ORDER OF REDUCTIONS OF ELLIPTIC CURVES IN ARITHMETIC PROGRESSION

by
ANTIGONA PAJAZITI

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

Sabancı University
July 2022

ABSTRACT

ORDER OF REDUCTIONS OF ELLIPTIC CURVES IN ARITHMETIC PROGRESSION

ANTIGONA PAJAZITI

Mathematics, Master Thesis, July 2022

Thesis Supervisor: Assoc. Prof. Mohammad Sadek

Keywords: elliptic curves, reduction, torsion subgroup

Let E be an elliptic curve defined over a number field K with ring of integers R. We consider the set S of all the orders of reductions of E modulo the primes of R. Given an integer $m > 1$, one may ask how many residue classes modulo m have an intersection of positive density with S. Using results of Serre and Katz, we show that there are at least two such residue classes; except for explicit families of elliptic curves and corresponding values of m. We then describe this exceptional set of elliptic curves and list the values of m when K is of degree at most 3; or K is Galois of degree 4.

We also consider the following divisibility question on orders of elliptic surfaces over finite fields. Given an integer $m \geq 2$ and a finite field k, is there an elliptic curve E_t over $k[t]$ such that for all k-rational values of t the order of $E_t(k)$ is divisible by m ? We suggest a method to construct such elliptic curves. Consequently, when $m = 3$, we provide two such elliptic curves over $k[t]$ whenever k is of prime order congruent to $1 \mod 3$.

Finally, we discuss how the growth of the order of the torsion subgroup of an elliptic curve E over K after a base change is linked to the divisibility of the orders of reductions of E modulo the primes of R. In particular, we provide examples of elliptic curves over the rational field for which we can list all the possible congruence classes of the orders of the reductions modulo a certain integer $m \geq 2$; together with the density of appearance of these congruence classes.

ÖZET

ARİTMETİK DİZİDE ELİPTİK EĞRİLERİN İNDİRGEMESİNİN MERTEBESİ

ANTIGONA PAJAZITI

Matematik, Yüksek Lisans Tezi, Temmuz 2022

Tez Danışmanı: Assoc. Prof. Mohammad Sadek

Anahtar Kelimeler: eliptik eğri, indirgeme, burulma alt grubu

E, tamsayı halkası R olan bir sayı cismi K üzerinde tanımlanan bir eliptik eğri olsun. S'yi, R'nin E-modülo asallarının indirgemelerinin tümünün eleman sayısı olarak ele alıyoruz. Bir $m > 1$ tamsayı verildiğinde, modülo m'nin kaç tane rezidü sınıfının S ile pozitif yoğunluğun kesişimine sahip olduğu sorulabilir. Serre ve Katz'ın sonuçlarını kullanarak, eliptik eğrilerin belirli aileleri ve karşılık gelen m değerleri hariç tutarak bu tür iki rezidü sınıfın olduğunu gösteriyoruz. Daha sonra bu istisnai eliptik eğriler kümesini tanımlarız ve K derecesi en fazla 3 veya K, 4. dereceden Galois olduğunda m'nin değerlerini listeleriz.

Ayrıca, sonlu cisimler üzerindeki eliptik yüzeylerin eleman sayıları hakkında aşağıdaki bölünebilirlik sorusunu ele alıyoruz. Bir $m \geq 2$ tamsayısı ve sonlu bir k cismi verildiğinde, t'nin tüm k-rasyonel değerleri için $E_t(k)$ kümesinin eleman sayının m'ye bölünebileceği şekilde $k[t]$ üzerinde bir E_t eliptik eğrisi var mıdır? Bu tür eliptik eğriler oluşturmak için bir metot öneriyoruz. Sonuç olarak, $m = 3$ olduğunda; k, 3 modülünde 1'e kongruent asal mertebeden olduğunda, $k[t]$ üzerinde böyle iki eliptik eğri elde ederiz.

Son olarak, R'nin E-modülo asallarının indirgemelerinin eleman sayılarının bölünebilmeleriyle ilişkili olan bir taban değişikliğinden sonra, K üzerindeki bir E eliptik eğrisinin burulmalı altgruplarının eleman sayılarının büyümesini ele alacağız. Özellikle, belirli bir $m \geq 2$ tamsayının modulo indirgeme eleman sayılarının tüm olası denklik sınıflarını listeleyebildiğimiz rasyonel cisim üzerindeki eliptik eğri örneklerini denklik sınıflarının görünüm yoğunluğu ile birlikte sunuyoruz.

ACKNOWLEDGEMENTS

I am extremely grateful to my supervisor Dr. Mohammad Sadek for his patient guidance, continuous encouragement and inspiring dedication. I have been very fortunate to have a supervisor who consistently motivated me. He always found the time to answer my questions with precious suggestions and valuable advice.

My sincere thanks go to my jury members Prof. Michel Lavrauw and Prof. Gökhan Soydan for their helpful comments and suggestions on my thesis.

I could not have taken this journey without my family, especially my parents and my sisters who gave me the love and support needed throughout this process.

I would like to offer my special thanks to my friends Mohamed Osama Darwish and Mohamed Wafik El- Sheikh. We started this journey together. I was so lucky to have them as my colleagues. Darwish and Wafik, I will cherish our time working together for a lifetime.

Additionally, this endeavor would not have been possible without my dearest friends Tuğba Yesin, Gülsemin Çonoğlu and Beyza Çepni. Thank you for your unwavering support and for always being there for me when I was stressed out.

Mathematics is the surest way to immortality
Paul Erdős

TABLE OF CONTENTS

1. Introduction

Let E be an elliptic curve defined over a number field K with ring of integers R. Elliptic curves can be represented by a Weierstrass equation of the form

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

with $a_1, ..., a_6 \in K$ together with the point at infinity $\mathcal{O}$. Elliptic curves have a group structure and we can describe the group law geometrically using the chord and tangent process. Let $E(K) = \{(x, y) \in K^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}\}$ be the set of K- rational points of E. We call $E(K)$ the *Mordell-Weill group* of E. Moreover, $E(K)$ is a finitely generated group, see [Theorem 1,[23]]. That is we can write, $E(K) \cong \mathbb{Z}^r \times E(K)_{tors}$, where $r \geq 0$ is the *Mordell-Weil rank* of E and $E(K)_{tors}$ is the *torsion subgroup* of the elliptic curve E.

The cardinality of the torsion subgroup of an elliptic curve E is finite. Merel in [22], showed that the possibilities of torsion subgroups for an elliptic curve over any number field are finite. Then the complete classification of possible torsion subgroups for an elliptic curve E defined over $\mathbb{Q}$ was given by Mazur in [20]. Similarly, for an elliptic curve defined over a quadratic field the complete classification of possible torsion subgroups for E was given by Kenku and Momose in [17], and for an elliptic curve defined over a cubic field in [5], by Derickx, Etropoloski, Morrow, Zuerick-Brown and Van Hoeij. Finally, for an elliptic curve defined over a quartic Galois field the complete classification of possible torsion subgroups for E was given by Chou in [2].

Let $\mathfrak{p}$ be a prime ideal in R with norm $N(\mathfrak{p}) = q = p^r$, p is a prime and $r \geq 1$ and, $k_{\mathfrak{p}}$ the residue field of K at $\mathfrak{p}$. We denote the reduction of the elliptic curve E modulo $\mathfrak{p}$ by $\widetilde{E}$. Now, if $\widetilde{E}$ is nonsingular then it is an elliptic curve, otherwise it has a singular point which can be a node or a cusp. If $\widetilde{E}$ has a node we say that E has *bad multiplicative reduction* at the prime $\mathfrak{p}$, if $\widetilde{E}$ has a cusp then E has *bad additive reduction* at the prime $\mathfrak{p}$. One important quantity that we associate to the elliptic curve $\widetilde{E}$ is the number of its rational points. We have that $\#\widetilde{E}(k_{\mathfrak{p}}) = 1 + q - a_{\mathfrak{p}}(E)$.

We call by $a_{\mathfrak{p}}(E)$ *the trace of Frobenius* of E at $\mathfrak{p}$. Hasse's theorem, [[32], Chapter 5, Theorem 1.1] implies that, $-2\sqrt{q} \leq a_{\mathfrak{p}}(E) \leq 2\sqrt{q}$.

Over a fixed finite field $k_{\mathfrak{p}}$, Waterhouse in [Theorem 2.1, [34]] provides necessary and sufficient conditions under which an element in the interval $[-2\sqrt{q}, 2\sqrt{q}]$ appears as the trace of Frobenius for an elliptic curve E. Now, fix an elliptic curve E defined over a number field K and an integer n. Can we have infinitely many primes $\mathfrak{p}$ such that the trace of Frobenius of E modulo $\mathfrak{p}$ is n? If so, what is the density of such primes?

We say that an elliptic curve E has *complex multiplication* if its endomorphism ring $End(E)$ does not equal $\mathbb{Z}$. In [6], Deuring showed that for all elliptic curves over $\mathbb{Q}$ with complex multiplication, $a_p(E) = 0$ for primes p of density $\frac{1}{2}$. Furthermore, in [15], Ji and Chin showed that for elliptic curves defined over $\mathbb{Q}$ with complex multiplication by an imaginary quadratic field L of class number 1, $a_p(E) = r \neq 0$, for specific nonzero integer r if and only if the prime p can be represented by a quadratic polynomial of the form $p = ax^2 + bx + c$ for some $a, b, c \in \mathbb{Z}$. In particular, for the integer 0 the case of elliptic curves over $\mathbb{Q}$ without complex multiplication, was treated by Elkies in [25]. He showed that for elliptic curves over $\mathbb{Q}$ without complex multiplication, $a_p(E) = 0$ for infinitely many primes p. Moreover, in [26], he extended his result to any elliptic curve E over any real number field.

In Chapter 2, we approach the question above using a different method. We investigate the possible values of congruence classes of $\#\widetilde{E}(k_{\mathfrak{p}})$ modulo a fixed integer $m \geq 2$. That is, we ask the following question

Question 1.1. *Let $m \geq 2$ and β a non-negative integer. Does there exist an elliptic curve E defined over a number field K such that $\#\widetilde{E}(k_{\mathfrak{p}}) \equiv \beta \mod m$ for almost all primes $\mathfrak{p}$?*

According to a result of Serre on the congruence classes of $\#\widetilde{E}(k_{\mathfrak{p}}) \mod m$, for some integer m, it follows that, if $\#\widetilde{E}(k_{\mathfrak{p}}) \equiv \beta \mod m$ holds for almost all primes $\mathfrak{p}$, then $\beta \equiv 0 \mod m$, see, [[29], Proposition 2.2] for elliptic curves over $\mathbb{Q}$ and [[12], Theorem 2.3] for elliptic curves defined over a number field K. We denote by $\mathcal{S}_d$ the set $\mathcal{S}_d = \{m : \text{there is an elliptic curve } E/K, \text{ where } [K : \mathbb{Q}] = d \text{ and } m | \#E(K)_{tors}\}$. Then using a result of Katz, see, [Theorem 2, [16]], in Chapter 3, Theorem 3.16, we describe the values of m explicitly when K is of degree at most 3, or K is Galois of degree 4. In particular, we show that the list of these m's is finite and it only depends on d.

Theorem 1.2. *Let $m \geq 2$ be an integer and K be a number field with $[K : \mathbb{Q}] = d$. Then there exists an elliptic curve E defined over K such that $\#\widetilde{E}(k_{\mathfrak{p}}) \equiv 0 \mod m$*

for all the primes of good reduction if and only if $m \in \mathcal{S}_d$ *where,*

(a) $\mathcal{S}_1 = \{2,3,4,5,6,7,8,9,10,12,14,16\}$*, if* $K = \mathbb{Q}$*,*

(b) $\mathcal{S}_2 = \{2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,18,20,24\}$*, if* K *is a quadratic field,*

(c) $\mathcal{S}_3 = \{2,3,4,5,6,7,8,9,10,11,12,13,15,18,20,21,24,28\}$*, if* K *is a cubic field,*

(d) $\mathcal{S}_4 = \{2,3,4,5,6,7,8,9,10,12,13,15,20,21,22,24,25,32,36\}$*, if* K *is a quartic Galois field.*

We then observe that if the elliptic curve E/K does not satisfy one of the following conditions:

(i) $\#\widetilde{E}(k_{\mathfrak{p}}) \equiv 0 \mod m$ for all primes of good reduction,

(ii) the integer m is not in $\mathcal{S}_d$,

then there are at least two possible values $\beta_i \mod m$ such that $\#\widetilde{E}(k_{\mathfrak{p}}) \equiv \beta_i \mod m$ for primes $\mathfrak{p}$ of positive density. This result can be found as Theorem 3.24 in Chapter 3.

The results above are provided for elliptic curves with good reduction for almost all primes $\mathfrak{p}$. One may explore the possiblity that the order of the reduction of an elliptic curve E is divisible by a certain integer m modulo **all** primes $\mathfrak{p}$. If an elliptic curve E has good reduction at every prime $\mathfrak{p}$, we say that E has *good reduction everywhere*. By [[32], Exercise 8.15], it follows that there is no elliptic curve E defined over $\mathbb{Q}$ with everywhere good reduction. However, this is not always true when we work over finite extensions of $\mathbb{Q}$. In Chapter 3, Section 3.1, we prove the existence of an elliptic curve satisfying $\#\widetilde{E}(k_{\mathfrak{p}}) \equiv 0 \mod m$ for all primes $\mathfrak{p}$. Moreover, for the case of elliptic curves defined over $\mathbb{Q}$, we show that $m \leq 5$. This result can be found in Section 3.1 as Theorem 3.29. Furthermore, we present examples of families of elliptic curves with non-trivial torsion subgroup for which such an integer $m \geq 2$ exists and other examples for which no such integer m exists.

Above we mentioned that the classification of possible torsion subgroups of E over $\mathbb{Q}$, was given by Mazur in [20]. Moreover, in [18], Kubert gave a parametrization of all elliptic curves over $\mathbb{Q}$ with a certain torsion subgroup. Similarly, we mentioned that a complete classification of possible torsion subgroups of E over a quadratic number field K, was given by Kenku and Momose in [17]. Then, in [30], Rabarison provided the parametrization of all elliptic curves over K with a certain torsion subgroup. For all primes of good reduction such that $p \nmid k(9k+4)$, in [4], Kim, Koo and Park exhibited a family of elliptic curves given by $E : y^2 = x^3 - (6k+3)x - (3k^2+6k+2)$

over a finite field $\mathbb{F}_p$, such that $\#E(\mathbb{F}_p) \equiv 0 \mod 3$. For any prime p, in Chapter 4, Theorem 4.3, we generalize the result of Kim, Koo and Park to obtain families of elliptic curves of the form $E_{A,B} : y^2 = x^3 + Ax + B$ over a finite field $k_{\mathfrak{p}}$ such that $\#E(k_{\mathfrak{p}}) \equiv 0 \mod p$ for some prime p.

Finally, let $E(\mathbb{Q})_{tors}$ be the torsion subgroup of an elliptic curve defined over $\mathbb{Q}$. In [Theorem 2, [8]], E. G. Jimenez and J. M. Tornero give the possible torsion subgroups of E that appear when we change the base from $\mathbb{Q}$ to a quadratic extension K. In [24], F. Najman gives a bound on the number of quadratic fields K such that $E(\mathbb{Q})_{tors} \neq E(K)_{tors}$ by counting the possible number of the torsion subgroups of quadratic twists E^d of the elliptic curve E. Moreover, in [[9], Theorem 2], by fixing an elliptic curve E, E. G. Jimenez and J. M. Tornero produce the exact number of possible quadratic fields K such that $E(\mathbb{Q})_{tors} \neq E(K)_{tors}$. Then in [[9], Theorem 3], they provide the list of torsion subgroups $E(K)_{tors}$ that appear for a fixed elliptic curve E depending on $E(\mathbb{Q})_{tors}$.

Using these results, in Chapter 5, we count all the possible congruence classes that can appear for $\#E(\mathbb{F}_p)$ such that $E(\mathbb{Q})_{tors} \neq E(K)_{tors}$. This can be found in Theorem 5.10 in Chapter 5. In particular, we show that the growth of torsion subgroup of an elliptic curve over a number field K has a close link with the congruence classes of the order of the reduction of this elliptic curve. Moreover, we provide explicit examples of families of elliptic curves, and integers m such that $\#\widetilde{E}(k_{\mathfrak{p}}) \equiv \beta_i \mod m$, $i = 1, ..., \ell$ with $2 \leq \ell \leq 4$ for primes of positive density.

2. Elliptic Curves

Let K be a perfect field. An elliptic curve is a non-singular abelian variety of dimension 1 that has a K-rational point $\mathcal{O} = (0:1:0)$ called the point at infinity. Any elliptic curve can be expressed explicitly by a Weierstrass equation of the form

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

with $a_1, ..., a_6 \in K$ together with the point $\mathcal{O}$. We say E is defined over K and we write E/K.

In the case of $\operatorname{char} K \neq 2, 3$ we obtain a simpler form of Weierstrass equation of E,

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

where $A, B \in K$. We define $\Delta(E) = -16(4A^3 + 27B^2)$ to be the discriminant of the latter equation. The fact that elliptic curve E is non-singular is equivalent to $\Delta(E) \neq 0$.

Remark 2.1. *The above Weierstrass equation is not unique. We preserve this form of the equation by applying the following changes of variables,*

$$y = u^3y' \text{ and } x = u^2x' \text{ for } u \in K^*.$$

That is, $A = u^4A'$ *and* $B = u^6B'$.

Throughout the thesis, we will be dealing with fields of characteristic different from 2 and 3. Therefore, we will be using the short Weierstrass equation of an elliptic curve.

Elliptic curves possess a group structure. We can describe the group law geometrically using the chord and tangent process. Let P_1, P_2 be two distinct points on the elliptic curve E. Let L be the line passing through P_1, P_2. Bézout Theorem implies the existence of a third intersection point between E and L, say, P_3. Then the reflection of P_3 about the x-axis is $P_1 \oplus P_2$, see figure 1. In case of $P_1 = P_2$ then

the line L is the tangent to E at P_1, and the third intersection point is the point at infinity. It is clear that the group law on E is abelian.

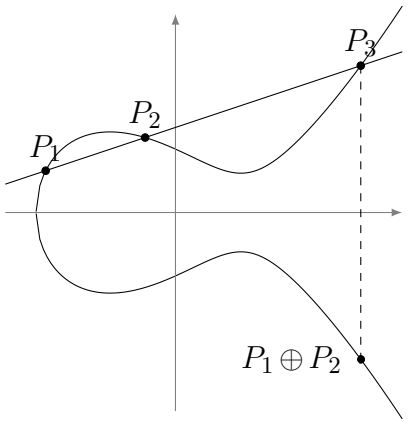

Figure 1: $y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Q}$.

Let $E(K)$ denote the set of K- rational points of E,

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

Remark 2.2. *The set $E(K)$ is a subgroup of the elliptic curve E together with the binary operation $\oplus$. We call $E(K)$ the Mordell-Weil group of E.*

Theorem 2.3 (Mordell-Weil)**.** *([19],Theorem 1) Let A be an abelian variety over a number field K, the group $A(K)$ of K-rational points of A is a finitely-generated abelian group.*

When $K = \mathbb{Q}$, the theorem is due Mordell [23]. For arbitrary elliptic curve over number fields, it follows from Weil [35].

Most of all, we have the following corollary,

Corollary 2.4. *We can find a non-negative integer r such that*

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

where r is the Mordell-Weil the rank of $E(K)$, $E(K)_{tors}$ is the torsion subgroup of the elliptic curve E and the cardinality of $E(K)_{tors}$ is finite.

2.1 Torsion Subgroup

The torsion subgroup of an elliptic curve E defined over a number field K, $E(K)_{tors}$, consists of all points in E that have finite order.

Definition 2.5. *Let $P=(x,y)$ be a rational point on the elliptic curve E defined over K. We say that P has finite order n if and only if $nP=\mathcal{O}$. If this is the case we call P a n-torsion point. We denote the set of all n-torsion points by $E[n]$.*

To find what the coordinates of P can be, we need to examine some polynomials called division polynomials of E.

Let $E: y^2=x^3+ax+b$ be an elliptic curve defined over K. The division polynomials of E are:

$\psi_1 = 1,$

$\psi_2 = 2y,$

$\psi_3 = 3x^4+6ax^2+12bx-a^2,$

$\psi_4 = 4y(x^6+5ax^4+20bx^3-5a^2x^2-4abx-8b^2-a^3),$

$\vdots$

$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3$ for $m \geq 2,$

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

All the polynomials above are defined in $\mathbb{Z}[x,y,a,b]$.

In particular, P is an n-torsion point if and only if the n^{th} division polynomial of E vanishes when evaluated at P.

Example 2.6. *Let $E: y^2=x^3+4$ be an elliptic curve defined over $\mathbb{Q}$. We calculate the third division polynomial of E, $\psi_3 = x(x^3+16)$. Then it follows that $(0,0)$ is a point of order 3 on E.*

The complete classification of all torsion subgroups of an elliptic curve E over any arbitrary number field K is still a working problem. Given any number field K and an elliptic curve E defined over K, L. Merel in [22] proved that $\#E(K)_{tors}$ has a uniform bound depending on the degree of the number field K. That is, the possibilities of torsion subgroups for an elliptic curve over any number field are finite. Namely,

Theorem 2.7. *([22], Merel's Theorem) For every integer $d \geq 1$, there is a constant $N(d)$ such that for all number fields K with $[K : \mathbb{Q}] = d$ and all elliptic curves E/K,*

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

We have a complete classification of possible torsion subgroups for a given elliptic curve E/K when $K = \mathbb{Q}$, K is a quadratic field, a cubic number field or a Galois quartic field.

Theorem 2.8. *[Mazur, [20], [21]]Let E be an elliptic curve defined over $\mathbb{Q}$. Then $E(\mathbb{Q})_{tors}$ is isomorphic to one of the following 15 groups:*

$$\mathbb{Z}/m\mathbb{Z} \text{ where } 1 \leq m \leq 12, m \neq 11$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z} \text{ where } 1 \leq m \leq 4$$

Theorem 2.9. *[M. A. Kenku, F. Momose, [17]] The torsion subgroup of an elliptic curve defined over a quadratic field is isomorphic to one of the following 26 groups:*

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

Theorem 2.10. *[Derickx, Etropoloski, Morrow, Zuerick-Brown and Van Hoeij, [5]] The torsion subgroup of an elliptic curve E defined over a cubic field K is isomorphic to one of the following 27 groups:*

$$\mathbb{Z}/m\mathbb{Z} \text{ where } m = 1, 2, ..., 18, 20, 21$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z} \text{ where } 1 \leq m \leq 7.$$

Theorem 2.11. *[Chou,[2]] The torsion subgroup of an elliptic curve over a quartic Galois field is isomorphic to one of the following 27 groups:*

$$\mathbb{Z}/m\mathbb{Z} \text{ where } m = 1, 2, ..., 16, m \neq 11, 14$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z} \text{ where } m = 1, 2, .., 6, 8$$
$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3m\mathbb{Z} \text{ where } m = 1, 2$$
$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4m\mathbb{Z} \text{ where } m = 1, 2$$
$$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$$
$$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$$

2.2 Elliptic Curves over Finite Fields

Let K be a number field, R be the ring of integers of K, and let $\mathfrak{p} \in R$ be a prime ideal with norm $N(\mathfrak{p}) = q$, where $q = p^r$ with p a prime and $r \geq 1$. We denote by $k_\mathfrak{p}$ the residue field of K at $\mathfrak{p}$.

Let E be an elliptic curve defined over the finite field $k_\mathfrak{p}$. It is clear that $E(k_\mathfrak{p})$ has finite order. This follows since the number of the pairs (x, y) with $x, y \in k_\mathfrak{p}$ is finite.

One of the most important quantities that we associate to the elliptic curve E is the cardinality of the group $E(k_\mathfrak{p})$. That is, its number of rational points. Hasse provides a bound for the number of rational points of $E/k_\mathfrak{p}$. Moreover,

Theorem 2.12 (Hasse)**.** *([32], Chapter 5, Theorem 1.1) Let E be an elliptic curve defined over a finite field $k_\mathfrak{p}$. Then,*

$$|\#E(k_\mathfrak{p}) - q - 1| \leq 2\sqrt{q}.$$

Set $a_\mathfrak{p}(E) := \#E(k_\mathfrak{p}) - q - 1$. $a_\mathfrak{p}(E)$ is called the trace of Frobenius. By Hasse's theorem $-2\sqrt{q} \leq a_\mathfrak{p}(E) \leq 2\sqrt{q}$.

Let E be an elliptic curve defined over K. We denote the reduction of E modulo $\mathfrak{p}$ by $\widetilde{E}/k_\mathfrak{p}$. The rational curve $\widetilde{E}/k_\mathfrak{p}$ will be an elliptic curve provided there are no singular points. That is $\widetilde{E}/k_\mathfrak{p}$ is an elliptic curve if and only if $\Delta(E) \not\equiv 0 \pmod{\mathfrak{p}}$.

Definition 2.13. *Let E be an elliptic curve defined over a number field K. A Weierstrass equation for E is called a minimal Weierstrass equation for E at prime $\mathfrak{p}$ if the valuation of the discriminant $\Delta(E)$ at the prime $\mathfrak{p}$ is minimal.*

All primes that divide the minimal discriminant $\Delta(E)$ are called bad primes of E, otherwise E is said to have good reduction. Note that, there are finitely many bad primes $\mathfrak{p}$.

We give a classification for the reduction $\widetilde{E}$ of E over a finite field $k_\mathfrak{p}$ depending on the reduction modulo $\mathfrak{p}$.

Let $\operatorname{char} k_\mathfrak{p} \neq 2, 3$ and let $\widetilde{E} : y^2 = x^3 + \widetilde{A}x + \widetilde{B}$ with $\widetilde{A}, \widetilde{B} \in k_\mathfrak{p}$.

(a) If $\widetilde{E}$ is non-singular then it is an elliptic curve. In this case, we say E has *good reduction* at the prime $\mathfrak{p}$.

(b) If $\widetilde{E}$ has a node then E has *bad multiplicative reduction* at the prime $\mathfrak{p}$.

(c) If $\widetilde{E}$ has a cusp then E has *bad additive reduction* at the prime $\mathfrak{p}$.

There are two types of bad multiplicative reduction, split and non-split. If the slopes of the tangent lines at the node belong to $k_\mathfrak{p}$ then we say E has *split reduction*, otherwise it is said to have *non-split reduction*.

Moreover, the order of $\widetilde{E}(k_\mathfrak{p})$, where $\mathfrak{p}$ is a bad prime is, [[32],Chapter 3, Exercise 3.5]:

$$\#\widetilde{E}(k_\mathfrak{p}) = \begin{cases} q, & \text{if E has split multiplicative reduction} \mod \mathfrak{p} \\ q+2, & \text{if E has non-split multiplicative reduction} \mod \mathfrak{p} \\ q+1, & \text{if E has additive reduction} \mod \mathfrak{p} \end{cases}$$

Let $E/k_\mathfrak{p}$ be an elliptic curve. It is clear that all points on $E/k_\mathfrak{p}$ are torsion points. Furthermore,

Proposition 2.14. *[[32], Chapter 8, Proposition 3.1, Application 3.2] Let E/K be an elliptic curve defined over a number field K. Let $n \geq 1$ be an integer that is relatively prime to* $\operatorname{char} k_\mathfrak{p}$. *Assume that the reduction $\widetilde{E}/k_\mathfrak{p}$ is nonsingular. Then the reduction map*

$$E(K)[n] \to \widetilde{E}(k_\mathfrak{p})$$

is injective. $E(K)[n]$ is the set of all points of order n in $E(K)$.

This proposition helps us analyse all torsion points of $E(K)$. It also provides a method for finding the torsion subgroup of E.

Example 2.15. *Let $E : y^2 + y = x^3 - x + 1$ be an elliptic curve defined over $\mathbb{Q}$, The minimal discriminant is $\Delta(E) = -13 \cdot 47$. $\widetilde{E}/\mathbb{F}_p$ is an elliptic curve for $p \neq 13, 47$. That is, $\widetilde{E}/\mathbb{F}_2$ is an elliptic curve since $2 \not| \Delta(E)$. Then it follows that $\widetilde{E}(\mathbb{F}_2) = \{\mathcal{O}\}$. By Proposition 2.14,*

$$E(\mathbb{Q})[n] \to \widetilde{E}(\mathbb{F}_2) = \{\mathcal{O}\}$$

as long as $\gcd(2, n) = 1$. *Also, $E(\mathbb{Q})[2] = \{\mathcal{O}\}$. Therefore, $E(\mathbb{Q})_{tors} = \{\mathcal{O}\}$.*

The following then describes the group structure of an elliptic curve $E/k_\mathfrak{p}$.

Theorem 2.16. *Let $E/k_\mathfrak{p}$ be an elliptic curve. Then $E(k_\mathfrak{p})$ is isomorphic to one of the following:*

$$\mathbb{Z}/m\mathbb{Z},$$

$$\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \text{ with } m|n.$$

2.3 Isogeny

We saw that elliptic curves own a group structure with respect to addition. One important point of elliptic curves is the point at infinity $\mathcal{O}$, the zero element of the group $E(K)$. So, for a further study of the structure of the group we are interested in maps that preserve the group law together with the point at infinity.

Definition 2.17. *Let E_1 and E_2 be two elliptic curves defined over a number field K. A non-zero morphism Φ from E_1 to E_2 such that $\Phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$ is called an isogeny.*

The sum of two isogenies ϕ and ρ is defined as follows,

$$(\phi + \rho)(P) = \phi(P) + \rho(P).$$

The multiplication of two isogenies ϕ and ρ is their composition,

$$(\phi\rho)(P) = \phi(\rho(P)).$$

The isogenies between elliptic curves form groups. We denote two of the corresponding groups of isogenies of E as follows,

(a) $\mathrm{Hom}(E_1, E_2) = \{isogenies \;\; E_1 \to E_2\}$ is a group with respect to addition. The group $\mathrm{Hom}(E_1, E_2)$ is called the homomorphism group of E.

(b) $\mathrm{End}(E) = \mathrm{Hom}(E, E)$ is a ring with respect to addition and composition. The ring $\mathrm{End}(E)$ is called the endomorphism ring of E.

Moreover, the following theorem says that all isogenies are homomorphisms.

Theorem 2.18. *Let $\phi : E_1 \to E_2$ be an isogeny. Then*

$$\phi(P + Q) = \phi(P) + \phi(Q)$$

for all $P, Q \in E$.

Let $\tau_P : E \to E$ be a translation map defined as $\tau_P(Q) = Q + P$ and $\psi : E \to E$ be a morphism. Then $\phi = \tau_{-\psi(\mathcal{O})} \circ \psi$ is an isogeny since $\phi(\mathcal{O}) = \mathcal{O}$.

Theorem 2.19. *Any morphism $\psi : E \to E$ is a composition of an isogeny and translation map*

$$\psi = \tau_{\psi(\mathcal{O})} \circ \phi.$$

Isogenies provide a strong relation between two elliptic curves that are defined over a finite field.

Theorem 2.20. *[[32], Chapter 5, Exercise 5.4] Let E_1 and E_2 be elliptic curves defined over $\mathbb{F}_p$. If E_1 and E_2 are isogenous over $\mathbb{F}_p$ then*

$$\#E_1(\mathbb{F}_p) = \#E_2(\mathbb{F}_p).$$

3. Order of reductions of elliptic curves for primes of good reduction

Let E be an elliptic curve defined over a number field K with ring of integers R, $\mathfrak{p}$ be a prime ideal in R and, $k_{\mathfrak{p}}$ be the residue field of K at $\mathfrak{p}$. Recall that $a_{\mathfrak{p}}(E)$ is the trace of Frobenius of E at $\mathfrak{p}$. By Hasse's theorem we have, $-2\sqrt{q} \leq a_{\mathfrak{p}}(E) \leq 2\sqrt{q}$, where $N(\mathfrak{p}) = q = p^r$, p is a prime and $r \geq 1$.

Theorem 3.1. *([34]) Let $k_{\mathfrak{p}}$ be a finite field. All the possible orders of $E(k_{\mathfrak{p}})$ are given by, $\#E(k_{\mathfrak{p}}) = 1 + q - a_{\mathfrak{p}}(E)$, with $q = p^r, r \geq 1$ and $a_{\mathfrak{p}}(E)$ is an integer with $|a_{\mathfrak{p}}(E)| \leq 2\sqrt{q}$ satisfying one of the following conditions:*

(a) $(a_{\mathfrak{p}}(E), p) = 1$

(b) If r is even: $a_{\mathfrak{p}}(E) = \pm 2\sqrt{q}$

(c) If r is even and $p \not\equiv 1 \mod 3$: $a_{\mathfrak{p}}(E) = \pm\sqrt{q}$

(d) If r is odd and $p = 2$ or 3: $a_{\mathfrak{p}}(E) = \pm p^{(n+1)/2}$

(e) If either r is odd or r is even, and $p \equiv 1 \mod 4$: $a_{\mathfrak{p}}(E) = 0$

By Theorem 3.1, we have that, if we fix a finite field $k_{\mathfrak{p}}$ then we have necessary and sufficient conditions under which an element in the interval $[-2\sqrt{q}, 2\sqrt{q}]$ is the trace of Frobenius for an elliptic curve E defined over $k_{\mathfrak{p}}$.

Now, one could ask:

Question 3.2. *Given an elliptic curve $E : y^2 = x^3 + Ax + B$ defined over a number field K and an integer n, are there infinitely many primes $\mathfrak{p}$ such that $a_{\mathfrak{p}}(E) = n$?*

Remark 3.3. *Recall* $\mathrm{End}(E)$ *the endomorphism ring of the elliptic curve E. If* $\mathrm{End}(E)$ *does not equal $\mathbb{Z}$, then we say that E has complex multiplication.*

If an elliptic curve over $\mathbb{Q}$ has complex multiplication then $a_p(E) = 0$ for half of primes p, [6]. Let E be an elliptic curve defined over the rationals with no complex multiplication, Elkies in [25], showed that $a_p(E) = 0$ for infinitely many primes p. Also, in [26], he expanded his result to any elliptic curve E over any real number

field.

Now, can we find an elliptic curve E defined over a number field K such that $a_{\mathfrak{p}}(E) = n$, where n is a nonzero integer, for infinitely many primes $\mathfrak{p}$?

For elliptic curves defined over $\mathbb{Q}$ with complex multiplication by an imaginary quadratic field L of class number 1, in [15], Ji and Chin showed that for specific nonzero integer n, $a_p(E) = n$ is satisfied if and only if $p = ax^2 + bx + c$ for some $a, b, c \in \mathbb{Z}$. Therefore, if the following conjecture of Hardy and Littlewood on primes being represented by quadratic polynomials, holds true, then the answer to Question 3.2 for these curves is affirmative.

Conjecture 3.4. *(Hardy-Littlewood conjecture)([11]) Let a,b and c be integers such that $gcd(a,b,c) = 1$. Assume that $a+b$ and c are not both even, and that $D = b^2 - 4ac$ is not a square. There are infinitely many primes of the form $at^2 + bt + c$.*

Example 3.5. *[15] Let $E : y^2 = x^3 + x$ be an elliptic curve defined over $\mathbb{Q}$. For some $t \in \mathbb{Z}$ and a prime p,*

$$a_p(E) = 2 \text{ if and only if } p = t^2 + 1$$

In particular, there are infinitely many primes p of the form $t^2 + 1$ if and only if $a_p(E) = 2$ for infinitely many primes.

We choose a different approach to this question. Instead of dealing with the exact value of $a_{\mathfrak{p}}(E)$, we investigate the congruence classes of $a_{\mathfrak{p}}(E)$.

Since there is a linear relation between $a_{\mathfrak{p}}(E)$ and $\#E(k_{\mathfrak{p}})$, we start by looking at the congruence classes of $\#E(k_{\mathfrak{p}})$. Mainly, if we fix an integer, say m, and a congruence class $\beta \mod m$ does there exist an elliptic curve E/K such that

$$\#\widetilde{E}(k_{\mathfrak{p}}) \equiv \beta \mod m$$

for infinitely many primes p? If so, what is the density of such primes?

By density of primes we mean,

Definition 3.6. *Let $\mathcal{P}$ be the set of prime ideals $\mathfrak{p} \in R$, and let $\mathcal{S} \subseteq \mathcal{P}$. The density of $\mathcal{S}$ is*

$$\delta(\mathcal{S}) = \lim_{x \to \infty} \frac{\#\{\mathfrak{p} \in \mathcal{S} : N(\mathfrak{p}) \leq x\}}{\#\{\mathfrak{p} \in \mathcal{P} : N(\mathfrak{p}) \leq x\}}$$

Moreover, it is valid to ask the following question,

Question 3.7. *Let $m \geq 2$ and β a non-negative integer. Does there exist an elliptic*

curve E defined over a number field K such that $\#\widetilde{E}(k_{\mathfrak{p}}) \equiv \beta \mod m$ for almost all primes $\mathfrak{p}$?

We recall a result of Serre on the congruence classes of the reduction group of an elliptic curve E defined over a number field K modulo a positive integer m. The following was proved by Serre for elliptic curves over $\mathbb{Q}$ in [[29], Proposition 2.2].

Theorem 3.8. *([12], Theorem 2.3) Let $m, \beta \in \mathbb{Z}$ and $m > 1$. Given an elliptic curve E defined over a number field K the following two conditions are equivalent:*

(a) $\#\tilde{E}(k_{\mathfrak{p}}) \equiv \beta \mod m$ for almost all primes $\mathfrak{p} \in R$.

(b) $1 + det(\sigma) - Tr(\sigma) \equiv \beta \mod m$ for all $\sigma \in G(E,m)$, where $G(E,m) \subset GL(2,\mathbb{Z}/m\mathbb{Z})$ is the subgroup defined by the action of the absolute Galois group $Gal(\overline{K}/K)$ on $E[m]$, the set of m-torsion points of E.

Corollary 3.9. *If there exists an elliptic curve E defined over a number field K satisfying the conditions in Theorem 3.8, then $m|\beta$.*

Proof. By applying $\sigma = I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ in Theorem 3.8, we have that $m|\beta$. □

Let $m > 1$ and β a non-negative integer, let E be an elliptic curve defined over a number field K. According to Theorem 3.8 and Corollary 3.9, if $\#\widetilde{E}(k_{\mathfrak{p}}) \equiv \beta \mod m$ for almost all primes $\mathfrak{p}$, then $\beta \equiv 0 \mod m$.

Now, we ask what the possible values of such an m are. To do so, we recall a result of Katz.

Theorem 3.10. *([16], Theorem 2) Let E be an elliptic curve over number a field K, and $m \geq 2$ an integer. For each prime $\mathfrak{p}$ of K at which E has good reduction let $\#\tilde{E}(k_{\mathfrak{p}}) \equiv 0 \mod m$ for almost all primes $\mathfrak{p}$, then there exists a K-isogenous elliptic curve E' over K for which $\#E'(K)_{tors} \equiv 0 \mod m$.*

Remark 3.11. *Let E_1 and E_2 be elliptic curves defined over a number field K. If E_1 and E_2 are isogenous over K it follows that they have the same primes of good reduction and bad reduction, [[33], Chapter 4, Exercise 4.40]*

Theorem 3.12. *Let E be an elliptic curve defind over a number field K. One has $\#\tilde{E}(k_{\mathfrak{p}}) \equiv \beta \mod m$ for almost all primes $\mathfrak{p}$ if and only if E is K-isogenous to an elliptic curve E', where $\#E'(K)_{tors} \equiv \beta \mod m$ and in that case $\beta \equiv 0 \mod m$.*

Proof. Let E be an elliptic curve defind over a number field K such that $\#\tilde{E}(k_{\mathfrak{p}}) \equiv \beta \mod m$ for almost all primes $\mathfrak{p}$ then it follows by Theorem 3.8 and Corollary 3.9,

that $\beta \equiv 0 \mod m$. Then by Theorem 3.10 there exists an elliptic curve E' is K-isogenous to E and $\#E'(K)_{tors} \equiv \beta \mod m$.

Conversely, let E' be an elliptic curve K-isogenous to E and $\#E'(K)_{tors} \equiv \beta \mod m$, where $\beta \equiv 0 \mod m$. Proposition 2.14 implies that, $E'(K)_{tors}$ is embedded in $E'(k_{\mathfrak{p}})$. Hence, $\#\tilde{E}(k_{\mathfrak{p}}) \equiv \beta \mod m$. □

Recall Merel's Theorems,

Theorem 3.13. *([22], Theorem 1) For every integer $d \geq 1$, there is a constant $N(d)$ such that for all number fields K with $[K : \mathbb{Q}] = d$ and all elliptic curves E/K,*

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

Theorem 3.14. *([22], Theorem 2) Let E be an elliptic curve over a number field K such that $[K : \mathbb{Q}] = d$ where $d > 1$. Let p be a prime number. If $E(K)$ has a p torsion point then $p < d^{3d^2}$.*

This bound was improved by Oesterle in [27], to be $(3^{d/2} + 1)^2$

Theorem 3.15. *Let E be an elliptic curve over a number field K such that $[K : \mathbb{Q}] = d$ where $d > 1$. Assume that E satisfies $\#\tilde{E}(k_{\mathfrak{p}}) \equiv \beta \pmod m$ for almost all primes p. Then*

(a) $\beta \equiv 0 \mod m$,

(b) there is a constant $B(d)$ such that $|m| < B(d)$,

(c) if a prime p divides m, then $p < (3^{d/2} + 1)^2$.

Proof. The proof of (a) follows by Theorem 3.8 and Corollary 3.9.

The proof of (b) it follows by Theorem 3.12 and Theorem 3.13.

The proof of (c) follows by Theorem 3.12 and Theorem 3.14 together with the improved bound on the prime p given by Oesterle in [27]. □

Moreover, in the following theorem we describe the list of the values of m when K is of degree at most 3, or K is Galois of degree 4.

Let $\mathcal{S}_d = \{m : \text{there is an elliptic curve } E/K, \text{ where } [K : \mathbb{Q}] = d \text{ and } m | \#E(K)_{tors}\}$.

Theorem 3.16. *Let $m \geq 2$ be an integer and K be a number field with $[K : \mathbb{Q}] = d$. Then there exists an elliptic curve E defined over K such that $\#\widetilde{E}(k_{\mathfrak{p}}) \equiv 0 \mod m$ for all primes of good reduction if and only if $m \in \mathcal{S}_d$ where,*

(a) $\mathcal{S}_1 = \{2,3,4,5,6,7,8,9,10,12,14,16\}$, *if* $K = \mathbb{Q}$,

(b) $\mathcal{S}_2 = \{2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,18,20,24\}$, *if* K *is a quadratic field,*

(c) $\mathcal{S}_3 = \{2,3,4,5,6,7,8,9,10,11,12,13,15,18,20,21,24,28\}$, *if* K *is a cubic field,*

(d) $\mathcal{S}_4 = \{2,3,4,5,6,7,8,9,10,12,13,15,20,21,22,24,25,32,36\}$, *if* K *is a quartic Galois field.*

Proof. Proof of (b). Suppose that there exists an elliptic curve E defined over a quadratic number field K such that $\#\widetilde{E}(k_{\mathfrak{p}}) \equiv 0 \mod m$. Then by Theorem 3.15, we have that the possible values for m are finite. Therefore, by Theorem 2.9 $m \in \{2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,18,20,24\}$.

Conversely, let $m \in \mathcal{S}_2$ where $2 = [K : \mathbb{Q}]$. Then by the Theorem 2.9 each of the above integers divides the order of the torsion subgroup $E(K)_{tors}$ of an elliptic curve E. By Proposition 2.14, $E(K)_{tors}$ is embedded in $\widetilde{E}(k_{\mathfrak{p}})$ for for almost all primes $\mathfrak{p}$. This implies that $\#\widetilde{E}(k_{\mathfrak{p}}) \equiv 0 \mod m$ for almost all primes $\mathfrak{p}$.

Proof of (a), (c) and (d) are similar. □

Remark 3.17. *Let* $f(x) = ax + b$ *with* $gcd(a,b) = 1$. *Dirichlet's theorem in arithmetic progression states that there are infinitely many primes represented by* $f(x)$. *That is for infinitely many primes* p *there is* $n_p \in \mathbb{Z}$ *such that* $f(n_p) = p$. *Moreover, the density of such primes is* $\frac{1}{\varphi(b)}$. *Can we put together a similar question in the case of elliptic curves?*

As a consequence of Theorem 3.12 and Theorem 3.16 we have the following result,

Corollary 3.18. *Let* $f(x) = mx + b$ *with* $m, b \in \mathbb{Z}$. *Let* $m > 1$ *be a positive integer. Let* E *be an elliptic curve defined over a number field* K *and* $[K : \mathbb{Q}] = d$. *The following are equivalent:*

(a) $\#\widetilde{E}(k_{\mathfrak{p}}) = f(x_{\mathfrak{p}})$ *for some* $x_{\mathfrak{p}} \in \mathbb{Z}$ *for almost all primes* $\mathfrak{p}$.

(b) E *is* K*-isogenous to an elliptic curve with non-trivial torsion over* K.

In the latter case; $b = 0$ *and* m *belongs to a finite set of integers* $\mathcal{S}_d$ *whose size depends on* $d = [K : \mathbb{Q}]$.

Proof. The proof follows by Theorem 3.12 and Theorem 3.16. □

If E/K is an elliptic curve defined over a number field K such that $\#\widetilde{E}(k_{\mathfrak{p}}) \equiv 0 \mod m$, then E is K-isogenous to an elliptic curve E' with a nontrivial torsion. We may ask what is $E(K)_{tors}$?

Theorem 3.19. *([32], Chapter 6, Corollary 6.2) Any elliptic curve E defined over a number field K is K-isogenous to finitely many elliptic curves defined over K.*

In [1], the classification of all pairs $(E(\mathbb{Q})_{tors}, E'(\mathbb{Q})_{tors})$ where E and E' are $\mathbb{Q}$-isogenous was done. Therefore, we can give an answer to the above question over $\mathbb{Q}$.

Example 3.20. *Let E be an elliptic curve defined over the rational field $\mathbb{Q}$ such that $\#\widetilde{E}(\mathbb{F}_p) \equiv 0 \mod 5$ for all primes p of good reduction. Then by Theorem 3.10 there exists an elliptic curve E' such that E' is $\mathbb{Q}$-isogenous to E and $\#E'(\mathbb{Q})_{tors} \equiv 0 \mod 5$. So, by Theorem 2.8 on torsion subgroups of an elliptic curve over $\mathbb{Q}$, it follows that $E'(\mathbb{Q})_{tors} \cong \mathbb{Z}/5\mathbb{Z}$ or $\mathbb{Z}/10\mathbb{Z}$. Then by Table 1 and Table 3 in [1], $E'(\mathbb{Q})_{tors} \cong \mathbb{Z}/5\mathbb{Z}$ implies $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/1\mathbb{Z}$ or $\mathbb{Z}/5\mathbb{Z}$. Also, if $E'(\mathbb{Q})_{tors} \cong \mathbb{Z}/10\mathbb{Z}$ then $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/10\mathbb{Z}$. So, the possibilities for $E(\mathbb{Q})$ are $\mathbb{Z}/1\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$ and $\mathbb{Z}/10\mathbb{Z}$.*

We may ask the following question,

Question 3.21. *Does there exists an integer, say n, such that $a_{\mathfrak{p}}(E) \neq n$?*

Observation. Let $E: y^2 + y = x^3 + x^2 + x$ with $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/3\mathbb{Z}$. Using Magma we calculate the value of $a_p(E)$ for $p \leq 500$,

[0, 3, -1, 3, -4, -3, 0, 6, -4, 2, -6, -1, -3, 12, -6, -1, -4, 6, -7, 8, 12, 12, 8, 6, 14, -18, -16, 6, 2, -15,-3, -13, 21, -10, 14, 20, -18, -18, -18, 2, 3, -4, 18, 11, 14, -10, 12, 5, -21, 15, -10, 21, 0, 9, 24, -16, -19, 6, -13, -12, 20, -3, -10, 6, -28, 32, 21, 17, -6, 15, 8, -4, -34, 12, 15, -7, 12, -4, -12,8, -24, 2, -10, -3, 0,-37, 9, -31, -27, -12, 2, 12, 5]

We notice that $a_p(E) \mod 3$ does not equal 1 in the range above. More precisely, the list above $\mod 3$ is

[0, 0, 2, 0, 2, 0, 0, 0, 2, 2, 0, 2, 0, 0, 0, 2, 2, 0, 2, 2, 0, 0, 2, 0, 2, 0, 2, 0, 2, 0, 0, 2, 0, 2, 2, 2, 0, 0, 0, 2, 0, 2, 0, 2, 2, 2, 0, 2, 0, 0, 2, 0, 0, 0, 0, 2, 2, 0, 2, 0, 2, 0, 2, 0, 2, 2, 0, 2, 0, 0, 2, 2, 0, 0, 2, 0, 2, 0, 2, 0, 2, 2, 0, 0, 2, 0, 2, 0, 0, 2, 0, 2]

Then we conclude the following:

Corollary 3.22. *Let E be an elliptic curve defined over a number field K with $\#E(K)_{tors} = m$. Then $a_{\mathfrak{p}}(E) \not\equiv 1 \mod m$ for almost all primes $\mathfrak{p}$ with $p \nmid m$, where $N(\mathfrak{p}) = p^r, r \geq 1$.*

Proof. Recall that $\#\widetilde{E}(k_\mathfrak{p}) = 1 + N(\mathfrak{p}) - a_\mathfrak{p}(E)$, where $N(\mathfrak{p}) = p^r, r \geq 1$. Then $a_\mathfrak{p}(E) \equiv p^r + 1 \mod m$. Since $gcd(p, m) = 1$, we have that $a_\mathfrak{p}(E) \not\equiv 1 \mod m$. □

Similarly,

Corollary 3.23. *Let E be an elliptic curve defined over a number field K. Let $\#E(K)_{tors} = 2k$ for some k. Then $a_\mathfrak{p}(E)$ is even for almost all primes $\mathfrak{p}$.*

Proof. We have that $\#\widetilde{E}(k_\mathfrak{p}) = 1 + N(\mathfrak{p}) - a_\mathfrak{p}(E)$, where $N(\mathfrak{p}) = p^r, r \geq 1$. Then $a_\mathfrak{p}(E) \equiv p^r + 1 \mod 2k$. Since $(p, 2k) = 1$ for $p \neq 2$, we have that $a_\mathfrak{p}(E)$ is even for almost all primes. □

Now, let E be an elliptic curve defined over a number field K and fix an integer $m > 1$. Assume that E and m are not given as in Theorem 3.16. That is either E is not K- isogenous to an elliptic curve E' with nontrivial torsion or m is not a divisor of the order of $E'(K)_{tors}$. Then according to Theorem 3.8, Corollary 3.9 and Theorem 3.10, there exist at least two possible congruence classes $\beta_1, \beta_2 \mod m$ such that $\#\widetilde{E}(k_\mathfrak{p}) \equiv \beta_i \mod m$ for primes of density δ_i, where $0 < \delta_i < 1$.

We summarize all of this in the following theorem,

Theorem 3.24. *Let E be an elliptic curve over a number field K and $m > 1$ an integer. Assume that either E is not K-isogenous to an elliptic curve with nontrivial torsion or m is not a divisor of the order of the torsion subgroup of any K-isogenous elliptic curve to E.*

There are at least two possible values $\beta_i \mod m$ such that $\#\widetilde{E}(k_\mathfrak{p}) \equiv \beta_i \mod m$ for primes $\mathfrak{p}$ of positive density.

Example 3.25. *([4]) Let $E : y^2 = x^3 - 12x - 11$ be an elliptic curve defined over $\mathbb{Q}$. E is $\mathbb{Q}$-isogenous to an elliptic curve with torsion $\mathbb{Z}/6\mathbb{Z}$.*

$$\#\widetilde{E}(\mathbb{F}_p) = \begin{cases} 0 \mod 12 & \text{if} \quad p \equiv 1, 9, 11, 13, 17, 19 \mod 20 \\ 6 \mod 12 & \text{if} \quad p \equiv 3, 7 \mod 20 \end{cases}$$

3.1 Order of reductions of elliptic curves for all primes

Definition 3.26. *Let K be a number field and R be the ring of integers of K. Let E be an elliptic curve defined over K. We say that E has good reduction everywhere if E has good reduction at every prime $\mathfrak{p} \in R$.*

There is no elliptic curve E defined over the rational field $\mathbb{Q}$ that has everywhere good reduction, [[32], Chapter 8, Exercise 8.15]. However, this is not the case when we work over the finite extensions of $\mathbb{Q}$.

Example 3.27. *Let be an elliptic curve defined over $K = \mathbb{Q}(\sqrt{6})$ by*

$$E : y^2 + \frac{3(-5-2\sqrt{6})+31}{2}xy + (-5+2\sqrt{6})^2 y = x^3$$

The elliptic curve has discriminant $\Delta(E) = -186298002\sqrt{6} + 456335045$. The norm of the discriminant is, $N(\Delta(E)) = 1$. Therefore, it has everywhere good reduction over K

That is, if an elliptic curve E defined over a number field K has everywhere good reduction and $m|\#E(K)_{tors}$, then it is easy to see that, $\#\widetilde{E}(k_{\mathfrak{p}}) \equiv 0 \mod m$ for all primes $\mathfrak{p}$. In the previous section we were interested in elliptic curves E defined over number field K such that $\#\widetilde{E}(k_{\mathfrak{p}}) \equiv 0 \mod m$ for allmost all primes. In what follows, we will investigate elliptic curves E over K with $\#\widetilde{E}(k_{\mathfrak{p}}) \equiv 0 \mod m$ for all primes $\mathfrak{p}$ and some integer m.

In this case, another question arises,

Question 3.28. *Let K be a number field. Does there exist an elliptic curve E defined over a number field K such that $\#\widetilde{E}(k_{\mathfrak{p}}) \equiv 0 \mod m$ for all primes $\mathfrak{p}$?*

Recall that,

$\mathcal{S}_d = \{m : \text{there is an elliptic curve } E/K, \text{ where } [K:\mathbb{Q}] = d \text{ and } m|\#E(K)_{tors}\}$, see Theorem 3.16.

Theorem 3.29. *Let K be a number field with $[K:\mathbb{Q}] = d$. Let $m > 1$ be an integer, and let $\mathfrak{p} \in R$ a prime ideal with norm $N(\mathfrak{p}) = q, q = p^r, r \geq 1$, p is a prime. There exists an elliptic curve E defined over K such that $\#\widetilde{E}(k_{\mathfrak{p}}) \equiv 0 \mod m$ for all primes*

$\mathfrak{p}$ *if and only if* $m \in \mathcal{S}_d$ *and* $m|m_{\mathfrak{p}}$*,where*

$$m_{\mathfrak{p}} = \begin{cases} q, & \text{if } E \text{ has split multiplicative reduction} \mod \mathfrak{p} \\ q+2, & \text{if } E \text{ has non-split multiplicative reduction} \mod \mathfrak{p} \\ q+1, & \text{if } E \text{ has additive reduction} \mod \mathfrak{p} \end{cases}$$

In particular, $m \leq 5$ *over* $\mathbb{Q}$*.*

Proof. Let K be a number field. Suppose that there exists an elliptic curve E defined over K such that $\#\widetilde{E}(k_{\mathfrak{p}}) \equiv 0 \mod m$ for all primes $\mathfrak{p}$. Then by Theorem 3.16 it follows that $m \in \mathcal{S}_d$ and since $m|\#\widetilde{E}(k_{\mathfrak{p}})$ for all primes $\mathfrak{p}$ it follows $m|m_{\mathfrak{p}}$.

Conversely, let $m \in \mathcal{S}_d$ and $m|m_{\mathfrak{p}}$. Then together with Theorem 3.16 we have that there exists an elliptic curve such that $\#\widetilde{E}(k_{\mathfrak{p}}) \equiv 0 \mod m$ for all primes $\mathfrak{p}$.

In particular over $\mathbb{Q}$, if we have good reduction at prime 2 when we apply Hasse bound we have, $|\#\widetilde{E}(\mathbb{F}_2)| \leq 5$. Moreover, if we have bad reduction at the prime 2 than $m_p = 2, 3$ or 4. Thus, $m \leq 5$ over $\mathbb{Q}$. □

Example 3.30. *The elliptic curve* $E : y^2 + xy + y = x^3 - x^2 - 199x + 510$ *has even reduction for every prime* p*.*

We have, $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/4\mathbb{Z}$*. Using Magma we calculate the bad primes of* E*. The only bad prime is* 17*.* E *has additive reduction at* $p = 17$*, then* $m_p = 18$*. Therefore, by Theorem 3.29 reduction of* E *is even for every prime* p*.*

Example 3.31. *The reduction of elliptic curve* $E : y^2 = x^3 + x^2 - 333x - 3537$ *is divisible by* 3 *for every prime* p*.*

The torsion subgroup of E *is* $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/3\mathbb{Z}$*. Using Magma we calculate the bad primes of* E*. The bad primes of* E *are* 2*,* 3 *and* 5*.* E *had additive reduction at both primes* 2 *and* 5*, and split multiplicative reduction at prime* 3*. Then,* $m_2 = 3$*,* $m_3 = 3$ *and* $m_5 = 6$*. Therefore, by Theorem 3.29 it follows that* $\#\widetilde{E}(\mathbb{F}_p) \equiv 0 \mod 3$ *for all primes* p*.*

Example 3.32. *The elliptic curve* $E : y^2 + xy = x^3 - x^2 - 1773x - 5270$ *satisfies* $\#\widetilde{E}(\mathbb{F}_p) \equiv 0 \mod 4$ *for every prime* p*.*

The torsion subgroup of E *is* $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$*. Using Magma we calculate the bad primes of* E*. The bad primes of* E *are* 3 *and* 7*.* E *had additive reduction at both primes* 3 *and* 7*. Then,* $m_3 = 4$*,* $m_7 = 8$*. Therefore, by Theorem 3.29 it follows that* $\#\widetilde{E}(\mathbb{F}_p) \equiv 0 \mod 4$ *for all primes* p*.*

Example 3.33. *Let E be an elliptic curve over $K = \mathbb{Q}(\sqrt{33})$ by*

$$E : y^2 = x^3 + 96(-32^3 - 1728)u^2x - 2(-32^3 - 1728)^2u^3$$

with $u = -462 - 84\sqrt{33}$. The torsion subgroup of E is, $E(K)_{tors} \cong \mathbb{Z}/3\mathbb{Z}$. Moreover, E has good reduction everywhere. Hence, $\#\widetilde{E}(k_{\mathfrak{p}}) \equiv 0 \mod 3$ for every prime ideal $\mathfrak{p}$.

Example 3.34. *Let E be an elliptic curve defined over $K = \mathbb{Q}(\sqrt{33})$ by*

$$E : y^2 = x^3 + (28296\sqrt{33} - 162675)x + 35441118 - 6168312\sqrt{33}.$$

E has torsion subgroup, $E(K)_{tors} \cong \mathbb{Z}/18\mathbb{Z}$. The bad places of E are at the prime ideals $(-1/2\sqrt{33} + 5/2)$ and $(-1/2\sqrt{33} - 5/2)$. E has bad split multiplicative reduction at prime ideal $(-1/2\sqrt{33} + 5/2)$ and $(-1/2\sqrt{33} - 5/2)$, respectively. Norm of these ideals is $N(-1/2\sqrt{33} + 5/2) = N(-1/2\sqrt{33} - 5/2) = 2$.

Thus, $m_{\mathfrak{p}_i} = 2$ for $\mathfrak{p}_1 = (-1/2\sqrt{33} + 5/2)$ and $\mathfrak{p}_2 = (-1/2\sqrt{33} - 5/2)$. Hence, by Theorem 3.29, $\#\widetilde{E}(k_{\mathfrak{p}}) \equiv 0 \mod 2$ for every prime ideal $\mathfrak{p}$.

Example 3.35. *Let E be an elliptic curve defined over $K = \mathbb{Q}(\sqrt{6})$ by*

$$E : y^2 + \frac{3(-5 - 2\sqrt{6}) + 31}{2}xy + (-5 + 2\sqrt{6})^2y = x^3.$$

$E(K)_{tors} \cong \mathbb{Z}/6\mathbb{Z}$ and E has good reduction everywhere. Then it follows $\#\widetilde{E}(k_{\mathfrak{p}}) \equiv 0 \mod 6$ for every prime $\mathfrak{p}$.

To investigate the primes of bad reduction for an elliptic curve E we associate to E a quantity called the conductor of E. We denote the conductor of E by N_E.

$$N_E = \prod_{p \text{ prime}} p^{\delta_{\mathfrak{p}}}$$

The conductor exponent $\delta_{\mathfrak{p}}$ is given as follows,

$$\delta_{\mathfrak{p}} = \begin{cases} 0 & \text{if E is nonsingular,} \\ 1 & \text{if E has bad multiplicative reduction at } p, \\ 2 & \text{if E has bad additive reduction and } p \neq 2, 3, \\ \geq 2 & \text{if E has additive reduction and } p = 2, 3 \end{cases}$$

for δ_2 and δ_3 refer to [[32], Chapter 10].

Corollary 3.36. *All elliptic curves E with conductor 7^2 and 17^2, with a rational point of order 2, have even reduction for all primes p.*

Proof. In [Table 1, [3]] the elliptic curves E with conductor 7^2 have bad additive reduction at the prime 7, and the elliptic curves with conductor 17^2 have bad additive reduction at the prime 17. Then $m_7 = 8$, $m_{17} = 18$, respectively. Together with the fact that they posses a rational point of order 2, Theorem 3.29 implies that these elliptic curves have even reduction for all primes p. □

Moreover, there are exactly four such elliptic curves with conductor 7^2, four elliptic curves with conductor 17^2. Cremona's table, [[3], Table 1] gives the isogeny class of these elliptic curves together with their conductor. In particular, the list of all elliptic curves in Corollary 3.36 of conductor 7^2 are

$$y^2 + xy = x^3 - x^2 - 2x - 1,$$

$$y^2 + xy = x^3 - x^2 - 37x - 78,$$

$$y^2 + xy = x^3 - x^2 - 107x + 552,$$

$$y^2 + xy = x^3 - x^2 - 1822x + 30393,$$

whereas the list of elliptic curves in Corollary 3.36 with conductor 17^2 are:

$$y^2 + xy + y = x^3 - x^2 - 199x + 510,$$

$$y^2 + xy + y = x^3 - x^2 - 1644x - 24922,$$

$$y^2 + xy + y = x^3 - x^2 - 26209x - 1626560,$$

$$y^2 + xy + y = x^3 - x^2 - 199x - 68272.$$

Example 3.37. *([7]) Consider the set of all elliptic curves E defined over the rationals $\mathbb{Q}$ with conductor $N_E = p^2$, $7 \leq p \leq 5000$ such that $|c_6(E)| \leq 25 \times 10^6$. In this list there are exactly two elliptic curves $\#\widetilde{E}(\mathbb{F}_p) \equiv 0 \mod 2$ for every prime p. These curves are,*

$$y^2 + xy = x^3 - x^2 - 37x - 78,$$

$$y^2 - xy = x^3 - x^2 - 2x - 1$$

Corollary 3.38. *Let E be an elliptic curve defined over $\mathbb{Q}$ with conductor $N_E = 3 \times 2^\lambda$ or $N_E = 9 \times 2^\lambda$. There exists no integer $d \geq 2$ such that $d|\#\widetilde{E}(\mathbb{F}_p)$ for every*

prime p.

Proof. In [28], Ogg showed that all of these curves have a rational point of order 2. The elliptic curves with conductor $N_E = 3 \times 2^\lambda$ have additive reduction at prime 2 and multiplicative reduction at prime 3. This implies that $m_2 = 3$ and if E has split multiplicative reduction at 3, we have $m_3 = 3$ ($m_3 = 5$ if E has non-split multiplicative reduction at 3). By Theorem 3.29 it follows that there exists no integer $d \geq 2$ such that $d|\#\widetilde{E}(\mathbb{F}_p)$ for every prime p.

Similarly, the elliptic curves with conductor $N_E = 9 \times 2^\lambda$, have additive reduction at primes 2 and 3. Then $m_2 = 3$ and $m_3 = 4$. Theorem 3.29 implies that there exists no integer $d \geq 2$ such that $d|\#\widetilde{E}_p(\mathbb{F}_p)$ for every prime p. □

Corollary 3.39. *Let E be an elliptic curve defined over $\mathbb{Q}$ of conductor $N_E = 3^l \times 5^m, l \geq 2, m \geq 1$, with a rational point of order 3. There exists no integer $d \geq 2$ such that $d|\#\widetilde{E}(\mathbb{F}_p)$ for every prime p.*

Proof. In [[10], Table 2] there are 10 such elliptic curves with torsion subgroup $E(\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$. The elliptic curves with conductor $N_E = 3^l \times 5^m, l \geq 2$ have additive reduction at the prime 3, that is $m_3 = 4$. Six curves have additive reduction at the prime 5, so, $m_5 = 6$ and four curves have multiplicative reduction at the prime 5, $m_5 = 5$. Hence, by Theorem 3.29 there exists no integer $d \geq 2$ such that $d|\#\widetilde{E}(\mathbb{F}_p)$ for every prime p. □

4. Parametrization of Elliptic Curves over Finite Fields

Let E be an elliptic curve defined over $\mathbb{Q}$. We recall that Mazur gave a complete classification of the possible order of the torsion subgroup of an elliptic curve $E/\mathbb{Q}$, see Theorem 2.8. Namely, the order of the torsion subgroup lies in the set $\{1,2,3,4,5,6,7,8,9,10,12,16\}$. In [18], Kubert gave a parametrization of all elliptic curves with a torsion point of order $n \in \{1,2,3,4,5,6,7,8,9,10,12,16\}$.

Let E be an elliptic curve defined over a quadratic number field K. Recall that Kenku and Momose gave a complete classification of the possible torsion subgroup that appear for E/K, see Theorem 2.9. In [30], Rabarison gave the parametrization of elliptic curves defined over a quadratic field with a certain torsion subgroup.

Now, let E be an elliptic curve defined over a finite field $\mathbb{F}_p$.

Theorem 4.1 ([4], Kim, Koo and Park)**.** *Let $p > 3$ be a prime and $k \in \mathbb{Z}$ such that $k(9k+4) \not\equiv 0 \mod p$. Let E be an elliptic curve given by,*

$$E : y^2 = x^3 - (6k+3)x - 3k^2 + 6k + 2.$$

Then $\#E(\mathbb{F}_p) \equiv 0 \mod 3$.

In this chapter, we generalize Theorem 4.1 to obtain families of elliptic curves over $k_{\mathfrak{p}}$ with $\#E(k_{\mathfrak{p}}) \equiv 0 \mod p$ for some prime p.

Let E_1 and E_2 be elliptic curves defined over $\mathbb{F}_p$. Recall that, if E_1 and E_2 are isogenous over $\mathbb{F}_p$ then

$$\#E_1(\mathbb{F}_p) = \#E_2(\mathbb{F}_p),$$

see [[32], Chapter 5, Exercise 5.4].

So, if an elliptic curve E is $\mathbb{Q}$- isogenous to an elliptic curve E' with a point of order n. Then it follows that $n|\#\widetilde{E}(\mathbb{F}_p)$ for primes p of good reduction.

Furthermore, recall that a point P of an elliptic curve E has order n if and only if the n^{th} division polynomial of E vanishes when evaluated at P.

Lemma 4.2. *Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve defined over a finite field $k_{\mathfrak{p}}$. Let P be a point in $E(k_{\mathfrak{p}})$ which is not a point at infinity. Then the following are equivalent,*

(a) P is a point of order n in $E(k_{\mathfrak{p}})$,

(b) The n^{th} division polynomial of E, $\psi_n(P) \equiv 0 \mod p$.

Recall that if E is an elliptic curve defined by $y^2 = x^3 + ax + b$, then the division polynomial ψ_m is a polynomial in $\mathbb{Z}[a, b, x]$, see [[32], exercise 3.7(a)].

Theorem 4.3. *Let $p \neq 2$ be a rational prime. Let K be a number field, with ring of integers R, and $\mathfrak{p}$ be a prime of K with $\operatorname{char} k_{\mathfrak{p}} \neq 2, 3$.*

Fix $T \in R$. Let (A, B) be a $k_{\mathfrak{p}}$-solution of the polynomial equation $G_T(a, b) \equiv 0 \mod \mathfrak{p}$, where

$$G_T(a, b) = \psi_p(a, b, T) \in k_{\mathfrak{p}}[a, b].$$

If the following two conditions hold

1) $4A^3 + 27B^2 \not\equiv 0 \mod \mathfrak{p}$, and

2) $T^3 + AT + B \equiv z_T^2 \mod \mathfrak{p}$ for some $z_T \in k_{\mathfrak{p}}$,

then the elliptic curve $E_{A,B} : y^2 = x^3 + Ax + B$ over $k_{\mathfrak{p}}$ satisfies $\#E_{A,B}(k_{\mathfrak{p}}) \equiv 0 \mod p$.

Proof. Condition 1) guarantees that $E_{A,B}$ is an elliptic curve over $k_{\mathfrak{p}}$. Moreover condition 2) implies that $P_T = (T, z_T) \in E_{A,B}(k_{\mathfrak{p}})$. Finally, the fact that $G_T(A, B) \equiv 0 \mod \mathfrak{p}$ together with Lemma 4.2 asserts that P_T is a point of order p in $E_{A,B}(k_{\mathfrak{p}})$. □

Corollary 4.4. *For every prime $p \equiv 1 \mod 3$, the following elliptic curve over $\mathbb{F}_p[t]$*

$$E_t : y^2 = x^3 + 2tx - \frac{t^2}{3} + t + \frac{1}{4}$$

satisfies $\#E_t(\mathbb{F}_p) \equiv 0 \mod 3$ where $(6t + 1)(2t + 3)^3 \not\equiv 0 \mod p$.

Proof. We have that,

$$\psi_{E_t,3}(x) = (x + 1)\Big(x^3 - x^2 + (4t + 1)x - \frac{4}{3}t^2\Big).$$

Then

$$(-1)^3 + 2t(-1) - \frac{t^2}{3} + t + \frac{1}{4} = \frac{-1}{12}(2t + 3)^2 \equiv z_t^2 \mod p$$

since $p \equiv 1 \mod 3$.

Therefore, by Theorem 4.3 it follows that $E_t : y^2 = x^3 + 2tx + \frac{-t^2}{3} + t + \frac{1}{4}$ satisfies $\#E_t(\mathbb{F}_p) \equiv 0 \mod 3$ for all primes p of good reduction such that $p \equiv 1 \mod 3$. □

Corollary 4.5. *For every prime $p \equiv 1 \mod 3$, the following elliptic curve over $\mathbb{F}_p[t]$*

$$E_t : y^2 = x^3 + 6tx - \frac{t^2}{12} + 108t + 9 \cdot 36^2$$

satisfies $\#E_t(\mathbb{F}_p) \equiv 0 \mod 3$ where $3(t+648)^3(t+72) \not\equiv 0 \mod p$.

Proof. The proof is similar as in Corollary 3.4. We have that,

$$\psi_{E_t,3} = (x+36)\Big(x^3 - 36x^2 + (12t+1296)x - \frac{1}{3}t^2\Big)$$

Also,

$$(-36)^3 + 6t(-36) - \frac{t^2}{12} + 108t + 9 \cdot 36^2 = \frac{-1}{12}(t + 2^3 3^4)^2 \equiv z_t^2 \mod p$$

since $p \equiv 1 \mod 3$.

Therefore, Theorem 4.3 implies that for all primes p of good reduction such that $p \equiv 1 \mod 3$, we have that $E_t : y^2 = x^3 + 6tx - (\frac{t^2}{12} - 108t - 9 \cdot 36^2)$ satisfies $\#E_t(\mathbb{F}_p) \equiv 0 \mod 3$ □

Furthermore, the factorization of the elliptic curve $E_t : y^2 = x^3 + 6tx - (\frac{t^2}{12} - 108t - 9 \cdot 36^2)$ in Corollary 3.5 for $t = -558, -522, -360, -198, -162, 810$ is as follows,

$$x^3 - 3348x - 74547 = (x+33)(x^2 - 33x - 2259)$$

$$x^3 - 3132x - 67419 = (x+33)(x^2 - 33x - 2043)$$

$$x^3 - 2160x - 38016 = (x+24)(x^2 - 24x - 1584)$$

$$x^3 - 1188x - 12987 = (x-39)(x^2 + 39x + 333)$$

$$x^3 - 972x - 8019 = (x+9)(x^2 - 9x - 891)$$

$$x^3 + 4860x + 44469 = (x+9)(x^2 - 9x + 4941)$$

Hence, any of the elliptic curves above has either one torsion point of order two or 4 torsion points of order two depending on their factorization modulo p. Therefore,

for all primes $p \equiv 1 \mod 3$ such that $p \nmid -3(t+648)^3(t+72)$, it follows that 6 or 12 divide $\#E_t(\mathbb{F}_p)$, where $t = -558, -522, -360, -198, -162, 810$.

5. The order of the reduction and base change

Let K be a quadratic number field with ring of integers R. Let $\mathfrak{p} \in R$ be a prime ideal in R and, $k_{\mathfrak{p}}$ be the residue field of K at $\mathfrak{p}$.

In Chapter 3, we showed that given an elliptic curve E defined over a number field K such that the conditions of Theorem 3.24 hold, there are at least two possible congruence classes $\beta_i \mod m$ such that $\#\widetilde{E}(k_{\mathfrak{p}}) \equiv \beta_i \mod m$ for primes $\mathfrak{p}$ of positive density.

Now, in this chapter we will investigate what happens to the congruence classes of the order of the reduction group $\#\widetilde{E}(\mathbb{F}_p)$ when we change the base field of E from $\mathbb{Q}$ to a quadratic number field K.

Let E be an elliptic curve defined over $\mathbb{Q}$ with torsion subgroup $E(\mathbb{Q})_{tors}$. We refer to Theorem 2 in [8] to see the possible torsion subgroups of E that appear when we change the base from $\mathbb{Q}$ to K, where $[K : \mathbb{Q}] = 2$.

We notice that if $E/\mathbb{Q}$ is an elliptic curve with $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/7\mathbb{Z}, \mathbb{Z}/9\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, $E(K)_{tors}$ stays the same when we change base from $\mathbb{Q}$ to a quadratic number field K.

We are interested in the cases where $E(\mathbb{Q})_{tors} \neq E(K)_{tors}$. The following theorem assures that there are finitely many such cases.

Theorem 5.1 ([14], Lemma 3.4)**.** *Let E be an elliptic curve defined over the rationals. Then there are finitely many quadratic extensions K of $\mathbb{Q}$ such that*

$$E(\mathbb{Q})_{tors} \neq E(K)_{tors}.$$

Recall, the division polynomials of an elliptic curve $E : y^2 = x^3 + ax + b$,

$\psi_1 = 1$,

$\psi_2 = 2y$,

$$\psi_3 = 3x^4 + 6ax^2 + 12bx - a^2,$$

$$\psi_4 = 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3),$$

$$\vdots$$

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \text{ for } m \geq 2,$$

$$\psi_{2m} = \left(\tfrac{\psi_m}{2y}\right) \cdot (\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \text{ for } m \geq 3.$$

All the polynomials above are defined in $\mathbb{Z}[x, y, a, b]$. Moreover, we can treat all of these polynomials in $\mathbb{Z}[x, a, b]$, see [[32], Chapter 3, Exercise 3.7(a)].

Recall that $\psi_n(x)$ satisfies $\psi_n(P) = 0$ for a point P of an elliptic curve E if and only if P has order n.

The following example shows how the factors of the division polynomial $\psi_n(x)$ may be used to determine the possible number fields L such that $E(\mathbb{Q})_{tors} \neq E(L)_{tors}$.

Example 5.2. *Let $E : y^2 + xy = x^3 - 34x - 217$ be an elliptic curve defined over $\mathbb{Q}$ with torsion subgroup $E(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$. The 4th division polynomial of E is,*

$$\psi_{E,4} = (x-20)\Big(x - \frac{31}{4}\Big)\Big(x + \frac{9}{2}\Big)(x^2 + 8x + 28)(x^4 + 16x^3 + 168x^2 - 296x + 3667).$$

The 4-torsion points of E are all points (x, y) such that x is a root of the division polynomial $\psi_{E,4}$. We have, the point $(20, y) \in E(\mathbb{Q}(\sqrt{3}))$, therefore $E(\mathbb{Q}(\sqrt{3}))_{tors} \cong \mathbb{Z}/4\mathbb{Z}$, the point $\left(\frac{31}{4}, y\right) \in E(\mathbb{Q})$ and $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z}$, the point $\left(\frac{-9}{2}, y\right) \in E(\mathbb{Q}(\sqrt{-1}))$, so, $E(\mathbb{Q}(\sqrt{-1}))_{tors} \cong \mathbb{Z}/4\mathbb{Z}$. Moreover, $\mathbb{Q}(\sqrt{-3})$ is the splitting field of the polynomial $x^2 + 8x + 28$, therefore $E(\mathbb{Q}(\sqrt{-3}))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Finally the splitting field of the polynomial $x^4 + 16x^3 + 168x^2 - 296x + 3667$ is $\mathbb{Q}(\sqrt{-3}, \sqrt[4]{-3})$ then $E(\mathbb{Q}(\sqrt{-3}, \sqrt[4]{-3}))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$

In particular, by Theorem 3 in [9], no other torsion subgroup can appear for E over a quadratic extension different from the torsion subgroups above.

Definition 5.3. *[[13], Chapter 5, Definition 5.38] Let K be a quadratic number field with ring of integers R and p be a prime in K. We say that,*

- *p splits in K if $(p) = \mathfrak{p}_1\mathfrak{p}_2$ for $\mathfrak{p}_1 \neq \mathfrak{p}_2$ two ideals of norm p.*
- *p is inert in K if (p) is a prime ideal in R of norm p^2.*
- *p is ramified in K if $(p) = \mathfrak{p}^2$ for some prime ideal $\mathfrak{p}$ of norm p.*

Remark 5.4. *For a number field K, the primes $p \neq 2$ in $\mathbb{Q}$ which ramify are those dividing the discriminant of the integer ring R of K. Therefore, there are finitely*

many such primes.

Theorem 5.5. *[[13], Chapter 5, Section 5.9] Consider $K = \mathbb{Q}(\sqrt{d})$, where d is a nonsquare. Let $p \neq 2$ be a prime. Then,*

(a) p splits in K if $\left(\frac{d}{p}\right) = 1$,

(b) p is inert in K if $\left(\frac{d}{p}\right) = -1$.

Let E be an elliptic curve defined over a number field L. Recall that,

$$\#\widetilde{E}(k_{\mathfrak{p}}) = 1 + N(\mathfrak{p}) - a_{\mathfrak{p}}(E),$$

where $a_{\mathfrak{p}}(E)$ is the trace of Frobenius of E at $\mathfrak{p}$. By Hasse's theorem we have, $|a_{\mathfrak{p}}(E)| \leq 2\sqrt{N(\mathfrak{p})}$, where $N(\mathfrak{p}) = p^r$, p is a prime and $r \geq 1$.

Now, let $E/\mathbb{F}_q$ be an elliptic curve, where $q = p^r$, p is a prime and $r \geq 1$. For each $n \geq 1$ let $a_n = 1 + q^n - \#E(\mathbb{F}_{q^n})$. Then the linear recurrence,

$$a_{n+2}(E) = a_1(E)a_{n+1}(E) - pa_n(E), \text{ for all } n \geq 0$$

where $a_0 = 2$ and $a_1 = 1 + q - \#E(\mathbb{F}_q)$, provides a way to compute the trace of Frobenius of E in extensions of $\mathbb{F}_q$, [[32], Chapter 5, Exercise 5.13].

Moreover, for an elliptic curve E given by $y^2 = x^3 + ax + b$ defined over $\mathbb{Q}$, we denote by $E^d : dy^2 = x^3 + ax + b$ its quadratic twist by a squarefree integer d.

Corollary 5.6 ([8], Corollary 4)**.** *Let E be an elliptic curve defined over $\mathbb{Q}$, d an square-free integer and $K = (\mathbb{Q}(\sqrt{d}))$. If n is odd, then there exists an isomorphism*

$$E(\mathbb{Q}(\sqrt{d}))[n] \cong E(\mathbb{Q})[n] \oplus E^d(\mathbb{Q})[n].$$

Lemma 5.7. *[[31], Proposition 3.21] Let E be an elliptic curve defined over a finite field $\mathbb{F}_p$ and let E^d be a twist of E. Then*

$$\#E(\mathbb{F}_p) + \#E^d(\mathbb{F}_p) = 2p + 2.$$

In the following theorem, we compute the order of the reduction of an elliptic curve when we change the base field from $\mathbb{Q}$ to $\mathbb{Q}(\sqrt{d})$.

Theorem 5.8. *Let $E/\mathbb{Q}$ be an elliptic curve. Let $K = \mathbb{Q}(\sqrt{d})$ where d is a square*

free integer, and $\mathfrak{p}$ *be a prime in* K*. Then,*

$$\#\widetilde{E}(k_{\mathfrak{p}}) = \begin{cases} \#\widetilde{E}(\mathbb{F}_p) & \text{if } p \neq 2 \text{ splits in } K \\ \#\widetilde{E}(\mathbb{F}_p) \cdot \#\widetilde{E}^d(\mathbb{F}_p) & \text{if } p \neq 2 \text{ is inert in } K \end{cases}.$$

Proof. Let $\mathfrak{p}$ be a prime ideal K, and let p be a prime that splits in K. Then by Definition 5.3, $N(\mathfrak{p}) = p$. Now, $p = N(\mathfrak{p}) = \#k_{\mathfrak{p}}$ implies that $k_{\mathfrak{p}} \cong \mathbb{F}_p$. Therefore, $\#\widetilde{E}(k_{\mathfrak{p}}) = \#\widetilde{E}(\mathbb{F}_p)$.

Let the prime p be inert in K. Then

$$a_{\mathfrak{p}}(E) = a_p^2 - 2p = (1 + p - \#\widetilde{E}(\mathbb{F}_p))^2 - 2p = 1 + p^2 - 2(1+p)\#\widetilde{E}(\mathbb{F}_p) + \#\widetilde{E}(\mathbb{F}_p)^2.$$

Hence,

$$\begin{aligned} \#\widetilde{E}(k_{\mathfrak{p}}) = 1 + p^2 - a_{\mathfrak{p}}(E) &= 1 + p^2 - (1 + p^2 - 2(1+p)\#\widetilde{E}(\mathbb{F}_p) + \#\widetilde{E}(\mathbb{F}_p)^2) \\ &= \#\widetilde{E}(\mathbb{F}_p)(2(1+p) - \#\widetilde{E}(\mathbb{F}_p)). \end{aligned}$$

Then it follows by Lemma 5.7 that $\#\widetilde{E}(k_{\mathfrak{p}}) = \#\widetilde{E}(\mathbb{F}_p) \cdot \#\widetilde{E}^d(\mathbb{F}_p)$. □

As a consequence of Theorem 5.8 we have the following Corollary.

Corollary 5.9. *Let* $E/\mathbb{Q}$ *be an elliptic curve with torsion subgroup* $G = E(\mathbb{Q})_{tors}$*. Let* $H = E(K)_{tors}$*, where* $[K : \mathbb{Q}] = 2$*, such that* $H \neq G$ *and* $m = |H|$*. Then*

$$\#\widetilde{E}(\mathbb{F}_p) \equiv 0 \mod m$$

for all primes p *of good reduction of* E *that split in* K*. In particular, the density of primes such that* $\#\widetilde{E}(\mathbb{F}_p) \equiv 0 \mod m$ *is at least* $\frac{1}{2}$*.*

Proof. It follows from Theorem 5.8 that for the primes that split in K, $\#\widetilde{E}(k_{\mathfrak{p}}) = \#\widetilde{E}(\mathbb{F}_p)$ where $\mathfrak{p}$ is a prime lying above p. The result follows by noting that $\#\widetilde{E}(k_{\mathfrak{p}}) \equiv 0 \mod m$. □

Let $E/\mathbb{Q}$ be an elliptic curve with torsion subgroup $E(\mathbb{Q})_{tors}$. In [24], F. Najman gives the possible orders of torsion subgroups of quadratic twist E^d of E in terms of the order of the torsion subgroup $E(\mathbb{Q})_{tors}$. Also in [[9], Theorem 2] Enrique Gonzalez-Jimenez and Jose M. Tornero give the exact number of possible quadratic fields K such that $E(\mathbb{Q})_{tors} \neq E(K)_{tors}$ for a fixed elliptic curve E defined over $\mathbb{Q}$. Moreover, they give the list of the possible torsion subgroups $E(K)_{tors}$. Using these

results, we classify the possible congruence classes that can appear for $\#\widetilde{E}(\mathbb{F}_p)$ given that $E(\mathbb{Q})_{tors} \neq E(K)_{tors}$.

Theorem 5.10. *Let E be an elliptic curve defined over $\mathbb{Q}$ with $E(\mathbb{Q})_{tors} = G$ and $E(K)_{tors} = H$, for some $[K:\mathbb{Q}] = 2$, such that $G \neq H$. Let ℓ be a prime divisor of $|H|$. Let $p \neq 2$ be a prime of good reduction of E. Then*

$$\#\widetilde{E}(\mathbb{F}_p) \equiv \begin{cases} 0 \mod \ell & \text{if } p \text{ splits in } K \\ 2p+2 \mod \ell & \text{if } p \text{ is inert in } K \text{ and } \ell \mid \#\widetilde{E}^d(\mathbb{F}_p) \\ 2p+2-\#\widetilde{E}^d(\mathbb{F}_p) \mod \ell & \text{if } p \text{ is inert in } K \text{ and } \ell \nmid \#\widetilde{E}^d(\mathbb{F}_p) \end{cases}$$

Proof. If the prime p splits in K then it follows by Theorem 5.8 that $\#\widetilde{E}(\mathbb{F}_p) \equiv 0 \mod m$. If the prime p is inert in K then the result follows from Lemma 5.7. □

In [Theorem 3, [9]] Enrique Gonzalez-Jimenez and Jose M. Tornero list all possible torsion subgroups that can appear for E over a quadratic extension of $\mathbb{Q}$. Moreover, in [Table 1, [9]] they give examples for every possible situation. Referring to Table 1, we give some examples where we can list the possible congruence classes that appear for an elliptic curve E with a given torsion subgroup $E(\mathbb{Q})_{tors}$.

All elliptic curves in the following examples are represented with a minimal equation of the form $E: y^2 + a_1xy + a_2y = x^3 + a_4x + a_6$.

Example 5.11. *Let $E: y^2 + y = x^3 - x^2 + 217x - 282$ be an elliptic curve defined over $\mathbb{Q}$ with $E(\mathbb{Q})_{tors} = \{0\}$ and $E(\mathbb{Q}(\sqrt{5}))_{tors} \cong \mathbb{Z}/3\mathbb{Z}$. The torsion subgroup of the quadratic twist of E^5 is $E^5(\mathbb{Q})_{tors} \cong \mathbb{Z}/3\mathbb{Z}$. We have that, a prime p splits in $\mathbb{Q}(\sqrt{5})$ if $p \equiv 1,4 \mod 5$, otherwise is inert. Then Theorem 5.10 implies that $\#\widetilde{E}(\mathbb{F}_p) \equiv 0 \mod 3$ for all primes $p \equiv 1,4 \mod 5$. Furthermore, since $3 \mid \#\widetilde{E}^d(\mathbb{F}_p)$, again by Theorem 5.10 it follows that*

$$\#\widetilde{E}(\mathbb{F}_p) \equiv 0,1 \mod 3 \quad \text{if} \quad p \equiv 2,3 \mod 5.$$

Therefore,

$$\#\widetilde{E}(\mathbb{F}_p) \equiv \begin{cases} 0 \mod 3 & \text{if} \quad p \equiv 1,4 \mod 5 \\ 0,1 \mod 3 & \text{if} \quad p \equiv 2,3 \mod 5 \end{cases}.$$

Remark 5.12. *One may see in the example above that $\#\tilde{E}(\mathbb{F}_p)$ is divisible by 3 for primes of density at least $1/2$. In addition, it follows from Theorem 3.24 that $\#\tilde{E}(\mathbb{F}_p) \equiv 1 \mod 3$ for primes p of positive density.*

Example 5.13. *Let $E: y^2 + y = x^3 - x^2 + 42x + 443$ be an elliptic curve defined*

over $\mathbb{Q}$ *with* $E(\mathbb{Q})_{tors} = \{0\}$ *and* $E(\mathbb{Q}(\sqrt{5}))_{tors} \cong \mathbb{Z}/5\mathbb{Z}$. *The torsion subgroup of the quadratic twist of* E^5 *is* $E^5(\mathbb{Q})_{tors} \cong \mathbb{Z}/5\mathbb{Z}$. *Similarly as in Example 5.11, by Theorem 5.10 it follows that,*

$$\#\widetilde{E}(\mathbb{F}_p) \equiv \begin{cases} 0 \mod 5 & \text{if} \quad p \equiv 1,4 \mod 5 \\ 1 \mod 5 & \text{if} \quad p \equiv 2 \mod 5 \\ 3 \mod 5 & \text{if} \quad p \equiv 3 \mod 5 \end{cases}.$$

Remark 5.14. *Notice that* $\#\widetilde{E}(\mathbb{F}_p) \equiv 0 \mod 5$ *for primes* p *of density* $\frac{1}{2}$. *In addition, we have that* $\#\widetilde{E}(\mathbb{F}_p) \equiv 1 \mod 5$ *and* $\#\widetilde{E}(\mathbb{F}_p) \equiv 3 \mod 5$ *for primes of density* $\frac{1}{4}$.

Example 5.15. *Let* $E : y^2 = x^3 - 43x - 166$ *be an elliptic curve defined over* $\mathbb{Q}$ *with* $E(\mathbb{Q})_{tors} = \{0\}$ *and* $E(\mathbb{Q}(\sqrt{-1}))_{tors} \cong \mathbb{Z}/7\mathbb{Z}$. *The torsion subgroup of the quadratic twist of* E^{-1} *is* $E^{-1}(\mathbb{Q})_{tors} \cong \mathbb{Z}/7\mathbb{Z}$. *We have that a prime* p *splits in* $\mathbb{Q}(\sqrt{-1})$ *if* $p \equiv 1 \mod 4$, *otherwise* p *is inert. Then similarly as in Example 5.11, by Theorem 5.8 it follows that,*

$$\#\widetilde{E}(\mathbb{F}_p) \equiv \begin{cases} 0 \mod 7 & \text{if} \quad p \equiv 1 \mod 4 \\ 0,1,3,4,5,6 \mod 7 & \text{if} \quad p \equiv 3 \mod 4 \end{cases}.$$

Remark 5.16. *One may notice that in the example above,* $\#\widetilde{E}(\mathbb{F}_p) \equiv 0 \mod 7$ *for primes* p *of density at least* $\frac{1}{2}$. *Moreover, it follows by Theorem 3.24, that* $\#\widetilde{E}(\mathbb{F}_p) \equiv 1,3,4,5,6 \mod 7$ *for primes* p *of positive density.*

Example 5.17. *Let* $E : y^2 + xy = x^3 - x^2 - 123x - 667$ *be an elliptic curve defined over* $\mathbb{Q}$ *with* $E(\mathbb{Q})_{tors} = \{0\}$ *and* $E(\mathbb{Q}(\sqrt{-3}))_{tors} \cong \mathbb{Z}/9\mathbb{Z}$. *Also, the torsion subgroup of the quadratic twist of* E^{-3} *is* $E^{-3}(\mathbb{Q})_{tors} \cong \mathbb{Z}/9\mathbb{Z}$. *Moreover, a prime* p *splits in* $\mathbb{Q}(\sqrt{-3})$ *if* $p \equiv 1 \mod 3$, *otherwise* p *is inert. So, similarly as in example 5.11, by Theorem 5.8 it follows,*

$$\#\widetilde{E}(\mathbb{F}_p) \equiv \begin{cases} 0 \mod 9 & \text{if} \quad p \equiv 1 \mod 3 \\ 0,3,6 \mod 9 & \text{if} \quad p \equiv 2 \mod 3 \end{cases}.$$

Remark 5.18. *Notice that* $\#\widetilde{E}(\mathbb{F}_p)$ *is divisible by* 9 *for primes* p *of density at least* $\frac{1}{2}$. *Moreover, it follows by Theorem 3.24 that,* $\#\widetilde{E}(\mathbb{F}_p) \equiv 3,6 \mod 9$ *for primes* p *of positive density.*

Example 5.19. *Let* $E : y^2 + xy = x^3 + x^2 - 1740x + 22184$ *be an elliptic curve defined*

over $\mathbb{Q}$ *with* $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z}$ *and* $E(\mathbb{Q}(\sqrt{-7}))_{tors} \cong \mathbb{Z}/6\mathbb{Z}$. *Moreover, the torsion subgroup of the quadratic twist of* E^{-7} *is* $E^{-7}(\mathbb{Q})_{tors} \cong \mathbb{Z}/6\mathbb{Z}$. *A prime* p *splits in* $\mathbb{Q}(\sqrt{-7})$ *if* $p \equiv 1, 2, 4 \mod 7$ *otherwise* p *is inert. Then as in Example 5.11, it follows by Theorem 5.10,*

$$\#\widetilde{E}(\mathbb{F}_p) \equiv \begin{cases} 0 \mod 6 & \text{if} \quad p \equiv 1, 2, 4 \mod 7 \\ 0, 4 \mod 6 & \text{if} \quad p \equiv 3, 5, 6 \mod 7 \end{cases}.$$

Remark 5.20. *One may see that* $\#\widetilde{E}(\mathbb{F}_p) \equiv 0 \mod 6$ *for primes* p *of density at least* $\frac{1}{2}$. *Furthermore, it follows by Theorem 3.24,* $\#\widetilde{E}(\mathbb{F}_p) \equiv 4 \mod 6$ *for primes* p *of positive density.*

Example 5.21. *Let* $E : y^2 = x^3 + 20148x + 586096$ *be an elliptic curve defined over* $\mathbb{Q}$ *with* $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z}$ *and* $E(\mathbb{Q}(\sqrt{-6}))_{tors} \cong \mathbb{Z}/8\mathbb{Z}$. *Also, the torsion subgroup of the quadratic twist of* E^{-6} *is* $E^{-6}(\mathbb{Q})_{tors} \cong \mathbb{Z}/8\mathbb{Z}$. *We have that, a prime* p *splits in* $\mathbb{Q}(\sqrt{-6})$ *if* $p \equiv 1, 5, 7, 11 \mod 24$ *otherwise* p *is inert. Therefore as in previous examples, by Theorem 5.10 it follows that*

$$\#\widetilde{E}(\mathbb{F}_p) \equiv \begin{cases} 0 \mod 8 & \text{if} \quad p \equiv 1, 5, 7, 11, 19, 23 \mod 24 \\ 4 \mod 8 & \text{if} \quad p \equiv 13, 17 \mod 24 \end{cases}.$$

Remark 5.22. *The congruence class* $\#\widetilde{E}(\mathbb{F}_p) \equiv 0 \mod 8$ *appears for primes of density at least* $\frac{1}{2}$. *It follows by Theorem 3.24,* $\#\widetilde{E}(\mathbb{F}_p) \equiv 4 \mod 8$ *for primes* p *of positive density.*

Example 5.23. *Let* $E : y^2 + xy = x^3 + x^2 - 700x + 34000$ *be an elliptic curve defined over* $\mathbb{Q}$ *with* $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z}$ *and* $E(\mathbb{Q}(\sqrt{5}))_{tors} \cong \mathbb{Z}/10\mathbb{Z}$. *The torsion subgroup of the quadratic twist* E^5 *is* $E^5(\mathbb{Q})_{tors} \cong \mathbb{Z}/10\mathbb{Z}$. *Thus, Theorem 5.10 implies that*

$$\#\widetilde{E}(\mathbb{F}_p) \equiv \begin{cases} 0 \mod 10 & \text{if} \quad p \equiv 1, 4 \mod 5 \\ 6 \mod 10 & \text{if} \quad p \equiv 2 \mod 5 \\ 8 \mod 10 & \text{if} \quad p \equiv 3 \mod 5 \end{cases}.$$

Remark 5.24. *Notice that* $\#\widetilde{E}(\mathbb{F}_p) \equiv 0 \mod 10$ *for primes* p *of density* $\frac{1}{2}$, *and* $\#\widetilde{E}(\mathbb{F}_p) \equiv 6 \mod 10$ *for primes of density* $\frac{1}{4}$, *similarly* $\#\widetilde{E}(\mathbb{F}_p) \equiv 8 \mod 10$ *for primes of density* $\frac{1}{4}$.

Example 5.25. *Let* $E : y^2 + xy + y = x^3 - x^2 + 47245x - 2990253$ *be an elliptic curve defined over* $\mathbb{Q}$ *with* $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z}$ *and* $E(\mathbb{Q}(\sqrt{-15}))_{tors} \cong \mathbb{Z}/16\mathbb{Z}$. *Also, the*

torsion subgroup of the quadratic twist E^{-15} *is* $E^{-15}(\mathbb{Q})_{tors} \cong \mathbb{Z}/8\mathbb{Z}$. *A prime* p *splits in* $\mathbb{Q}(\sqrt{-15})$ *if* $p \equiv 1,2,4,8 \mod 15$ *otherwise* p *is inert. Moreover, if* $p \equiv 7,11,13,14 \mod 15$ *then* $\#\widetilde{E}^{-15}(\mathbb{F}_p) \equiv 0,8 \mod 16$ *and* $2p+2 \equiv 0,4,8,12 \mod 16$. *It follows by Theorem 5.10,*

$$\#\widetilde{E}(\mathbb{F}_p) \equiv \begin{cases} 0 \mod 16 & \text{if} \quad p \equiv 1,2,4,8 \mod 15 \\ 0,4,8,12 \mod 16 & \text{if} \quad p \equiv 7,11,13,14 \mod 15 \end{cases}.$$

Remark 5.26. *One may notice that* $\#\widetilde{E}(\mathbb{F}_p) \equiv 0 \mod 16$ *for primes* p *of density at least* $\frac{1}{2}$. *Moreover, it follows by Theorem 3.24 that* $\#\widetilde{E}(\mathbb{F}_p) \equiv 4,8,12 \mod 16$ *for primes* p *of positive density.*

Example 5.27. *Let* $E : y^2 + xy + y = x^3 - 171x - 874$ *be an elliptic curve defined over* $\mathbb{Q}$ *with* $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z}$ *and* $E(\mathbb{Q}(\sqrt{-7}))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. *Moreover, the torsion of the quadratic twist* E^{-7} *is* $E^{-7}(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z}$. *In particular, a prime* p *splits in* $\mathbb{Q}(\sqrt{-7})$ *if* $p \equiv 1,2,4 \mod 7$, *otherwise* p *is inert. Then similarly as in Example 5.25 together with Theorem 5.10 we have that,*

$$\#\widetilde{E}(\mathbb{F}_p) \equiv \begin{cases} 0 \mod 4 & \text{if} \quad p \equiv 1,2,4 \mod 7 \\ 0,2 \mod 4 & \text{if} \quad p \equiv 3,5,6 \mod 7 \end{cases}.$$

Remark 5.28. *One may notice that* $\#\widetilde{E}(\mathbb{F}_p) \equiv 0 \mod 4$ *for primes* p *of density at least* $\frac{1}{2}$. *In addition, it follows by Theorem 3.24 that* $\#\widetilde{E}(\mathbb{F}_p) \equiv 2 \mod 4$ *for primes* p *of positive density.*

Example 5.29. *Let* $E : y^2 = x^3 - 27$ *be an elliptic curve defined over* $\mathbb{Q}$ *with* $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z}$ *and* $E(\mathbb{Q}(\sqrt{-3}))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. *Also, the torsion of the quadratic twist* E^{-3} *is* $E^{-3}(\mathbb{Q})_{tors} \cong \mathbb{Z}/6\mathbb{Z}$. *A prime* p *splits in* $\mathbb{Q}(\sqrt{-3})$ *if* $p \equiv 1 \mod 3$, *otherwise* p *is inert. Then similarly as in Example 5.25 and by Theorem 5.10, we have*

$$\#\widetilde{E}(\mathbb{F}_p) \equiv \begin{cases} 0 \mod 12 & \text{if} \quad p \equiv 1 \mod 3 \\ 0,6 \mod 12 & \text{if} \quad p \equiv 2 \mod 3 \end{cases}.$$

Remark 5.30. *One may notice that* $\#\widetilde{E}(\mathbb{F}_p) \equiv 0 \mod 12$ *for primes* p *of density at least* $\frac{1}{2}$. *Moreover, it follows by Theorem 3.24 that* $\#\widetilde{E}(\mathbb{F}_p) \equiv 6 \mod 12$ *for primes* p *of positive density.*

Example 5.31. *Let* $E : y^2 + xy + y = x^3 - x^2 - 6305x - 924303$ *be an elliptic curve*

defined over $\mathbb{Q}$ *with* $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z}$ *and* $E(\mathbb{Q}(\sqrt{-15}))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$. *Also, the torsion subgroup of the quadratic twist* E^{-15} *is* $E^{-15}(\mathbb{Q})_{tors} \cong \mathbb{Z}/10\mathbb{Z}$. *In particular, a prime* p *splits in* $\mathbb{Q}(\sqrt{-15})$ *if* $p \equiv 1, 2, 4, 8 \mod 15$, *otherwise* p *is inert. Then similarly as in Example 5.25, it follows by Theorem 5.10 that*

$$\#\widetilde{E}(\mathbb{F}_p) \equiv \begin{cases} 0 \mod 20 & \text{if} \quad p \equiv 1, 2, 4, 8 \mod 15 \\ 6, 16 \mod 20 & \text{if} \quad p \equiv 7 \mod 15 \\ 4, 14 \mod 20 & \text{if} \quad p \equiv 11 \mod 15 \\ 8, 18 \mod 20 & \text{if} \quad p \equiv 13 \mod 15 \\ 0, 10 \mod 20 & \text{if} \quad p \equiv 14 \mod 15 \end{cases}.$$

Remark 5.32. *One may notice that* $\#\widetilde{E}(\mathbb{F}_p) \equiv 0 \mod 20$ *for primes* p *of density at least* $\frac{1}{2}$. *Moreover, it follows by Theorem 3.24 that all the other congruence classes happen for primes* p *of positive density.*

Example 5.33. *Let* $E : y^2 + xy + y = x^3 - 76x + 298$ *be an elliptic curve defined over* $\mathbb{Q}$ *with* $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/3\mathbb{Z}$ *and* $E(\mathbb{Q}(\sqrt{5}))_{tors} \cong \mathbb{Z}/15\mathbb{Z}$. *Also, the torsion subgroup of the quadratic twist* E^5 *is* $E^5(\mathbb{Q})_{tors} \cong \mathbb{Z}/5\mathbb{Z}$. *Then as in Example 5.25, by Theorem 5.10 it follows,*

$$\#\widetilde{E}(\mathbb{F}_p) \equiv \begin{cases} 0 \mod 15 & \text{if} \quad p \equiv 1, 4 \mod 5 \\ 3 \mod 15 & \text{if} \quad p \equiv 3 \mod 5 \\ 6 \mod 15 & \text{if} \quad p \equiv 2 \mod 5 \end{cases}.$$

Remark 5.34. *Notice that* $\#\widetilde{E}(\mathbb{F}_p) \equiv 0 \mod 15$ *for primes* p *of density* $\frac{1}{2}$, *and the other two congruence classes* $\#\widetilde{E}(\mathbb{F}_p) \equiv 3 \mod 15$ *and* $\#\widetilde{E}(\mathbb{F}_p) \equiv 6 \mod 15$ *each happen for primes* p *of density* $\frac{1}{4}$.

Example 5.35. *Let* $E : y^2 + y = x^3 + x^2 - 9x - 15$ *be an elliptic curve defined over* $\mathbb{Q}$ *with* $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/3\mathbb{Z}$ *and* $E(\mathbb{Q}(\sqrt{-3}))_{tors} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. *Furthermore, the torsion subgroup of the quadratic twist* E^{-3} *is* $E^{-3}(\mathbb{Q})_{tors} \cong \mathbb{Z}/3\mathbb{Z}$. *Similarly as in Example 5.25, by Theorem 5.10 we have,*

$$\#\widetilde{E}(\mathbb{F}_p) \equiv \begin{cases} 0 \mod 9 & \text{if} \quad p \equiv 1, 2 \mod 3 \\ 0, 3, 6 \mod 9 & \text{if} \quad p \equiv 2 \mod 3 \end{cases}.$$

Remark 5.36. *One may see that in the example above,* $\#\widetilde{E}(\mathbb{F}_p) \equiv 0 \mod 9$ *for primes* p *of density at least* $\frac{1}{2}$. *Moreover, it follows by Theorem 3.24 that* $\#\widetilde{E}(\mathbb{F}_p) \equiv$

$3,6 \mod 9$ *for primes* p *of positive density.*

Example 5.37. *Let* $E : y^2 + xy + y = x^3 - x^2 - x - 14$ *be an elliptic curve defined over* $\mathbb{Q}$ *with* $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/4\mathbb{Z}$ *and* $E(\mathbb{Q}(\sqrt{-1}))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$*. Moreover, the torsion subgroup of the quadratic twist* E^{-1} *is* $E^{-1}(\mathbb{Q})_{tors} \cong \mathbb{Z}/4\mathbb{Z}$*. Then by Theorem 5.10 it follows,*

$$\#\widetilde{E}(\mathbb{F}_p) \equiv \begin{cases} 0 \mod 8 & \text{if} \quad p \equiv 1 \mod 4 \\ 0,4 \mod 8 & \text{if} \quad p \equiv 3 \mod 4 \end{cases}.$$

Remark 5.38. *One may notice that* $\#\widetilde{E}(\mathbb{F}_p) \equiv 0 \mod 8$ *for primes* p *of density at least* $\frac{1}{2}$*. In addition, it follows by Theorem 3.24 that* $\#\widetilde{E}(\mathbb{F}_p) \equiv 4 \mod 8$ *for primes* p *of positive density.*

Example 5.39. *Let* $E : y^2 = x^3 + x^2 + 63x - 1377$ *be an elliptic curve defined over* $\mathbb{Q}$ *with* $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/4\mathbb{Z}$ *and* $E(\mathbb{Q}(\sqrt{-2}))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$*. We have that the torsion subgroup of the quadratic twist* E^{-2} *is* $E^{-2}(\mathbb{Q})_{tors} \cong \mathbb{Z}/8\mathbb{Z}$*. Furthermore, a prime* p *splits in* $\mathbb{Q}(\sqrt{-2})$ *if* $p \equiv 1,3 \mod 8$*, otherwise* p *is inert. Then similarly to Example 5.25, by Theorem 5.10 it follows*

$$\#\widetilde{E}(\mathbb{F}_p) \equiv \begin{cases} 0 \mod 16 & \text{if} \quad p \equiv 1,3 \mod 8 \\ 4,12 \mod 16 & \text{if} \quad p \equiv 5 \mod 8 \\ 0,8 \mod 16 & \text{if} \quad p \equiv 7 \mod 8 \end{cases}.$$

Remark 5.40. *We notice that in the example above,* $\#\widetilde{E}(\mathbb{F}_p) \equiv 0 \mod 16$ *for primes* p *of density at least* $\frac{1}{2}$*. Moreover, it follows by Theorem 3.24 that* $\#\widetilde{E}(\mathbb{F}_p) \equiv 4,8,12 \mod 16$ *for primes* p *of positive density.*

Example 5.41. *Let* $E : y^2 + xy + y = x^3 + x^2 - 338x - 7969$ *be an elliptic curve defined over* $\mathbb{Q}$ *with* $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/4\mathbb{Z}$ *and* $E(\mathbb{Q}(\sqrt{-15}))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$*. Also, the torsion subgroup of the quadratic twist* E^{-15} *is* $E^{-15}(\mathbb{Q})_{tors} \cong \mathbb{Z}/12\mathbb{Z}$*. Then by Theorem 5.10 it follows,*

$$\#\widetilde{E}(\mathbb{F}_p) \equiv \begin{cases} 0 \mod 24 & \text{if} \quad p \equiv 1,2,4,8 \mod 15 \\ 0,12 \mod 24 & \text{if} \quad p \equiv 11,14 \mod 15 \\ 4,16 \mod 24 & \text{if} \quad p \equiv 7,13 \mod 15 \end{cases}.$$

Remark 5.42. *One may notice that* $\#\widetilde{E}(\mathbb{F}_p) \equiv 0 \mod 24$ *for primes* p *of density at least* $\frac{1}{2}$*. Furthermore, it follows by Theorem 3.24 that* $\#\widetilde{E}(\mathbb{F}_p) \equiv 4,12,16 \mod 24$

for primes p of positive density.

Example 5.43. *Let $E : y^2 + xy + y = x^3 + x^2 - 3x + 1$ be an elliptic curve defined over $\mathbb{Q}$ with $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/5\mathbb{Z}$ and $E(\mathbb{Q}(\sqrt{5}))_{tors} \cong \mathbb{Z}/15\mathbb{Z}$. Furthermore, the torsion subgroup of the quadratic twist E^5 is $E^5(\mathbb{Q})_{tors} \cong \mathbb{Z}/3\mathbb{Z}$. Then by Theorem 5.10 we have that,*

$$\#\widetilde{E}(\mathbb{F}_p) \equiv \begin{cases} 0 \mod 15 & \text{if} \quad p \equiv 1,4 \mod 5 \\ 0,10 \mod 15 & \text{if} \quad p \equiv 2,3 \mod 5 \end{cases}.$$

Remark 5.44. *One may see that, $\#\widetilde{E}(\mathbb{F}_p) \equiv 0 \mod 15$ for primes p of density at least $\frac{1}{2}$. Moreover, it follows by Theorem 3.24 that $\#\widetilde{E}(\mathbb{F}_p) \equiv 10 \mod 15$ for primes p of positive density.*

Example 5.45. *Let $E : y^2 + xy + y = x^3 - x$ be an elliptic curve defined over $\mathbb{Q}$ with $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/6\mathbb{Z}$ and $E(\mathbb{Q}(\sqrt{-7}))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Also, the torsion subgroup of the quadratic twist E^{-7} is $E^{-7}(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z}$. Then by Theorem 5.10 it follows,*

$$\#\widetilde{E}(\mathbb{F}_p) \equiv \begin{cases} 0 \mod 12 & \text{if} \quad p \equiv 1,2,4 \mod 7 \\ 0,6 \mod 12 & \text{if} \quad p \equiv 3,5,6 \mod 7 \end{cases}.$$

Remark 5.46. *Notice that in the example above, $\#\widetilde{E}(\mathbb{F}_p) \equiv 0 \mod 12$ for primes p of density at least $\frac{1}{2}$. In addition, it follows by Theorem 3.24 that $\#\widetilde{E}(\mathbb{F}_p) \equiv 6 \mod 12$ for primes p of positive density.*

Example 5.47. *Let $E : y^2 + xy + y = x^3 + 4x - 6$ be an elliptic curve defined over $\mathbb{Q}$ with $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/6\mathbb{Z}$ and $E(\mathbb{Q}(\sqrt{-3}))_{tors} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Also, the torsion subgroup of the quadratic twist E^{-3} is $E^{-3}(\mathbb{Q})_{tors} \cong \mathbb{Z}/6\mathbb{Z}$. Then by Theorem 5.10,*

$$\#\widetilde{E}(\mathbb{F}_p) \equiv \begin{cases} 0 \mod 18 & \text{if} \quad p \equiv 1 \mod 3 \\ 0,6,12 \mod 18 & \text{if} \quad p \equiv 2 \mod 3 \end{cases}.$$

Remark 5.48. *One may notice that $\#\widetilde{E}(\mathbb{F}_p) \equiv 0 \mod 18$ for primes p of density at least $\frac{1}{2}$. Moreover, it follows by Theorem 3.24 that $\#\widetilde{E}(\mathbb{F}_p) \equiv 6,12 \mod 18$ for primes p of positive density.*

Example 5.49. *Let $E : y^2 + xy + y = x^3 + x^2 + 35x - 28$ be an elliptic curve defined over $\mathbb{Q}$ with $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/8\mathbb{Z}$ and $E(\mathbb{Q}(\sqrt{-1}))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. In particular, the torsion subgroup of the quadratic twist E^{-1} is $E^{-1}(\mathbb{Q})_{tors} \cong \mathbb{Z}/4\mathbb{Z}$. Then by*

Theorem 5.10 we have that,

$$\#\widetilde{E}(\mathbb{F}_p) \equiv \begin{cases} 0 \mod 16 & \text{if } p \equiv 1 \mod 4 \\ 0,8 \mod 16 & \text{if } p \equiv -1 \mod 4 \end{cases}.$$

Remark 5.50. *One may see that* $\#\widetilde{E}(\mathbb{F}_p) \equiv 0 \mod 16$ *for primes* p *of density at least* $\frac{1}{2}$*. Moreover, it follows by Theorem 3.24 that* $\#\widetilde{E}(\mathbb{F}_p) \equiv 8 \mod 16$ *for primes* p *of positive density.*

Example 5.51. *Let* $E : y^2 + xy = x^3 - x^2 - 36x + 27$ *be an elliptic curve defined over* $\mathbb{Q}$ *with* $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times Z/2\mathbb{Z}$ *and* $E(\mathbb{Q}(\sqrt{-3}))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$*. Furthermore, the torsion subgroup of the quadratic twist* E^{-3} *is* $E^{-3}(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times Z/4\mathbb{Z}$*. Then by Theorem 5.10 it follows,*

$$\#\widetilde{E}(\mathbb{F}_p) \equiv \begin{cases} 0 \mod 16 & \text{if } p \equiv 1 \mod 3 \\ 0,4,8,12 \mod 16 & \text{if } p \equiv -1 \mod 3 \end{cases}.$$

Remark 5.52. *One may notice that* $\#\widetilde{E}(\mathbb{F}_p) \equiv 0 \mod 16$ *for primes* p *of density at least* $\frac{1}{2}$*. Moreover, it follows by Theorem 3.24 that* $\#\widetilde{E}(\mathbb{F}_p) \equiv 4,8,12 \mod 16$ *for primes* p *of positive density.*

Example 5.53. *Let* $E : y^2 = x^3 + x^2 - 21345x + 1190943$ *be an elliptic curve defined over* $\mathbb{Q}$ *with* $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times Z/2\mathbb{Z}$ *and* $E(\mathbb{Q}(\sqrt{6}))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$*. Moreover, the torsion subgroup of the quadratic twist* E^6 *is* $E^6(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times Z/6\mathbb{Z}$*. Then by Theorem 5.10 we have that,*

$$\#\widetilde{E}(\mathbb{F}_p) \equiv \begin{cases} 0 \mod 24 & \text{if } p \equiv 1,5,19,23 \mod 24 \\ 4,16 \mod 24 & \text{if } p \equiv 7,13 \mod 24 \\ 0,12 \mod 24 & \text{if } p \equiv 11,17 \mod 24 \end{cases}.$$

Remark 5.54. *Notice that in the example above,* $\#\widetilde{E}(\mathbb{F}_p) \equiv 0 \mod 24$ *for primes* p *of density at least* $\frac{1}{2}$*. Moreover, it follows by Theorem 3.24 that* $\#\widetilde{E}(\mathbb{F}_p) \equiv 4,12,16 \mod 24$ *for primes* p *of positive density.*

Example 5.55. *Let* $E : y^2 + xy + y = x^3 + x^2 - 5x + 2$ *be an elliptic curve defined over* $\mathbb{Q}$ *with* $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times Z/4\mathbb{Z}$ *and* $E(\mathbb{Q}(\sqrt{5}))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$*. Moreover, the torsion subgroup of the quadratic twist* E^5 *is* $E^5(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times Z/2\mathbb{Z}$*. Then*

by Theorem 5.10 it follows that,

$$\#\widetilde{E}(\mathbb{F}_p) \equiv \begin{cases} 0 \mod 16 & \text{if} \quad p \equiv 1,4 \mod 5 \\ 0,8 \mod 16 & \text{if} \quad p \equiv 2,3 \mod 5 \end{cases}.$$

Remark 5.56. *One may notice that* $\#\widetilde{E}(\mathbb{F}_p) \equiv 0 \mod 16$ *for primes* p *of density at least* $\frac{1}{2}$*. In addition, it follows by Theorem 3.24 that* $\#\widetilde{E}(\mathbb{F}_p) \equiv 8 \mod 16$ *for primes* p *of positive density.*

Example 5.57. *Let* $E : y^2 + xy + y = x^3 - x^2 - 3002x + 63929$ *be an elliptic curve defined over* $\mathbb{Q}$ *with* $E(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times Z/6\mathbb{Z}$ *and* $E(\mathbb{Q}(\sqrt{6}))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$*. Moreover, the torsion subgroup of the quadratic twist* E^6 *is* $E^6(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \times Z/2\mathbb{Z}$*. Then by Theorem 5.10 it follows,*

$$\#\widetilde{E}(\mathbb{F}_p) \equiv \begin{cases} 0 \mod 24 & \text{if} \quad p \equiv 1,5,19,23 \mod 24 \\ 0,12 \mod 24 & \text{if} \quad p \equiv 7,11,13,17 \mod 24 \end{cases}.$$

Remark 5.58. *One may notice that* $\#\widetilde{E}(\mathbb{F}_p) \equiv 0 \mod 24$ *for primes* p *of density at least* $\frac{1}{2}$*. Furthermore, it follows by Theorem 3.24 that* $\#\widetilde{E}(\mathbb{F}_p) \equiv 12 \mod 24$ *for primes* p *of positive density.*

BIBLIOGRAPHY

[1] G. Chiloyan and Lozano-Robeldo. A classification of isogeny-torsion graphs of Q-isogeny classes of elliptic curves. *arXiv*, 2020. doi: https://doi.org/10.48550/arXiv.2001.05616.

[2] M. Chou. Torsion of rational elliptic curves over quartic galois number fields. *Journal of Number Theory*, 160:603–628, Mar. 2016. doi: 10.1016/j.jnt.2015.09.013.

[3] J. E. Cremona. *Algorithms for Modular Elliptic Curves/ Online Edition*. Cambridge University Press, 1997. ISBN http://homepages.warwick.ac.uk/ masgaj/book/fulltext/index.html.

[4] J. D. Kim and Y. K. Park. On the elliptic curves modulo p. *Journal of Number Theory*, 128:945–953, 2008. doi: 10.1016/j.jnt.2007.04.015.

[5] M. Derickx, A. Etropolski, M. van Hoeij, J. Morrow, and D. Zureick-Brown. Sporadic Cubic Torsion. *Algebra and Number Theory*, 15:1837–1864, 2021. doi: 0.2140/ant.2021.15.1837.

[6] M. Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkorper. *Abh. Math. Sem. Univ. Hamburg*, 14:197–272, 1941. doi: https://doi.org/10.1007/BF02940746.

[7] B. Edixhoven, A. D. Groot, and J. Top. Elliptic Curves over the Rationals with bad reduction at only one prime. *Mathematics of Computation*, 54:413–419, 1990. doi: 10.1090/S0025-5718-1990-0995209-4.

[8] E. Gonzalez-Jimenez and J. M. Tornero. Torsion of rational elliptic curves over quadratic fields. *Revista de la Real Academia de Ciencias Exactas, Fisicas y Naturales. Serie A. Matematicas. 108*, 2:923–934, 2014. doi: https://doi.org/10.1007/s13398-013-0152-4.

[9] E. Gonzalez-Jimenez and J. M. Tornero. Torsion of rational elliptic curves over quadratic fields II. *Serie A. Matemática RACSAM, 110*, 1:121–143, 2016. doi: https://doi.org/10.48550/arXiv.1411.3468.

[10] T. Hadano. Elliptic Curves with a rational point of finite order. *Manuscripta Mathematica*, 39:49–79, 1982. doi: https://link.springer.com/content/pdf/10.1007/BF01312445.pdf.

[11] G. H. Hardy and J. E. Littlewood. Some problems of partitio numberorum III. *Acta Math.*, 44:1–70, 1923. doi: 10.1007/BF02403921.

[12] L. Illusie. Miscellany on traces in ℓ-adic cohomology: a survey. *Japan J. Math.*, 1:107–136, 2006. doi: https://doi.org/10.1007/s11537-006-0504-3.

[13] F. Jarvis. *Algebraic Number Theory*. Springer, 2014. ISBN 978-3-319-07544-0.

[14] D. Jeon, C. H. Kim, and E.Park. On the torsion of elliptic curves over quartic number fields. *Journal of the London Mathematical Society*, 74(01):1–12, Aug. 2006. doi: 10.1112/s0024610706022940.

[15] Q. Ji and H. Qin. CM elliptic curves and primes captured by quadratic polynomials. *ASIAN J. MATH.*, 18:707–726, 2014. doi: 1415284984.pdf.

[16] N. M. Katz. Galois Properties of Torsion Points on abelian varieties. *Inventiones mathematicae*, 62(3):481–502, 1981. doi: https://link.springer.com/content/pdf/10.1007/BF01394256.pdf.

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

[18] D. S. Kubert. Universal bounds on the torsion of elliptic curves. *Proc. London Math. Soc.*, 3:193–237, 1976. URL http://www.numdam.org/item/CM_1979__38_1_121_0/.

[19] S. Lang. *Fundamentals of Diophantine Geometry*. Springer, 1983. ISBN 1475718101.

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

[21] B. Mazur and D. Goldfeld. Rational isogenies of prime degree. *Inventiones Mathematicae*, 44(2):129–162, 1978. doi: 10.1007/bf01390348.

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

[23] L. J. Mordell. On the rational solutions of the indeterminate equation of the third and fourth degrees. *Proc. Cambridge Phi/os. Soc.*, 21:179–192, 1922.

[24] F. Najman. The number of twists with large torsion of an elliptic curve. *Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Math. RACSAM*, 190:535–547, 2015. doi: https://doi.org/10.1007/s13398-014-0199-x.

[25] N.Elkies. The existence of infinitely many supersingular primes for every elliptic curve over Q. *Invent. Math.*, 89:561–568, 1987. doi: https://eudml.org/doc/143494.

[26] N.Elkies. Supersingular primes for elliptic curves over real number fields. *Compositio Math.*, 72:165–172, 1989. doi: http://www.numdam.org/item/CM_1989___72_2_165_0.pdf4.

[27] J. Oesterle. Torsion des courbes elliptiques sur les corps de nombres.

[28] A. P. Ogg. Abelian curves of small conductor. *Journal für die reine und angewandte Mathematik*, 226:204–215, 1967. doi: https://eudml.org/doc/150797.

[29] D. Qiu. On some congruence properties of elliptic curves. *Archiv der Mathematik*, 94(2):139–145, Jan. 2010. doi: 10.1007/s00013-009-0100-x. URL https://doi.org/10.1007/s00013-009-0100-x.

[30] F. P. Rabarison. Structure de torsion des courbes elliptiques sur les corps quadratiques. *Acta Arithmetica*, 144(1):17–52, 2010. doi: 10.4064/aa144-1-3.

[31] S. Schmitt and H. G. Zimmer. *Elliptic Curves*. De Gruyter, 2003. ISBN 3110168081.

[32] J. H. Silverman. *The Arithmetics of Elliptic Curves*. Springer, 1986. ISBN 978-0-387-09493-9.

[33] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer, 1994. ISBN 99783540943259.

[34] W. Waterhouse. Abelian varieties over finite fields. *Ann. Sei. École Norm. Sup.*, 4:521–560, 1969.

[35] A. Weil. L'arithmetique sur les eourbes algebriques. *Acta Math.*, 52:281–315, 1928. doi: 10.1007/bf02592688.