Diophantine m-tuples, can be. This question is completely solved in the integer case. On the other hand, it seems that in the rational case, we do not have even a widely accepted conjecture. In particular, no absolute upper bound for the size of rational Diophantine m-tuples is known.

4.1.2 How large are these sets ?

We can handle this question in two cases, integer and rational.

In the integer case, it is easy to prove that there exist infinitely many integer Diophantine quadruples. There are parametric families for Diophantine quadruples involving polynomials and Fibonacci numbers, such as

$$\{k, k+2, 4k+4, 16k^3+48k^2+44k+12\},$$

$$\{F_k, F_{k+2}, F_{k+4}, 4F_{2k+1}F_{2k+2}F_{2k+3}. \text{ for } k \geq 1\}.$$

The nonexistence of a Diophantine quintuple was the folklore conjecture (i.e. an unpublished result with no clear originator, but which is well-circulated and believed to be true among the specialists).

It was proved in 2004 by Dujella that a Diophantine sextuple does not exist and that there are only finitely many Diophantine quintuples, [18]. Since then, the bound for the number of possible Diophantine quintuples has been improved by several authors. He, Togbé and Ziegler announced in 2016 and published in 2019 a proof of a couple of decades old conjecture that there are no Diophantine quintuples, [41].

For the rational case, Euler showed that Fermat's set $\{1, 3, 8, 120\}$ can be extended to a rational Diophantine quintuple by adding 777480/8288641 to the set. Also, he showed that there exist infinitely many rational Diophantine quintuples. In 2019, Stoll proved that the extension of Fermat's set to a rational quintuple with the same property is unique, [66]. In 1999 Gibbs found the first rational Diophantine sextuple

$$\left\{\frac{11}{192}, \frac{35}{192}, \frac{155}{27}, \frac{512}{27}, \frac{1235}{48}, \frac{180873}{16}\right\}$$

while in 2016 Dujella, Kazalicki, Mikie and Szikszai proved that there exist infinitely many rational Diophantine sextuplets, [27]. No example of a rational Diophantine septuple is known.

4.1.3 Diophantine $D(q)$ m-tuples

We can replace the number 1 in the condition "$a_i a_j + 1$ is a square" with a fixed number q in Definition 4.1.

Definition 4.3 *Let q be an integer (rational number). A set of m positive integers (rationals) $\{a_1, a_2, ..., a_m\}$ is said to have the property $D(q)$ if $a_i a_j + q$ is a perfect square for all $1 \leq i < j \leq m$. Such a set is called a (rational) Diophantine m-tuple with the property $D(q)$ (or (rational) $D(q)$ m-tuple).*

Several authors considered the problem of the existence of Diophantine quadruples with the property $D(q)$. This problem is almost completely solved. In 1985, Brown, Gupta & Singh and Mohanty & Ramasamy proved independently the following

result, which gives the first part of the answer.

Theorem 4.1 *If n is an integer of the form $n = 4k+2$, then there does not exist a Diophantine quadruple with the property $D(n)$.*

PROOF: The proof of Theorem 4.2 is very simple. Indeed, assume that $\{a_1, a_2, a_3, a_4\}$ has the property $D(n)$. Since the square of an integer is congruent to 0 or 1 (mod 4), we have that $a_i a_j \equiv 2$ *or* $3 \pmod 4$. It implies that none of the a_i is divisible by 4. Therefore, we may assume that $a_1 \equiv a_2 \pmod 4$. But now we have that $a_1 a_2 \equiv 0$ *or* $1 \pmod 4$, a contradiction. □

In 1993, Dujella gave the second part of the answer.

Theorem 4.2 *If an integer n does not have the form $4k+2$ and $n \notin S = \{-4, -3, -1, 3, 5, 8, 12, 20\}$, then there exist at least one Diophantine quadruple with the property $D(n)$.*

Conjecture 4.1 *For $n \in S$ there does not exist a Diophantine quadruple with the property $D(n)$.*

If n is a perfect square, say $n = k^2$, then by multiplying elements of a $D(1)$-quadruple by k we obtain a $D(k^2)$-quadruple, and thus we conclude that there exist infinitely many $D(k^2)$-quadruples. The following conjecture was proposed in 2008 by Dujella.

Conjecture 4.2 *If a nonzero integer n is not a perfect square, then there exist only finitely many $D(n)$-quadruples.*

One may ask what is the least positive integer n_1, and what is the greatest negative integer n_2, for which there exists a Diophantine quintuple with the property $D(n_i)$, $i = 1, 2$. It is known that $n_1 \leq 256$ and $n_2 \geq -255$, since the sets $\{1, 33, 105, 320, 18240\}$ and $\{5, 21, 64, 285, 6720\}$ have the property $D(256)$, and the set $\{8, 32, 77, 203, 528\}$ has the property $D(-255)$.

Let n be a nonzero integer. We may ask how large a set with the property $D(n)$ can be. Let define

$$M_n = sup\{|S| : S \text{ has the property } D(n)\},$$

where $|S|$ denotes the number of elements in the set S. By the results of Integer Case, we know that $M_1 = 4$ if S contains only integers, otherwise $M_1 \geq 6$.

Dujella proved that M_n is finite for all n. More precisely, it holds:

Theorem 4.3

$$M_n \leq 31 \ for \ |n| \leq 400,$$

$$M_n < 15.476 \log |n| \ for \ |n| > 400.$$

4.2 Application: Diophantine $D(q)$-quintuples

There are only finitely many ways of extending a rational $D(q)$-quadruple to a rational $D(q)$-quintuple, see [42]. The following theorem,[14], gives an explicit expression for the element extending a rational $D(q)$-quadruple to a rational $D(q)$-quintuple was provided if q is a rational square.

Theorem 4.4 *Let q, x_1, x_2, x_3, x_4 be rational numbers such that $x_i x_j + q^2 = y_{ij}^2$, $y_{ij} \in \mathbb{Q}$ for all $1 \leq i < j \leq 4$. Assume that $x_1 x_2 x_3 x_4 \neq q^4$. Then a rational number $x_5 = \frac{A}{B}$, where*

$$\begin{aligned} A &= q^3\Big(\pm 2y_{12}y_{13}y_{14}y_{23}y_{24}y_{34} + qx_1x_2x_3x_4(x_1+x_2+x_3+x_4) + \\ &\quad + 2q^3(x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4) + q^5(x_1+x_2+x_3+x_4)\Big), \\ B &= (x_1x_2x_3x_4 - q^4)^2. \end{aligned}$$

has the property that $x_i x_5 + q^2$ is a square of a rational number for $i = 1, 2, 3, 4$.

The definition 4.3 can be extended over the ring of polynomials with rational coefficients as follows.

Definition 4.4 *Let $q \in \mathbb{Q}[x]$ be a nonzero polynomial. Let $\{a_1, a_2, \cdots, a_m\}$ be a set of m nonzero polynomials with rational coefficients. We assume that there does not exist a polynomial $p \in \mathbb{Q}[x]$ such that $a_1/p, \cdots, a_m/p$ and q/p^2 are rational numbers. The set $\{a_1, a_2, \cdots, a_m\}$ is called a* polynomial $D(q)$-m-tuple *if $a_i a_j + q = b_{ij}^2$, for all $1 \leq i < j \leq m$, where $b_{ij} \in \mathbb{Q}[x]$.*

The assumption that there is no polynomial p such that $a_1/p, \cdots, a_m/p$ and q/p^2 are rational numbers implies that if q is constant then not all elements $a_1, \cdots, a_m$ of a polynomial $D(q)$-m-tuple are allowed to be constant. When q is a linear polynomial, the latter condition is trivially always satisfied.

In what follows we will be interested in polynomial $D(q)$-m-tuples whose elements

are linear polynomials, and q is also a linear polynomial. We define

$L_1 = \sup\{|S| : S \text{ is a polynomial } D(ax+b)\text{-tuple consisting of linear polynomials for some } a \neq 0 \text{ and } b\}$.

It was shown that $L_1 = 4$, see [26, Theorem 1]. Therefore, the set $\{x, 16x+8, 25x+14, 36x+20\}$ which is a polynomial $D(16x+9)$-quadruple cannot be extended to a polynomial $D(16x+9)$-quintuple using a linear polynomial. In this section, we show that for infinitely many rational values of x, the latter rational $D(16x+9)$-quadruple can be extended to a rational $D(16x+9)$-quintuple. The main tool is the following straightforward corollary of Theorem 3.2.

Corollary 4.1 *Let C be a smooth genus 1 curve over $\mathbb{Q}$ defined by an equation of the form*

$$y^2 = (a_1x+b_1)(a_2x+b_2)(a_3x+b_3)(a_4x+b_4), \qquad \text{where } a_i \in \mathbb{Q}^\times, b_i \in \mathbb{Q}.$$

We set $\phi : C \longrightarrow E := J(C)$ to be a $\mathbb{Q}$-birational isomorphism with $\phi((x_0, y_0)) = O_E$ for some $(x_0, y_0) \in C(\mathbb{Q})$, $x_0 \neq -b_i/a_i$, $i = 1,2,3,4$. Assume, moreover, that $f_i(x_0)f_j(x_0) \in \mathbb{Q}^2$, for all $i,j = 1,2,3,4$, where $f_i(x) = a_ix+b_i$. Let $Q \in C(\mathbb{Q})$.

Then $Q \in 2C(\mathbb{Q})$ if and only if there exists $\delta_Q \in \mathbb{Q}$ such that

$$a_ix(Q)+b_i = \delta_Q \cdot z_i^2 \text{ for some } z_i \in \mathbb{Q}$$

for all $i \in \{1,2,3,4\}$.

Corollary 4.1 implies the following result on extending a rational $D(q)$-quadruple to a $D(q)$-quintuple.

Corollary 4.2 *Let q be a nonzero rational number. Let $S = \{a_1, a_2, a_3, a_4\}$ be a $D(q)$-quadruple. Consider the smooth genus one curve*

$$C_S : y^2 = (a_1x+q)(a_2x+q)(a_3x+q)(a_4x+q).$$

We fix the birational isomorphism $\phi_1 : C_S \longrightarrow J(C_S)$ defined as in §3.3. Then S can be extended to a rational $D(q)$-quintuple if and only if there is a point $Q \in 2C_S(\mathbb{Q})$ with $\delta_Q \in \mathbb{Q}^2$.

In the following theorems, we extend some of the known polynomial $D(q)$-quadruples consisting of linear polynomials to $D(q)$-quintuples for infinitely many rational values of x.

Theorem 4.5 *The polynomial $D(16t+9)$-quadruple $\{t, 16t+8, 225t+14, 36t+20\}$*

can be extended to a rational $D(16t+9)$-quintuple for infinitely many $t \in \mathbb{Q}$.

PROOF: Let $k_1 = t$, $k_2 = 16t+8$, $k_3 = 25t+14$, $k_4 = 36t+20$, $q = 16t+9$. Consider the smooth genus one curve C defined by

$$v^2 = (k_1u+q)(k_2u+q)(k_3u+q)(k_4u+q) \tag{4.1}$$

over $\mathbb{Q}(t)$. By using the birational isomorphism $\phi_1 : C \to E$, defined in §3.3, we have the elliptic curve

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

with the coefficients

$$\begin{aligned}
a_1 &= 6(7+13t)(9+16t),\\
a_2 &= (9+16t)^2(111+8t(55+54t)),\\
a_3 &= 8(7+13t)(9+16t)^3(80+t(318+313t)),\\
a_4 &= -128t(1+2t)(5+9t)(9+16t)^4(14+25t),\\
a_6 &= -128t(1+2t)(5+9t)(9+16t)^6(14+25t)(111+8t(55+54t))
\end{aligned}$$

where $(x_0, y_0) = (0, q^2)$ is such that $\phi_1(x_0, y_0) = O_E$.

We take the point $P = (0, -q^2) \in C(\mathbb{Q}(t))$. Then

$$S := \phi_1(P) = (-(9+16t)^2(111+8t(55+54t)),\ 2(1+2t)(7+13t)(9+16t)^3(13+22t)).$$

Using MAGMA, [3], $Q = 2S = (x_1, y_1)$ is given by

$$x_1 = \frac{u(t)}{(4(1+2t)^2(7+13t)^2(13+22t)^2)}, \quad y_1 = -\frac{v(t)}{8(1+2t)^3(7+13t)^3(13+22t)^3}.$$

where

$$\begin{aligned}
u(t) = {} & 4965468561 + 87791232672t + 698248164432t^2 + 3289862320448t^3 + 10168707377552t^4\\
& + 21544947073664t^5 + 31689009677248t^6 + 31949101618688t^7 + 21130944883712t^8\\
& + 8278920101888t^9 + 1459071221760t^{10}
\end{aligned}$$

and

$$\begin{aligned}v(t) = {} & 583640570599605 + 15590162461394376t + 19431730950968228 4t^2 + 14991503484825547 20t^3 \\ & + 8006205664274122032t^4 + 3135149911634996684 8t^5 + 9299603699465215884 8t^6 \\ & + 2127721007146438481 92t^7 + 3785896551793687040 00t^8 + 5238736167977310453 76t^9 \\ & + 5591497378571982602 24t^{10} + 4520680248236910837 76t^{11} + 2679962897192572682 24t^{12} \\ & + 1099767129924488396 80t^{13} + 2793472865053389619 2t^{14} + 3310873413836341248t^{15}\end{aligned}$$

Then $\phi_1^{-1}(Q) = (u_1, v_1)$, where

$$u_1 = -\frac{4(1+2t)(7+13t)(13+22t)}{1369+32t(232+t(419+252t))},$$

$$v_1 = \frac{(85+302t+268t^2)(111+398t+356t^2)(71+8t(31+27t))(97+8t(43+38t))}{(1369+32t(232+t(419+252t)))^2}.$$

Therefore, we obtain

$$k_1u_1 + q = \frac{(111+398t+356t^2)^2}{1369+32t(232+t(419+252t))},$$

$$k_2u_1 + q = \frac{(97+8t(43+38t))^2}{1369+32t(232+t(419+252t))},$$

$$k_3u_1 + q = \frac{(85+302t+268t^2)^2}{1369+32t(232+t(419+252t))},$$

$$k_4u_1 + q = \frac{(71+8t(31+27t))^2}{1369+32t(232+t(419+252t))}.$$

One has $\delta_Q = \frac{1}{1369+32t(232+t(419+252t))}$. In view of Corollary 4.2, if $\delta_Q \in \mathbb{Q}^2$, then $k_iu_1 + q \in \mathbb{Q}^2$ for all $i = 1, 2, 3, 4$.

The elliptic curve $r^2 = 1369 + 32t(232 + t(419 + 252t))$ has Mordell-Weil rank 2 over $\mathbb{Q}$, [3]. It follows that there are infinitely many $t \in \mathbb{Q}$ such that $\delta_Q \in \mathbb{Q}^2$, and hence

the set

$$\left\{t, 16t+8, 225t+14, 36t+20, -\frac{4(1+2t)(7+13t)(13+22t)}{1369+32t(232+t(419+252t))}\right\}$$

is a rational $D(16t+9)$-quintuple.

□

By choosing t to be the t-coordinate of a rational point on the elliptic curve $r^2 = 1369+32t(232+t(419+252t))$, the set

$$\left\{t, 16t+8, 225t+14, 36t+20, -\frac{4(1+2t)(7+13t)(13+22t)}{1369+32t(232+t(419+252t))}\right\}$$

is a rational $D(q)$-quintuple produced by extending the polynomial $D(q)$-quadruple in Theorem 4.5 when evaluated at t. In the following table, we give examples of such $D(q)$-quintuples.

t	q	$D(q)$-quintuple
$t=\frac{672}{8064}$	$q=\frac{31}{3}$	$\{\frac{1}{2}, \frac{28}{3}, \frac{193}{12}, 23, -\frac{60431}{225228}\}$
$t=-\frac{3264}{8064}$	$q=\frac{53}{21}$	$\{-\frac{17}{42}, \frac{32}{21}, \frac{163}{42}, \frac{38}{7}, -\frac{50224}{240429}\}$
$t=\frac{-3600}{8084}$	$q=\frac{13}{7}$	$\{-\frac{25}{56}, \frac{6}{7}, \frac{159}{56}, \frac{55}{14}, -\frac{17889}{103544}\}$
$t=\frac{-4192}{8084}$	$q=\frac{43}{63}$	$\{-\frac{131}{252}, -\frac{20}{63}, \frac{253}{252}, \frac{9}{7}, \frac{60085}{183708}\}$
$t=-\frac{4572}{8064}$	$q=-\frac{1}{14}$	$\{-\frac{127}{224}, -\frac{15}{14}, -\frac{39}{224}, -\frac{23}{56}, -\frac{73455}{123704}\}$
$t=-\frac{4615}{8064}$	$q=-\frac{79}{504}$	$\{-\frac{4615}{8064}, -\frac{583}{504}, -\frac{2479}{8064}, -\frac{135}{224}, -\frac{3414104551}{6009297336}\}$

Theorem 4.6 *The following polynomial $D(q)$-quadruples can be extended to a rational $D(q)$-quintuple for infinitely many $t \in \mathbb{Q}$.*

(i) $\{4t, 144t+8, 25t+1, 49t+3\}$, *where* $q = 16t+1$, *can be extended using* $\frac{-4(2+37t)(3+58t)(5+82t)}{-1+32t(13+t(529+5148t))}$, *where t is the t-coordinate of a rational point on the elliptic curve* $E : r^2 = -1+32t(13+t(529+5148t))$.

(ii) $\{t, 9t+26, 4t+12, 16t+40\}$, *where* $q = 16t+49$, *can be extended using* $\frac{4(1+2t)(13+5t)(27+10t)(49+16t)}{96721+16t(6521+2342t+280t^2)}$, *where t is the t-coordinate of a rational point on the elliptic curve* $E : r^2 = (96721+16t(6521+2342t+280t^2))(16t+49)$.

(iii) $\{t, \frac{t}{4}-1, \frac{9t}{4}+5, 4t+8\}$, *where* $q = 4t+9$, *can be extended using* $\frac{(2+t)(9+4t)(8+5t)(14+5t)}{324+8t(62+t(31+5t))}$, *where t is the t-coordinate of a rational points on the elliptic curve* $E : r^2 = (81+2t(62+t(31+5t)))(9+4t)$.

PROOF: The proof is similar to the proof of Theorem 4.5. □

Remark 4.1 *The Mordell-Weil rank r_E of $E(\mathbb{Q})$ in Theorem 4.6 is $r_E = 3$ in (i) and (ii), whereas $r_E = 2$ in (iii).*

Example 4.3 *Let $t = -\frac{318}{121}$ in the $D(16t+49)$-quadruple given in Theorem 4.6. We then obtain the following $D(\frac{841}{121})$-quintuple*

$$\left\{\frac{180}{121}, -\frac{318}{121}, \frac{284}{121}, -\frac{248}{121}, \frac{2562308340}{2164017361}\right\}.$$

On the other hand, since $\frac{841}{121}$ is a square, Theorem 4.4 implies that the rational $D(\frac{841}{121})$-quadruple $\{180/121, -318/121, 284/121, -248/121\}$ can be extended to a $D(\frac{841}{121})$-quintuple using either the rational number $x_5 = \frac{1255545720}{540051121}$ or $x_5 = -\frac{143212695780}{74048750161}$. In particular, we obtain two almost $D(\frac{841}{121})$-sextuple, i.e., $x_i x_j + q^2$ is a rational square for all $1 \leq i < j \leq 6$ except when $(i,j) = (5,6)$.

5. A Dynamical Analogue of a question of Fermat

In this chapter, we investigate the existence of consecutive squares in the orbit of a rational point under the iteration of a given quadratic polynomial with rational coefficients. We display three different constructions of 1-parameter quadratic polynomials with orbits containing three consecutive squares. In addition, we show that there exists at least one polynomial of the form $x^2 + c$ with a rational point whose orbit under this map contains four consecutive squares. This can be viewed as a dynamical analogue of a question of Fermat on rational squares in arithmetic progression. Finally, assuming a standard conjecture on exact periods of periodic points of quadratic polynomials over the rational field, we give necessary and sufficient conditions under which the orbit of a periodic point contains only rational squares.

5.1 Consecutive Three Squares

Let K be a number field. Let $f \in K[x]$ and $x_0 \in K$. We say that $\mathrm{Orb}_f(x_0)$ contains *m-consecutive squares* if there is $y \in \mathrm{Orb}_f(x_0)$ such that

$$y, f(y), \ldots, f^{m-1}(y)$$

are all K-rational squares. We note that in the latter case $\mathrm{Orb}_f(y)$ itself contains m-consecutive squares. Therefore, for the sake of simplicity, when we say that $\mathrm{Orb}_f(x_0)$ contains *m-consecutive squares* we mean

$$x_0, f(x_0), \ldots, f^{m-1}(x_0)$$

are all K-rational squares.

We start with the following observation.

Proposition 5.1 *Fix a,b,c in a number field K. There are only finitely many $x_0 \in K$ such that $\mathrm{Orb}_f(x_0)$, where $f(x) = ax^2+bx+c$, contains 3 consecutive squares unless one of the following cases occurs.*

1.1 $a = 0$

1.2 $b^2 - 4ac = 0$

1.3 $b = 0$ *and* $c = \frac{-1}{a}$

1.4 $b = 4$ *and* $c = 0$

1.5 $1+2b \in \mathbb{Q}^{\times 2}$ *and* $c = \frac{b^2-2b-2\pm 2\sqrt{1+2b}}{4a}$

Moreover, if $f(x)$ is an irreducible quadratic polynomial, then none of the cases above occurs, hence the finiteness of such x_0's holds unconditionally.

Proof: This follows immediately by observing that the existence of three consecutive squares can be expressed equivalently by

$$ax_0^4 + bx_0^2 + c = y^2, \qquad ay^4 + by^2 + c = z^2.$$

This implies the existence of a rational point on the genus-3 curve

$$C : z^2 = a(ax_0^4 + bx_0^2 + c)^2 + b(ax_0^4 + bx_0^2 + c) + c,$$

By Faltings' Theorem, for fixed K-rational values a,b,c such that the curve is smooth, the latter curve possesses only finitely many K-rational points. It remains to check the discriminant of the curve. Using Mathematica, the discriminant is given by

$$\Delta = 256\,a^{15}c(1+b+ac)(b^2-4ac)^4(-4b^3+b^4+16ac+16abc-8ab^2c+16a^2c^2)^2.$$

This gives the following cases for the curve not to be smooth:

2.1 $a = 0$, and for that case $f(x)$ is not a quadratic polynomial.

2.2 $b^2 - 4ac = 0$, in which case $f(x) = \frac{(b+2ax)^2}{4a}$. So, either a is a square which gives that for any $x_0 \in \mathbb{Q}^{\times 2}$ the orbit will contain infinitely many consecutive squares; or a is not a square, in which case for any $x_0 \in \mathbb{Q}$, $f(x_0)$ is not a square.

2.3 $c=0$ which gives rise to the curve

$$C_1 : Z_1^2 := \left(\frac{z}{x_0}\right)^2 = (ax_0^2+b)(a^2x_0^4+abx_0^2+b).$$

This is again a genus 2 curve and so Faltings' Theorem can still be applied, unless the discriminant of that curve given by $-64\,a^{15}(-4+b)^2b^8$ is zero. This gives that either $a=0$ covered in (i); $b=0$ implying that $b^2-4ac=0$ which is covered in (ii); or $b=4$ covered in (iv).

2.4 $1+b+ac=0$ or $b=-1-ac$ gives rise to the curve

$$C_2 : Z_1^2 := \left(\frac{z}{x_0}\right)^2 = (ax_0^2-ac-1)(a^2x_0^4-(a^2c+a)x_0^2+ac-1).$$

The discriminant of the latter genus 2 curve is given by $64\,a^{15}(-1+ac)^5(1+ac)(5-2ac+a^2c^2)^2$. If the curve is not smooth, then either $ac=1$ which means $b=-2$ and so $b^2-4ac=0$; ac is a root of the irreducible polynomial x^2-2x+5, i.e, $ac\notin\mathbb{Q}$; or $ac=-1$ which gives rise to (iii).

2.5 Finally, the vanishing of the factor $-4b^3+b^4+16ac+16abc-8ab^2c+16a^2c^2$ in Δ yields that ac is a root of the quadratic polynomial $16x^2+16(1+b-b^2)x+b^4-4b^3$ giving rise to the case (v).

This concludes the proof. One can check easily that the aforementioned cases implies that $f(x)$ is reducible. □

Remark 5.1 *Two polynomials f_1 and f_2 are called K-linearly equivalent if there is a map $\ell(x)=ax+b\in K[x]$ such that $f_1=\ell\circ f_2\circ\ell^{-1}$. It is a simple exercise to see that any polynomial map of degree 2 in $K[x]$ is K-linearly equivalent to map of the form x^2+c, $c\in K$. In what follows we focus on consecutive squares in orbits of points under maps of the form $f_c(x)=x^2+c$, $c\in\mathbb{Q}^\times$.*

Theorem 5.1 *For each $\beta\in\mathbb{Q}$, there are infinitely many rational numbers α,γ, and c such that $f_c(\alpha^2)=\beta^2$ and $f_c(\beta^2)=\gamma^2$.*

In particular, one may choose

$$\begin{aligned}
\alpha &= \frac{\beta^2(3-4\beta^4)^2}{(1+8\beta^2+4\beta^4)^2},\\
\gamma &= \frac{\beta(-1+24(\beta^2+3\beta^4+4\beta^6+2\beta^8))}{(1+8\beta^2+4\beta^4)^2},\\
c &= \frac{\beta^2-49\beta^4+400\beta^6+2864\beta^8+7264\beta^{10}+8864\beta^{12}+6400\beta^{14}+2816\beta^{16}+256\beta^{18}-256\beta^{20}}{(1+8\beta^2+4\beta^4)^4}.
\end{aligned}$$

PROOF: Let $\alpha \in \mathbb{Q}$ be such that $f_c(\alpha) = \beta^2$ and $f_c(f_c(\alpha)) = \gamma^2$ for some $\gamma, \beta \in \mathbb{Q}, c \in \mathbb{Q}^\times$. This can be written as

$$\alpha^2 + c = \beta^2$$
$$\beta^4 + c = \gamma^2.$$

Eliminating c, one has

$$\alpha^2 + \gamma^2 = \beta^4 + \beta^2. \tag{5.1}$$

For a fixed β, equation (1) defines a conic C_β over $\mathbb{Q}(\beta)$ possessing a rational point P_β defined by $(\alpha, \gamma) = (\beta^2, \beta) \in C_\beta(\mathbb{Q}(\beta))$. Parameterizing the rational points $(\alpha, \gamma) \in C_\beta(\mathbb{Q}(\beta))$, using the point P_β, yields that

$$\alpha = \frac{\beta(-2m - \beta + m^2\beta)}{1+m^2}, \qquad \gamma = m(\alpha - \beta^2) + \beta = -\frac{\beta(-1 + 2\beta m + m^2)}{1+m^2}, \qquad \text{where } m \in \mathbb{Q}.$$

Now, forcing α to be a rational square, say k^2, we obtain the following quartic curve defined over $\mathbb{Q}(\beta)$

$$H_\beta : k^2 = \beta(\beta m^4 - 2m^3 z - 2mz^3 - \beta z^4)$$

with the rational point $(m : z : k) = (1 : 0 : \beta)$, hence H_β is an elliptic curve over $\mathbb{Q}(\beta)$. The curve H_β is $\mathbb{Q}$-birationally equivalent to the elliptic curve

$$E_\beta : y^2 = x^3 + (4\beta^4 + 4\beta^2)x.$$

We set $P_\beta = (1 : 0 : \beta)$ and $\phi : H_\beta \to E_\beta$ to be the birational isomorphism. One sees that $\phi(P_\beta) = (1 : 2\beta^2 + 1 : 1)$ is of infinite order in $E_\beta(\mathbb{Q}(\beta))$ using MAGMA ,[3]. Proving the first part of the theorem.

Now one has $\phi^{-1}\left(2\phi(P_\beta)\right)$ is given by

$$\left(\left(-\frac{1}{2}\beta^4 - \frac{1}{8}\right) / \left(\beta^3 + \frac{1}{2}\beta\right) : \left(-\frac{1}{4}\beta^8 - \frac{1}{2}\beta^6 + \frac{1}{8}\beta^4 + \frac{3}{8}\beta^2 + \frac{3}{64}\right) / \left(\beta^5 + \beta^3 + \frac{1}{4}\beta\right) : 1\right),$$

where the corresponding m-coordinate on H_β must be $\left(-\frac{1}{2}\beta^4 - \frac{1}{8}\right) / \left(\beta^3 + \frac{1}{2}\beta\right)$. Consequently, one has the values given in the theorem. □

Corollary 5.1 *There are infinitely many $c \in \mathbb{Q}$ such that for some $x_0 \in \mathbb{Q}$, the orbit $\mathrm{Orb}_{f_c}(x_0)$, where $f_c(x) = x^2 + c$, has three distinct consecutive squares.*

Example 5.2 *Setting $\beta = 2$, it can be seen that for the quadratic map $f(x) = x^2 + 132583668/88529281$ and $\alpha = 122/97$, one has*

$$f_c(\alpha^2) = 2^2 \text{ and } f_c(4) = (39358/9409)^2.$$

Theorem 5.2 *Let $a \in \mathbb{Q}$. There exist infinitely many $\delta, \gamma, b \in \mathbb{Q}$ such that for the map $f(x) = x^2 + ax + b$, one has $f(\delta^2) = a^2$ and $f(a^2) = \gamma^2$. In particular, one can choose*

$$b = \frac{a^2 - a^3 - 69a^4 - 196a^5 + 314a^6 + 2226a^7 + 7622a^8 + 15308a^9 + 25285a^{10} + 30279a^{11}}{(1 + a(2 + a(9 + 4a(1 + a))))^4}$$

$$+ \frac{31599a^{12} + 24864a^{13} + 16624a^{14} + 6496a^{15} + 160a^{16} - 3072a^{17} - 2560a^{18} - 1280a^{19} - 256a^{20}}{(1 + a(2 + a(9 + 4a(1 + a))))^4}$$

and

$$\delta = \frac{a(1 + a)(-3 + a + 4a^3)}{(1 + a(2 + a(9 + 4a(1 + a))))}, \quad \gamma = \frac{a(-1 + a^2(5 + 4a(1 + a))(6 + a(8 + 3a(5 + 4a(1 + a)))))}{(1 + a(2 + a(9 + 4a(1 + a))))^2}.$$

It follows that there exist infinitely many polynomials $f(x) = x^2 + ax + b \in \mathbb{Q}[x]$ such that $\mathrm{Orb}_f(x)$ contains three distinct consecutive squares for some $x \in \mathbb{Q}$.

Proof: Let $\alpha \in \mathbb{Q}$ and assume $f(\alpha) = \alpha^2 + a\alpha + b = \beta^2$ and $f(f(\alpha)) = \beta^4 + a\beta^2 + b = \gamma^2$ for some $\beta, \gamma \in \mathbb{Q}$. By eliminating b, we have

$$\alpha^2 + a\alpha - \beta^2 = \beta^4 + a\beta^2 - \gamma^2.$$

One observes that setting $\beta = a$, the equation above describes a conic $C_a : \alpha^2 + \gamma^2 + a\alpha = a^4 + a^3 + a^2$ over $\mathbb{Q}(a)$ possessing a rational point P_a defined by $(\alpha, \gamma) = (a^2, a) \in C_a(\mathbb{Q}(a))$. We parameterize the rational points $(\alpha, \gamma) \in C_a(\mathbb{Q}(a))$ using the point P_a as follows

$$\alpha = \frac{a(-1 - a - 2m + am^2)}{1 + m^2}, \quad \gamma = m(\alpha - a^2) + a = -\frac{a(-1 + m + 2am + m^2)}{1 + m^2}, \quad m \in \mathbb{Q}.$$

Now, forcing α to be a rational square, say k^2, we obtain the following quartic curve defined over $\mathbb{Q}(a)$

$$H_a : k^2 = a^2m^4 - 2am^3 - am^2 - 2am - a^2 - a$$

with a rational point $(m : k : z) = (1 : a : 0)$. Therefore, H_a is an elliptic curve

over $\mathbb{Q}(a)$ and it is $\mathbb{Q}$-birationally equivalent to the elliptic curve E_a defined by the Weierstrass equation

$$E_a : y^2 - \frac{2}{a}xy - \frac{4a^2+2a+2}{a^3}y = x^3 + \frac{2a+2}{a^2}x^2 + \frac{4a^4+4a^3+a^2+2a+1}{a^4}x$$

One sees that the image of the point $Q_a = (1 : a : 0)$ in E_a under the birational isomorphism $\psi : H_a \to E_a$ is $((0 : \frac{4a^2+2a+2}{a^3} : 1))$ which is of infinite order, MAGMA [3]. Now the m-coordinate of the rational point $\psi^{-1}(2\psi(Q_a))$ in H_a is given by

$$\left(-\frac{1}{2}a^4 - \frac{1}{2}a^3 - \frac{1}{8}a^2 - \frac{1}{4}a - \frac{1}{8}\right) / \left(a^3 + \frac{1}{2}a^2 + \frac{1}{2}a\right).$$

With the latter m-coordinate, we get the values for b, δ and γ as in the statement of the theorem. □

Example 5.3 *Setting $a = \frac{1}{2}$, it can be seen that for the quadratic map $f(x) = x^2 + \frac{1}{2}x + \frac{1969}{10000}$, one has*

$$\mathrm{Orb}_f\left(\left(\frac{9}{100}\right)\right) = \left\{\left(\frac{3}{10}\right)^2, \left(\frac{1}{2}\right)^2, \left(\frac{31}{50}\right)^2, \ldots\right\}.$$

The following theorem also describes an explicit construction of three consecutive squares in the orbit of polynomials of the form $x^2 + ax - a$.

Theorem 5.3 *Let $\alpha \in \mathbb{Q}$ and $a = -\frac{(-1+\alpha)\alpha^2(-9+\alpha^2)}{(4+\alpha-\alpha^2)^2}$. For the polynomial $f(x) = x^2 + ax - a$, one has*

$$\mathrm{Orb}_f(\alpha) = \left\{\alpha, \left(\frac{\alpha^2-5\alpha}{\alpha^2-\alpha-4}\right)^2, \left(\frac{3\alpha^5-13\alpha^4+13\alpha^3-15\alpha^2+12\alpha}{(\alpha^4-2\alpha^3-7\alpha^2+8\alpha+16)(\alpha-1)}\right)^2\right\}.$$

In particular, for any rational number $x_0 \in \mathbb{Q}$, there exists an $a \in \mathbb{Q}$ such that the polynomial $f(x) = x^2 + ax - a$ satisfies $f(x_0^2)$ and $f^2(x_0^2)$ are rational squares.

PROOF: Let $\alpha \in \mathbb{Q}$ be such that $f(\alpha) = \alpha^2 + a\alpha - a = \beta^2$ and $f(f(\alpha)) = \beta^4 + a\beta^2 - a = \gamma^2$ for some $\beta, \gamma \in \mathbb{Q}$. One obtains

$$a = \frac{\beta^2 - \alpha^2}{\alpha - 1} = \frac{\gamma^2 - \beta^4}{\beta^2 - 1}.$$

This gives a certain level of confidence.

$$\alpha\beta^4 + (-1-\alpha^2)\beta^2 + \alpha^2 = (\alpha-1)\gamma^2$$

which defines the following quartic curve over $\mathbb{Q}(\alpha)$

$$C_\alpha : \alpha(\alpha-1)\beta^4+(\alpha-1)(-1-\alpha^2)\beta^2+(\alpha-1)\alpha^2=\theta^2$$

where $\theta=(\alpha-1)\gamma$, with a rational point $T_\alpha=(1:\alpha-1:1)$.

There is a birational isomorphism $\psi : C_\alpha \to E_\alpha$ where E_α is an elliptic curve described by the following Weierstrass equation over $\mathbb{Q}(\alpha)$

$$E_\alpha : y^2+(2\alpha+2)xy+\frac{2\alpha^4-6\alpha^3-2\alpha^2-2\alpha}{\alpha-1}y=x^3+\frac{2\alpha^3-8\alpha^2-2\alpha}{\alpha-1}x^2+\frac{\alpha^6-8\alpha^5+14\alpha^4+4\alpha^3+5\alpha^2}{\alpha^2-2\alpha+1}x.$$

Then $R_\alpha := \psi(T_\alpha)=(0:(-2\alpha^4+6\alpha^3+2\alpha^2+2\alpha)/(\alpha-1):1)$ is a point of infinite order in $E_\alpha(\mathbb{Q}(\alpha))$. Moreover,

$$\psi^{-1}(2R_\alpha)=\left(\frac{\alpha^2-5\alpha}{\alpha^2-\alpha-4}:\frac{3\alpha^5-13\alpha^4+13\alpha^3-15\alpha^2+12\alpha}{\alpha^4-2\alpha^3-7\alpha^2+8\alpha+16}:1\right).$$

Now the β-coordinate of the latter rational point gives rise to the a-value and the corresponding orbit in the statement of the theorem. □

Example 5.4 *Let $\alpha=\frac{1}{4}$. We can observe that for the polynomial $f(x)=x^2-\frac{429}{17956}x+\frac{429}{17956}$, we have*

$$\mathrm{Orb}_f(\alpha)=\left\{\left(\frac{1}{2}\right)^2,\left(\frac{19}{67}\right)^2,\left(\frac{757}{4489}\right)^2,\dots\right\}.$$

5.2 Consecutive four squares

Let K be a number field. Let $f(x)=x^2+c\in K[x]$ and $x_0\in K$. If one wants to force $x_0^2, f_c(x_0^2), f_c^2(x_0^2)$ and $f_c^3(x_0^2)$ to be all K-rationals, then this can be written as

$$x_0^4+c=y^2,\qquad y^4+c=z^2,\qquad z^4+c=w^2. \tag{5.2}$$

Equivalently, the existence of four consecutive squares in the orbit of a rational point under f_c is equivalent to the existence of a rational point (x_0,y,z,w) on the surface

$\mathcal{S}$ defined by

$$z^2+x^4=y^2+y^4, \qquad w^2+y^4=z^2+z^4. \tag{5.3}$$

Proposition 5.5 *Let $c \in \mathbb{Q}$ be such that $\mathrm{Orb}_{f_c}(x_0)$ contains four consecutive squares, i.e, $f^i(x_0)$, $i=0,1,2,3$, are all rational squares. Then $x_0 \neq 0$.*

PROOF: It can be seen that by eliminating y and z in (5.2), one obtains that

$$\begin{aligned} w^2 &= f_c^2(x_0^2) = ((x_0^4+c)^2+c)^2+c \\ &= x_0^{16}+4cx_0^{12}+2c(1+3c)x_0^8+4c^2(1+c)x_0^4+c(1+c+2c^2+c^3). \end{aligned}$$

If $x_0=0$, then this means that $w^2=c(1+c+2c^2+c^3)$ which describes an elliptic curve E over $\mathbb{Q}$, whose Mordell-Weil group $E(\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$ corresponding to the point $(0,0)$ and the two points at infinity. None of these points gives rise to non-trivial four consecutive squares. □

Theorem 5.4 *There exists a polynomial $f(x)=x^2+c \in \mathbb{Q}[x]$ such that there are four distinct consecutive squares in $\mathrm{Orb}_f(x_0^2)$ for some $x_0 \in \mathbb{Q}$ if and only if there exist rational solutions $p,q,r \in \mathbb{Q}$ to the polynomial equation $M(p,q,r)=x_0^4$ where*

$$\begin{aligned} M(p,q,r) = &-2048p^7q-1536p^6q^2-768p^5q^3+128p^4q^4+192p^3q^5+96p^2q^6+16pq^7+q^8+4096p^6qr+ \\ &1280p^5q^2r-960p^3q^4r-448p^2q^5r-160pq^6r-24q^7r-512p^6r^2-1280p^5qr^2+1792p^4q^2r^2+ \\ &1664p^3q^3r^2+1152p^2q^4r^2+368pq^5r^2+76q^6r^2+768p^5r^3-2048p^4qr^3-1920p^3q^2r^3-1280p^2q^3r^3- \\ &384pq^4r^3-72q^5r^3+384p^4r^4+1728p^3qr^4+480p^2q^2r^4+240pq^3r^4-10q^4r^4-704p^3r^5-64p^2qr^5- \\ &32pq^2r^5+24q^3r^5+64p^2r^6-112pqr^6+44q^2r^6+64pr^7-56qr^7+17r^8. \end{aligned}$$

PROOF: In (5.3), we set $x_0^2=X$, $y^2=Y$ and $z^2=Z$. Then we have the following equations

$$Y+Y^2=Z+X^2, \tag{5.4}$$

$$Z+Z^2=w^2+Y^2. \tag{5.5}$$

One may homogenize equation (5.5) and complete the square so that the equation may be written as

$$\gamma^2=w^2+Y^2+\mu^2, \qquad \text{where } \mu=\frac{T}{2}, \gamma=Z+\mu.$$

Therefore, one may obtain the following parameterization.

$$\gamma = s^2+t^2+u^2, \quad w = 2su, \quad Y = s^2+t^2-u^2, \quad \mu = 2tu.$$

Since $Z = \gamma - \mu$ and $T = 2\mu$, we have $z^2 = -2tu + s^2 + t^2 + u^2$ and $T = 4tu$. Also $Y = y^2 = s^2 + t^2 - u^2$ yielding the following parametrization for t, s, u, y:

$$\begin{aligned} s &= 4p^2+2qp-2pr-q^2+r^2 \quad , \quad t = 4qp+q^2-2qr+r^2, \\ u &= 4p^2+2qp-2pr+q^2-r^2 \quad , \quad y = 4pr+2qr-q^2-r^2. \end{aligned}$$

It follows that (5.4) in homogeneous form, $YT + Y^2 = ZT + X^2$, may be written as

$$x_0^4 = y^2T + y^4 - Tz^2 = M(p,q,r)$$

where $M(p,q,r)$ is given as in the statement of the theorem. □

Theorem 5.5 *There exists at least one polynomial of the form $f(x) = x^2 + c \in \mathbb{Q}[x]$ and $x_0 \in \mathbb{Q}$ such that $\mathrm{Orb}_f(x_0)$ has four distinct consecutive squares. Namely, $c = 5103/4096$ and*

$$\mathrm{Orb}_f((3/8)^2) = \{(3/8)^2, (9/8)^2, (27/16)^2, (783/256)^2, \ldots\}.$$

PROOF: Fixing y in equations (5.3) and setting $X = x_0^2$, one obtains

$$(y^2+y^4)T^2 = z^2 + X^2.$$

The latter equation gives rise to the following parametrization

$$z = -yp^2 + 2y^2ps + ys^2, \qquad X = y^2 + p^2 + 2yps - y^2s^2, \qquad T = p^2 + s^2.$$

Let $X_1 = \frac{X}{T}$ and $z_1 = \frac{z}{T}$. Then we have the following.

$$X_1 = \frac{z(2ps + p^2z - s^2z)}{p^2+s^2} = \square,$$

$$z_1^2+z_1^4-y^4=\frac{y^4(-p^2+s^2+2psy)^4+y^2(-p^2+s^2+2psy)^2(p^2+s^2)^2-y^4(p^2+s^2)^4}{(p^2+s^2)^4}=\square.$$

Searching for rational solutions to the system above using MAGMA , [3], yields the polynomial $f(x)$ together with the mentioned orbit. $\square$

Remark 5.2 *In Theorem 5.5, we were able to find a rational point on the variety $\mathcal{S}$ defined in (5.3). This variety contains the subvariety (up to sign) $x=y=z=w$ with infinitely many rational points that give rise to no nontrivial four distinct consecutive squares. We suspect that there are likely only finitely many other nontrivial rational points, and perhaps the rational point we found might be the only one.*

As for polynomials $f(x)$ with $d=\deg f>2$, the existence of a rational square α^2 such that $f\left(\alpha^2\right)$ is rational itself, implies the existence of a rational point on a curve of genus $\lfloor 2d-1\rfloor/2>1$, on which there are only finitely many rational points. Therefore, finding a rational point whose orbit under f contains three consecutive squares is quite improbable.

5.3 Finite orbits consisting of squares

As mentioned in Remark 5.1, any quadratic polynomial map $f(x)=Ax^2+Bx+C\in K[x]$ is linearly conjugate over K to a map of the form x^2+c for some $c\in K$. If K is chosen to be the rational field $\mathbb{Q}$, a complete classification of quadratic polynomial maps with periodic points of periods $1,2$, or 3 was given in [69]. We recall that the orbit of a periodic point is called a *periodic orbit*.

The following conjecture can be found in [56].

Conjecture 5.6 *If $N\geq 4$, then there is no quadratic polynomial $f(x)\in\mathbb{Q}[x]$ with a rational point of exact period N .*

The conjecture has been proved for $N=4$, [54], for $N=5$, [34], and conditionally on Birch-Swinnerton-Dyer Conjecture for $N=6$, [65]. Although proving the uniform boundedness of the number of preperiodic points of polynomial maps of a fixed

degree is currently far from our reach, some uniform bounds were given for certain polynomial maps in [44, 59].

Assuming Conjecture 5.6 holds, one notices that if $f(x) = x^2 + c \in \mathbb{Q}[x]$ is such that $x_0 \in \mathbb{Q}$ is a periodic point of $f(x)$, then for x_0 to be a rational square of period 1 one has either $1/2+\rho$ or $1/2-\rho$ is a rational square with $c = 1/4-\rho^2$. Similarly, one sees easily that x_0 cannot be a point of period 2 whose orbit contains only rational squares since otherwise both $-1/2+\sigma$ and $-1/2-\sigma$ are rational squares for some $\sigma \in \mathbb{Q}$. Finally, for x_0 to be a periodic point of period 3 for which $\mathrm{Orb}_f(x_0)$ contains only rational squares, one must have in Theorem 2.6 that $x_1 = r_1^2,\ x_2 = r_2^2,\ x_3 = r_3^2$ where $r_i \in \mathbb{Q}$, $i = 1,2,3$. The latter is a singular curve of genus 17 with only two singularities $(\tau, r_1, r_2, r_3) = (-1,0,0,0), (0,0,0,0)$. Again, by Faltings' Theorem, [33], there are only finitely many rational points on the latter curve. Therefore, one investigates the possibility of having infinitely many polynomials of the form $x^2+ax+b,\ a \neq 0$, with rational periodic points whose orbits are of length at least 2 and contain only rational squares.

One notices that if x_0 is a rational periodic point of the map x^2+ax+b, then $x_0 + a/2$ is a periodic point of the map x^2+c where $c = b - a^2/4 + a/2$.

Theorem 5.6 *The polynomial map $f(x) = x^2+ax+b \in \mathbb{Q}[x]$ has a periodic orbit of length 2 whose elements are rational squares if and only if $a = -1-m^2-k^2$ and $b = m^2+k^2+m^2k^2$ for some $m,k \in \mathbb{Q}$. In this case, one has $f(m^2) = k^2$ and $f(k^2) = m^2$.*

Proof: That the polynomial $f(x) = x^2+ax+b$ with $a = -1-m^2-k^2$ and $b = m^2+k^2+m^2k^2$, $m,k \in \mathbb{Q}$, has such a periodic orbit is a direct calculation.

Now, if $f(k^2) = m^2$ and $f(m^2) = k^2$ for some $m,k \in \mathbb{Q}$, then one knows that $g(m^2 + a/2) = k^2 + a/2$ and $g(k^2+a/2) = m^2 + a/2$ where $g(x) = x^2 + b - a^2/4 + a/2$. This yields that

$$k^2 + \frac{a}{2} = -\frac{1}{2} - \sigma \ \text{ and } \ m^2 + \frac{a}{2} = -\frac{1}{2} + \sigma, \qquad \text{for some } \sigma \in \mathbb{Q},$$

see Theorem 2.6. It follows that $a = -1-m^2-k^2$ and $b = m^2+k^2+m^2k^2$. □

One sees that $\mathrm{Orb}_f(4) = \{4, \frac{1}{4}\}$ where $f(x) = x^2 - \frac{21}{4}x + \frac{21}{4}$ and $\mathrm{Orb}_g(9) = \{9,4\}$ where $g(x) = x^2 - 14x + 49$.

Theorem 5.7 *Let $m,n,r \in \mathbb{Q}$ be distinct. There exists a polynomial map $f(x) = x^2+ax+b \in \mathbb{Q}[x]$ such that $f(m^2) = n^2$, $f(n^2) = r^2$, and $f(r^2) = m^2$ if and only if*

$$m^4(1-n^2+r^2) + m^2(-n^2+n^4-r^2(1+r^2)) + r^4 - n^4(-1+r^2) + n^2r^2(-1+r^2) = 0.$$

In this case, the polynomial $f(x)$ is determined by

$$a=\frac{-m^6+m^2n^4-n^6+m^4r^2+n^2r^4-r^6}{(m^2-n^2)(m^2-r^2)(n^2-r^2)},\qquad b=\frac{m^6n^2-m^4n^4+n^6r^2-m^4r^4-n^4r^4+m^2r^6}{(-m^2+n^2)(n^2-r^2)(-m^2+r^2)}.$$

PROOF: One needs to solve the following system of linear equations in d,a,b

$$dm^4+am^2+b=n^2,\quad dn^4+an^2+b=r^2,\quad dr^4+ar^2+b=m^2$$

to get the expressions for a and b as in the statement, whereas $d=(m^4-m^2n^2+n^4-m^2r^2-n^2r^2+r^4)/((m^2-n^2)(m^2-r^2)(n^2-r^2))$. The statement now holds once we force the polynomial $f(x)$ to be monic by setting $d=1$. □

One remarks that each of the triples m,n,k satisfying the identity in Theorem 5.7 gives rise to a rational solution to the system of equations

$$m^2+a/2=\frac{\tau^3+2\tau^2+\tau+1}{2\tau(\tau+1)},\quad n^2+a/2=\frac{\tau^3-\tau-1}{2\tau(\tau+1)},\quad r^2+a/2=-\frac{\tau^3+2\tau^2+3\tau+1}{2\tau(\tau+1)}$$

for some rational value of $\tau\in\mathbb{Q}\setminus\{-1,0\}$.

As examples, one sees that the following polynomial maps have periodic orbits of length 3 that contain only rational squares.

$$\begin{aligned}
f_1(x)&=x^2-\tfrac{29}{8}\,x+\tfrac{841}{256},\quad \mathrm{Orb}_{f_1}((7/4)^2)&&=\{(7/4)^2,(5/4)^2,(1/4)^2\},\quad \tau=-1/2,\\
f_2(x)&=x^2-\tfrac{301}{72}\,x+\tfrac{90601}{20736},\quad \mathrm{Orb}_{f_2}((23/12)^2)&&=\{(23/12)^2,(19/12)^2,(5/12)^2\},\quad \tau=2,\\
f_3(x)&=x^2-\tfrac{421}{72}\,x+\tfrac{177241}{20736},\quad \mathrm{Orb}_{f_3}((25/12)^2)&&=\{(25/12)^2,(17/12)^2,(11/12)^2\},\quad \tau=1/2,\\
f_4(x)&=x^2-\tfrac{1849}{288}\,x+\tfrac{3418801}{331776},\quad \mathrm{Orb}_{f_4}((55/24)^2)&&=\{(55/24)^2,(49/24)^2,(23/24)^2\},\quad \tau=3,\\
f_5(x)&=x^2-\tfrac{74333}{4356}\,x+\tfrac{211660729}{4743684},\quad \mathrm{Orb}_{f_5}((115/66)^2)&&=\{(115/66)^2,(47/33)^2,(124/33)^2\},\quad \tau=-12.
\end{aligned}$$

6. Arithmetic progressions in polynomial orbits

6.1 Intersection of polynomial orbits with linear polynomial orbits

Throughout this work, K is a number field with algebraic closure $\overline{K}$ and the ring of integers $\mathcal{O}_K$.

We recall that the n-th iteration of a polynomial $f(x)$ is defined to be $f^n(x) = f(f^{n-1}(x)), n \geq 1$, and $f^0(x) = x$. Given $a \in \overline{K}$, the orbit of a under f is the set $\mathrm{Orb}_f(a) = \{f^n(a), n \geq 0\}$. We can also denote by $\mathrm{Orb}_f^{\pm}(a) := \{f^n(a), n \in \mathbb{Z}\}$ the union of both the forward and backward orbits of a point a under the iterates of f. This is mostly useful when referring to a linear map f where the backward orbit is always infinite. A point $a \in K$ is called *preperiodic* under f of type (m, n) if $f^{m+n}(a) = f^m(a)$ for some $m \geq 0, n \geq 1$. A point $a \in K$ is called *periodic* under f if a is preperiodic of type $(0, n)$. Moreover, if n is the smallest such integer, then a is said to be a periodic point of *exact period* n. If $a \in K$ is not preperiodic under f, then a is called a *wandering* point for f.

We define an equivalence relation on polynomials in $K[x]$ of a given degree $d \geq 2$ as follows. Two polynomial maps f_1 and f_2 in $K(x)$ of degree $d \geq 2$ are *conjugate* if there is $\phi \in \mathrm{PGL}_2(\overline{K})$ such that $f_2 = f_1^{\phi} := \phi \circ f_1 \circ \phi^{-1}$. If $\phi \in \mathrm{PGL}_2(K)$, then f_1 and f_2 are said to be K-conjugate. We remark that if a is a periodic point of exact period n for f, then $\phi(a)$ is a point of exact period n for f^{ϕ}. One can argue similarly for preperiodic points of f and f^{ϕ}. Moreover, if f, ϕ, and a are defined over K such that $f^n(a) = a$, then $g := f^{\phi}$ and $b := \phi(a)$ are defined over K with $g^n(b) = b$.

If two complex polynomials f and g of degree at least 2 have orbits with infinite intersection, then f and g must have a common iterate, [36, 37]. The assumption that both polynomials must be nonlinear is essential as may be emphasised by the example $\mathrm{Orb}_{2X^2+2}(1) \subset \mathrm{Orb}_{X+2}(0)$.

It is obvious that if $\phi = \alpha x + \beta \in K[x]$, $\alpha \neq 0$, then

$$\mathrm{Orb}_{f^\phi}(\phi(x)) = \{\phi(x), \phi(f(x)), \cdots, \phi(f^n(x)), \cdots\}$$

for any polynomial map $f \in K[x]$ and any $x \in K$. In addition, If $f(x) = ax + b$, $a \neq 0$, then $f^\phi(x) = ax + \alpha b - \beta(a-1)$.

In what follows we consider the case when $g(x) = ax + b \in \mathbb{Q}[x]$ whereas $f(x)$ is an arbitrary polynomial. We remark that

$$\mathrm{Orb}_g(x) = \{x, ax+b, a^2x+b(a+1), a^3x+b(a^2+a+1), \cdots, a^nx+b(a^n-1)/(a-1), \cdots\}.$$

We notice that for a power of a linear map $f(x) = (\beta x)^m$, $m \geq 2$, and $g(x) = \beta x$, one has that $\mathrm{Orb}_f(0) \cap \mathrm{Orb}_g(1)$ is infinite. In what follows, we consider the latter intersection when $f(x)$ is not a power of a linear polynomial.

Proposition 6.1 *Let $f(x) \in K[x]$ be of degree at least 2 such that $f(x)$ is not a power of a linear polynomial. Let $g(x) = ax + b \in K[x]$ be such that $\mathrm{Orb}_f(s) \cap \mathrm{Orb}_g^{\pm}(t)$ is infinite for some fixed $s, t \in K$. Then a is a root of unity in $\mathcal{O}_K$.*

Proof: Using a conjugation via $\phi(x) = x + b/(a-1)$, one may assume without loss of generality that $g(x) = ax$ and $t \neq 0$. We write

$$f(x) = a_d x^d + \cdots + a_0 = a_d \prod_{i=1}^{e} (x - c_i)^{r_i}, r_i \geq 1, a_d \neq 0, c_i \neq c_j \text{ for } i \neq j.$$

We also set

$$S = \{\mathfrak{p} \in \mathcal{O}_K \text{ is prime } : \nu_\mathfrak{p}(s) < 0 \text{ or } \nu_\mathfrak{p}(t) < 0 \text{ or } \nu_\mathfrak{p}(a_i) < 0 \text{ for some } 0 \leq i \leq d\},$$

where $\nu_\mathfrak{p}$ is the associated discrete valuation to the prime $\mathfrak{p}$.

Now, we assume on the contrary that a is not a root of unity. The hypothesis implies that $f^m(s) = a^n t$ for infinitely many pairs of integers (m, n). We also notice that for two such pairs (m_1, n_1) and (m_2, n_2), both $m_1 \neq m_2$ and $n_1 \neq n_2$, since otherwise, $f^{m_1}(s) = f^{m_2}(s)$ or $g^{n_1}(t) = g^{n_2}(t)$ respectively. The latter implies that s is a preperiodic point for f, hence $\mathrm{Orb}_f(s)$ is finite, or t is the fixed point 0 of $g(x)$.

Let q be an odd rational prime such that $q > r_i$ for all i. The latter argument shows that there is $\ell \mod q$ such that there are infinitely many pairs $(m_i, qi + \ell)$ where $f^{m_i}(s) = a^{qi+\ell} t$. This yields infinitely many S-integer points $(x, y) = (f^{m_i - 1}(s), a^i)$ on the curve $a^\ell t y^q = f(x)$.

Building on earlier work of Siegel, [61, 62], Lang and LeVeque proved that if the number of S-integer points on a curve $C : y^q = f(x)$, $q \geq 2$, $f(x) \in K[x]$, is infinite, then the genus of the curve C must be zero, [51, 68]. The reader may also consult [4] for further references and literature. LeVeque also gave necessary and sufficient conditions for the genus of C to be zero, [52]. More precisely, setting $q_i = q/\gcd(q, r_i)$, and assuming without loss of generality that $q_1 \geq q_2 \geq \cdots \geq q_e$, the curve C has infinitely many S-integer points if and only if $(q_1, q_2, q_3, \cdots, q_e) = (2, 2, 1, \cdots, 1)$ or $(s, 1, 1, \cdots, 1)$, $s \geq 1$.

In view of the latter fact, since the tuple $(2, 2, 1, \cdots, 1)$ is not realized due to the fact that q is odd, either $f(x)$ has a root of multiplicity divisible by q, corresponding to the case $e \geq 2$ and $q_2 = 1$, contradicting the assumption that $q > r_i$ for all i; or $e = 1$ implying that $f(x)$ has a unique root, contradicting our assumption that $f(x)$ is not a power of a linear polynomial. □

Remark 6.1 *The remark following Proposition 5.3 of [36] shows that if f and g are non-monic linear polynomials such that $\mathrm{Orb}_f(s) \cap \mathrm{Orb}_g(t)$ is infinite, then f and g must have a common iterate.*

Proposition 6.1 justifies the fact that we will only consider intersections of orbits of polynomials f of arbitrary degrees with orbits of monic linear polynomials. In fact, we will mainly focus on the latter intersection when f has integer coefficients. This may be justified by the following example.

Example 6.2 *Let $f(x) = x^d + a/b$, $d \geq 2$, $|b| > 1$, $\gcd(a, b) = 1$. One may easily see that $f^n(0) = a_n/b^{d^n}$ for some sequence $a_n \in \mathbb{Z}$, $n \geq 1$. In addition, $\mathrm{Orb}_{x+r/s}(0) = \{nr/s : n \geq 1\}$. Therefore, $\mathrm{Orb}_f(0) \cap \mathrm{Orb}_{x+r/s}(0)$ contains only finitely many points for any choice of r/s.*

Lemma 6.1 *Let $g(x) = x + \frac{a}{b}$ with $a, b \in \mathbb{Z}$. Then $\mathrm{Orb}_g(t) = \frac{1}{b}\mathrm{Orb}_{x+a}(bt)$ for any $t \in \mathbb{Q}$.*

Proof: This follows immediately by observing $g^n(t) = \dfrac{bt + na}{b}$ for any $n \geq 1$. □

In view of Lemma 6.1, it is sufficient to focus on orbits of linear polynomials of the form $g(x) = x + a$ with $a \in \mathbb{Z}$.

Lemma 6.2 *Let $g_i(x) = x + m_i, m_i \in \mathbb{Z}$, $i = 1, 2$ and $\gcd(m_1, m_2) = 1$. Set $g(x) = x + m_1 m_2$. Then $\mathrm{Orb}_g(t) = \mathrm{Orb}_{g_1}(t) \cap \mathrm{Orb}_{g_2}(t)$ for any $t \in \mathbb{Q}$.*

Proof: Let k be a rational number such that $k \in \mathrm{Orb}_g(t)$. Then we have $k = t + r m_1 m_2$ for some $r \in \mathbb{Z}$. Hence $k \in \mathrm{Orb}_{g_1}(t) \cap \mathrm{Orb}_{g_2}(t)$. Now assume $k \in \mathrm{Orb}_{g_1}(t) \cap \mathrm{Orb}_{g_2}(t)$. Then $k = t + s_1 m_1 = t + s_2 m_2$ for some $s_1, s_2 \in \mathbb{Z}$. Since $\gcd(m_1, m_2) = 1$,

$m_1|s_2$ and $m_2|s_1$. Thus, there exists $s \in \mathbb{Z}$ such that $k = t + sm_1m_2$, i.e., $k \in \mathrm{Orb}_g(t)$.
□

Proposition 6.3 *Let $f(x)$ be a polynomial in $\mathbb{Z}[x]$ and $g(x) = x + p$ where p is a rational prime. Assume that n is the minimum positive integer such that $f^n(t) \in \mathrm{Orb}_g^{\pm}(t)$ for some $t \in \mathbb{Z}$. Then $f^k(t) \in \mathrm{Orb}_g^{\pm}(t)$ if and only if $n|k$.*

PROOF: Since $f^n(t) \in \mathrm{Orb}_g^{\pm}(t)$, one sees that $f^n(t) = t + mp$ for some integer m. It follows that t is a periodic point of $\widetilde{f}(x) \in \mathbb{F}_p[x]$ with exact period n where $\widetilde{f}$ is the reduction of f modulo p.

Assuming that $f^k(t) \in \mathrm{Orb}_g^{\pm}(t)$ for some integer k, one has $f^k(t) = t + rp \equiv t \bmod p$ for some integer r. Since n is the exact period of t, n must divide k.

Assuming that $k = nc$ for some integer c and knowing that $f^n(t) \equiv t \mod p$, it follows that

$$f^k(t) \equiv f^{nc}(t) \equiv \underbrace{f^n \circ \cdots \circ f^n}_{c-\text{times}}(t) \equiv t \mod p.$$

Thus, $f^k(t) \in \mathrm{Orb}_g^{\pm}(t)$. □

In fact, one has the following result for intersections with orbits of monic linear polynomials.

Proposition 6.4 *Let $f(x)$ be a polynomial in $\mathbb{Z}[x]$ and $g(x) = x + a$ where a is an integer. Let t be an integer such that n is the minimum positive integer for which $f^n(t) \in \mathrm{Orb}_g^{\pm}(t)$. Then $f^k(t) \in \mathrm{Orb}_g^{\pm}(t)$ if and only if $n|k$.*

PROOF: We assume that $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_e^{\alpha_e}$ where $p_1, \cdots, p_e$ are distinct primes. As $f^n(t) = t + am$ for some $m \in \mathbb{Z}$, one obtains $f^n(t) \equiv t \mod p_i^{\alpha_i}$ for all i.

If $n|k$, then $f^k(t) \equiv t \mod p_i^{\alpha_i}$. Since the primes p_i are distinct, one has $f^k(t) \equiv t \mod a$.

Now one assumes that $f^k(t) \in \mathrm{Orb}_g^{\pm}(t)$. This gives $f^k(t) \equiv t \mod a$, hence $f^k(t) \equiv t \mod p_i^{\alpha_i}$ for all $i = 1, \cdots, e$. We set n_i to be the exact period of t for the image $\widetilde{f}(x)$ of $f(x)$ in $\in \mathbb{Z}/(p_i^{\alpha_i}\mathbb{Z})[x]$. Letting l be the least common multiple of all n_i, $i = 1, \dots, e$, one observes that $l|k$ as each $n_i|k$. In addition, one sees that $f^l(t) \equiv t \mod a$. This must yield that $l = n$, hence $n|k$.

□

6.2 Primitive divisors and intersections with linear orbits

We recall the following definition.

Definition 6.1 *For an integer sequence a_n, $n \geq 1$, a positive integer (rational prime) $u \geq 2$ is said to be a* primitive divisor (primitive prime divisor) *of a_m, if $u|a_m$ and $u \nmid a_s$ for all $1 \leq s < m$.*

For example, letting $\{a_n : n \geq 1\}$ be a sequence in which

$$a_1 = 1, \quad a_2 = 2, \quad a_3 = 3, \quad a_4 = 6,$$

one sees that 2 is a primitive (prime) divisor for a_2, 3 is a primitive (prime) divisor for a_3. However, a_4 does not have any primitive prime divisors, but 6 is a primitive divisor of a_4.

Given a polynomial $f(x) \in \mathbb{Z}[x]$ and $t \in \mathbb{Z}$, we will investigate the set of primitive divisors of the sequence $t_0 = 0$ and $t_n = f^n(t) - t$, $n \geq 1$.

Lemma 6.3 *Let $t \in \mathbb{Z}$ and $f(x) \in \mathbb{Z}[x]$. Define the sequence $t_0 = 0$ and $t_n = f^n(t) - t$, $n \geq 1$. There exists a monic linear polynomial $g(x) = x + a \in \mathbb{Z}[x]$, $a \notin \{0, \pm 1\}$, such that $\mathrm{Orb}_f(t) \cap \mathrm{Orb}_g^{\pm}(t) \neq \{t\}$ if and only if a is a primitive divisor of t_m for some $m \geq 1$. In this case, $\mathrm{Orb}_f(t) \cap \mathrm{Orb}_g^{\pm}(t)$ is infinite.*

Proof: If $g(x) = x + a \in \mathbb{Z}[x]$ is such that $\mathrm{Orb}_f(t) \cap \mathrm{Orb}_g^{\pm}(t) \neq \{t\}$, then this is equivalent to the fact that there are integers $m, n \geq 1$ such that $f^m(t) = t + na$. Assuming that m is the smallest such positive integer, one sees that a is a primitive divisor of $f^m(t) - t$. The infinitude of the intersection follows from Proposition 6.4. □

Proposition 6.5 *Let $f(x) \in \mathbb{Z}[x]$ and $t \in \mathbb{Z}$. If a is a primitive divisor of $f^m(t) - t$ for some $m \geq 1$, then $\mathrm{Orb}_{f^m}(t) \subset \mathrm{Orb}_g^{\pm}(t)$ where $g(x) = x + a$. Moreover,*

$$\mathrm{Orb}_{f^m}(t) \cap \mathrm{Orb}_g^{\pm}(t) = \{t + n_i a : i \geq 0\}$$

where $t + n_{i+1}a = f^m(t + n_i a)$.

Proof: Since $a | f^m(t) - t$, then $f^m(t) = t + an = g^n(t) \in \mathrm{Orb}_g^{\pm}(t)$. Since a is primitive for $f^m(t) - t$, then m is the minumum positive integer for which $f^m(t) \in \mathrm{Orb}_g^{\pm}(t)$. So, by Proposition 6.4, $f^{mk}(t) \in \mathrm{Orb}_g^{\pm}(t)$ implying that $\mathrm{Orb}_{f^m}(t) \subset \mathrm{Orb}_g^{\pm}(t)$. □

Corollary 6.1 *Let $f(x) \in \mathbb{Z}[x]$ and $t \in \mathbb{Z}$. Let $h(x) := (f)^{\phi^{-1}}(x) \in \mathbb{Z}[x]$, where $\phi(x) = ax+t$. If a is a primitive divisor of $f(t)-t$, then the primitive prime divisors of $f^i(t)-t$ are the primitive prime divisors of $h^i(0)$ for all $i \geq 1$.*

PROOF: Since $a \mid (f(t)-t)$, one easily sees that the map $h(x) = (f(t+ax)-t)/a \in \mathbb{Z}[x]$. □

Example 6.6 *Consider the linear map $g(x) = x+k$ for some $k \in \mathbb{Q}^\times$. Let $a \in \mathbb{Q}^\times$ be such that $ak \in \mathbb{Z}$, and p be a rational number. There exists nonzero rational numbers b, c such that the quadratic map $f(x) = ax^2+bx+c$ satisfies*

$$\mathrm{Orb}_f(p) \subset \mathrm{Orb}_g(p).$$

where $b = 1-ak-2ap$ and $c = k+akp+ap^2$. More precisely,

$$\mathrm{Orb}_f(p) = \{p, p+k, p+2k, p+n_0k, p+n_1k, \cdots, p+n_ik, \cdots\}$$

where $n_0 = 3+2ak$, and $n_i = h^i(n_0)$, $i = 1, 2, \cdots$, where $h(x) = akx^2+(1-ak)x+1$.

For example, let $f(x) = 2x^2-37x+163$, $g(x) = x+7$ and $p = 6$. Then one can have

$$\mathrm{Orb}_f(p) = \{6, 13, 20, 223, 91370, \ldots,\} \subset \mathrm{Orb}_g(p) = \{6, 13, 20, 26, \ldots, 223, 91370, \ldots,\}.$$

Corollary 6.2 *Let $f(x) \in \mathbb{Z}[x]$. For all but finitely many integers t, there exists an integer $a \notin \{0, \pm 1\}$, such that $\mathrm{Orb}_f(t) \subset \mathrm{Orb}_g^{\pm}(t)$ where $g(x) = x+a$.*

PROOF: One sees that there are only finitely many t such that $f(t)-t \in \{0, \pm 1\}$. For any other integer t, $f(t)-t$ has a primitive divisor a. Now the result follows by Proposition 6.5. □

6.3 Relative density of orbits intersections

Given a polynomial f in $\mathbb{Z}[x]$, an integer s, and a set $A \subseteq \mathbb{Z}$, we define the *relative density of A in the orbit of s under f* to be the limit

$$\delta_{f,s}(A) := \lim_{X \to \infty} \frac{|\{x \in A \cap \mathrm{Orb}_f(s) : x \leq X\}|}{|\{x \in \mathrm{Orb}_f(s) : x \leq X\}|},$$

provided that this limit exists.

Given a polynomial $g \in \mathbb{Z}[x]$ and an integer t, we will concern ourselves with $\delta_{f,s}(\mathrm{Orb}_g(t))$.

Lemma 6.4 *Let $f, g \in \mathbb{Z}[x]$ and $s, t \in \mathbb{Z}$. The following statements hold.*

i) $\delta_{f,s}(\mathbb{Z}) = 1$.

ii) $\delta_{f,s}(\mathrm{Orb}_g(t)) = 0$ *if* $\deg f, \deg g > 1$ *where f and g have no common iterate; or* $\deg f = \deg g = 1$ *where f and g have no common iterate and both f and g are non-monic.*

iii) $\delta_{f,s}(\mathrm{Orb}_g(t)) = 0$ *if* $\deg f = 1$, $\deg g > 1$ *and $g(x)$ is not a power of a linear polynomial.*

Proof: For i), it is clear as $f \in \mathbb{Z}[x]$ and $t \in \mathbb{Z}$.

For ii), if $\deg f, \deg g > 1$ where f and g have no common iterate, Theorem 1 in [37] gives that $\mathrm{Orb}_f(s) \cap \mathrm{Orb}_g(t)$ is finite. Hence, $\delta_{f,s}(\mathrm{Orb}_g(t)) = 0$. If $\deg f = \deg g = 1$ where f and g have no common iterate and both f and g are non-monic, then the result follows from the Remark 6.1.

For iii), let $f(x) = ax + b$ for some $a, b \in \mathbb{Z}$ and a is not a unit. Then by Proposition 6.1, $\mathrm{Orb}_f^{\pm}(s) \cap \mathrm{Orb}_g(t)$ is finite. Hence, $\delta_{f,s}(\mathrm{Orb}_g(t)) = 0$. Now assume $f(x) = x + b$ where $b \in \mathbb{Z}$. This gives $\mathrm{Orb}_f^{\pm}(s) = \{s + bk : k \in \mathbb{Z}\}$. Let $m_1 \geq 0$ be the least integer such that $g^{m_1}(t) \in \mathrm{Orb}_f(s)$, i.e., $g^{m_1}(t) = s + br_1$ for some $r_1 \in \mathbb{Z}$. Let m_2 be the least integer such that $m_2 > m_1$ and $g^{m_2}(t) \in \mathrm{Orb}_f^{\pm}(s)$, i.e., $g^{m_2}(t) = s + br_2$ for some $r_2 \in \mathbb{Z}$. One can construct a sequence $m_1 < m_2 < \cdots < m_i < \ldots$ such that $g^{m_i}(t) = s + br_i$ for some $r_i \in \mathbb{Z}$. We observe that

$$g^{m_i - m_1}(g^{m_1}(t)) = g^{m_i}(t) = g^{m_1}(t) + b(r_i - r_1) \quad \text{for all } i.$$

So, this implies $g^{m_1}(t)$ is periodic $\mod b$ for $g(x)$ with exact period $m_2 - m_1$. By periodicity, we have

$$g^{m_i}(t) = g^{m_i - m_1}(g^{m_1}(t)) = g^{i(m_2 - m_1)}(g^{m_1}(t)).$$

Let $g^{m_2 - m_1}(x) = \sum_{j=0}^{d} a_j x^j$. Then

$$g^{m_i}(t) = g^{m_i - m_1}(g^{m_1}(t)) = g^{m_1}(t) + b(r_i - r_1),$$

and

$$g^{m_{i+1}}(t) = g^{m_2 - m_1}(g^{m_i}(t)) = \sum_{j=0}^{d} a_j (g^{m_1}(t) + b(r_i - r_1))^j = g^{m_1}(t) + b(r_{i+1} - r_1).$$

This implies that $r_{i+1} = h(r_i)$ where $h(x)$ is a polynomial of degree d. This means that $r_i = h^{i-j}(r_j)$ is a polynomial of degree d^{i-j} in r_j. Thus,

$$\lim_{M\to\infty} \frac{|\{f^m(s) \in \mathrm{Orb}_g(t) : -M \le m \le M\}|}{2M} = \lim_{i\to\infty} \frac{i}{r_i} = 0$$

This implies that

$$\delta_{f,s}(\mathrm{Orb}_g(t)) = \lim_{M\to\infty} \frac{|\{f^m(s) \in \mathrm{Orb}_g(t) : 0 \le m \le M\}|}{M} = 0.$$

□

Corollary 6.3 *Let $f(x)$ be a polynomial in $\mathbb{Z}[x]$ and $g(x) = x + a$ where $a \in \mathbb{Z}$ is such that $a \neq 0, \pm 1$. Let $t \in \mathbb{Z}$. The following statements are equivalent:*

(i) t is a periodic point of $f(x) \mod a$ with exact period $n \ge 1$.

(ii) a is primitive divisor of $f^n(t) - t$.

(iii) $\delta_{f,t}(\mathrm{Orb}_g^{\pm}(t)) = \frac{1}{n}$.

(iv) $|\mathrm{Orb}_f(t) \cap \mathrm{Orb}_g^{\pm}(t)| = \infty$.

PROOF: This is Proposition 6.4 and Lemma 6.3. □

Remark 6.2 *In Corollary 6.3, if $a = p_1^{\alpha_1} \cdots p_e^{\alpha_e}$, then n is the least common multiple of all n_i, $i = 1, \cdots, e$, where n_i is the exact period of t for the image $\widetilde{f}(x)$ of $f(x)$ in $\in \mathbb{Z}/(p_i^{\alpha_i}\mathbb{Z})[x]$, see the proof of Proposition 6.4.*

6.4 Covering polynomial orbits using arithmetic progressions

In view of Corollary 6.3, the infinitude of the intersection of a linear orbit with the orbit of an integer t under a polynomial f of arbitrary degree is equivalent to the existence of a primitive divisor for an element in the sequence $\{f^i(t) - t\}_i$.

In fact, for the polynomial $f(x) = x^d + c \in \mathbb{Z}[x]$, it was proved in [10] that the sequence $f^i(0)$ has a primitive prime divisor for all i except finitely many. For $x^d + c \in \mathbb{Q}[x]$, it was shown in [50] that the sequence $f^i(0)$ has a primitive prime divisor for all i except possibly for 23 values. Moreover, it was shown in [58] that

for two classes of polynomials $f(x) \in \mathbb{Z}[x]$ and and any integer t, the sequence $f^n(t)$, $n \geq 1$, has only finitely many terms with no primitive prime divisor.

If t is a point whose orbit is infinite under $f(x) \in \mathbb{Z}[x]$, then for all but finitely many integers n, $f^n(t)$ has a primitive prime divisor under the *abc*-conjecture, see [39]. Moreover, if t is a critical point of $f(x)$, then for all but finitely many integers n, $f^n(t) - t$ has a primitive prime divisor, see [57].

Definition 6.2 *Let $f(x) \in \mathbb{Z}[x]$ and t be an integer. A finite system*

$$A = \{a_s + n_s\mathbb{Z}\}_{s=1}^{k}, \qquad a_s, n_s \in \mathbb{Z}, \quad n_s > 0, \quad 1 \leq s \leq k,$$

is said to be a cover *of* $\mathrm{Orb}_f(t)$ *if*

$$\mathrm{Orb}_f(t) \subset \cup_{s=1}^{k} a_s + n_s\mathbb{Z}.$$

If $\{a_s + n_s\mathbb{Z}\}_{\substack{s=1 \\ s\neq u}}^{k}$ is not a cover of $\mathrm{Orb}_f(t)$, then A is a cover of $\mathrm{Orb}_f(t)$ for which $a_u + n_u\mathbb{Z}$ is essential. A minimal cover *of $\mathrm{Orb}_f(t)$ is a cover in which all the arithmetic sequences are essential. If $\mathrm{Orb}_f(t) \cap a_s + n_s\mathbb{Z} \cap a_{s'} + n_{s'}\mathbb{Z} = \emptyset$ for all $s \neq s'$, then A is called a* disjoint cover *of $\mathrm{Orb}_f(t)$. A t-cover of A is a cover of $\mathrm{Orb}_f(t)$ for which $t \in \cap_{s=1}^{k} a_s + n_s\mathbb{Z}$.*

For a positive integer n, one sees that $\{r + n\mathbb{Z}\}_{r=0}^{n-1}$ is a disjoint cover of $\mathrm{Orb}_f(t)$ for any $f(x) \in \mathbb{Z}[x]$ and any integer t.

Given $f(x) \in \mathbb{Z}[x]$ and $t \in \mathbb{Z}$, we will mainly focus on disjoint covers and covers of $\mathrm{Orb}_f(t)$ of the form $A = \{t + n_s\mathbb{Z}\}_{s=1}^{k}$, where the latter covers are t-covers of $\mathrm{Orb}_f(t)$. In other words, we consider covers of $\mathrm{Orb}_f(t)$ using linear orbits of the form $\{\mathrm{Orb}_{x+n_s}(a_s)\}_{s=1}^{k}$, where $\mathrm{Orb}_f(t) \cap \mathrm{Orb}_{x+n_r}(a_r) \cap \mathrm{Orb}_{x+n_s}(a_s) = \emptyset$ if $r \neq s$; or covers of the form $\{\mathrm{Orb}_{x+n_s}(t)\}_{s=1}^{k}$.

Theorem 6.1 *Let $f(x)$ be a polynomial in $\mathbb{Z}[x]$ and $t \in \mathbb{Z}$. Let $g_i(x)$, $1 \leq i \leq k$, be a finite family of monic linear polynomials in $\mathbb{Z}[x]$. The following statements are equivalent.*

i) $\delta_{f,t}\left(\bigcup_{i=1}^{k} \mathrm{Orb}_{g_i}^{\pm}(t)\right) = 1.$

ii) $\delta_{f,t}\left(\mathrm{Orb}_{g_i}^{\pm}(t)\right) = 1$ *for some i, $1 \leq i \leq k$.*

iii) $\mathrm{Orb}_f(t) \subset \mathrm{Orb}_{g_i}^{\pm}(t)$ *for some i, $1 \leq i \leq k$.*

Proof: The implication iii) yields i) is clear. We assume that $\delta_{f,t}\left(\bigcup_i \mathrm{Orb}_{g_i}^{\pm}(t)\right) = 1$. We assume without loss of generality that $|\mathrm{Orb}_f(t) \cap \mathrm{Orb}_{g_i}^{\pm}(t)| = \infty$ for all i. By Corollary 6.3, $\delta_{f,t}(\mathrm{Orb}_{g_i}^{\pm}(t)) = \frac{1}{n_i}$ for some positive integer n_i. Moreover, if $g_i(x) =$

$x+a_i$, then a_i is a primitive divisor of $f^{n_i}(t)-t$. We assume that $n_i>1$ for all i. Proposition 6.4 implies that $f^m(t)\in \mathrm{Orb}^{\pm}_{g_i}(t)$ if and only if $n_i|m$. Let $n=\prod_i n_i$. Now it is clear that $n_i\nmid (hn+1)$ for any integer h. In particular, $f^{hn+1}(t)\notin \mathrm{Orb}^{\pm}_{g_i}(t)$ for any i, $1\le i\le k$. This implies that $\delta_{f,t}\left(\bigcup_i \mathrm{Orb}^{\pm}_{g_i}(t)\right)\le 1-\frac{1}{n}$; which contradicts our assumption, hence $n_i=1$ for some i. Assuming ii), Corollary 6.4 ii) implies that a_i is a primitive divisor of $f(t)-t$. In view of Proposition 6.5, one sees that $\mathrm{Orb}_f(t)\subset \mathrm{Orb}^{\pm}_{g_i}(t)$. □

Corollary 6.4 *Let $f(x)$ be a polynomial in $\mathbb{Z}[x]$ and $t\in\mathbb{Z}$. If $A=\{t+n_s\mathbb{Z}\}_{s=1}^k$ is a minimal t-cover of $\mathrm{Orb}_f(t)$, then $k=1$. In particular, if $A=\{t+n_s\mathbb{Z}\}_{s=1}^k$, $k\ge 1$, is a system of arithmetic progressions such that $\delta_{f,t}(t+n_s\mathbb{Z})<1$, for all $s=1,\cdots,k$, then $\delta_{f,t}\left(\bigcup_{i=1}^k (t+n_s\mathbb{Z})\right)<1$.*

Definition 6.3 *Let $f(x)\in\mathbb{Z}[x]$ and $t\in\mathbb{Z}$. Let δ be a real number such that $0\le\delta\le 1$. If there is a system of arithmetic progressions of the form $A=\{t+n_s\mathbb{Z}\}_{s=1}^k$ such that $\delta_{f,t}\left(\bigcup_{s=1}^k t+n_s\mathbb{Z}\right)=\delta$, then δ is said to be* (f,t,k)-accessible.

For $f(x)\in\mathbb{Z}[x]$ and $t\in\mathbb{Z}$, we set

$$\mathcal{PD}(f,t)=\{a : a \text{ is a primitive divisor of } f^n(t)-t \text{ for some } n\ge 1\}.$$

The set $\mathcal{PD}(f,t)$ contains the set of primitive prime divisors of $f^n(t)-t$. If t is a wandering point for f, then it is clear that $\mathcal{PD}(f,t)$ is infinite since otherwise t will be a preperiodic point under f. We also set

$$S(f,t)=\{n\ge 1 : f^n(t)-t \text{ has a primitive divisor}\}.$$

Again, if t is a wandering point for f, then $S(f,t)$ is infinite.

Definition 6.4 *Let $S\subseteq\mathbb{Z}$. A nonnegative rational number $\delta<1$ is said to be an* (S,k)-inclusion-exclusion fraction *if there are $n_i\in S$, $i=1,\cdots,k$, with*

$$\delta=\sum_{i=1}^k\frac{1}{n_i}-\sum_{1\le i_1<i_2\le k}\frac{1}{\mathrm{lcm}(n_{i_1},n_{i_2})}+\sum_{1\le i_1<i_2<i_3\le k}\frac{1}{\mathrm{lcm}(n_{i_1},n_{i_2},n_{i_3})}+\cdots+(-1)^{k+1}\frac{1}{\mathrm{lcm}(n_1,\cdots,n_k)}.$$

Theorem 6.2 *Let $f(x)\in\mathbb{Z}[x]$ and $t\in\mathbb{Z}$ be a wandering point for f. Let $k\ge 1$ be an integer. An $(S(f,t),k)$-inclusion-exclusion fraction is (f,t,k)-accessible.*

Proof: Let δ be an $(S(f,t),k)$-inclusion-exclusion fraction. Let $n_i\in S(f,t)$ for $1\le i\le k$ be as in Definition 6.4. Let a_i be a primitive prime divisor of $f^{n_i}(t)-t$ which exist by the definition of $S(f,t)$. Let $g_i=x+a_i$. By Corollary 6.3, $\delta_{f,t}(\mathrm{Orb}^{\pm}_{g_i}(t))=\frac{1}{n_i}$. By setting $A=\{t+a_i\mathbb{Z}\}$, we can see that

$$\begin{aligned}
\delta_{f,t}(\bigcup_{i=1}^{k} t+a_i\mathbb{Z}) &= \delta_{f,t}(\bigcup_{i=1}^{k} \mathrm{Orb}^{\pm}_{g_i}(t)) \\
&= \lim_{X\to\infty} \frac{|\{x \in \bigcup_{i=1}^{k} \left(\mathrm{Orb}^{\pm}_{g_i}(t) \cap \mathrm{Orb}_f(t)\right) : x \le X\}|}{|x \in \mathrm{Orb}_f(t) : x \le X\}|} \\
&= \sum_{j=1}^{k}(-1)^{j+1} \sum_{1\le i_1<i_2<\cdots<i_j\le k} \lim_{X\to\infty} \frac{|\{x \in \bigcap_{r=1}^{j} \left(\mathrm{Orb}^{\pm}_{g_{i_r}}(t) \cap \mathrm{Orb}_f(t)\right) : x \le X\}|}{|x \in \mathrm{Orb}_f(t) : x \le X\}|} \\
&= \sum_{j=1}^{k}(-1)^{j+1} \sum_{1\le i_1<i_2<\cdots<i_j\le k} \lim_{M\to\infty} \frac{|\{f^m(t) \in \bigcap_{r=1}^{j} \mathrm{Orb}^{\pm}_{g_{i_r}}(t) : m \le M\}|}{M} \\
&= \sum_{j=1}^{k}(-1)^{j+1} \sum_{1\le i_1<i_2<\cdots<i_j\le k} \frac{1}{\mathrm{lcm}(n_{i_1},\ldots,n_{i_j})}.
\end{aligned}$$

The third equality is by inclusion and exclusion. The last equality is by Corollary 6.3 and Proposition 6.4, since $f^m(t) \in \mathrm{Orb}^{\pm}_{g_{i_r}}(t)$ if and only if $n_{i_r}|m$ which implies that $f^m(t) \in \bigcap_{r=1}^{j} \mathrm{Orb}^{\pm}_{g_{i_r}}(t)$ if and only if $\mathrm{lcm}(n_{i_1},\ldots,n_{i_j})|m$. Thus, the result holds.

□

Corollary 6.5 *Let $f(x) \in \mathbb{Z}[x]$ and $t \in \mathbb{Z}$ be a wandering point for f. If $n \in S(f,t)$, then $1/n$ is $(f,t,1)$-accessible.*

Proof: This follows from Corollary 6.3. □

Proposition 6.7 *Let $f(x) \in \mathbb{Z}[x]$ and $t \in \mathbb{Z}$ be a wandering point for f.*

i) If $n, n-1 \in S(f,t)$, then $2/n$ is $(f,t,2)$-accessible.

ii) Let n be an odd integer such that $n, n-1, n-2 \in S(f,t)$, then $3/n$ is $(f,t,3)$-accessible.

iii) Let $m,n \in \mathbb{Z}$ such that $(m-1)|(n-1)$ and $n,(n-1)/(m-1) \in S(f,t)$, then m/n is $(f,t,2)$-accessible.

Proof: For i), if $n, n-1 \in S(f,t)$ then $1/n$ and $1/(n-1)$ are $(f,t,1)$-accessible from Corollary 6.5. Since $\gcd(n,n-1)=1$, one can have that

$$\frac{1}{n} + \frac{1}{n-1} - \frac{1}{n(n-1)} = \frac{2}{n}$$

is $(f,t,2)$-accessible by using Theorem 6.2.

For ii), Corollary 6.5 and assumption give that $1/n, 1/(n-1)$ and $1/(n-2)$ are $(f,t,1)$-accessible. Since n is odd integer, we have $\gcd(n,n-1) = \gcd(n,n-2) =$

$\gcd(n-1,n-2)=1$. Then by using Theorem 6.5, one can have that

$$\frac{1}{n}+\frac{1}{n-1}+\frac{1}{n-2}-\frac{1}{n(n-1)}-\frac{1}{n(n-2)}-\frac{1}{(n-1)(n-2)}+\frac{1}{n(n-1)(n-2)}=\frac{3}{n}$$

is $(f,t,3)$-accessible.

For iii), one may apply the same way to prove that m/n is $(f,t,2)$-accessible.

□

Remark 6.3 *From the Theorem 6.4, we can get the density $\frac{1}{n}$ with one linear polynomial $g(x)$. Also, Proposition 6.7 gives us we can get $\frac{2}{n}$ and $\frac{3}{n}$ (in this case, n is odd) with 2 and 3 linear polynomials, respectively. However, this is not correct in general, i.e., to get density $\frac{i}{n}$, we can not say we must have i linear polynomials. The following example proves this.*

Example 6.8 *Assume that $f(x)$ be a polynomial in $\mathbb{Z}[x]$ and $t\in\mathbb{Z}$, then there does not exist linear polynomials $g_1(x),\ldots,g_4(x)$ in $\mathbb{Z}[x]$ such that*

$$\delta_{f,t}(\mathrm{Orb}^{\pm}_{g_1}(t)\cup\mathrm{Orb}^{\pm}_{g_2}(t)\cup\mathrm{Orb}^{\pm}_{g_3}(t)\cup\mathrm{Orb}^{\pm}_{g_4}(t))=\frac{4}{5}.$$

One can observe that if n_1,n_2,n_3,n_4 be chosen as least four positive prime integers such that $\delta_{f,t}(\mathrm{Orb}^{\pm}_{g_i}(t))=\frac{1}{n_i}$, then

$$\delta_{f,t}(\mathrm{Orb}^{\pm}_{g_1}(t)\cup\mathrm{Orb}^{\pm}_{g_2}(t)\cup\mathrm{Orb}^{\pm}_{g_3}(t)\cup\mathrm{Orb}^{\pm}_{g_4}(t))<\frac{4}{5}.$$

This means, to get the density $\frac{4}{5}$, we need at least 5 linear polynomials.

Theorem 6.3 *Let $f(x)\in\mathbb{Z}[x]$ and $t\in\mathbb{Z}$ be a wandering point for f. Let $m,n\in\mathbb{Z}$ and p_i's are prime in order. If k is an positive integer such that*

$$\delta_k=1-\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)<\frac{m}{n},$$

then m/n is not (f,t,k)-accessible. In particular, there does not exist k linear polynomials $g_1(x),\ldots,g_k(x)$ such that

$$\delta_{f,t}\left(\bigcup_{i=1}^{k}\mathrm{Orb}^{\pm}_{g_i}(t)\right)=\frac{m}{n}.$$

Corollary 6.6 *For $k=2$, $1-\prod_{i=1}^{2}\left(1-\frac{1}{p_i}\right)=1-\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)=\frac{2}{3}$. So, for $\frac{m}{n}>$*

$\frac{2}{3}$, $\frac{m}{n}$ *is not* $(f,t,2)-$*accessible for any* f *and* t.

Remark 6.4 *Let* $k>0$ *be an integer. Then there exist an interval* $(a,1)$ *where* $a\in\mathbb{Q}$ *and* $0<a<1$ *such that* c *is not* $(f,t,k)-$*accessible for any* f, t *and* $c\in(a,1)$.

Theorem 6.4 *Let the set of all rational primes by* $\mathcal{P}$, $f(x)$ *be a polynomial in* $\mathbb{Z}[x]$ *and* $t\in\mathbb{Z}$ *such that* $\mathcal{P}\subset S(f,t)$. *Then for all* $\epsilon>0$, *there exists a finite family of linear polynomials* $g_i(x)$ *such that*

$$\delta_{f,t}\left(\mathrm{Orb}_f(t)\cap\left(\bigcup_i \mathrm{Orb}_{g_i}^{\pm}(t)\right)\right)\geq 1-\epsilon.$$

Proof: Let n_i be the exact period of t under $f(x)$ $(mod\ m_i)$ for some positive integer m_i. (Here, m_i is primitive divisor (not nec. prime) of $\{f^{n_i}(t)-t\}$). If $n_i's$ are coprime, then one can observe the following equality,

$$1-\prod_i\left(1-\frac{1}{n_i}\right)=\sum_i\frac{1}{n_i}-\sum_{i,j}\frac{1}{n_in_j}+\sum_{i,j,k}\frac{1}{n_in_jn_k}-\dots$$

where the RHS is the required density. Now, n_i can be chosen as primes p_i in order. Then we have

$$\delta_{f,t}\left(\mathrm{Orb}_f(t)\cap\left(\bigcup_i \mathrm{Orb}_{g_i}^{\pm}(t)\right)\right)=1-\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)=1-\frac{1}{(\prod_{i=1}^{k}(1-\frac{1}{p_i}))^{-1}}$$

Moreover, we know that

$$\lim_{k\to\infty}\left(1-\frac{1}{(\prod_{i=1}^{k}(1-\frac{1}{p_i}))^{-1}}\right)=\left(1-\frac{1}{\lim_{k\to\infty}\lim_{s\to1^+}(\prod_{i=1}^{k}(1-\frac{1}{p_i^s}))^{-1}}\right)=1-\frac{1}{\lim_{s\to1^+}\zeta(s)}=1-0=1$$

where ζ is the Riemann-Zeta function, which has a simple pole at 1.

By the definition of the limit, for all ϵ, there is an integer N such that

$$1-\left(1-\frac{1}{(\prod_{i=1}^{N}(1-\frac{1}{p_i}))^{-1}}\right)\leq\epsilon$$

which concludes the result. □

Corollary 6.7 *Let* $(x,1)$ *be an open interval. Then there exist* f,t,k *and* $x_0\in(x,1)$ *such that* x_0 *is* $(f,t,k)-$ *accessible.*

BIBLIOGRAPHY

[1] W. W. Adams and M. J. Razar. Multiples of points on elliptic curves and continued fractions. *Proceedings of The London Mathematical Society*, pages 481–498, 1980.

[2] B. Bekker and Y. G. Zarhin. The divisibility by 2 of rational points on elliptic curves. *arXiv: Number Theory*, 2017.

[3] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. ISSN 0747-7171. doi: 10.1006/jsco.1996.0125. URL http://dx.doi.org/10.1006/jsco.1996.0125. Computational algebra and number theory (London, 1993).

[4] Y. Bugeaud. Bounds for the solutions of superelliptic equations. *Compositio Mathematica*, 107:187–219, 1997.

[5] M. Chou. Torsion of rational elliptic curves over quartic galois number fields. *Journal of Number Theory*, 160:603–628, 2015.

[6] I. Connell. *Elliptic Curve Handbook*. McGill University, Montreal. 1999.

[7] J. Cremona. Classical invariants and 2-descent on elliptic curves. *J. Symb. Comput.*, 31:71–87, 2001.

[8] J. Cremona, T. A. Fisher, and M. Stoll. Minimisation and reduction of 2-, 3- and 4-coverings of elliptic curves. *Algebra & Number Theory*, 4:763–820, 2009.

[9] M. Derickx, A. Etropolski, M. van Hoeij, J. S. Morrow, and D. Zureick-Brown. Sporadic cubic torsion. *Algebra / Number Theory*, 15(7):1837–1864, 2021.

[10] K. Doerksen and A. Haensch. Primitive prime divisors in zero orbits of polynomials. In *Integers*, 2010.

[11] G. Dražić. Rational D(q)-quintuples. *Revista de la Real Academia de Ciencias Exactas, Físicas y Naturales. Serie A. Matemáticas*, 116, 2021.

[12] G. Dražić and M. Kazalicki. Rational D(q)-quadruples. *Indagationes Mathematicae*, 33:440–449, 2020.

[13] A. Dujella. Some polynomial formulas for Diophantine quadruples. *Grazer Math. Ber.*, 328:25–30, 1996.

[14] A. Dujella. On Diophantine quintuples. *Acta Arithmetica*, 81:69–79, 1997.

[15] A. Dujella. On the size of Diophantine m-tuples. *Mathematical Proceedings of the Cambridge Philosophical Society*, 132:23 – 33, 2000.

[16] A. Dujella. Irregular Diophantine m-tuples and elliptic curves of high rank. *Proc. Japan Acad. Ser. A Math. Sci.*, 76:66–67, 2000.

[17] A. Dujella. Diophantine m-tuples and elliptic curves. *Journal de Theorie des Nombres de Bordeaux*, 13:111–124, 2001.

[18] A. Dujella. There are only finitely many Diophantine quintuples. *Crelle's Journal*, 2004:183–214, 2004.

[19] A. Dujella. What is a Diophantine m-tuple? *Notices of the American Mathematical Society*, 63:772–774, 2016.

[20] A. Dujella. *Number Theory*. Manualia universitatis studiorum zagrabiensis. Školska knjiga, 2021. ISBN 9789530308978. URL https://books.google.com/books?id=sISFzgEACAAJ.

[21] A. Dujella and C. Fuchs. A polynomial variant of a problem of diophantus and euler. *Rocky Mountain Journal of Mathematics*, 33:797–811, 2003.

[22] A. Dujella and V. Petričević. Strong Diophantine triples. *Experimental Mathematics*, 17:83 – 89, 2008.

[23] A. Dujella and V. Petričević. Doubly regular Diophantine quadruples. *Revista de la Real Academia de Ciencias Exactas, Físicas y Naturales. Serie A. Matemáticas*, 114, 2020.

[24] A. Dujella and G. Soydan. On elliptic curves induced by rational Diophantine quadruples. *Proceedings of the Japan Academy, Series A, Mathematical Sciences*, 98(1):1–6, 2022.

[25] A. Dujella, C. Fuchs, and R. F. Tichy. Diophantine m-tuples for linear polynomials. *Periodica Mathematica Hungarica*, 45:21–33, 2002.

[26] A. Dujella, C. Fuchs, and G. Walsh. Diophantine m-tuples for linear polynomials ii. equal degrees. *Journal of Number Theory*, 120:213–228, 2006.

[27] A. Dujella, M. Kazalicki, M. Mikić, and M. Szikszai. There are infinitely many rational Diophantine sextuples. *arXiv: Number Theory*, 2015.

[28] A. Dujella, I. Gusić, V. Petričević, and P. Tadić. Strong eulerian triples. *Glasnik Matematicki*, 2018.

[29] A. Dujella, M. Kazalicki, and V. Petričević. D(n)-quintuples with square elements. *Revista de la Real Academia de Ciencias Exactas, Físicas y Naturales. Serie A. Matemáticas*, 115, 2020.

[30] A. Dujella, M. Kazalicki, and J. C. Peral. Elliptic curves with torsion groups $\mathbb{Z}/8\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. *Revista de la Real Academia de Ciencias Exactas, Físicas y Naturales. Serie A. Matemáticas*, 2021.

[31] D. S. Dummit and R. M. Foote. Abstract algebra. 1999.

[32] P. Erdős. On integers of the form $2^k + p$ and some related problems. *Summa Brasil. Math.*, 2:113–123, 1950.

[33] G. Faltings. Endlichkeitssätze für abelsche varietäten über zahlkörpern. *Inventiones mathematicae*, 75:381, 1983.

[34] E. V. Flynn, B. Poonen, and E. F. Schaefer. Cycles of quadratic polynomials and rational points on a genus-2 curve. *Duke Mathematical Journal*, 90:435–463, 1995.

[35] S. D. Galbraith. Mathematics of public key cryptography. *Cambridge University Press*, 2012.

[36] D. Ghioca, T. J. Tucker, and M. E. Zieve. Intersections of polynomial orbits, and a dynamical mordell–lang conjecture. *Inventiones mathematicae*, 171:463–483, 2007.

[37] D. Ghioca, T. J. Tucker, and M. E. Zieve. Linear relations between polynomial orbits. *Duke Mathematical Journal*, 161:1379–1410, 2008.

[38] E. González-Jiménez and X. Xarles. Five squares in arithmetic progression over quadratic fields. *Revista Matemática Iberoamericana*, 29(4):1211–1238, 2013. doi: 10.4171/rmi/754. URL https://doi.org/10.4171%2Frmi%2F754.

[39] C. Gratton, K. V. Nguyen, and T. J. Tucker. Abc implies primitive prime divisors in arithmetic dynamics. *Bulletin of the London Mathematical Society*, 45, 2012.

[40] R. Hartshorne. Algebraic geometry. In *Graduate texts in mathematics*, 1977.

[41] B. He, A. Togbé, and V. Ziegler. There is no Diophantine quintuple. *Transactions of the American Mathematical Society*, 2016.

[42] E. Herrmann, A. Pethő, and H. G. Zimmer. On fermat's quadruple equations. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 69: 283–291, 1999.

[43] D. Husemöller. *Galois Cohomology and Isomorphism Classification of Elliptic Curves over Arbitrary Fields*, pages 138–151. Springer New York, New York, NY, 1987. ISBN 978-1-4757-5119-2. doi: 10.1007/978-1-4757-5119-2_8. URL https://doi.org/10.1007/978-1-4757-5119-2_8.

[44] P. Ingram. Canonical heights and preperiodic points for weighted homogeneous families of polynomials. *arXiv: Number Theory*, 2015.

[45] B. W. Jones. A second variation of a problem of davenport and diophantus. Fibonacci Quart., 15:323–330, 1972.

[46] B. W. Jones. A variation on a problem of davenport and diophantus. *Quarterly Journal of Mathematics*, 27:349–353, 1976.

[47] S. Kamienny. Torsion points on elliptic curves and q-coeffincients of modular forms. *Inventiones mathematicae*, 109(2):221–230, 1992. URL http://eudml.org/doc/144019.

[48] M. A. Kenku and F. Momose. Torsion points on elliptic curves defined over quadratic fields. *Nagoya Mathematical Journal*, 109:125 – 149, 1975.

[49] A. Knapp. *Elliptic Curves*. Mathematical Notes - Princeton University Press. Princeton University Press, 1992. ISBN 9780691085593. URL https://books.google.com.bn/books?id=-e_qVoKF8H8C.

[50] H. Krieger. Primitive prime divisors in the critical orbit of $z^d + c$. *arXiv: Dynamical Systems*, 2012.

[51] S. Lang. Integral points on curves. *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, 6:27–43, 1960.

[52] W. J. LeVeque. On the equation $y^m = f(x)$. *Acta Arithmetica*, 9:209–219, 1964.

[53] B. Mazur and D. Goldfeld. Rational isogenies of prime degree. *Inventiones mathematicae*, 44:129–162, 1978.

[54] P. Morton. Arithmetic properties of periodic points of quadratic maps, ii. *Acta Arithmetica*, 87:89–102, 1992.

[55] F. Najman. Complete classification of torsion of elliptic curves over quadratic cyclotomic fields. *arXiv: Number Theory*, 2010.

[56] B. Poonen. The classification of rational preperiodic points of quadratic polynomials over $\mathbb{Q}$: a refined conjecture. *Math. Z.*, 228(1):11–29, 1998. ISSN 0025-5874. doi: 10.1007/PL00004405. URL https://doi.org/10.1007/PL00004405.

[57] R. Ren. Primitive prime divisors in the critical orbits of one-parameter families of rational polynomials. *Mathematical Proceedings of the Cambridge Philosophical Society*, 171:569 – 584, 2019.

[58] B. Rice. Primitive prime divisors in polynomial arithmetic dynamics. 2007.

[59] M. Sadek. Families of polynomials of every degree with no rational preperiodic points. *Comptes Rendus. Mathématique. Académie des Sciences. Paris*, 359: 195–197, 2021.

[60] M. Sadek and T. Yesin. Divisibility by 2 on quartic models of elliptic curves and rational Diophantine D(q)-quintuples. *Revista de la Real Academia de Ciencias Exactas, Físicas y Naturales. Serie A. Matemáticas*, 116:1–17, 2022.

[61] C. L. Siegel. The integer solutions of the equation $y^2 = ax^n + bx^{n-1} + \cdots + k$. 1926.

[62] C. L. Siegel. Über einige anwendungen diophantischer approximationen. 1929.

[63] J. H. Silverman. *The Arithmetic of Dynamical Systems*. Springer, 2007.

[64] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Graduate texts in mathematics. Springer, Dordrecht, 2009. doi: 10.1007/978-0-387-09494-6. URL https://cds.cern.ch/record/1338326.

[65] M. Stoll. Rational 6-cycles under iteration of quadratic polynomials. *arXiv: Number Theory*, 2008.

[66] M. Stoll. Diagonal genus 5 curves, elliptic curves over $\mathbb{Q}(t)$, and rational diophantine quintuples. *Acta Arithmetica*, 190:239–261, 2019.

[67] R. Taylor and A. Wiles. Ring-theoretic properties of certain hecke algebras. *Annals of Mathematics*, 141:553–572, 1995.

[68] W. J. L. Veque. Rational points on curves of genus greater than 1. *Crelle's Journal*, 206:45–52, 1961.

[69] R. Walde and P. Russo. Rational periodic points of the quadratic function $Q_c(x) = x^2 + c$. *Amer. Math. Monthly*, 101(4):318–331, 1994. ISSN 0002-9890. doi: 10.2307/2975624. URL https://doi.org/10.2307/2975624.

[70] X. Xarles. Squares in arithmetic progression over number fields. *arXiv: Algebraic Geometry*, 2009.