# TORSION STRUCTURE OF ELLIPTIC CURVES OVER SMALL NUMBER FIELDS

by
MUSTAFA UMUT KAZANCIOĞLU

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
December 2023

# ABSTRACT

TORSION STRUCTURE OF ELLIPTIC CURVES OVER SMALL NUMBER FIELDS

MUSTAFA UMUT KAZANCIOĞLU

Mathematics, Master Thesis, December 2023

Thesis Supervisor: Assoc. Prof. Mohammad Sadek

Keywords: elliptic curves, hyperelliptic curves, modular curves, torsion subgroup, cubic number fields, quartic number fields, quintic number fields, sextic number fields

Although it is well known which groups appear as torsion subgroup of an elliptic curve over a number field $K$ where $[K:\mathbb{Q}] = 1,2,3$, a similar classification is not known for number fields of higher degrees. On the other hand, it is well known which groups can arise as a torsion subgroup for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves over a number field $K$ where $[K:\mathbb{Q}] = 4,5,6$. In this thesis, we focus on the torsion subgroups of elliptic curves occurring over a fixed number field $K$ with $[K:\mathbb{Q}] = 4,5,6$. Our approach relies on analyzing the arithmetic structure of the modular curves $X_1(m,mn)$, $m \geq 1$. First, we investigate the possibility of the growth in torsion subgroups of $X_1(m,mn)$ over quartic, quintic and sextic number fields. In the case of growth in torsion, we check the new points and try to answer the following question: "Do new points give an elliptic curve with the desired torsion?". Secondly, we check the existence of torsion subgroups over cubic, quartic and quintic number fields with the smallest discriminant and having different Galois groups.

# ÖZET

KÜÇÜK SAYI CISIMLERI ÜZERINE ELIPTIK EĞRILERIN BURULMA YAPISI

MUSTAFA UMUT KAZANCIOĞLU

Matematik, Yüksek Lisans Tezi, Aralık 2023

Tez Danışmanı: Assoc. Prof. Mohammad Sadek

Anahtar Kelimeler: eliptik eğri, hipereliptik eğri, moduler eğri , burulma alt grubu, üçüncü dereceden sayı cisimleri, dördüncü dereceden sayı cismi, beşinci dereceden sayı cismi, altıncı dereceden sayı cismi

Hangi grupların $[K:\mathbb{Q}]=1,2,3$ koşulunu sağlayan $K$ sayı cismi üzerindeki bir eliptik eğrinin burulmalı alt grubu olarak ortaya çıktığı bilinmesine rağmen, daha yüksek dereceli sayı cisimleri için benzer bir sınıflandırma bilinmemektedir. Öte yandan, $[K:\mathbb{Q}]=4,5,6$ koşulunu sağlayan $K$ sayı cismi üzerindeki eliptik eğrilerin sonsuz sayıda $\overline{\mathbb{Q}}$-izomorfizm sınıfları için hangi grupların burulmalı alt grubu olarak ortaya çıkabileceği bilinmektedir. Bu tezde, $[K:\mathbb{Q}]=4,5,6$ olan sabit bir $K$ sayı cismi üzerinde oluşan eliptik eğrilerin burulmalı alt gruplarına odaklanıyoruz. Yaklaşımımız $X_1(m,mn)$, $m \geq 1$ modüler eğrilerinin aritmetik yapısını analiz etmeye dayanmaktadır. İlk olarak, derecesi 4, 5 ve 6 olan sayı cisimleri üzerinde $X_1(m,mn)$ 'in burulmalı alt gruplarında büyüme olasılığını araştırıyoruz. Burulmalı alt grubunda bir büyüme olması durumunda yeni noktaları kontrol ediyoruz ve aşağıdaki soruyu cevaplamaya çalışıyoruz: "Yeni noktalar istenen burulmalı alt gruba sahip bir eliptik eğri veriyor mu?". İkinci olarak, derecesi 3, 4 ve 5 olan sayı cisimleri üzerinde en küçük diskriminanta ve farklı Galois gruplarına sahip burulmalı alt gruplarının varlığını kontrol ediyoruz.

# ACKNOWLEDGEMENTS

I express my deep gratitude to Dr. Mohammad Sadek, my supervisor, for his invaluable guidance, encouragement, and dedication to my work. I consider myself fortunate to have a supervisor who steadily motivated me and took the time to provide me with crucial suggestions and advice.

I would also like to extend my sincere thanks to the jury members for their helpful comments and suggestions on my thesis.

My family, especially my parents and brother, have been determined in their support throughout this journey, and I am immensely grateful to them.

I would like to give my special thanks to my friend Mesut Buğday, who has been with me from the beginning of this journey. Having such a friend by my side has been a stroke of luck, and we have always encouraged each other throughout the process. Mesut, I will always cherish the time we spent working together.

Additionally, I would like to acknowledge the unwavering support of my dear friends Ezgi Öztekin, Antigona Pajaziti, Melike Efe, Burcu Barsakçı, Mohamed Osama Darwish and Mohamed Wafik El-Sheikh. Thank you for always being there to help me when I faced challenges.

Furthermore, I would like to convey my gratitude to Professor Andrew Sutherland for his assistance with the computations related to some certain modular curves.

Lastly, I am grateful for the support provided by TÜBİTAK program 1001, project number 122F312.

*Algebra is the offer made by the devil to the mathematician.*
*Michael Francis Atiyah*

# TABLE OF CONTENTS

# 1. Introduction

The celebrated theorem of Mordell-Weil asserts the set $E(K)$ of $K$-rationals points on an elliptic curve $E$ over a number field $K$ is a finitely generated abelian group. In particular, $E(K)$ can be expressed as $\mathbb{Z}^r \oplus T$ where $r \in \mathbb{Z}^{\geq 0}$ and $T$ is the torsion subgroup of $E(K)$.

The following theorem of Mazur [20], [21] classifies the possible torsion groups of elliptic curves over $\mathbb{Q}$.

**Theorem 1.0.1.** *If $K = \mathbb{Q}$, then the torsion subgroup of $E(K)$ is isomorphic to one of the* 15 *groups in the following list:*

$$\Phi(1) = \{(1,n) : 1 \leq n \leq 12, n \neq 11\} \cup \{(2,2n) : 1 \leq n \leq 4\}.$$

*The following theorem of Kenku, Momose [17] and Kamienny [16] classifies the possible torsion groups of elliptic curves over quadratic fields.*

**Theorem 1.0.2.** *Let $K$ be a quadratic field and $E$ be an elliptic curve over $K$. Then the torsion subgroup of $E(K)$ is isomorphic to one of the* 26 *groups in the following list:*

$$\Phi(2) = \{(1,n) : 1 \leq n \leq 18, n \neq 17\} \cup \{(2,2n) : 1 \leq n \leq 6\} \cup \{(3,3),(3,6),(4,4)\}.$$

*In addition, infinitely many $\overline{\mathbb{Q}}$- isomorphism classes exist for each of these torsion subgroups.*

*We also have the complete classification of torsion subgroups of elliptic curves over cubic number fields. This was recently achieved in [7].*

**Theorem 1.0.3.** *Let $K$ be a cubic field and $E$ be an elliptic curve over $K$. Then the torsion subgroup of $E(K)$ is isomorphic to one of the* 26 *groups in the following list:*

$$\Phi(3) = \{(1,n) : 1 \leq n \leq 21, n \neq 17, 19\} \cup \{(2,2n) : 1 \leq n \leq 7\}.$$

*There are infinitely many $\overline{\mathbb{Q}}$-isomorphism classes that possess each of these torsion subgroups, except for $\mathbb{Z}/21\mathbb{Z}$ where the elliptic curve* 162*b*1 *over* $\mathbb{Q}(\zeta_9)^+$ *is the unique elliptic curve with* $\mathbb{Z}/21\mathbb{Z}$*-torsion.*

*In [18], Kubert provided parametrization of elliptic curves over* $\mathbb{Q}$ *realizing a given group from Theorem 1.0.1 as a torsion subgroup. For example, consider the following modular curve* $X_1(9)$ *of genus* 0*. The general equation of the elliptic curve with torsion subgroup* $\mathbb{Z}/9\mathbb{Z}$*,[1], is the following:*

$$y^2+(s-rs+1)xy+(rs-r^2s)y=x^3+(rs-r^2s)x^2$$

*where* $r=u^2-u+1,\ s:=u$ *and* $u\in\mathbb{Q}$*.*

*Similar work was done by Rabarison in [25] for elliptic curves over quadratic number fields.*

*The work of Najman [22] on cubic number field investigated the following questions:*

*Q1: How many non-isomorphic curves does each of the groups from* $\Phi(3)$ *appear as a torsion subgroup for any fixed cubic number field* $K$*?*

*Q2: Can we check existence of all the torsion subgroups from* $\Phi(3)$ *as torsion subgroup of an elliptic curve over the number fields with smallest discriminant and having Galois group* $S_3$ *and* $\mathbb{Z}/3\mathbb{Z}$*.*

*Q3: Can we find the field with smallest discriminant field for every group from* $\Phi(3)$ *such that that group occur as a torsion subgroup of an elliptic curve?*

*For a number field* $K$*, where* $[K:\mathbb{Q}]=4,5,6,$ *we still do not have a complete classification of possible torsion subgroup of* $E(K)$*. However, the following theorems of Derickx and Sutherland [6] classifies the possible torsion groups that occur for infinitely many* $\bar{\mathbb{Q}}$*-isomorphism classes of elliptic curves defined over quartic, quintic and sextic number fields.*

**Theorem 1.0.4.** *Let* $K$ *be a quartic field and* $E$ *be an elliptic curve over* $K$*. Then the torsion subgroup of* $E(K)$ *that arise for infinitely many* $\overline{\mathbb{Q}}$*-isomorphism classes is isomorphic to one of the groups in the following list:*

$$\begin{aligned}\Phi^\infty(4)=\{(1,n):1\le n\le 24, n\ne 19,23\}\cup\{(2,2n):1\le n\le 9\}\\ \cup\{(3,3n):1\le n\le 3\}\cup\{(4,4),(4,8),(5,5),(6,6)\}.\end{aligned}$$

**Theorem 1.0.5.** *Let* $K$ *be a quintic field and* $E$ *be an elliptic curve over* $K$*. Then* *the torsion subgroup of $E(K)$ that arise for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes is isomorphic to one of the groups in the following list:*

$$\Phi^\infty(5) = \{(1,n) : 1 \leq n \leq 25, n \neq 23\} \cup \{(2,2n) : 1 \leq n \leq 8\}.$$

**Theorem 1.0.6.** *Let $K$ be a sextic field and $E$ be an elliptic curve over $K$. Then the torsion subgroup of $E(K)$ that arise for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes is isomorphic to one of the groups in the following list:*

$$\begin{aligned}\Phi^\infty(6) = \{(1,n) : 1 \leq n \leq 30, n \neq 23, 25, 29\} \cup \{(2,2n) : 1 \leq n \leq 10\} \\ \cup \{(3,3n) : 1 \leq n \leq 4\} \cup \{(4,4),(4,8),(6,6)\}.\end{aligned}$$

*In this thesis, for every possible $G \in \Phi^\infty(d)$, $d = 4,5,6$, and every number field $K$, $[K:\mathbb{Q}] = d$, we investigate whether there are infinitely many non-isomorphic elliptic curves with the torsion $G$ over $K$. For this reason we will study the possible group structure of $X_1(m,mn)$ over the number field $K$, $[K:\mathbb{Q}] = d$, for the modular curves with genus $g \leq 1$. The reason why we only look at curves with genus $g \leq 1$ is quite simple because genus 1 curves are elliptic curves and we have a group structure on them, whereas it is straight forward how to find rational points on genus 0 curves. As for the curves $C$ with genus $g > 1$, we already have $\mid C(K) \mid < \infty$ for any number field $K$, Falting's theorem, [8].*

*In order to motivate over fundings, we briefly discuss the existence of elliptic curves over quartic number field with torsion subgroup $\mathbb{Z}/15\mathbb{Z}$.*

**Example 1.0.7.** *Let $K$ be a quartic number field. Then*

$$Tors(X_1(15),K) \simeq \begin{cases} \mathbb{Z}/16\mathbb{Z} & \textit{if } K \simeq L_1 := \mathbb{Q}[x]/\langle x^4 - 7x^3 - 6x^2 + 2x + 1\rangle, \\ \mathbb{Z}/16\mathbb{Z} & \textit{if } K \simeq L_2 := \mathbb{Q}[x]/\langle x^4 + 3x^3 + 4x^2 + 2x + 1\rangle, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} & \textit{if } K \simeq L_3 := \mathbb{Q}[x]/\langle x^4 - x^2 + 4\rangle, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} & \textit{if } K \supseteq L_4 := \mathbb{Q}[x]/\langle x^2 + \frac{1}{4}x + \frac{1}{4}\rangle, \\ \mathbb{Z}/8\mathbb{Z} & \textit{if } K \supseteq L_5 := \mathbb{Q}[x]/\langle x^2 - x - 1\rangle, \\ \mathbb{Z}/8\mathbb{Z} & \textit{if } K \supseteq L_6 := \mathbb{Q}[x]/\langle x^2 + x + 1\rangle, \\ \mathbb{Z}/4\mathbb{Z} & \textit{otherwise.} \end{cases}$$

*$X_1(15)$ has rank 0 over the number fields in the above examples. This implies that we can have only finitely many elliptic curves with torsion subgroup $\mathbb{Z}/15\mathbb{Z}$ over the number fields in the above examples. It is possible to obtain positive rank over*

*the number fields that contains $L_4$, $L_5$ and $L_6$. For example, Rank$(X_1(15),L)$ is positive where $L$ is the number field generated by the polynomial $x^4+\frac{1}{2}x^3+\frac{3}{2}x^2+2x+1$,and $L$ contains the number field $L_4$. In this case, we have infinitely many elliptic curve over the number field $L$ with torsion $\mathbb{Z}/15\mathbb{Z}$.*

*In the second part of this thesis we try to answer the following question: Can we check the existence of all the torsion subgroups from $\Phi^\infty(d)$, $d=3,4,5$ as torsion subgroup of an elliptic curve over the number field with smallest discriminant and different Galois groups? We were only able to partially answer this question. For $d=3$ we did not encounter any problem, but for $d=4,5$ we could not answer the existence question in some cases. It is easier to check the existence of torsion subgroup over some number field for $d=3$ than $d=4,5$ for two reasons. The first reason is that there are fewer number fields with different Galois groups.*

*In the following tables we list the cubic and quartic number fields with different Galois group and smallest discriminant. In the table, D is the discriminant of the field, G its Galois group, and the last column is the generating polynomial of field $K_i$ where $1\le i\le 5$.*

| Field | D | G | Polynomial |
|---|---|---|---|
| $K_1$ | $-23$ | $S_3$ | $x^3-x^2+1$ |
| $K_2$ | 49 | $C_3$ | $x^3-x^2-2x+1$ |

Table 1.1 Cubic Number Fields with Smallest Discriminant

| Field | D | G | Polynomial |
|---|---|---|---|
| $K_1$ | 125 | $C_4$ | $x^4-x^3+x^2-x+1$ |
| $K_2$ | 144 | $V_4$ | $x^4-x^2+1$ |
| $K_3$ | 117 | $D_4$ | $x^4-x^3-x^2+x+1$ |
| $K_4$ | 3136 | $A_4$ | $x^4-2x^3+2x^2+2$ |
| $K_5$ | 229 | $S_4$ | $x^4-x+1$ |

Table 1.2 Quartic Number Fields with Smallest Discriminant

*The second reason is that there are fewer cases where we need to check the existence of rational points over number fields. For example we could not produce a method to check the existence of rational points over on $X_1(17)$, $X_1(21)$ and $X_1(22)$ over quartic, quintic and sextic number field, but we do not face these modular curves over cubic number number fields since $\mathbb{Z}/17\mathbb{Z}$ and $\mathbb{Z}/22\mathbb{Z}$ cannot occur as a torsion subgroups of an elliptic curve over a cubic number field and there is only one elliptic curve with torsion subgroup $\mathbb{Z}/21\mathbb{Z}$ over a cubic number field. For instance,* *the method that we used to check the existence of torsion group $\mathbb{Z}/16\mathbb{Z}$ over quartic number field did not work for the quartic number fields $K_2$ and $K_4$ but we did not encounter such a problem when we are working over cubic number fields.*

*For the torsion subgroups $T$ corresponding to modular curves with genus $\leq 1$, we are able to answer the question of the realization of the group $T$ as a torsion subgroup of elliptic curves over a fixed number field of degree $d = 4, 5$.*

*Throughout this paper, we use* MAGMA *to compute rank and torsion computations on elliptic curves.*

# 2. Elliptic Curves

## 2.1 Preliminaries

*Let $K$ be a number field. We define an elliptic curve as a non-singular abelian variety of dimension $1$ with a $K$-rational point $\mathcal{O}$ called the point at infinity. It is possible to express any elliptic curve with 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 $\mathcal{O} = (0:1:0)$.*

*In the case of $\operatorname{char} K \neq 2, 3$ we can write an elliptic in the following form,*

$$E(A,B) : y^2 = x^3 + Ax + B$$

*where $A, B \in K$.*

*Let $\Delta(E)$ be a discriminant of the elliptic curve $E$, then*

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

*where*

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2. \end{aligned}$$

*In the case $E(A,B)$, the discriminant $\Delta(E(A,B))$ is $-16(4A^3 + 27B^2)$. Since the elliptic curve $E$ is non-singular, we know that $\Delta(E) \neq 0$.*

*It is well-known that elliptic curves have a group structure and it is possible to explain the group law using a geometric description, namely the chord and tangent process.*

*In what follows, we geometrically describe the group law on $E(A,B)$.*

*Let $P_1, P_2$ be two distinct points on the elliptic curve $E$. Let* L *be the line passing through $P_1, P_2$. By Bézout Theorem we know the existence of a third intersection point between elliptic curve $E$ and line* L*. Let $P_3$ be the third intersection point. Then $P_1 \oplus P_2$ is the reflection of $P_3$ respect the $x$-axis. In case $P_1 = P_2$, the line $L$ is the tangent to $E$ at $P_1$. Since process does not affected by the order of the points, it is clear that $E$ is an abelian group.*

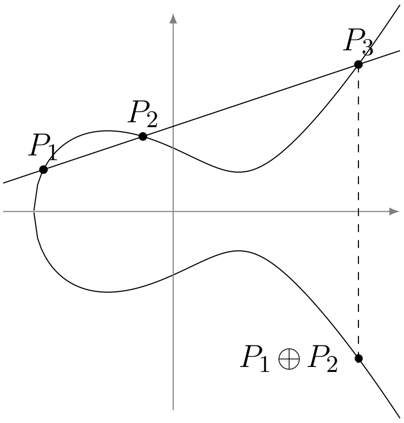

*Figure 1: $y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Q}$.*

*Let $E(K)$ be the set of $K$- rational points of $E$ defined as follow:*

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

**Remark 2.1.1.** *By definition the set $E(K)$ is a subgroup of the elliptic curve $E$ with the binary operation $\oplus$. We call $E(K)$ the Mordell-Weil group of $E$ over $K$.*

**Theorem 2.1.2** (Mordell-Weil)**.** *([28]) The group E(K) is finitely generated.*

*According to the Fundamental Theorem of Finitely Generated Abelian group, we obtain the following Corollary.*

**Corollary 2.1.3.** *There is a integer $r \geq 0$ such that*

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

*where $r$ is the rank of the group $E(K)$, $T$ is the torsion subgroup of the elliptic curve $E$ and $T$ is finite.*

## 2.2 Torsion Subgroup and Modular Curves

**Definition 2.2.1.** *Let $P = (x_n, y_n)$ be a rational point in $E(K)$. We say that $P$ is an $n$-torsion point if $nP = \mathcal{O}$.*

*To find $n$-torsion points $P$ on $E(K)$, we need division polynomials of $E$.*

*Let $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ be an elliptic curve defined over $K$. The division polynomials of $E$ are:*

$$\Psi_1 = 1,$$

$$\Psi_2 = 2y,$$

$$\Psi_3 = 3x^4 + 6ax^2 + 12bx - a^2,$$

$$\Psi_4 = 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3),$$

$$\vdots$$

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

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

*The polynomials above are defined over $\mathbb{Z}[x, y, a, b]$.*

*We call $P$ as an $n$-torsion point if and only if $P$ is the root of $n$-division polynomial of $E$.*

**Example 2.2.2.** *Let $E : y^2 = x^3 + 1$ be an elliptic curve over $\mathbb{Q}$. Then the 2-division polynomial of $E$ is $\Psi_2(x) = (x+1)(x^2 - x + 1)$. We can say that $(-1,0)$ is a point of order 2 in $E(\mathbb{Q})$, since $-1$ is a root of $\Psi_2(x)$ and $(-1,0) \in E(\mathbb{Q})$.*

*We do not have a complete classification of all torsion subgroups of an elliptic curve $E$ over any number field $K$. But if $[K : \mathbb{Q}] = 1, 2, 3$ then we have complete classification of all torsion subgroups of an elliptic curve $E$ over number field $K$. Although it is not a complete classification, It is well known such a groups can arise for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes as a torsion subgroups of an elliptic curve over a number field $K$ when $[K : \mathbb{Q}] = 4, 5, 6$. In what follows, we describe these classifications.*

**Theorem 2.2.3** (Mazur). *([20], [21]) If $K = \mathbb{Q}$, then the torsion subgroup of*

*$E(K)$ is isomorphic to one of the 15 groups in the following list:*

$$\Phi(1) = \{(1,n) : 1 \leq n \leq 12, n \neq 11\} \cup \{(2,2n) : 1 \leq n \leq 4\}.$$

**Theorem 2.2.4** (Kenku, Momose, Kamienny)**.** *([16],[17]) Let $K$ be a quadratic field and $E$ be an elliptic curve over $K$. Then the torsion subgroup of $E(K)$ is isomorphic to one of the 26 groups in the following list:*

$$\Phi(2) = \{(1,n) : 1 \leq n \leq 12, n \neq 11\} \cup \{(2,2n) : 1 \leq n \leq 6\} \cup \{(3,3),(3,6),(4,4)\}.$$

*In addition, infinitely many $\overline{\mathbb{Q}}$- isomorphism classes exist for each of these torsion subgroups.*

**Theorem 2.2.5.** *([7]) Let $K$ be a cubic field and $E$ be an elliptic curve over $K$. Then the torsion subgroup of $E(K)$ is isomorphic to one of the 26 groups in the following list:*

$$\Phi(3) = \{(1,n) : 1 \leq n \leq 21, n \neq 17,19\} \cup \{(2,2n) : 1 \leq n \leq 7\}.$$

**Theorem 2.2.6.** *([6]) Let $K$ be a quartic field and $E$ be an elliptic curve over $K$. Then the torsion subgroup of $E(K)$ that arise for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes is isomorphic to one of the groups in the following list:*

$$\begin{aligned}\Phi^{\infty}(4) = \{(1,n) : 1 \leq n \leq 24, n \neq 19,23\} \cup \{(2,2n) : 1 \leq n \leq 9\}\\ \cup \{(3,3n) : 1 \leq n \leq 3\} \cup \{(4,4),(4,8),(5,5),(6,6)\}.\end{aligned}$$

**Theorem 2.2.7.** *([6]) Let $K$ be a quintic field and $E$ be an elliptic curve over $K$. Then the torsion subgroup of $E(K)$ that arise for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes is isomorphic to one of the groups in the following list:*

$$\Phi^{\infty}(5) = \{(1,n) : 1 \leq n \leq 25, n \neq 23\} \cup \{(2,2n) : 1 \leq n \leq 8\}.$$

**Theorem 2.2.8.** *([6]) Let $K$ be a sextic field and $E$ be an elliptic curve over $K$. Then the torsion subgroup of $E(K)$ that arise for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes is isomorphic to one of the groups in the following list:*

$$\begin{aligned}\Phi^{\infty}(6) = \{(1,n) : 1 \leq n \leq 30, n \neq 23,25,29\} \cup \{(2,2n) : 1 \leq n \leq 10\}\\ \cup \{(3,3n) : 1 \leq n \leq 4\} \cup \{(4,4),(4,8),(6,6)\}.\end{aligned}$$

*Assume that the curve*

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

*has a non-trivial rational point on $K$. Then we can obtain curve*

$$E(b,c) : y^2 + (1-c)xy + by = x^3 + bx^2$$

*from $E$ and we call $E(b,c)$ an elliptic curve in Tate-Normal form. Clearly, the point $P = (0,0)$ is on the $E(b,c)$ curve.*

**Definition 2.2.9.** *Let $K$ be a number field. We define $Y_1(m,mn)$ as the affine modular curve such that its $K$-rational points determine isomorphism classes of triples $(E,P_m,P_{mn})$, where $E$ is an elliptic curve over $K$, $P_m$ and $P_{mn}$ generators of the subgroup of $E$ which is isomorphic to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mn\mathbb{Z}$.*

*In the case $m = 1$, instead of $Y_1(1,n)$, we write $Y_1(n)$. We define $X_1(m,mn)$ as a compactification of $Y_1(m,mn)$ derived by adjoining its cusps.*

*Similarly, we define $Y_0(n)$ as the affine curve whose $K$-rational points determine isomorphism classes of pairs $(E,C)$, where $E$ is an elliptic curve over $K$ and $C$ is a $n$-cycle. Analogously, $X_0(n)$ is obtained by adjoining the cusps to $Y_0(n)$.*

**Remark 2.2.10.** *For the construction of $X_1(n)$, where $4 \leq n$, we use curve $E(b,c)$. Since the point $P = (0,0)$ is on the curve $E(b,c)$, we assume $P = (0,0)$ is the torsion point and by using the group law we obtain following relation:*

- *If $n$ is even we use the relation $[n/2]P = [-n/2]P$.*
- *If $n$ is odd we use the relation $[(n+1)/2]P = [-(n-1)/2]P$.*

*Then from these relation we obtain elliptic curve $E(b,c) = [1-c,b,b,0,0]$.*

**Remark 2.2.11.** *Note that by construction the modular curve $X_1(m,mn)$ is defined over the cyclotomic field $\mathbb{Q}(\zeta_m)$, though we can have points on the equation over smaller fields, these points do not give an elliptic curve with desired torsion over smaller fields. Models of $X_1(n)$ and $X_1(m,mn)$ can be found in the website of Professor Andrew Sutherland [1].*

**Example 2.2.12.** *The modular curve*

$$X_1(13) : y^2 = x^6 - 2x^5 + x^4 - 2x^3 + 6x^2 - 4x + 1$$

*is a genus* 2 *curve. The modular curve*

$$X_1(2,10) : y^2 = x^3 + x^2 - x$$

*is a genus* 1 *curve.*

**Definition 2.2.13.** *We call point $P$ new torsion point if $P \notin Tors(X_1(m,mn)(\mathbb{Q}))$ but $P \in Tors(X_1(m,mn)(K))$ where $[K : \mathbb{Q}] \geq 2$.*

*Throughout this thesis a will be the primitive element of the given field extension.*

# 3. Torsion Structure of Elliptic Curves over Cubic Number Fields

*Throughout this thesis $f_i$ will denote a irreducible polynomial of degree $i$ and in each chapter we focus on the torsion parts occurring over a cubic, quartic, quintic and sextic number field but not over $\mathbb{Q}$. Since if a torsion occurs over $\mathbb{Q}$, it occurs over all number fields.*

*In this chapter, $K$ will be a number field with $[K:\mathbb{Q}]=3$. The results in this chapter can be found in [22].*

**Remark 3.0.1.** *If the modular curve $X_1(m,mn)$, where $m \geq 1$, $n \geq 2$, has genus $g > 1$, then by Falting's theorem, [8], $\mid X_1(m,mn)(K) \mid < \infty$ for any number field.*

**Remark 3.0.2.** *We notice that the modular curves $X_1(13)$, $X_1(16)$, $X_1(18)$, $X_1(20)$ and $X_1(2,14)$ are curves of genus 2,2,2,3 and 4, respectively.*

***Question*** *Are there infinitely many cubic points on any of the curves $X_1(m,mn)$ in Remark 3.0.2 when the genus is $g > 1$?*

*The following theorem from [14] answers this question.*

**Theorem 3.0.3.** *(a) The modular curve $X_1(N)$ has infinitely many cubic points if and only if $N = 1,...,16,18,20$.*

*(b) The modular curve $X_1(2,2N)$ has infinitely many cubic points if and only if $N = 1,...,7$.*

*We use the following lemma from [23] in this chapter.*

**Lemma 3.0.4.** *[23] Let $K$ be a number field where $[K:\mathbb{Q}]=3$. $E(K)$ can not have subgroups isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/18\mathbb{Z}$.*

*In what follows, we only consider the curves $X_1(m,mn)$ of genus 1.*

***Case 1:*** $\mathbb{Z}/11\mathbb{Z} \subseteq Tors(E,K)$.

*Consider the following modular curves*

$$X_1(11): y^2 - y = x^3 - x^2$$

*We have*

$$\mathbb{Z}/5\mathbb{Z} \simeq Tors(X_1(11), \mathbb{Q}) \subseteq Tors(X_1(11), K).$$

*By Theorem 2.2.5 $Tors(X_1(11), K)$ must be one of the following groups:*

$$\mathbb{Z}/n\mathbb{Z},\ n = 5, 10, 15, 20$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}.$$

**Theorem 3.0.5.** *Let $K$ be a cubic number field. Then*

$$Tors(X_1(11), K) \simeq \begin{cases} \mathbb{Z}/10\mathbb{Z} & \text{if } K \simeq L := \mathbb{Q}[x]/\langle x^3 - x^2 + \frac{1}{4}\rangle, \\ \mathbb{Z}/5\mathbb{Z} & \text{otherwise.} \end{cases}$$

***Proof:*** *Notice that $Tors(X_1(11), K)$ cannot be $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$, by Lemma 3.0.4.*

*The 3 and 4 division polynomial of $X_1(11)$ are*

$$\Psi_3(x) = 3x^4 - 4x^3 + 3x - 1$$

*and*

$$\Psi_4(x) = (x^3 - x^2 + \frac{1}{4})(x^6 - 2x^5 + 5x^3 - 5x^2 + 2x - \frac{1}{2}).$$

*It is easy to see that a cubic number field can not contain a root of $\Psi_3(x)$ since if it contains a root of $\Psi_3(x)$, it must also contain the number field obtained by adjoining the root of $\Psi_3(x)$, but this is not possible. Hence we can not have $\mathbb{Z}/15\mathbb{Z}$ as a torsion subgroup of $X_1(11)$ over a cubic number field.*

*In the case $\Psi_4(x)$ we can have a cubic number field containing a root of $\Psi_4(x)$. By* MAGMA *$Tors(X_1(11), L) \simeq \mathbb{Z}/10\mathbb{Z}$ where $L$ is the number field generated by $x^3 - x^2 + \frac{1}{4}$. Notice that since we cannot have a point of order 4, So, we could not obtain $\mathbb{Z}/20\mathbb{Z}$ as a torsion subgroup of $X_1(11)$ over a cubic number field.*

| Point from $X_1(11)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/11\mathbb{Z}$ |
|---|---|
| $(-2a+2, 4a^2-4a+2)$ | $y^2 + (-8a^2+6a)xy + (136a^2-192a+80)y = x^3 + (48a^2-68a+28)x^2$ |

Table 3.1 All non-isomorphic Elliptic Curves obtained from new torsion points of $X_1(11)$ over the number field generated by $x^3 - x^2 + \frac{1}{4}$

□

***Case 2:*** *$\mathbb{Z}/14\mathbb{Z} \subseteq Tors(E,K)$.*

*Consider the following modular curve*

$$X_1(14) : y^2 + xy + y = x^3 - x.$$

*We have*

$$\mathbb{Z}/6\mathbb{Z} \simeq Tors(X_1(14),\mathbb{Q}) \subseteq Tors(X_1(14),K).$$

*By Theorem 2.2.5, $Tors(X_1(14),K)$ must be one of the following groups:*

$$\mathbb{Z}/n\mathbb{Z},\ n = 6,12,18$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z},\ n = 3,6$$

**Theorem 3.0.6.** *Let $K$ be a cubic number field. Then*

$$Tors(X_1(14),K) \simeq \begin{cases} \mathbb{Z}/18\mathbb{Z} & \text{if } K \simeq L := \mathbb{Q}[x]/\langle x^3 - x^2 - 2x + 1\rangle, \\ \mathbb{Z}/6\mathbb{Z} & \text{otherwise.} \end{cases}$$

***Proof:*** *First we will show that the cases $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ are not possibly. First, notice that $(-1,0)$ is a 2-torsion point. Now we will show that there is no other 2- torsion point. By [28] if there is a 2-torsion point it must be of the form $P = (x_0,0)$. So $x$ coordinate of point $P$ must be a root of $x^2 - 1$ and $x^2 - 1$ is a degree 2 polynomial. But if a cubic field contains a root of $x^2 - 1$, then it must also contain the field generated with the polynomial $x^2 - 1$ which is degree 2. But this is not possible since $2 \nmid 3$. Thus $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ cannot occur as a torsion subgroup of $X_1(14)$ over a cubic number field.*

*The 4 division polynomial of $X_1(14)$ is*

$$\Psi_4(x) = (x+1)(x^2 - \frac{3}{4}x + \frac{1}{4})(x^2 + 2x - 1)(x^4 - \frac{3}{2}x^3 + \frac{3}{2}x^2 + \frac{1}{2}x + \frac{1}{2}).$$

*Clearly, a cubic number field cannot contain a root of $\Psi_4(x)$, so we cannot obtain $\mathbb{Z}/12\mathbb{Z}$ as a torsion subgroup of $X_1(14)$ over a cubic number field. The 9-division polynomial of $X_1(14)$ is*

$$\Psi_9(x) = x(x^3 - 2x^2 - x + 1)(x^3 + \frac{1}{3}x^2 - x + 1)f_6 f_{27}$$

*By* MAGMA*, $Tors(X_1(14),L) \simeq \mathbb{Z}/6\mathbb{Z}$ where $L$ is the number field generated by*

$x^3+\frac{1}{3}x^2-x+1$.

*By* MAGMA, *$Tors(X_1(14),L) \simeq \mathbb{Z}/18\mathbb{Z}$ where $L$ is the number field generated by $x^3-2x^2-x+1$.*

| Point from $X_1(14)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/14\mathbb{Z}$ |
|---|---|
| $(2a^2-6a+3, 6a^2-16a+6)$ | $y^2+\frac{1}{7}(4a^2-17a+15)xy+\frac{1}{7}(-4a^2+1)y = x^3+\frac{1}{7}(-4a^2+1)x^2$ |
| $(-a^2+a+2, 2a^2-3a-4)$ | $y^2+\frac{1}{7}(5a^2-2a+3)xy+\frac{1}{7}(7a^2+a-3)y = x^3+\frac{1}{7}(7a^2+a-3)x^2$ |

Table 3.2 All non-isomorphic Elliptic Curves obtained from new torsion points of $X_1(14)$ over the number field generated by $x^3-2x^2-x+1$

□

**Remark 3.0.7.** *By* MAGMA, *$Rank(X_1(14),L)$ is positive where $L$ is the number field generated by $x^3+\frac{1}{3}x^2-x+1$, so we have infinitely many elliptic curve over the number field $L$ with torsion $\mathbb{Z}/14\mathbb{Z}$.*

***Case 3:*** $\mathbb{Z}/15\mathbb{Z} \subseteq Tors(E,K)$.

*Consider the following modular curve*

$$X_1(15): y^2+xy+y = x^3+x^2.$$

*We have*

$$\mathbb{Z}/4\mathbb{Z} \simeq Tors(X_1(15),\mathbb{Q}) \subseteq Tors(X_1(15),K).$$

*By Theorem 2.2.5, $Tors(X_1(15),K)$ must be one of the following groups:*

$$\mathbb{Z}/n\mathbb{Z},\ n = 4,8,12,16,20$$

$$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2n\mathbb{Z},\ n = 2,4,6$$

**Theorem 3.0.8.** *Let $K$ be a cubic number field. Then*

$$Tors(X_1(15),K) \simeq \mathbb{Z}/4\mathbb{Z}.$$

***Proof:*** *The cases $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$ are not possible like in previous case. Just notice that there is no 2-torsion point other than $(-1,0)$.*

*The* 3*-division polynomial of* $X_1(15)$ *is*

$$\Psi_3(x) = 3x^4 + 5x^3 + 3x^2 + 3x + 1.$$

*It is clear that a cubic number field can not contain a root of* $\Psi_3(x)$ *since a cubic number field cannot contain quartic number field Hence we can not obtain* $\mathbb{Z}/12\mathbb{Z}$ *as a torsion subgroup of* $X_1(15)$ *over a cubic number field.*

*The* 5*-division polynomial of* $X_1(15)$ *is*

$$\Psi_5(x) = 5x^{12} + 25x^{11} + 56x^{10} + 145x^9 + 330x^8 + 480x^7 + 435x^6 + 249x^5 + 90x^4 \\ + 10x^3 - 10x^2 - 5x - 1$$

*Similarly, a cubic number field can not contain a root of degree* 12 *irreducible polynomial. Thus we cannot have* $\mathbb{Z}/20\mathbb{Z}$ *as a torsion subgroup of* $X_1(15)$ *over a cubic number field.*

*The* 8*-division polynomial of* $X_1(15)$ *is*

$$\Psi_8(x) = x(x+1)(x+2)(x^2 - x - 1)(x^2 + \frac{1}{4}x + \frac{1}{4})(x^2 + x + 1)f_4^{(1)} f_4^{(2)} f_{16}.$$

*It is clear that a cubic number field cannot contain a root of degree* 2*,* 4 *and* 16 *irreducible polynomial.*

*So, we cannot obtain a point of order* 8 *over a cubic number field. Thus* $\mathbb{Z}/8\mathbb{Z}$ *and* $\mathbb{Z}/16\mathbb{Z}$ *cannot occur as a torsion subgroup of* $X_1(15)$ *over a cubic number field. Hence*

$$Tors(X_1(15), K) = \mathbb{Z}/4\mathbb{Z}.$$

□

***Case 4:*** $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \subseteq Tors(E,K)$.

*Consider the following modular curve*

$$X_1(2,10) : y^2 = x^3 + x^2 - x = x(x^2 + x - 1) = xf(x).$$

*We have*

$$\mathbb{Z}/6\mathbb{Z} \simeq Tors(X_1(2,10), \mathbb{Q}) \subseteq Tors(X_1(2,10), K).$$

*By Theorem 2.2.5,* $Tors(X_1(2,10), K)$ *must be one of the following groups:*

$$\mathbb{Z}/n\mathbb{Z},\ n = 6, 12, 18$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z},\ n = 3, 6$$

**Theorem 3.0.9.** *Let $K$ be a cubic number field. Then*

$$Tors(X_1(2,10), K) \simeq \mathbb{Z}/6\mathbb{Z}.$$

***Proof:*** *The groups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ cannot occur as subgroup of $X_1(2,10)$ over cubic number field, like in previous cases. Just notice that there is no 2-torsion point other than $(0,0)$.*

*If we can have $\mathbb{Z}/12\mathbb{Z}$, this means that we have a point of order 4. So it must be half of the point of order 2. By the duplication formula from [28] we get*

$$x^4 + 2x^2 + 1 = (x^2+1)^2 = 0.$$

*So if we have a point of order 4, $x$-coordinate of that point must be root of $x^2+1$, but clearly a cubic number field cannot contain a root of degree 2 irreducible polynomial. Hence, $\mathbb{Z}/12\mathbb{Z}$ cannot occur as torsion subgroup of $X_1(2,10)$ over a cubic number field.*

*The 9-division polynomial of $X_1(2,10)$ is*

$$\Psi_9(x) = (x-1)(3x^3 + 7x^2 + x + 1) f_9 f_{27}.$$

*By* MAGMA*, $Tors(X_1(2,10), L) \simeq \mathbb{Z}/6\mathbb{Z}$ where $L$ is the number field generated by the polynomial $3x^3 + 7x^2 + x + 1$. So it is not possible to obtain $\mathbb{Z}/18\mathbb{Z}$ as a torsion subgroup of $X_1(2,10)$ over a cubic number field.*

*Thus*

$$Tors(X_1(2,10), K) = \mathbb{Z}/6\mathbb{Z}.$$

□

***Case 5:*** $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \subseteq Tors(E,K)$.

*Consider the following modular curve*

$$X_1(2,12) : y^2 = x^3 - x^2 + x = x(x^2 - x + 1) = xf(x).$$

*We have*

$$\mathbb{Z}/4\mathbb{Z} \simeq Tors(X_1(2,12), \mathbb{Q}) \subseteq Tors(X_1(2,12), K).$$

*By Theorem 2.2.5, $Tors(X_1(2,12), K)$ must be one of the following groups:*

$$\mathbb{Z}/n\mathbb{Z},\ n=4,8,12,16,20$$

$$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2n\mathbb{Z},\ n=2,4,6$$

**Theorem 3.0.10.** *Let $K$ be a cubic number field. Then*

$$Tors(X_1(2,12),K)\simeq\mathbb{Z}/4\mathbb{Z}.$$

***Proof:*** *We cannot have $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$ as a torsion subgroup of $X_1(2,12)$ over cubic number field, like in previous cases since we can not get a 2-torsion point over any cubic number field other than $(0,0)$.*

*The 3-division polynomial of $X_1(2,12)$ is*

$$\Psi_3(x)=3x^4-4x^3+6x^2-1.$$

*Clearly, a cubic number field cannot contain a root of degree 4 irreducible polynomial. So, we cannot obtain $\mathbb{Z}/12\mathbb{Z}$ as a torsion subgroup of $X_1(2,12)$ over a cubic number field.*

*The 5-division polynomial of $X_1(2,12)$ is*

$$\Psi_5(x)=5x^{12}-20x^{11}+78x^{10}-80x^9-105x^8+360x^7-540x^6+432x^5-285x^4+140x^3\\-50x^2+1$$

*Similarly, a cubic number field cannot contain a root of $\Psi_5(x)$, which is degree 12 irreducible polynomial. Hence $\mathbb{Z}/20\mathbb{Z}$ cannot occur as a torsion subgroup of $X_1(2,12)$ over a cubic number field.*

*The 8-division polynomial of $X_1(2,12)$ is*

$$\Psi_8(x)=f_{16}(x^4+4x^3-6x^2+4x+1)(x^4-2x^3+6x^2-2x+1)(x^2-x+1)(x^2-4x+1)\\(x^2+1)(x-1)(x+1)x.$$

*Obviously, a cubic number field can not contain any root of the irreducible polynomial of degree 2,4 and 16, since cubic number fields cannot contain a field of degree 2, 4, or 16. So, we cannot have a point of order of 8. Hence we cannot obtain $\mathbb{Z}/8\mathbb{Z}$ and $\mathbb{Z}/16\mathbb{Z}$ as a torsion subgroup of $X_1(2,12)$ over a cubic number field. Thus*

$$Tors(X_1(2,12),K)=\mathbb{Z}/4\mathbb{Z}.$$

□

# 4. Torsion Structure of Elliptic Curves over Quartic Number Fields

*In this chapter, $K$ will be a number field with $[K:\mathbb{Q}]=4$.*

**Remark 4.0.1.** *If the modular curve $X_1(m,mn)$ where, $m \geq 1$ and $n \geq 2$, has genus $g>1$, then by Falting's theorem ,[8], $|X_1(m,mn)(K)| < \infty$ for any number field.*

**Remark 4.0.2.** *Notice that the modular curves $X_1(13)$, $X_1(16)$, $X_1(17)$, $X_1(18)$ $X_1(20)$, $X_1(21)$, $X_1(22)$, $X_1(24)$, $X_1(2,14)$, $X_1(2,16)$ and $X_1(2,18)$ are curves of genus 2, 2, 5, 2, 3, 5, 6, 5, 4, 5 and 7, respectively.*

*By Theorem 2.2.6, there are infinitely many quartic points on any of the curves $X_1(m,mn)$, see Remark 4.0.2.*

*In what follows, we only consider the curves $X_1(m,mn)$ when $g \leq 1$.*

***Case 1:*** *$\mathbb{Z}/11\mathbb{Z} \subseteq Tors(E,K)$.*

*Consider the following modular curve*

$$X_1(11): y^2 - y = x^3 - x^2$$

*We have*

$$\mathbb{Z}/5\mathbb{Z} \simeq Tors(X_1(11),\mathbb{Q}) \subseteq Tors(X_1(11),K).$$

*By Theorem 2.2.6, $Tors(X_1(11),K)$ must be one of the following groups:*

$$\mathbb{Z}/n\mathbb{Z},\ n = 5,10,15,20$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$$

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

**Theorem 4.0.3.** *Let $K$ be a quartic number field. Then*

$$Tors(X_1(11),K) \simeq \mathbb{Z}/5\mathbb{Z}.$$

***Proof:*** *The* 2*-division polynomial of* $X_1(11)$ *is*

$$\Psi_2(x) = 4x^3 - 4x^2 + 1.$$

*Clearly, a quartic number field cannot contain a root of degree* 3 *irreducible polynomial. So, groups* $\mathbb{Z}/10\mathbb{Z}$*,* $\mathbb{Z}/20\mathbb{Z}$ *and* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ *cannot seen as a torsion group of* $X_1(11)$ *over a quartic number field.*

*The* 3*-division polynomial of* $X_1(11)$ *is*

$$\Psi_3(x) = 3x^4 - 4x^3 + 3x - 1.$$

*By* MAGMA*,* $Tors(X_1(11), L) \simeq \mathbb{Z}/5\mathbb{Z}$ *where* $L$ *is the number field generated by* $\Psi_3(x)$*. Hence, we cannot obtain* $\mathbb{Z}/15\mathbb{Z}$ *over a quartic number field as torsion group of* $X_1(11)$*.*

*Therefore, we are left the possibly that* $Tors(X_1(11), K) \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$*, see Theorem 2.2.6.*

*The* 5*-division polynomial of* $X_1(11)$ *is*

$$\Psi_5(x) = x(x-1)f_{10}.$$

*If there is a new* 5*-torsion point, then the* $x$*-coordinate of the point must be a root of* $f_{10}$*. But a root of* $f_{10}$ *cannot be contained in a quartic number field.*

*Hence*

$$Tors(X_1(11), K) \simeq \mathbb{Z}/5\mathbb{Z}.$$

□

**Remark 4.0.4.** *By* MAGMA*,* $Rank(X_1(11), L)$ *is positive where* $L$ *is the number field generated by* $3x^4 - 4x^3 + 3x - 1$*. So, we have infinitely many elliptic curve over the number field* $L$ *with torsion* $\mathbb{Z}/11\mathbb{Z}$*.*

***Case 2:*** $\mathbb{Z}/14\mathbb{Z} \subseteq Tors(E, K)$*.*

*Consider the following modular curve*

$$X_1(14) : y^2 + xy + y = x^3 - x.$$

*We have*

$$\mathbb{Z}/6\mathbb{Z} \simeq Tors(X_1(14), \mathbb{Q}) \subseteq Tors(X_1(14), K).$$

*By Theorem 2.2.6,* $Tors(X_1(14), K)$ *must be one of the following groups:*

$$\mathbb{Z}/n\mathbb{Z},\ n = 6, 12, 18, 24$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z},\ n = 3, 6, 9$$

$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$$

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

**Theorem 4.0.5.** *Let $K$ be a quartic number field. Then*

$$Tors(X_1(14), K) \simeq \begin{cases} \mathbb{Z}/12\mathbb{Z} & \textit{if } K \simeq M := \mathbb{Q}[x]/\langle x^4 - 4x^3 - 1\rangle, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} & \textit{if } K \supseteq L := \mathbb{Q}[x]/\langle x^2 - \frac{3}{4}x + \frac{1}{4}\rangle, \\ \mathbb{Z}/6\mathbb{Z} & \textit{otherwise.} \end{cases}$$

***Proof:*** *The* 2*-division polynomial of $X_1(14)$ is*

$$\Psi_2(x) = (x+1)\left(x^2 - \frac{3}{4}x + \frac{1}{4}\right).$$

$(-1, 0)$ *is a* 2*-torsion point on the curve. If there is another* 2*-torsion point on the curve then the $x$-coordinate of that point must be a root of the polynomial* $x^2 - \frac{3}{4}x + \frac{1}{4}$*. By* MAGMA*, we obtain that $Tors(X_1(14), L) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ where $L$ is the number field generated by the polynomial* $x^2 - \frac{3}{4}x + \frac{1}{4}$*.*

| Point from $X_1(14)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/14\mathbb{Z}$ |
|---|---|
| $(\frac{-4a+3}{4}, \frac{4a-7}{8})$ | $y^2 + \frac{2a+15}{14}xy + \frac{a+1}{14}y = x^3 + \frac{a+1}{14}x^2$ |
| $(a, \frac{-a-1}{2})$ | $y^2 + \frac{-4a+33}{28}xy + \frac{-4a+7}{56}y = x^3 + \frac{-4a+7}{56}x^2$ |

Table 4.1 All non-isomorphic Elliptic Curves obtained from new torsion points of $X_1(14)$ over the number field generated by $x^2 - \frac{3}{4}x + \frac{1}{4}$

*The* 12*-division polynomial of $X_1(14)$ is*

$$\Psi_{12}(x) = x(x-1)(x+1)\left(x^2 - \frac{3}{4}x + \frac{1}{4}\right)(x^2+x+2)(x^2+2x-1)(x^4-4x^3-1) \left(x^4 - \frac{3}{2}x^3 + \frac{3}{2}x^2 + \frac{1}{2}x + \frac{1}{2}\right) f_3^{(1)} f_3^{(2)} f_6 f_8 f_{12} f_{24}.$$

*First notice that the fields generated by* $x^2 - \frac{3}{4}x + \frac{1}{4}$ *and* $x^2 + x + 2$ *are isomorphic.*

*By* MAGMA*, $Tors(X_1(14), L) \simeq \mathbb{Z}/6\mathbb{Z}$ where $L$ is the number field generated by the polynomial* $x^2 + 2x - 1$*.*

*By* MAGMA*, $Tors(X_1(14), L) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ where $L$ is the number field generated by the polynomial* $x^4 - \frac{3}{2}x^3 + \frac{3}{2}x^2 + \frac{1}{2}x + \frac{1}{2}$ *but it is easy to see that the* *field generated by the polynomial $x^2 - \frac{3}{4}x + \frac{1}{4}$ is contained in the field generated by the polynomial $x^4 - \frac{3}{2}x^3 + \frac{3}{2}x^2 + \frac{1}{2}x + \frac{1}{2}$.*

| Point from $X_1(14)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/14\mathbb{Z}$ |
|---|---|
| $(\frac{1}{2}(-2a^3+5a^2-4a-1), -2)$ | $y^2 + \frac{1}{7}(-4a^3+10a^2-8a+7)xy + \frac{1}{7}(-2a^3+5a^2-4a+1)y = x^3 + \frac{1}{7}(-2a^3+5a^2-4a+1)x^2$ |

Table 4.2 All non-isomorphic Elliptic Curves obtained from new torsion points of $X_1(14)$ over the number field generated by $x^4 - \frac{3}{2}x^3 + \frac{3}{2}x^2 + \frac{1}{2}x + \frac{1}{2}$

*In this case the point $(\frac{1}{8}(-2a^3+5a^2-4a+3), \frac{1}{16}(2a^3-5a^2+4a-11))$ gives rise to the elliptic curve*

$$y^2 + \frac{1}{56}(2a^3-5a^2+4a+63)xy + \frac{1}{112}(2a^3-5a^2+4a+11)y = x^3 + \frac{1}{112}(2a^3-5a^2+4a+11)x^2$$

*with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$ over the number field generated by $x^4 - \frac{3}{2}x^3 + \frac{3}{2}x^2 + \frac{1}{2}x + \frac{1}{2}$.*

*By* MAGMA, *$Tors(X_1(14), L) \simeq \mathbb{Z}/12\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^4 - 4x^3 - 1$.*

| Point from $X_1(14)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/14\mathbb{Z}$ |
|---|---|
| $(\frac{1}{2}(-a^3+5a^2-5a+3), \frac{1}{2}(-3a^3+13a^2-5a+3))$ | $y^2 + \frac{1}{7}(-4a^3+18a^2-9a+15)xy + \frac{1}{14}(3a^3-14a^2+11a-4)y = x^3 + \frac{1}{14}(3a^3-14a^2+11a-4)x^2$ |
| $(\frac{1}{2}(-a^3+5a^2-3a-3), \frac{1}{2}(3a^3-11a^2-5a+1))$ | $y^2 + \frac{1}{14}(-17a^3+59a^2+37a+13)xy + \frac{1}{14}(5a^3-20a^2-3a+8)y = x^3 + \frac{1}{14}(5a^3-20a^2-3a+8)x^2$ |

Table 4.3 All non-isomorphic Elliptic Curves obtained from new torsion points of $X_1(14)$ over the number field generated by $x^4 - 4x^3 - 1$

*Notice that we cannot have the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ as torsion subgroup of $X_1(14)$ over quartic number field. Since we already examined $\Psi_{12}(x)$ for all possible torsion subgroup over quartic number field.*

*The 9-division polynomial of $X_1(14)$ is*

$$\Psi_9(x) = x(x^3 - 2x^2 - x + 1)\left(x^3 + \frac{1}{3}x^2 - x + 1\right) f_6 f_{27}$$

*Clearly, a quartic number field cannot contain a root of irreducible polynomial of degree 3, 6 and 27. So, the groups $\mathbb{Z}/18\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$ cannot occur as a torsion group of $X_1(14)$ over a quartic number field.*

*The* 24*-division polynomial of* $X_1(14)$ *is*

$$\Psi_{24}(x) = x(x-1)(x+1)\left(x^2 - \frac{3}{4}x + \frac{1}{4}\right)(x^2+x+2)(x^2+2x-1)(x^4-4x^3-1)$$
$$\left(x^4 - \frac{3}{2}x^3 + \frac{3}{2}x^2 + \frac{1}{2}x + \frac{1}{2}\right) f_3^{(1)} f_3^{(2)} f_6 f_8^{(1)} f_8^{(2)} f_{12} f_{16}^{(1)} f_{16}^{(2)} f_{24} f_{32} f_{48} f_{96}.$$

*We cannot have the group* $\mathbb{Z}/24\mathbb{Z}$ *over a quartic number field as a torsion group of* $X_1(14)$*, since the roots which can be in a quartic number fields does not give a point of order* 24*. We already did necessary calculations when we are working on* $\Psi_{12}(x)$*.*

*The* 3*-division polynomial of* $X_1(14)$ *is*

$$\Psi_3(x) = x\left(x^3 + \frac{1}{3}x^2 - x + 1\right).$$

*If there is a another* 3*-torsion point then the* $x$*-coordinate of the point must be the root of the polynomial* $x^3 + \frac{1}{3}x^2 - x + 1$*, however a quartic number field cannot contain a root of a degree* 3 *irreducible polynomial. So, we cannot see* $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ *and* $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ *as torsion subgroup of* $X_1(14)$ *over a quartic number field.* □

**Remark 4.0.6.** *By* MAGMA*,* $Rank(X_1(14), L)$ *is positive where* $L$ *is the number field generated by the polynomial* $x^4 - \frac{3}{2}x^3 + \frac{3}{2}x^2 + \frac{1}{2}x + \frac{1}{2}$*, so we have infinitely many elliptic curve over the number field* $L$ *with torsion* $\mathbb{Z}/14\mathbb{Z}$*.*

***Case 3:*** $\mathbb{Z}/15\mathbb{Z} \subseteq Tors(E, K)$.

*Consider the following modular curve*

$$X_1(15) : y^2 + xy + y = x^3 + x^2.$$

*We have*

$$\mathbb{Z}/4\mathbb{Z} \simeq Tors(X_1(15), \mathbb{Q}) \subseteq Tors(X_1(15), K).$$

*By Theorem 2.2.6,* $Tors(X_1(15), K)$ *must be one of the following groups:*

$$\mathbb{Z}/n\mathbb{Z},\ n = 4, 8, 12, 16, 20, 24$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z},\ n = 2, 4, 6, 8$$

$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4n\mathbb{Z},\ n = 1, 2$$

**Theorem 4.0.7.** *Let $K$ be a quartic number field. Then*

$$Tors(X_1(15),K) \simeq \begin{cases} \mathbb{Z}/16\mathbb{Z} & \text{if } K \simeq L_1 := \mathbb{Q}[x]/\langle x^4-7x^3-6x^2+2x+1\rangle, \\ \mathbb{Z}/16\mathbb{Z} & \text{if } K \simeq L_2 := \mathbb{Q}[x]/\langle x^4+3x^3+4x^2+2x+1\rangle, \\ \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z} & \text{if } K \simeq L_3 := \mathbb{Q}[x]/\langle x^4-x^2+4\rangle, \\ \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z} & \text{if } K \supseteq L_4 := \mathbb{Q}[x]/\langle x^2+\frac{1}{4}x+\frac{1}{4}\rangle, \\ \mathbb{Z}/8\mathbb{Z} & \text{if } K \supseteq L_5 := \mathbb{Q}[x]/\langle x^2-x-1\rangle, \\ \mathbb{Z}/8\mathbb{Z} & \text{if } K \supseteq L_6 := \mathbb{Q}[x]/\langle x^2+x+1\rangle, \\ \mathbb{Z}/4\mathbb{Z} & \text{otherwise.} \end{cases}$$

***Proof:*** *The 3-division polynomial of $X_1(15)$ is*

$$\Psi_3(x) = x^4+\frac{5}{3}x^3+x^2+x+\frac{1}{3}.$$

*So, it is possible to obtain a a quartic number field that contain root of $\Psi_3(x)$. Let $L$ be the number field generated by the polynomial $x^4+\frac{5}{3}x^3+x^2+x+\frac{1}{3}$. By* MAGMA*, we have $Tors(X_1(15),L) \simeq \mathbb{Z}/4\mathbb{Z}$. So, there is no growth in torsion. Hence the groups $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/24\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$ cannot occur as a torsion group of $X_1(15)$ over a quartic number field.*

*The 5-division polynomial of $X_1(15)$ is*

$$\Psi_5(x) = x^{12}+5x^{11}+\frac{56}{5}x^{10}+29x^9+66x^8+96x^7+87x^6+\frac{249}{5}x^5+18x^4+2x^3-2x^2-x-\frac{1}{5}.$$

*Clearly, a quartic number field cannot contain a root of degree 12 irreducible polynomial. So, we cannot have a 5-torsion point over a quartic number field. Hence we cannot obtain $\mathbb{Z}/20\mathbb{Z}$ over a quartic number field as a torsion subgroup of $X_1(15)$.*

*The 8-division polynomial of $X_1(15)$ is*

$$\Psi_8(x) = x(x+1)(x+2)(x^2-x-1)\left(x^2+\frac{1}{4}x+\frac{1}{4}\right)(x^2+x+1) \left(x^4+\frac{1}{2}x^3+\frac{3}{2}x^2+2x+1\right)(x^4+8x^3+9x^2+2x+1)f_{16}.$$

*Clearly, a quartic number field cannot contain a root of degree 16 irreducible polynomial. Notice that the number fields generated by the polynomials $x^2-x-1$, $x^2+\frac{1}{4}x+\frac{1}{4}$ and $x^2+x+1$ are not isomorphic. Since a quartic number field can contain a quadratic number field we need to consider number field generated by above polynomials.*

*By* MAGMA*, $Tors(X_1(15),L) \simeq \mathbb{Z}/8\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^2-x-1$.*

| Point from $X_1(15)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/15\mathbb{Z}$ |
|---|---|
| $(a,-2a-1)$ | $y^2+\frac{(2a-1)}{2}xy+\frac{(-11a+18)}{2}y=x^3+\frac{(-11a+18)}{2}x^2$ |

Table 4.4 All non-isomorphic Elliptic Curves obtained from new torsion points of $X_1(15)$ over the number field generated by $x^2-x-1$

*By* MAGMA*, $Tors(X_1(15),L) \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^2+\frac{1}{4}x+\frac{1}{4}$.*

| Point from $X_1(15)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/15\mathbb{Z}$ |
|---|---|
| $(-2,-4a)$ | $y^2+(8a+1)xy+(24a+8)y=x^3+(24a+8)x^2$ |

Table 4.5 All non-isomorphic Elliptic Curves obtained from new torsion points of $X_1(15)$ over the number field generated by $x^2+\frac{1}{4}x+\frac{1}{4}$

*By* MAGMA*, $Tors(X_1(15),L) \simeq \mathbb{Z}/8\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^2+x+1$. But in this case, new torsion points do not give rise to an elliptic curve with torsion subgroup $\mathbb{Z}/15\mathbb{Z}$.*

*By* MAGMA*, $Tors(X_1(15),L) \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^4+\frac{1}{2}x^3+\frac{3}{2}x^2+2x+1$. But it is easy to see that the number field generated by the polynomial $x^4+\frac{1}{2}x^3+\frac{3}{2}x^2+2x+1$ contains the number field generated by the polynomial $x^2+\frac{1}{4}x+\frac{1}{4}$.*

| Point from $X_1(15)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/15\mathbb{Z}$ |
|---|---|
| $(-2,-2a^3+a^2-2a-1)$ | $y^2+(4a^3-2a^2+4a+3)xy+(12a^3-6a^2+12a+14)y=x^3+(12a^3-6a^2+12a+14)x^2$ |

Table 4.6 All non-isomorphic Elliptic Curves obtained from new torsion points of $X_1(15)$ over the number field generated by $x^4+\frac{1}{2}x^3+\frac{3}{2}x^2+2x+1$

*By* MAGMA*, $Tors(X_1(15),L) \simeq \mathbb{Z}/4\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^4+8x^3+9x^2+2x+1$. So, there is no growth in torsion in this case. But, in this case rank is positive so we have infinitely many elliptic curve over the number field $L$ with torsion $\mathbb{Z}/15\mathbb{Z}$.*

*We also need to consider the compositum of the quadratic field.*

*$L_4$ is the number field generated by $x^2+\frac{1}{4}x+\frac{1}{4}$*

*$L_5$ is the number field generated by $x^2-x-1$*

*$L_6$ is the number field generated by $x^2+x+1$*

*Let $F_{ij}$ be the compositum of the number field $L_i$ and $L_j$. Then By* MAGMA*, $F_{45}$, $F_{56}$ and $F_{46}$ are the number fields generated by $16x^4-24x^3-19x^2+21x+31$, $x^4-x^2+4$ and $16x^4+40x^3+69x^2+55x+19$, respectively. Notice that $F_{45}$, $F_{56}$ and $F_{46}$ are isomorphic to each other, so we only need to consider one of them. We will work on $F_{56}$.*

*By* MAGMA*, $Tors(X_1(15), L) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^4-x^2+4$.*

| Point from $X_1(15)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/15\mathbb{Z}$ |
|---|---|
| $(-\frac{a^2}{4}, \frac{a^2-4}{8})$ | $y^2+\frac{(7a^2+69)}{64}xy+\frac{(79a^2+93)}{2048}y = x^3+\frac{(79a^2+93)}{2048}x^2$ |
| $(\frac{a^3-3a+2}{4}, \frac{a^3-3a+2}{4})$ | $y^2+\frac{(5a^3-15a-20)}{2}xy+\frac{(47a^3-141a-210)}{2}y = x^3+\frac{(47a^3-141a-210)}{2}x^2$ |

Table 4.7 All non-isomorphic Elliptic Curves obtained from new torsion points of $X_1(15)$ over the number field generated by $x^4-x^2+4$

*The 16-division polynomial of $X_1(15)$ is*

$$\Psi_{16}(x) = x(x+1)(x+2)(x^2-x-1)\left(x^2+\frac{1}{4}x+\frac{1}{4}\right)(x^2+x+1)\left(x^4+\frac{1}{2}x^3+\frac{3}{2}x^2+2x+1\right)$$
$$(x^4+8x^3+9x^2+2x+1)(x^4-7x^3-6x^2+2x+1)(x^4+3x^3+4x^2+2x+1)f_8 f_{16}^{(1)} f_{16}^{(2)} f_{64}.$$

*The only polynomials, we need to consider are $(x^4-7x^3-6x^2+2x+1)$ and $(x^4+3x^3+4x^2+2x+1)$ since we already examined the other polynomials when we are working on $\Psi_8(x)$.*

*By* MAGMA*, $Tors(X_1(15), L) \simeq \mathbb{Z}/16\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^4-7x^3-6x^2+2x+1$.*

| Point from $X_1(15)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/15\mathbb{Z}$ |
|---|---|
| $(\frac{1}{3}(-a^3+8a^2-a-3), \frac{1}{3}(2a^3-16a^2+2a+3))$ | $y^2+\frac{1}{6}(-2a^3+16a^2-2a-9)xy+\frac{1}{6}(11a^3-88a^2+11a+87)y = x^3+\frac{1}{6}(11a^3-88a^2+11a+87)x^2$ |
| $(\frac{1}{3}(7a^3-51a^2-27a+20), \frac{1}{3}(-23a^3+168a^2+87a-73))$ | $y^2+\frac{1}{3}(106a^3-694a^2-949a-224)xy+\frac{1}{3}(-18224a^3+119150a^2+164384a+39466)y = x^3+\frac{1}{3}(-18224a^3+119150a^2+164384a+39466)x^2$ |

Table 4.8 All non-isomorphic Elliptic Curves obtained from new torsion points of $X_1(15)$ over the number field generated by $x^4-7x^3-6x^2+2x+1$

*By* MAGMA*, $Tors(X_1(15),L) \simeq \mathbb{Z}/16\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^4+3x^3+4x^2+2x+1$.*

| Point from $X_1(15)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/15\mathbb{Z}$ |
|---|---|
| $(a^3+3a^2+3a,-a^2-2a-2)$ | $y^2+(-3a^3-11a^2-16a-7)xy+(-16a^3-45a^2-50a-8)y=x^3+(-16a^3-45a^2-50a-8)x^2$ |
| $(-a^3-2a^2-a+1,-a^3-2a^2-a+1)$ | $y^2+(-10a^3-20a^2-10a-5)xy+(-94a^3-188a^2-94a-58)y=x^3+(-94a^3-188a^2-94a-58)x^2$ |

Table 4.9 All non-isomorphic Elliptic Curves obtained from new torsion points of $X_1(15)$ over the number field generated by $x^4+3x^3+4x^2+2x+1$

*The 4-division polynomial of $X_1(15)$ is*

$$\Psi_4(x) = x(x+1)(x+2)\left(x^2+\frac{1}{4}x+\frac{1}{4}\right)\left(x^4+\frac{1}{2}x^3+\frac{3}{2}x^2+2x+1\right).$$

*If $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ occur over quartic number field as a torsion subgroup of $X_1(15)$, it must occur over number fields generated by the above polynomial, but we already examined all of them and it didn't occur. So, we cannot have $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/16\mathbb{Z}$ as a torsion subgroup of $X_1(15)$ over a quartic number field.* □

**Remark 4.0.8.** *By* MAGMA*, $Rank(X_1(15),L)$ is positive where $L$ is the number field generated by the polynomial $x^4+\frac{1}{2}x^3+\frac{3}{2}x^2+2x+1$, so we have infinitely many elliptic curve over the number field $L$ with torsion $\mathbb{Z}/15\mathbb{Z}$.*

***Case 4:*** $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z}$

*Consider following modular curve*

$$X_1(2,10): y^2 = x^3+x^2-x = x(x^2+x-1).$$

*We have*

$$\mathbb{Z}/6\mathbb{Z} \simeq Tors(X_1(2,10),\mathbb{Q}) \subseteq Tors(X_1(2,10),K).$$

*By Theorem 2.2.6, $Tors(X_1(2,10),K)$ must be one of the following groups:*

$$\mathbb{Z}/n\mathbb{Z},\ n=6,12,18,24$$

$$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2n\mathbb{Z},\ n=3,6,9$$

$$\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$$

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

**Theorem 4.0.9.** *Let $K$ be a quartic number field. Then*

$$Tors(X_1(2,10),K) \simeq \begin{cases} \mathbb{Z}/12\mathbb{Z} & \text{if } K \simeq L := \mathbb{Q}[x]/\langle x^4+4x^3+6x^2-4x+1\rangle, \\ \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z} & \text{if } K \supseteq M := \mathbb{Q}[x]/\langle x^2-4x-1\rangle, \\ \mathbb{Z}/6\mathbb{Z} & \text{otherwise.} \end{cases}$$

***Proof:*** *The 9-division polynomial of $X_1(2,10)$ is*

$$\Psi_9(x) = (x-1)\left(x^3+\frac{7}{3}x^2+\frac{1}{3}x+\frac{1}{3}\right)f_9 f_{27}.$$

*But a quartic number field cannot contain any roots of $\left(x^3+\frac{7}{3}x^2+\frac{1}{3}x+\frac{1}{3}\right)$, $f_9$ and $f_{27}$. So, we cannot obtain $\mathbb{Z}/18\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/18\mathbb{Z}$ as a torsion subgroup of $X_1(2,10)$ over a quartic number field.*

*The 12- division polynomial of $X_1(2,10)$ is*

$$\Psi_{12}(x) = x(x-1)(x+1)(x^2-4x-1)(x^2+1)(x^2+x-1)(x^4+2x^3-6x^2-2x+1) \\ (x^4+4x^3+6x^2-4x+1)f_3^{(1)}f_3^{(2)}f_6f_8f_{12}f_{24}.$$

*Notice that the number fields generated by the polynomials $x^2-4x-1$ and $x^2+x-1$ are isomorphic, so it is enough to consider only one of them.*

*By* MAGMA, *$Tors(X_1(2,10),L) \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^2-4x-1$. But in this case, new torsion points do not give rise to an elliptic curve with torsion subgroup $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z}$.*

*By* MAGMA, *$Tors(X_1(2,10),L) \simeq \mathbb{Z}/6\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^2+1$.*

*By* MAGMA, *$Tors(X_1(2,10),L) \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^4+2x^3-6x^2-2x+1$. Notice that the number field generated by the polynomial $x^4+2x^3-6x^2-2x+1$ contains the number field generated by the polynomial $x^2-4x-1$. But in this case, new torsion points do not give rise to an elliptic curve with torsion subgroup $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z}$.*

*By* MAGMA, *$Tors(X_1(2,10),L) \simeq \mathbb{Z}/12\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^4+4x^3+6x^2-4x+1$.*

| Point from $X_1(2,10)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z}$ |
|---|---|
| $(a^3+4a^2+6a-4, \frac{a^3+5a^2+11a+5}{2})$ | $y^2=x^3+\frac{(-3a^3-18a^2-39a-6)}{10}x^2+\frac{(2a^3+8a^2+14a-2)}{5}x$ |

Table 4.10 All non-isomorphic Elliptic Curves obtained from new torsion points of $X_1(2,10)$ over the number field generated by $x^4+4x^3+6x^2-4x+1$

*The* $3$*-division polynomial of* $X_1(2,10)$ *is*

$$\Psi_3(x)=(x-1)\left(x^3+\frac{7}{3}x^2+\frac{1}{3}x+\frac{1}{3}\right).$$

*So if there is a new* $3$*-torsion point, its* $x$*-coordinate must be root of the polynomial* $\left(x^3+\frac{7}{3}x^2+\frac{1}{3}x+\frac{1}{3}\right)$*. But a quartic number cannot contain a root of this polynomial. Hence we cannot have groups* $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ *and* $\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ *as torsion group of* $X_1(2,10)$ *over a quartic number field.*

*The case* $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$ *cannot occur over a quartic number field since if they occur over a quartic number field then* $x$*-coordinate of the new* $2$*-torsion point must came from root of degree* $2$ *or* $4$ *polynomial which is component of* $\Psi_{12}(x)$*, but this is not possible.*

*The* $24$*- division polynomial of* $X_1(2,10)$ *is*

$$\Psi_{24}(x)=\Psi_{12}(x)f_8^{(2)}f_{16}^{(1)}f_{16}^{(2)}f_{32}f_{48}f_{96}.$$

*We notice that there is no new root can be contained in a quartic number field. So, the case* $\mathbb{Z}/24\mathbb{Z}$ *cannot occur as a torsion subgroup of an elliptic curve over a quartic number field.* □

***Case 5:*** $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$

*Consider following the modular curve*

$$X_1(2,12): y^2=x^3-x^2+x=x(x^2-x+1).$$

*We have*

$$\mathbb{Z}/4\mathbb{Z}\simeq Tors(X_1(2,12),\mathbb{Q})\subseteq Tors(X_1(2,12),K).$$

*By Theorem 2.2.6,* $Tors(X_1(2,12),K)$ *must be one of the following groups:*

$$\mathbb{Z}/n\mathbb{Z},\ n=4,8,12,16,20,24$$

$$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2n\mathbb{Z},\ n=2,4,6,8$$

$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4n\mathbb{Z},\ n = 1,2$$

**Theorem 4.0.10.** *Let $K$ be a quartic number field. Then*

$$Tors(X_1(2,12),K) \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} & \text{if } K \simeq L := \mathbb{Q}[x]/\langle x^4 - 2x^3 + 5x^2 - 4x + 1\rangle, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} & \text{if } K \supseteq M_1 := \mathbb{Q}[x]/\langle x^2 - x + 1\rangle, \\ \mathbb{Z}/8\mathbb{Z} & \text{if } K \supseteq M_2 := \mathbb{Q}[x]/\langle x^2 - 4x + 1\rangle, \\ \mathbb{Z}/8\mathbb{Z} & \text{if } K \supseteq M_3 := \mathbb{Q}[x]/\langle x^2 + 1\rangle, \\ \mathbb{Z}/4\mathbb{Z} & \text{otherwise.} \end{cases}$$

***Proof:****The 3-division polynomial of $X_1(2,12)$ is*

$$\Psi_3(x) = x^4 - \frac{4}{3}x^3 + 2x^2 - \frac{1}{3}.$$

*By* MAGMA, *$Tors(X_1(2,12),L) \simeq \mathbb{Z}/4\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^4 - \frac{4}{3}x^3 + 2x^2 - \frac{1}{3}$.*

*Since we cannot obtain a 3-torsion point, $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/24\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ cannot occur as torsion group of $X_1(2,12)$ over a quartic number field.*

*The 5-division polynomial of $X_1(2,12)$ is*

$$\Psi_5(x) = x^{12} - 4x^{11} + \frac{78}{5}x^{10} - 16x^9 - 21x^8 + 72x^7 - 108x^6 + \frac{432}{5}x^5 - 57x^4 + 28x^3 - 10x^2 + \frac{1}{5}.$$

*A quartic number field cannot contain a root of degree 12 irreducible polynomial. Hence we cannot have $\mathbb{Z}/20\mathbb{Z}$ as torsion subgroup of $X_1(2,12)$ over a quartic number field.*

*The 8-division polynomial of $X_1(2,12)$ is*

$$\Psi_8(x) = x(x-1)(x+1)(x^2-4x+1)(x^2-x+1)(x^2+1)(x^4-2x^3+6x^2-2x+1) \\ (x^4+4x^3-6x^2+4x+1)f_{16}.$$

*By* MAGMA, *$Tors(X_1(2,12),L) \simeq \mathbb{Z}/8\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^2 - 4x + 1$. But in this case, new torsion points do not give rise to an elliptic curve with torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$.*

*By* MAGMA, *$Tors(X_1(2,12),L) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^2 - x + 1$.But in this case, new torsion points do not give rise to an elliptic curve with torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$.*

*By* MAGMA, *$Tors(X_1(2,12),L) \simeq \mathbb{Z}/8\mathbb{Z}$ where $L$ is the number field generated by* *the polynomial $x^2+1$. But in this case new torsion points do not give rise to an elliptic curve with torsion subgroup $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$.*

*By* MAGMA*, $Tors(X_1(2,12),L)\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^4-2x^3+6x^2-2x+1$. But it is easy to notice that the number field generated by the polynomial $x^4-2x^3+6x^2-2x+1$ contain the number field generated by the polynomial $x^2-x+1$.*

*By* MAGMA*, $Tors(X_1(2,12),L)\simeq\mathbb{Z}/8\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^4+4x^3-6x^2+4x+1$. But it is easy to notice that the number field generated by the polynomial $x^4+4x^3-6x^2+4x+1$ contain the number field generated by the polynomial $x^2-4x+1$.*

*We also need to consider the compositum of the quadratic fields $M_1$, $M_2$ and $M_3$.*

*Let $F_{ij}$ be the compositum of the number field $M_i$ and $M_j$. Then By* MAGMA*, $F_{12}$, $F_{13}$ and $F_{23}$ are the number fields generated by $x^4-10x^3+33x^2-40x+25$, $x^4-2x^3+5x^2-4x+1$ and $x^4-8x^3+20x^2-16x+16$, respectively. Notice that $F_{12}$, $F_{13}$ and $F_{23}$ are isomorphic to each other, so we only need to consider one of them. We will work on $F_{13}$.*

*By* MAGMA*, $Tors(X_1(2,12),L)\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^4-2x^3+5x^2-4x+1$. But in this case, new torsion points do not give rise to an elliptic curve with torsion subgroup $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$. So we cannot have $\mathbb{Z}/16\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/16\mathbb{Z}$ as a torsion group of $X_1(2,12)$ over a quartic number field.*

*The 4-division polynomial of $X_1(2,12)$ is*

$$\Psi_4(x)=x(x-1)(x+1)(x^2-x+1)(x^4-2x^3+6x^2-2x+1).$$

*So we cannot have the groups $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$ as a torsion group of $X_1(2,12)$ over a quartic number field. Since if there is new 4-torsion point, its $x$-coordinate must be root of the $\Psi_4(x)$, but this is not possible. We already did necessary calculations when we are working on $\Psi_8(x)$.* □

**Remark 4.0.11.** *By* MAGMA*, $Rank(X_1(2,12),L)$ is positive where $L$ is the number field generated by the polynomial $x^4-\frac{4}{3}x^3+2x^2-\frac{1}{3}$, so we have infinitely many elliptic curve over the number field $L$ with torsion $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$.*

**Remark 4.0.12.** *For the remaining cases we do not need to consider new points over quadratic number fields since following torsions cannot occur over quadratic number field.*

***Case 6:*** $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$

*Consider following the modular curve $X_1(3,3)$ of genus $0$. The general equation of the elliptic curve with torsion subgroup $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$, [1], is the following:*

$$\mathcal{E}(3,3): y^2+((z+2)v+(1-z))xy+((z+1)v^2-zv)y = x^3$$

*where $v\in K$, $z=\zeta_3$ and $X_1(3,3)$ is defined over the field $\mathbb{Q}(\zeta_3)$. Then the discriminant is given by*

$$\Delta(3,3) = -27(-vz+v^2(1+z))^4+(-vz+v^2(1+z))^3(1-z+v(2+z))^3.$$

*Notice that $\Delta(3,3)=0$ if and only if $v=0$, $v=1$, $v=\frac{z}{1+z}$ and $v=\frac{(-1+z)^3}{(2+z)^3}$. So other than the points $(0,0)$, $(0,1)$, $(0,\frac{z}{1+z})$ and $(0,\frac{(-1+z)^3}{(2+z)^3})$, we can have an elliptic curve with torsion $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$.*

***Case 7:*** $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$

*Consider following the modular curve $X_1(3,6)$ of genus $0$. The general equation of the elliptic curve with torsion subgroup $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$, [1], is the following:*

$$\mathcal{E}(3,6): y^2+(t+2)xy+(-t(t+1))y = x^3+(-t(t+1))x^2$$

*where $t=\frac{4v^2+6v+3}{v^3}$, $v\in K$ and and $X_1(3,6)$ is defined over the field $\mathbb{Q}(\zeta_3)$. Then the discriminant is given by*

$$\begin{aligned}\Delta(3,6) = -27t^4(t+1)^4+8t^3(t+2)^3(t+1)^3+t^3\left((t+2)^2-4t(t+1)\right)^2(t+1)^3\\ -9t^3(t+2)\left((t+2)^2-4t(t+1)\right)(t+1)^3.\end{aligned}$$

*Notice that $\Delta(3,6)=0$ if and only if $v=-1$, $v=-\frac{3}{2}$, $v=\frac{1}{4}\left(-3-i\sqrt{3}\right)$, $v=\frac{1}{4}\left(-3+i\sqrt{3}\right)$, $v=\frac{1}{2}\left(-3-i\sqrt{3}\right)$ and $v=\frac{1}{2}\left(-3+i\sqrt{3}\right)$. So other than the points $(0,v)$, where $v$ is the root of $\Delta(3,6)$, we can have an elliptic curve with torsion $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$.*

***Case 8:*** $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/9\mathbb{Z}$

*Consider following the modular curve*

$$X_1(3,9): y^2+y = x^3$$

*We have*

$$\mathbb{Z}/3\mathbb{Z}\simeq Tors(X_1(3,9),\mathbb{Q})\subseteq Tors(X_1(3,9),K).$$

*By Theorem 2.2.6, $Tors(X_1(3,9),K)$ must be one of the following groups:*

$$\mathbb{Z}/n\mathbb{Z},\ n = 3,6,9,12,15,18,21,24$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z},\ n = 3,6,9$$

$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3n\mathbb{Z},\ n = 1,2,3$$

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

**Theorem 4.0.13.** *Let $K$ be a quartic number field. Then*

$$Tors(X_1(3,9),K) \simeq \begin{cases} \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & \text{if } K \supseteq L := \mathbb{Q}[x]/\langle x^2 - x + 1\rangle, \\ \mathbb{Z}/3\mathbb{Z} & \text{otherwise.} \end{cases}$$

***Proof:****The 2-division polynomial of $X_1(3,9)$ is*

$$\Psi_2(x) = x^3 + \frac{1}{4}.$$

*Clearly a quartic number field cannot contain a root of a degree 3 irreducible polynomial. So we cannot have a point of order 2. Hence the groups $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/18\mathbb{Z}$, $\mathbb{Z}/24\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ cannot occur as torsion group of $X_1(3,9)$ over a quartic number field.*

*The 5-division polynomial of $X_1(3,9)$ is*

$$\Psi_5(x) = x^{12} + 19x^9 - 3x^6 - 5x^3 - \frac{1}{5}.$$

*Clearly a quartic number field cannot contain a root of a degree 12 irreducible polynomial. So, we cannot obtain the group $\mathbb{Z}/15\mathbb{Z}$.*

*The 7-division polynomial of $X_1(3,9)$ is*

$$\Psi_7(x) = (x^6 - \frac{1}{7}x^3 + \frac{1}{7})f_{18}.$$

*Clearly a quartic number field cannot contain a root of a degree 6 and 18 irreducible polynomial. So, we cannot obtain the group $\mathbb{Z}/21\mathbb{Z}$.*

*The 9-division polynomial of $X_1(3,9)$ is*

$$\Psi_9(x) = x(x+1)(x^2 - x + 1)(x^3 - 3x^2 + 1)f_6 f_9 f_{18}.$$

*Clearly a quartic number field cannot contain a root of a degree 3, 6, 9 and 18 irreducible polynomial. So, we only need to consider the polynomial $x^2 - x + 1$. By*

MAGMA, *$Tors(X_1(3,9),L) \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^2 - x + 1$. But since we cannot have $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ as torsion group of an elliptic curve over a quadratic number field, we do not need to consider new points in the torsion. Also, we cannot obtain the groups $\mathbb{Z}/9\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ as torsion group of $X_1(3,9)$ over a quartic number field.* □

***Case 9:*** $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$

*Consider following the modular curve $X_1(4,4)$ of genus $0$.*

*The general equation of the elliptic curve with torsion subgroup $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, [1], is the following:*

$$\mathcal{E}(4,4) : y^2 + xy + (-t)y = x^3 + (-t)x^2$$

*where $t = \frac{(1-v)(v^2-2v+2)}{2v^4}$, $v \in K$ and $X_1(4,4)$ is defined over the field $\mathbb{Q}(\zeta_4)$. Then the discriminant is given by*

$$\Delta(4,4) = -27t^4 + (1-4t)^2 t^3 - 9(1-4t)t^3 + 8t^3.$$

*Notice that $\Delta(4,4) = 0$ if and only if $v = 1$, $v = 2$, $v = 1 - i$ and $v = 1 + i$. So other than the points $(0,1)$, $(0,2)$, $(0,1-i)$ and $(0,1+i)$ we can have an elliptic curve with torsion $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.*

***Case 10:*** $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$

*Consider following the modular curve*

$$X_1(4,8) : y^2 = x^3 - x.$$

*We have*

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq Tors(X_1(4,8),\mathbb{Q}) \subseteq Tors(X_1(4,8),K).$$

*By Theorem 2.2.6, $Tors(X_1(4,8),K)$ must be one of the following groups:*

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z},\ n = 1,2,3,4,5,6$$

$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4n\mathbb{Z},\ n = 1,2$$

**Theorem 4.0.14.** *Let $K$ be a quartic number field. Then*

$$Tors(X_1(4,8),K) \simeq \begin{cases} \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} & \text{if } K \simeq L := \mathbb{Q}[x]/\langle x^4 - 4x^3 + 4x^2 + 8 \rangle, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} & \text{if } K \supseteq M_1 := \mathbb{Q}[x]/\langle x^2 - 2x - 1 \rangle, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} & \text{if } K \supseteq M_2 := \mathbb{Q}[x]/\langle x^2 + 1 \rangle, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{otherwise.} \end{cases}$$

***Proof:*** *The* 3*-division polynomial of* $X_1(4,8)$ *is*

$$\Psi_3(x) = x^4 - 2x^2 - \frac{1}{3}.$$

*By* MAGMA*,* $Tors(X_1(4,8),L) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *where* $L$ *is the number field generated by the polynomial* $x^4 - 2x^2 - \frac{1}{3}$*. There is no growth in torsion.*

*So, also* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ *and* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ *cannot occur as torsion subgroup of* $X_1(4,8)$ *over a quartic number field.*

*The* 4*-division polynomial of* $X_1(4,8)$ *is*

$$\Psi_4(x) = x(x-1)(x+1)(x^2-2x-1)(x^2+1)(x^2+2x-1).$$

*First notice that the number fields generated by the polynomials* $x^2 - 2x - 1$ *and* $x^2 + 2x - 1$ *are isomorphic. So, it is enough to consider only one of them.*

*By* MAGMA*,* $Tors(X_1(4,8),L) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ *where* $L$ *is the number field generated by the polynomial* $x^2 - 2x - 1$*.*

*By* MAGMA*,* $Tors(X_1(4,8),L) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ *where* $L$ *is the number field generated by the polynomial* $x^2 + 1$*.*

*There is no quartic polynomial in* $\Psi_4(x)$ *but we also need to consider compositum of the fields generated by the polynomials* $x^2 - 2x - 1$ *and* $x^2 + 1$*.*

*Let* $M$ *be the compositum of the fields generated by the polynomials* $x^2 - 2x - 1$ *and* $x^2 + 1$*. Then* $M$ *is the number field generated by the polynomial* $x^4 - 4x^3 + 4x^2 + 8$*.*

*By* MAGMA*,* $Tors(X_1(4,8),L) \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ *where* $L$ *is the number field generated by the polynomial* $x^4 - 4x^3 + 4x^2 + 8$*. But all of the torsion points are cusps. So new torsion points do not give rise to an elliptic curve with the torsion subgroup* $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$*. (double checked)*

*The* 8*-division polynomial of* $X_1(4,8)$ *is*

$$\Psi_8(x) = \Psi_4(x) f_8^{(1)} f_8^{(2)} f_8^{(3)}.$$

*There isn't any new polynomials we need to consider in* $\Psi_8(x)$ *because we already examined all of them when we are working on* $\Psi_4(x)$*. So, the cases* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ *and* $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ *cannot occur as torsion subgroup of* $X_1(4,8)$ *over a quartic number field.*

*The 5-division polynomial of $X_1(4,8)$ is*

$$\Psi_5(x) = \left(x^4 - \frac{2}{5}x^2 + \frac{1}{5}\right) f_8.$$

*By* MAGMA, *$Tors(X_1(4,8), L) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^4 - \frac{2}{5}x^2 + \frac{1}{5}$ and all new torsion points are cusps. It is easy to see that the field generated by the polynomial $x^2 + 1$ is contained in the field generated by the polynomial $x^4 - \frac{2}{5}x^2 + \frac{1}{5}$. So we could not obtain a point of order 5. Hence, we cannot obtain $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ as torsion subgroup of $X_1(4,8)$ over a quartic number field.* □

**Remark 4.0.15.** *By* MAGMA, *$Rank(X_1(4,8), L)$ is positive where $L$ is the number field generated by the polynomial $x^4 - 2x^2 - \frac{1}{3}$, but $L$ does not contain $\zeta_4$. So, even we have a positive rank, we cannot obtain an elliptic curve with torsion $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ over $L$.*

***Case 11:*** $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$

*Consider following the modular curve $X_1(5,5)$ of genus $0$. The general equation of the elliptic curve with torsion subgroup $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, [1], is the following:*

$$\mathcal{E}(5,5) : y^2 + (1-t)xy + (-t)y = x^3 + (-t)x^2$$

*where $t = \frac{U}{V(U+1)}$ and $X_1(5,5)$ is defined over the field $\mathbb{Q}(\zeta_5)$. $U$ and $V$ are defined as following*

$$U = \frac{\frac{(2-a)v^2}{5} + \frac{(2-a)v}{5} + \frac{a+3}{5}}{v+1}$$

*and*

$$V = \frac{-((a+2)v^2 + (5a+9)v + (25a+41))}{(v^3 + (-3a-2)v^2 + (2a+6)v + (5a+9))}$$

*where $a = \frac{z+1}{z}$, $z = \zeta_5$ and $v \in K,$. Then*

$$\Delta(5,5) = -27t^4 + 8(1-t)^3t^3 + \left((1-t)^2 - 4t\right)^2 t^3 - 9\left((1-t)^2 - 4t\right)(1-t)t^3.$$

*So other than the points $(0,v)$ where $v$ is the root of $\Delta(5,5)$ we can have an elliptic curve with torsion $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.*

***Case 12:*** $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$

*Consider following the modular curve*

$$X_1(6,6) : y^2 = x^3 + 1.$$

*We have*

$$\mathbb{Z}/6\mathbb{Z} \simeq Tors(X_1(6,6),\mathbb{Q}) \subseteq Tors(X_1(6,6),K).$$

*By Theorem 2.2.6, $Tors(X_1(6,6),K)$ must be one of the following groups:*

$$\mathbb{Z}/n\mathbb{Z},\ n = 6,12,18,24$$

$$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2n\mathbb{Z},\ n = 3,6,9$$

$$\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$$

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

**Theorem 4.0.16.** *Let $K$ be a quartic number field. Then*

$$Tors(X_1(6,6),K) \simeq \begin{cases} \mathbb{Z}/12\mathbb{Z} & \text{if } K \simeq L := \mathbb{Q}[x]/\langle x^4-8x^3-8x-8\rangle, \\ \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z} & \text{if } K \supseteq M := \mathbb{Q}[x]/\langle x^2-x+1\rangle, \\ \mathbb{Z}/6\mathbb{Z} & \text{otherwise.} \end{cases}$$

***Proof:*** *The 2-division polynomial of $X_1(6,6)$ is*

$$\Psi_2(x) = (x+1)(x^2-x+1).$$

*By* MAGMA*, we obtain that $Tors(X_1(6,6),L) \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ where $L$ is the number field is generated by the polynomial $x^2-x+1$.*

*The 12-division polynomial of $X_1(6,6)$ is*

$$\Psi_{12}(x) = x(x-2)(x+1)(x^2-x+1)(x^2+2x-2)(x^2+2x+4)(x^4-8x^3-8x-8)$$
$$(x^4-2x^3+6x^2+4x+4)f_3^{(1)}f_3^{(2)}f_6f_8f_{12}f_{24}.$$

*First notice that the number fields generated by the polynomials $x^2-x+1$ and $x^2+2x+4$ are isomorphic and we already examined the polynomial $x^2-x+1$.*

*By* MAGMA*, $Tors(X_1(6,6),L) \simeq \mathbb{Z}/6\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^2+2x-2$.*

*By* MAGMA*, $Tors(X_1(6,6),L) \simeq \mathbb{Z}/12\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^4-8x^3-8x-8$. Since $L$ does not contain $\zeta_6$, new points from torsion do not give rise to an elliptic curve with torsion $\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$.*

*By* MAGMA*, $Tors(X_1(6,6),L) \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^4-2x^3+6x^2+4x+4$ but it is easy to see that the number field generated by the polynomial $x^4-2x^3+6x^2+4x+4$ contain the number* *field generated by the polynomial $x^2-x+1$. New points from torsion are cusps, so they do not give rise to an elliptic curve with torsion subgroup $\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$.*

*We also need to consider the compositum of the number fields generated by the polynomials $x^2-x+1$ and $x^2+2x-2$. Their compositum is the number field generated by the polynomial $x^4+2x^3-3x^2-4x+13$. We notice the number fields generated by the polynomials $x^4+2x^3-3x^2-4x+13$ and $x^4-2x^3+6x^2+4x+4$ are isomorphic.*

*Notice that we cannot have the case $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$ as torsion subgroup of $X_1(6,6)$ over quartic number field. Since we already examined $\Psi_{12}(x)$ for all possible torsion subgroup over quartic number field.*

*The $9$-division polynomial of $X_1(6,6)$ is*

$$\Psi_9(x)=x(x^3+4)f_9f_{27}.$$

*Clearly a quartic number field cannot contain a root of the polynomials $(x^3+4)$, $f_9$ and $f_{27}$. So, the groups $\mathbb{Z}/18\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/18\mathbb{Z}$ cannot occur as a torsion subgroup of $X_1(6,6)$ over a quartic number field.*

*The $24$-division polynomial of $X_1(6,6)$ is*

$$\begin{aligned}\Psi_{24}(x)=x(x-2)(x+1)(x^2-x+1)(x^2+2x-2)(x^2+2x+4)(x^4-8x^3-8x-8)\\ (x^4-2x^3+6x^2+4x+4)f_3^{(1)}f_3^{(2)}f_6f_8^{(1)}f_8^{(2)}f_{12}f_{16}^{(1)}f_{16}^{(2)}f_{24}f_{32}f_{48}f_{96}.\end{aligned}$$

*Notice that we already examined the necessary polynomials when we are working on $\Psi_{12}(x)$. So the case $\mathbb{Z}/24\mathbb{Z}$ cannot occur.*

*The $3$-division polynomial of $X_1(6,6)$ is*

$$\Psi_9(x)=x(x^3+4).$$

*If there exist a new independent $3$-torsion point, it must be root of the polynomial $x^3+4$ but a quartic number field cannot contain root of degree $3$ irreducible polynomial. So we cannot have the cases $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ as torsion subgroup of $X_1(6,6)$ over a quartic number field.* □

# 5. Torsion Structure of Elliptic Curves over Quintic Number Fields

*In this chapter, $K$ will be a number field with $[K:\mathbb{Q}]=5$.*

**Remark 5.0.1.** *If the modular curve $X_1(m,mn)$, where $m\geq 1$ and $n\geq 2$, has genus $g>1$, then by Falting's theorem, [8], $\mid X_1(m,mn)(K)\mid<\infty$ for any number field.*

**Remark 5.0.2.** *Notice that the modular curves $X_1(13)$, $X_1(16)$, $X_1(17)$, $X_1(18)$, $X_1(19)$, $X_1(20)$, $X_1(21)$, $X_1(22)$, $X_1(24)$, $X_1(25)$ $X_1(2,14)$ and $X_1(2,16)$ are curves of genus 2, 2, 5, 2, 7, 3, 5, 6, 5, 12, 4 and 5, respectively.*

*By Theorem 2.2.7, there are infinitely many quintic points on any of the curves $X_1(m,mn)$, see Remark 5.0.2.*

*In what follows, we only consider the curves $X_1(m,mn)$ when $g=1$.*

***Case 1:*** $\mathbb{Z}/11\mathbb{Z}\subseteq Tors(E,K)$.

*Consider the following modular curve*

$$X_1(11): y^2-y=x^3-x^2$$

*We have*

$$\mathbb{Z}/5\mathbb{Z}\simeq Tors(X_1(11),\mathbb{Q})\subseteq Tors(X_1(11),K).$$

*By Theorem 2.2.7, $Tors(X_1(11),K)$ must be one of the following groups:*

$$\mathbb{Z}/n\mathbb{Z},\ n=5,10,15,20$$

$$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z}$$

**Theorem 5.0.3.** *Let $K$ be a quintic number field. Then*

$$Tors(X_1(11),K)\simeq\begin{cases}\mathbb{Z}/25\mathbb{Z} & \text{if } K\simeq L:=\mathbb{Q}[x]/\langle x^5-18x^4+35x^3-16x^2-2x+1\rangle,\\ \mathbb{Z}/5\mathbb{Z} & \text{otherwise.}\end{cases}$$

***Proof:*** *The* $2$*-division polynomial of* $X_1(11)$ *is*

$$\Psi_2(x) = 4x^3 - 4x^2 + 1.$$

*It is easy to see that a quintic number field can not contain a root of* $\Psi_2(x)$ *since if it contains a root of* $\Psi_2(x)$*, it must also contain the number field obtained by adjoining the root of* $\Psi_2(x)$*, but this is not possible. Hence we cannot obtain* $\mathbb{Z}/10\mathbb{Z}$*,* $\mathbb{Z}/20\mathbb{Z}$ *and* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ *as a torsion subgroup of* $X_1(11)$ *over a quintic number field.*

*The* $3$*-division polynomial of* $X_1(11)$ *is*

$$\Psi_3(x) = 3x^4 - 4x^3 + 3x - 1.$$

*Similarly, a quintic field can not contain a root of degree* $4$ *irreducible polynomial. Hence* $\mathbb{Z}/15\mathbb{Z}$ *cannot occur as the torsion subgroup of* $X_1(11)$ *over a quintic number field.*

*Now consider* $25$*-division polynomial of* $X_1(11)$*, which are*

$$\Psi_{25}(x) = x(x-1)(x^5 - 18x^4 + 35x^3 - 16x^2 - 2x + 1)(x^5 - 7x^4 + 13x^3 - 5x^2 - 2x + 1) \\ f_{10} f_{20}^{(1)} f_{20}^{(2)} f_{250}$$

*Clearly, a quintic number field can not contain a root of irreducible polynomials* $f_{10}$*,* $f_{20}^{(1)}$*,* $f_{20}^{(2)}$ *and* $f_{250}$*.*

*Also notice that the fields generated by the polynomials*

$$x^5 - 18x^4 + 35x^3 - 16x^2 - 2x + 1,$$

$$x^5 - 7x^4 + 13x^3 - 5x^2 - 2x + 1$$

*are isomorphic. So it is enough to consider only one of them.*

*By* MAGMA*,* $Tors(X_1(11), L) \simeq \mathbb{Z}/25\mathbb{Z}$ *where* $L$ *is the number field generated by the polynomial* $x^5 - 18x^4 + 35x^3 - 16x^2 - 2x + 1$*.*

| Point from $X_1(11)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/11\mathbb{Z}$ |
|---|---|
| $(\frac{1}{11}(a^4-19a^3+50a^2-3a+3), \frac{1}{11}(10a^4-168a^3+148a^2+25a-3))$ | $y^2+\frac{1}{11}(61a^4-1017a^3+786a^2+43a-42)xy+\frac{1}{11}(9199a^4-153213a^3+115964a^2+8589a-6848)y = x^3+\frac{1}{11}(2183a^4-36363a^3+27587a^2+2037a-1629)x^2$ |
| $(\frac{1}{11}(a^4-19a^3+50a^2-3a+3), \frac{1}{11}(-10a^4+168a^3-148a^2-25a+14))$ | $y^2+\frac{1}{11}(10a^4-160a^3+22a^2+10a+4)xy+\frac{1}{11}(-3325a^4+55475a^3-43435a^2-3104a+2565)y = x^3+\frac{1}{11}(-831a^4+13888a^3-11227a^2-775a+663)x^2$ |
| $(\frac{1}{11}(15a^4-271a^3+546a^2-327a+60), \frac{1}{11}(49a^4-897a^3+1986a^2-1330a+229))$ | $y^2+\frac{1}{11}(-2401a^4+43799a^3-94630a^2+61254a-9956)xy+\frac{1}{11}(36813276a^4-671514575a^3+1450365472a^2-938692534a+152690206)y = x^3+(211054a^4-3849857a^3+8315088a^2-5381621a+875389)x^2$ |

Table 5.1 All non-isomorphic Elliptic Curves obtained from new torsion points of $X_1(11)$ over the number field generated by $x^5-18x^4+35x^3-16x^2-2x+1$

□

***Case 2:*** $\mathbb{Z}/14\mathbb{Z} \subseteq Tors(E,K)$.

*Consider the following modular curve*

$$X_1(14): y^2+xy+y = x^3-x.$$

*We have*

$$\mathbb{Z}/6\mathbb{Z} \simeq Tors(X_1(14),\mathbb{Q}) \subseteq Tors(X_1(14),K).$$

*By Theorem 2.2.7, $Tors(X_1(14),K)$ must be one of the following groups:*

$$\mathbb{Z}/n\mathbb{Z},\ n = 6,12,18,24$$

$$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2n\mathbb{Z},\ n = 3,6$$

**Theorem 5.0.4.** *Let $K$ be a quintic number field. Then*

$$Tors(X_1(14),K) \simeq \mathbb{Z}/6\mathbb{Z}.$$

***Proof:*** *We cannot obtain groups $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$ as torsion subgroup of $X_1(14)$ over a quintic number field because if there is a 2-torsion point other than $(-1,0)$ then x-coordinates of that point must be a root of polynomial $x^2-1$, but this implies that the field generated by the polynomial $x^2-1$ must be contained in a quintic number field, which is not possible.*

*The* 4*-division polynomial of* $X_1(14)$ *is*

$$\Psi_4(x) = x+1)(x^2 - \frac{3}{4}x + \frac{1}{4})(x^2+2x-1)f_4.$$

*Clearly, a quintic number field can not contain a root of degree* 2 *and* 4 *irreducible polynomials. So,* $\mathbb{Z}/12\mathbb{Z}$ *and* $\mathbb{Z}/24\mathbb{Z}$ *cannot occur as torsion subgroup of* $X_1(14)$ *over a quintic number field.*

*The* 9*-division polynomial of* $X_1(14)$ *is*

$$\Psi_9(x) = x(x^3-2x^2-x+1)(x^3+\frac{1}{3}x^2-x+1)f_6f_{27}.$$

*Clearly, a quintic number field can not contain a root of degree* 3*,* 6*, and* 27 *irreducible polynomials. So,* $\mathbb{Z}/18\mathbb{Z}$ *cannot occur as torsion subgroup of* $X_1(14)$ *over a quintic number field.*

*Hence*

$$Tors(X_1(14), K) \simeq \mathbb{Z}/6\mathbb{Z}.$$

□

***Case 3:*** $\mathbb{Z}/15\mathbb{Z} \subseteq Tors(E,K)$.

*Consider the following modular curve*

$$X_1(15) : y^2 + xy + y = x^3 + x^2.$$

*We have*

$$\mathbb{Z}/4\mathbb{Z} \simeq Tors(X_1(15), \mathbb{Q}) \subseteq Tors(X_1(15), K).$$

*By Theorem 2.2.7* $Tors(X_1(15), K)$ *must be one of the following groups:*

$$\mathbb{Z}/n\mathbb{Z},\ n = 4, 8, 12, 16, 20, 24$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z},\ n = 2, 4, 6, 8$$

**Theorem 5.0.5.** *Let* $K$ *be a quintic number field. Then*

$$Tors(X_1(15), K) \simeq \mathbb{Z}/4\mathbb{Z}.$$

***Proof:*** *The groups* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$*,* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$*,* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ *and* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$ *cannot occur as torsion group of* $X_1(15)$ *over a quintic number field. Just notice that there is no* 2*-torsion point other than* $(-1,0)$*.*

*The* 5*-division polynomial of* $X_1(15)$ *is*

$$\Psi_5(x) = 5x^{12} + 25x^{11} + 56x^{10} + 145x^9 + 330x^8 + 480x^7 + 435x^6 + 249x^5 + 90x^4 + 10x^3 - 10x^2 - 5x - 1.$$

*Surely, a quintic number field can not contain a root of a degree* 12 *irreducible polynomial. So, we cannot obtain* $\mathbb{Z}/20\mathbb{Z}$ *as a torsion subgroup of* $X_1(15)$ *over a quintic number field.*

*The* 6*-division polynomial of* $X_1(15)$ *is*

$$\Psi_6(x) = (x+1)(x^2 + \frac{1}{4}x + \frac{1}{4})f_4^{(1)} f_4^{(2)} f_8.$$

*A quintic number field cannot contain a root of degree* 2*,* 4*, and* 8 *irreducible polynomial. So,* $\mathbb{Z}/12\mathbb{Z}$ *and* $\mathbb{Z}/24\mathbb{Z}$ *cannot occur over a quintic number field as a torsion subgroup of* $X_1(15)$*.*

*The* 8*-division polynomial of* $X_1(15)$ *is*

$$\Psi_8(x) = x(x+1)(x+2)(x^2 - x - 1)(x^2 + \frac{1}{4}x + \frac{1}{4})(x^2 + x + 1)f_4^{(1)} f_4^{(2)} f_{16}.$$

*Like in previous cases a quintic number field can not contain a root of degree* 2*,* 4*, and* 16 *irreducible polynomial. As a result,* $\mathbb{Z}/8\mathbb{Z}$ *and* $\mathbb{Z}/16\mathbb{Z}$ *cannot occur over a quintic number field as a torsion subgroup of* $X_1(15)$*.*

*Hence*

$$Tors(X_1(15), K) \simeq \mathbb{Z}/4\mathbb{Z}.$$

□

***Case 4:*** $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$

*Consider following modular curve*

$$X_1(2,10) : y^2 = x^3 + x^2 - x = x(x^2 + x - 1).$$

*We have*

$$\mathbb{Z}/6\mathbb{Z} \simeq Tors(X_1(2,10), \mathbb{Q}) \subseteq Tors(X_1(2,10), K).$$

*By Theorem 2.2.7,* $Tors(X_1(2,10), K)$ *must be one of the following groups:*

$$\mathbb{Z}/n\mathbb{Z},\ n = 6, 12, 18, 24$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z},\ n = 3, 6$$

**Theorem 5.0.6.** *Let $K$ be a quintic number field. Then*

$$Tors(X_1(2,10),K) \simeq \mathbb{Z}/6\mathbb{Z}.$$

***Proof:*** *Like in previous cases we cannot have a 2-torsion point other than $(0,0)$. Hence the groups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ cannot occur as torsion subgroup of $X_1(2,10)$ over a quintic number field.*

*The 4-division polynomial of $X_1(2,10)$ is*

$$\Psi_4(x) = x(x^2+1)(x^2+x-1)(x^4+2x^3-6x^2-2x+1).$$

*Apparently, a quintic number field cannot contain a root of polynomials $(x^2+1)$, $(x^2+x-1)$, $(x^4+2x^3-6x^2-2x+1)$. Thus we cannot have $\mathbb{Z}/12\mathbb{Z}$ and $\mathbb{Z}/24\mathbb{Z}$ as torsion subgroup of $X_1(2,10)$ over a quintic number field.*

*The 9-division polynomial of $X_1(2,10)$ is*

$$(x-1)(x^3+\frac{7}{3}x^2+\frac{1}{3}x+\frac{1}{3})f_9f_{27}.$$

*A quintic number field can not contain a root of degree 3, 9, and 27 irreducible polynomials. So, $\mathbb{Z}/18\mathbb{Z}$ cannot occur over a quintic number field as a torsion subgroup of $X_1(2,10)$.*

*Therefore*

$$Tors(X_1(2,10),K) \simeq \mathbb{Z}/6\mathbb{Z}.$$

□

***Case 5:*** $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$

*Consider following the modular curve*

$$X_1(2,12) : y^2 = x^3 - x^2 + x = x(x^2-x+1).$$

*We have*

$$\mathbb{Z}/4\mathbb{Z} \simeq Tors(X_1(2,12),\mathbb{Q}) \subseteq Tors(X_1(2,12),K).$$

*By Theorem 2.2.7, $Tors(X_1(2,12),K)$ must be one of the following groups:*

$$\mathbb{Z}/n\mathbb{Z},\ n = 4,8,12,16,20,24$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z},\ n = 2,4,6,8$$

**Theorem 5.0.7.** *Let $K$ be a quintic number field. Then*

$$Tors(X_1(2,12),K) \simeq \mathbb{Z}/4\mathbb{Z}.$$

***Proof:*** *We cannot obtain $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/16\mathbb{Z}$ as torsion subgroup of $X_1(2,12)$ over a quintic number field, since there is no 2-torsion point other than $(0,0)$ as a quintic number field can not contain a field that generated by a degree 2 irreducible polynomial.*

*The 5-division polynomial of $X_1(2,12)$ is*

$$\Psi_5(x) = 5x^{12}-20x^{11}+78x^{10}-80x^9-105x^8+360x^7-540x^6+432x^5-285x^4+140x^3-50x^2+1.$$

*It is clear that a quintic number field cannot contain a root of a degree 12 irreducible polynomial. As a result, $\mathbb{Z}/20\mathbb{Z}$ cannot occur over a quintic number field as torsion subgroup of $X_1(2,12)$.*

*The 6-division polynomial of $X_1(2,12)$ is*

$$\Psi_6(x) = x(x^2-x+1)(x^4-\frac{4}{3}x^3+2x^2-\frac{1}{3})(x^4-6x^2+4x-3)f_8.$$

*Like in previous cases a quintic number field cannot contain a root of degree 2, 4, and 8 irreducible polynomials. So, $\mathbb{Z}/12\mathbb{Z}$ and $\mathbb{Z}/24\mathbb{Z}$ cannot occur as a torsion subgroup of $X_1(2,12)$ over a quintic number field.*

*The 8-division polynomial of $X_1(2,12)$ is*

$$\Psi_8(x) = x(x-1)(x+1)(x^2-4x+1)(x^2-x+1)(x^2+1)f_4^{(1)}f_4^{(2)}f_8.$$

*Precisely, a quintic number field cannot contain a root of degree 2, 4, and 16 irreducible polynomials. Hence, we cannot obtain $\mathbb{Z}/8\mathbb{Z}$ and $\mathbb{Z}/16\mathbb{Z}$ over a quintic number field as a torsion subgroup of $X_1(2,12)$.*

*Thus*

$$Tors(X_1(2,12),K) \simeq \mathbb{Z}/4\mathbb{Z}.$$

□

# 6. Torsion Structure of Elliptic Curves over Sextic Number Fields

*In this chapter, $K$ will be a number field with $[K:\mathbb{Q}]=6$.*

**Remark 6.0.1.** *If the modular curve $X_1(m,mn)$, where $m\geq 1$ and $n\geq 2$, has genus $>1$, then by Falting's theorem, [8], $\mid X_1(m,mn)(K)\mid<\infty$ for any number field.*

**Remark 6.0.2.** *Notice that the modular curves $X_1(13)$, $X_1(16)$, $X_1(17)$, $X_1(18)$, $X_1(19)$, $X_1(20)$, $X_1(21)$, $X_1(22)$, $X_1(24)$, $X_1(25)$, $X_1(26)$, $X_1(27)$, $X_1(28)$, $X_1(30)$, $X_1(2,14)$, $X_1(2,16)$, $X_1(2,18)$, $X_1(2,20)$, $X_1(3,12)$ are curves of genus 2, 2, 5, 2, 7, 3, 5, 6, 5, 12, 10, 13, 10, 9, 4, 5, 7, 9 and 3, respectively.*

*By Theorem 2.2.8, there are infinitely many sextic points on any of the curves $X_1(m,mn)$, see Remark 6.0.2.*

*In what follows, we only consider the curves $X_1(m,mn)$ when $g\leq 1$.*

***Case 1:*** $\mathbb{Z}/11\mathbb{Z}\subseteq Tors(E,K)$.

*Consider the following modular curve*

$$X_1(11): y^2-y=x^3-x^2$$

*We have*

$$\mathbb{Z}/5\mathbb{Z}\simeq Tors(X_1(11),\mathbb{Q})\subseteq Tors(X_1(11),K).$$

*By Theorem 2.2.8, $Tors(X_1(11),K)$ must be one of the following groups:*

$$\mathbb{Z}/n\mathbb{Z},\ n=5,10,15,20,30$$

$$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2n\mathbb{Z},\ n=5,10$$

**Theorem 6.0.3.** *Let $K$ be a sextic number field. Then*

$$Tors(X_1(11),K) \simeq \begin{cases} \mathbb{Z}/10\mathbb{Z} & \text{if } K \supseteq L := \mathbb{Q}[x]/\langle 4x^3-4x^2+1\rangle, \\ \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z} & \text{if } K \simeq M_1 := \mathbb{Q}[x]/\langle 16x^6-32x^4+16x^2+11\rangle, \\ \mathbb{Z}/5\mathbb{Z} & \text{otherwise.} \end{cases}$$

***Proof:*** *The 3-division polynomial of a $X_1(11)$ is*

$$\Psi_3(x) = 3x^4-4x^3+3x-1.$$

*Clearly, a sextic number field cannot contain a root of degree 4 irreducible polynomial. So we cannot have $\mathbb{Z}/15\mathbb{Z}$ and $\mathbb{Z}/30\mathbb{Z}$ as a torsion subgroup of $X_1(11)$ over sextic number field.*

*The 4-division polynomial of $X_1(11)$ is*

$$\Psi_4(x) = (4x^3-4x^2+1)(2x^6-4x^5+10x^3-10x^2+4x-1).$$

*By* MAGMA, *we obtain that $Tors(X_1(11),L) \simeq \mathbb{Z}/10\mathbb{Z}$ where $L$ is the number field generated the by the polynomial $4x^3-4x^2+1$.*

| Point from $X_1(11)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/11\mathbb{Z}$ |
|---|---|
| $(-2a+2, 4a^2-4a+2)$ | $y^2+(-8a^2+6a)xy+(136a^2-192a+80)y = x^3+(48a^2-68a+28)x^2$ |

Table 6.1 All non-isomorphic Elliptic Curves obtained from new torsion points of $X_1(11)$ over the number field generated by $4x^3-4x^2+1$

*By* MAGMA, *we obtain that $Tors(X_1(11),L) \simeq \mathbb{Z}/10\mathbb{Z}$ where $L$ is the number field generated the by the polynomial $2x^6-4x^5+10x^3-10x^2+4x-1$. Notice that the number field generated the by the polynomial $2x^6-4x^5+10x^3-10x^2+4x-1$ contains the number field generated the by the polynomial $4x^3-4x^2+1$*

| Point from $X_1(11)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/11\mathbb{Z}$ |
|---|---|
| $(\frac{1}{11}(-8a^5+7a^4+12a^3-32a^2+4a+5), \frac{1}{2})$ | $y^2+\frac{1}{44}(-48a^5+42a^4+72a^3-192a^2+24a+19)xy+\frac{1}{176}(2a^5-10a^4+8a^3+19a^2-34a+7)y = x^3+\frac{1}{88}(10a^5-17a^4-4a^3+51a^2-38a+13)x^2$ |

Table 6.2 All non-isomorphic Elliptic Curves obtained from new torsion points of $X_1(11)$ over the number field generated by $2x^6-4x^5+10x^3-10x^2+4x-1$

*We also need to consider the splitting field of $4x^3-4x^2+1$. Let $L$ be the splitting* *field of $4x^3-4x^2+1$ and we obtain that $L$ is generated by the polynomial $16x^6-32x^4+16x^2+11$.*

*By* MAGMA, *we obtain that $Tors(X_1(11),L)\simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z}$ where $L$ is the number field generated the by the polynomial $16x^6-32x^4+16x^2+11$.*

| Point from $X_1(11)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/11\mathbb{Z}$ |
|---|---|
| $(\frac{1}{19}(-12a^4+20a^2+1),\frac{1}{2})$ | $y^2+\frac{1}{76}(-72a^4+120a^2-13)xy+\frac{1}{304}(-16a^4+14a^2-5)y = x^3+\frac{1}{152}(-4a^4-6a^2+13)x^2$ |
| $(\frac{1}{38}(12a^4-20a^2-19a+18),\frac{1}{2})$ | $y^2+\frac{1}{76}(36a^4-60a^2-57a+35)xy+\frac{1}{304}(-12a^5+8a^4+20a^3-7a^2-18a-7)y = x^3+\frac{1}{304}(-24a^5+4a^4+40a^3+6a^2-17a+6)x^2$ |
| $(\frac{1}{38}(12a^4-20a^2+19a+18),\frac{1}{2})$ | $y^2+\frac{1}{76}(36a^4-60a^2+57a+35)xy+\frac{1}{304}(12a^5+8a^4-20a^3-7a^2+18a-7)y = x^3+\frac{1}{304}(24a^5+4a^4-40a^3+6a^2+17a+6)x^2$ |

Table 6.3 All non-isomorphic Elliptic Curves obtained from new torsion points of $X_1(11)$ over the number field generated by $16x^6-32x^4+16x^2+11$

*If there is a 4-torsion point, $x$-coordinate of that point must came from $\Psi_4(x)$ but we saw that roots of $\Psi_4(x)$ does not give a 4-torsion point. So we cannot have $\mathbb{Z}/20\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/20\mathbb{Z}$ as torsion subgroup of $X_1(11)$ over a sextic number field.* □

**Remark 6.0.4.** *By* MAGMA, *$Rank(X_1(11),L)$ is positive where $L$ is the number field generated the by the polynomial $2x^6-4x^5+10x^3-10x^2+4x-1$. It follows that there are infinitely many elliptic curve over the number field $L$ with torsion $\mathbb{Z}/11\mathbb{Z}$.*

***Case 2:*** $\mathbb{Z}/14\mathbb{Z}\subseteq Tors(E,K)$.

*Consider the following modular curve*

$$X_1(14): y^2+xy+y=x^3-x.$$

*We have*

$$\mathbb{Z}/6\mathbb{Z}\simeq Tors(X_1(14),\mathbb{Q})\subseteq Tors(X_1(14),K).$$

*By Theorem 2.2.8, $Tors(X_1(14),K)$ must be one of the following groups:*

$$\mathbb{Z}/n\mathbb{Z},\ n=6,12,18,24,30$$

$$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2n\mathbb{Z},\ n=3,6,9$$

$$\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3n\mathbb{Z},\ n=2,4$$

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

**Theorem 6.0.5.** *Let $K$ be a sextic number field. Then*

$$Tors(X_1(14),K)\simeq\begin{cases}\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z} & \textit{if } K\supseteq L_1:=\mathbb{Q}[x]/\langle x^2-\frac{3}{4}x+\frac{1}{4}\rangle,\\ \mathbb{Z}/18\mathbb{Z} & \textit{if } K\supseteq L_2:=\mathbb{Q}[x]/\langle x^3-9x^2-x+1\rangle,\\ \mathbb{Z}/18\mathbb{Z} & \textit{if } K\simeq M_1:=\mathbb{Q}[x]/\langle x^6+x^4+2x^3+x^2-2x+1\rangle,\\ \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/18\mathbb{Z} & \textit{if } K\simeq M_2:=\mathbb{Q}[x]/\langle 64x^6-1296x^5+7372x^4-8275x^3+3802x^2-848x+344\rangle\\ \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z} & \textit{if } K\simeq M_3:=\mathbb{Q}[x]/\langle 81x^6-504x^4+784x^2+2352\rangle,\\ \mathbb{Z}/6\mathbb{Z} & \textit{otherwise.}\end{cases}$$

***Proof:*** *The 4-division polynomial of $X_1(14)$ is*

$$\Psi_4(x)=(x+1)(x^2-\frac{3}{4}x+\frac{1}{4})(x^2+2x-1)f_4.$$

*Clearly, a sextic number field cannot contain a root of degree 4 irreducible polynomial.*

*By* MAGMA, *we obtain that $Tors(X_1(14),L)\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ where $L$ is the number field generated the by the polynomial $x^2-\frac{3}{4}x+\frac{1}{4}$.*

| Point from $X_1(14)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/14\mathbb{Z}$ |
|---|---|
| $(\frac{(-4a+3)}{4},\frac{(4a-7)}{8})$ | $y^2+\frac{(2a+15)}{14}xy+\frac{(a+1)}{14}y=\frac{(a+1)}{14}x^2$ |
| $(a,\frac{(-a-1)}{2})$ | $y^2+\frac{(-4a+33)}{28}xy+\frac{(-4a+7)}{56}y=x^3+\frac{(-4a+7)}{56}x^2$ |

Table 6.4 All non-isomorphic Elliptic Curves obtained from new torsion points of $X_1(14)$ over the number field generated by $x^2-\frac{3}{4}x+\frac{1}{4}$

*By* MAGMA, *we obtain that $Tors(X_1(14),L)\simeq\mathbb{Z}/6\mathbb{Z}$ where $L$ is the number field generated the by the polynomial $x^2+2x-1$. So, we cannot obtain a 4-torsion point. Hence we cannot obtain $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/24\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$ as torsion subgroup of $X_1(14)$ over a sextic number field.*

*The 5-division polynomial of $X_1(14)$ is*

$$\Psi_5(x)=x^{12}+x^{11}-6x^{10}+17x^9+9x^8-6x^7-10x^5+11x^4-3x^3-2x^2+x-\frac{1}{5}.$$

*Clearly, a sextic number field cannot contain a root of degree 12 irreducible polynomial. So, we cannot obtain $\mathbb{Z}/30\mathbb{Z}$ as a torsion subgroup of $X_1(14)$ over a sextic number field.*

*The* $6$*-division polynomial of* $X_1(14)$ *is*

$$\Psi_6(x) = x(x-1)(x+1)(x^2 - \frac{3}{4}x + \frac{1}{4})(x^2+x+2)(x^3+\frac{1}{3}x^2-x+1)(x^3+5x^2-x+1)$$
$$(x^6-4x^5+9x^4+6x^3-3x^2-2x+1).$$

*We already investigated the case* $x^2 - \frac{3}{4}x + \frac{1}{4}$. *Also notice that the fields generated by the polynomials* $(x^2 - \frac{3}{4}x + \frac{1}{4})$, $(x^2+x+2)$ *are isomorphic.*

*By* MAGMA, *we obtain that* $Tors(X_1(14), L) \simeq \mathbb{Z}/6\mathbb{Z}$ *where* $L$ *is the number field generated the by the polynomial* $x^3 + \frac{1}{3}x^2 - x + 1$ *Also notice that the fields generated by the polynomials* $x^3 + \frac{1}{3}x^2 - x + 1$, $x^3 + 5x^2 - x + 1$ *are isomorphic.*

*By* MAGMA, *we obtain that* $Tors(X_1(14), L) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, *where* $L$ *is the number field generated by the polynomial* $x^6 - 4x^5 + 9x^4 + 6x^3 - 3x^2 - 2x + 1$. *Also notice that the number field* $L$ *contains the number field generated by the polynomial* $x^2 - \frac{3}{4}x + \frac{1}{4}$.

| Point from $X_1(14)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/14\mathbb{Z}$ |
|---|---|
| $(\frac{1}{8}(-a^5 + 3a^4 - 5a^3 - 15a^2 - 2a + 6), \frac{1}{16}(a^5 - 3a^4 + 5a^3 + 15a^2 + 2a - 14))$ | $y^2 + \frac{1}{56}(a^5 - 3a^4 + 5a^3 + 15a^2 + 2a + 60)xy + \frac{1}{112}(a^5 - 3a^4 + 5a^3 + 15a^2 + 2a + 8)y = x^3 + \frac{1}{112}(a^5 - 3a^4 + 5a^3 + 15a^2 + 2a + 8)x^2$ |
| $(\frac{1}{2}(-a^5 + 3a^4 - 5a^3 - 15a^2 - 2a + 2), -2)$ | $y^2 + \frac{1}{7}(-2a^5 + 6a^4 - 10a^3 - 30a^2 - 4a + 13)xy + \frac{1}{7}(-a^5 + 3a^4 - 5a^3 - 15a^2 - 2a + 4)y = x^3 + \frac{1}{7}(-a^5 + 3a^4 - 5a^3 - 15a^2 - 2a + 4)x^2$ |

Table 6.5 All non-isomorphic Elliptic Curves obtained from new torsion points of $X_1(14)$ over the number field generated by $x^6 - 4x^5 + 9x^4 + 6x^3 - 3x^2 - 2x + 1$

*Now we need to consider the compositum field generatad by the polynomials* $x^2 - \frac{3}{4}x + \frac{1}{4}$ *and* $x^3 + \frac{1}{3}x^2 - x + 1$ *and also the splitting field of the polynomial* $x^3 + \frac{1}{3}x^2 - x + 1$.

*The compositum field of* $x^2 - \frac{3}{4}x + \frac{1}{4}$ *and* $x^3 + \frac{1}{3}x^2 - x + 1$ *is generated by the polynomial* $576x^6 - 912x^5 - 404x^4 + 2133x^3 - 754x^2 - 1752x + 1276$ *and it is isomorphic to the number field generated by the polynomial* $x^6 - 4x^5 + 9x^4 + 6x^3 - 3x^2 - 2x + 1$.

*The splitting field of the polynomial* $x^3 + \frac{1}{3}x^2 - x + 1$ *is generated by the polynomial* $81x^6 - 504x^4 + 784x^2 + 2352$. *By* MAGMA, *we obtain that* $Tors(X_1(14), L) \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ *where* $L$ *is the number field generated the by the polynomial* $81x^6 - 504x^4 + 784x^2 + 2352$.

| Point from $X_1(14)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/14\mathbb{Z}$ |
|---|---|
| $(\frac{1}{2436}(-243a^4+1260a^2-1316), \frac{1}{14616}(-162a^5+729a^4+3276a^3-3780a^2-10892a-3360))$ | $y^2+\frac{1}{34104}(4293a^5-1296a^4-32004a^3+11592a^2+85232a+7056)xy+\frac{1}{159152}(-7695a^5+22302a^4+60606a^3-168420a^2-166992a+466872)y = x^3+\frac{1}{159152}(-7695a^5+22302a^4+60606a^3-168420a^2-166992a+466872)x^2$ |
| $(\frac{1}{2436}(-243a^4+1260a^2-1316), \frac{1}{14616}(162a^5+729a^4-3276a^3-3780a^2+10892a-3360))$ | $y^2+\frac{1}{34104}(-4293a^5-1296a^4+32004a^3+11592a^2-85232a+7056)xy+\frac{1}{159152}(7695a^5+22302a^4-60606a^3-168420a^2+166992a+466872)y = x^3+\frac{1}{159152}(7695a^5+22302a^4-60606a^3-168420a^2+166992a+466872)x^2$ |
| $(\frac{1}{3248}(-243a^5+216a^4+1260a^3-1932a^2+1120a-2800), \frac{1}{1624}(-162a^5+567a^4-378a^3-504a^2+476a-2072))$ | $y^2+\frac{1}{11368}(432a^5-1035a^4-210a^3+1036a^2-1540a+18424)xy+\frac{1}{477456}(135a^5+3276a^4-7602a^3-13468a^2+3528a+78792)y = x^3+\frac{1}{477456}(135a^5+3276a^4-7602a^3-13468a^2+3528a+78792)x^2$ |
| $(\frac{1}{3248}(243a^5+216a^4-1260a^3-1932a^2-1120a-2800), \frac{1}{1624}(162a^5+567a^4+378a^3-504a^2-476a-2072))$ | $y^2+\frac{1}{11368}(-432a^5-1035a^4+210a^3+1036a^2+1540a+18424)xy+\frac{1}{477456}(-135a^5+3276a^4+7602a^3-13468a^2-3528a+78792)y = x^3+\frac{1}{477456}(-135a^5+3276a^4+7602a^3-13468a^2-3528a+78792)x^2$ |

Table 6.6 All non-isomorphic Elliptic Curves obtained from new torsion points of $X_1(14)$ over the number field generated by $81x^6-504x^4+784x^2+2352$

*We cannot obtain $\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ as torsion subgroup of $X_1(14)$ over a sextic number field.*

*The 18-division polynomial of $X_1(14)$ is*

$$\begin{gathered}\Psi_{18}(x) = x(x-1)(x+1)(x^2-\frac{3}{4}x+\frac{1}{4})(x^2+x+2)(x^3-9x^2-x+1)(x^3-2x^2-x+1)\\ (x^3+\frac{1}{3}x^2-x+1)(x^3+5x^2-x+1)(x^6-4x^5+9x^4+6x^3-3x^2-2x+1)\\ (x^6+x^4+2x^3+x^2-2x+1)(x^6+2x^5+11x^4+3x^2-2x+1)\\ (x^6+3x^5+2x^4-x^3+4x^2-2x+1)f_{12}f_{27}^{(1)}f_{27}^{(2)}f_{54}\end{gathered}$$

*By* MAGMA*, we obtain that $Tors(X_1(14),L)\simeq\mathbb{Z}/18\mathbb{Z}$ where $L$ is the number field generated the by the polynomial $x^3-9x^2-x+1$. Also notice that the fields generated by the polynomials $x^3-9x^2-x+1$, $x^3-2x^2-x+1$ are isomorphic.*

| Point from $X_1(14)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/14\mathbb{Z}$ |
|---|---|
| $(\frac{1}{4}(a^2-10a+5), \frac{1}{4}(-3a^2+28a-9))$ | $y^2+\frac{1}{14}(-a^2+13a+12)xy+\frac{1}{28}(a^2+6a+1)y = x^3+\frac{1}{28}(a^2+6a+1)x^2$ |
| $(\frac{1}{2}(-3a^2+26a+11), -4a^2+35a+13)$ | $y^2+\frac{1}{28}(-17a^2+144a+85)xy+\frac{1}{7}(-2a-1)y = x^3+\frac{1}{7}(-2a-1)x^2$ |

Table 6.7 All non-isomorphic Elliptic Curves obtained from new torsion points of $X_1(14)$ over the number field generated by $x^3-9x^2-x+1$

*By* MAGMA, *we obtain that* $Tors(X_1(14), L) \simeq \mathbb{Z}/18\mathbb{Z}$ *where* $L$ *is the number field generated the by the polynomial* $x^6+x^4+2x^3+x^2-2x+1$*. Also notice that the fields generated by the polynomials* $x^6+x^4+2x^3+x^2-2x+1$ *and* $x^6+2x^5+11x^4+3x^2-2x+1$ *are isomorphic.*

| Point from $X_1(14)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/14\mathbb{Z}$ |
|---|---|
| $(2a^5+a^4+2a^3+5a^2+4a-3, \frac{1}{2}(-7a^5-a^4-6a^3-14a^2-7a+15))$ | $y^2+\frac{1}{42}(-48a^5-25a^4-60a^3-122a^2-106a+93)xy+\frac{1}{42}(4a^5+2a^4+a^3+9a^2+5a-11)y = x^3+\frac{1}{42}(4a^5+2a^4+a^3+9a^2+5a-11)x^2$ |
| $(\frac{1}{2}(a^5+a^4+2a^3+2a^2+a-1), -a^5-a^2-a+1)$ | $y^2+\frac{1}{14}(5a^4+2a^3+6a+27)xy+\frac{1}{98}(-46a^5-12a^4-47a^3-107a^2-73a+97)y = x^3+\frac{1}{98}(-46a^5-12a^4-47a^3-107a^2-73a+97)x^2$ |
| $(\frac{1}{2}(-2a^5-a^4-2a^3-4a^2-4a+3), \frac{1}{2}(-a^5-a^4-2a^3-4a^2-3a-1))$ | $y^2+\frac{1}{14}(a^5+3a^4-4a^3-10a^2-a+23)xy+\frac{1}{14}(-6a^5+a^4+5a^3-3a^2-9a+8)y = x^3+\frac{1}{14}(-6a^5+a^4+5a^3-3a^2-9a+8)x^2$ |

Table 6.8 All non-isomorphic Elliptic Curves obtained from new torsion points of $X_1(14)$ over the number field generated by $x^6+x^4+2x^3+x^2-2x+1$

*In this case the point* $(a, \frac{1}{2}(a^4-1))$ *gives rise to the elliptic curve*

$$y^2+\frac{1}{7}(-a^5+a^4-4a^2+3a+7)xy+\frac{1}{98}(-a^5-10a^4+25a^3-39a^2+22a+5)y = x^3+\frac{1}{98}(-a^5-10a^4+25a^3-39a^2+22a+5)x^2$$

*with torsion* $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/14\mathbb{Z}$ *over the number field generated by* $x^6+x^4+2x^3+x^2-2x+1$.

*Again we need to consider the compositum field of the degree* 3 *and* 2 *polynomial and the splitting field of the degree* 3 *polynomial which we did not consider before.*

*Notice that the splitting field of the number field generated by the polynomial* $x^3-9x^2-x+1$ *is itself.*

*The compositum field of polynomials* $x^2 - \frac{3}{4}x + \frac{1}{4}$ *and* $x^3 - 9x^2 - x + 1$ *generatd by the polynomial* $64x^6 - 1296x^5 + 7372x^4 - 8275x^3 + 3802x^2 - 848x + 344$.

*By* MAGMA, *we obtain that* $Tors(X_1(14), L) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$ *where* $L$ *is the number field generated the by the polynomial*
$64x^6 - 1296x^5 + 7372x^4 - 8275x^3 + 3802x^2 - 848x + 344$

| Point from $X_1(14)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/14\mathbb{Z}$ |
|---|---|
| $(\frac{1}{14640836}(-399360a^5 + 7918848a^4 - 42923648a^3 + 37033728a^2 - 18681856a + 9401719), \frac{1}{29281672}(399360a^5 - 7918848a^4 + 42923648a^3 - 37033728a^2 + 18681856a - 24042555))$ | $y^2 + \frac{1}{51242926}(199680a^5 - 3959424a^4 + 21461824a^3 - 18516864a^2 + 9340928a + 55692589)xy + \frac{1}{25621463}(49920a^5 - 989856a^4 + 5365456a^3 - 4629216a^2 + 2335232a + 2027468)y = x^3 + \frac{1}{25621463}(49920a^5 - 989856a^4 + 5365456a^3 - 4629216a^2 + 2335232a + 2027468)x^2$ |
| $(\frac{1}{7320418}(209792a^5 - 3902512a^4 + 17679120a^3 + 5217645a^2 - 7567338a + 3028910), \frac{1}{3660209}(-310704a^5 + 6048280a^4 - 31351523a^3 + 18443167a^2 - 4294033a - 848048))$ | $y^2 + \frac{1}{51242926}(-1302480a^5 + 26068008a^4 - 139589749a^3 + 90414809a^2 - 15196845a + 66791476)xy + \frac{1}{102485852}(-1148880a^5 + 22378744a^4 - 114392685a^3 + 53445594a^2 - 16498374a + 14949160)y = x^3 + \frac{1}{102485852}(-1148880a^5 + 22378744a^4 - 114392685a^3 + 53445594a^2 - 16498374a + 14949160)x^2$ |
| $(\frac{1}{3660209}(-399360a^5 + 7918848a^4 - 42923648a^3 + 37033728a^2 - 18681856a + 2081301), -2)$ | $y^2 + \frac{1}{25621463}(-1597440a^5 + 31675392a^4 - 171694592a^3 + 148134912a^2 - 74727424a + 41267085)xy + \frac{1}{25621463}(-798720a^5 + 15837696a^4 - 85847296a^3 + 74067456a^2 - 37363712a + 11483020)y = x^3 + \frac{1}{25621463}(-798720a^5 + 15837696a^4 - 85847296a^3 + 74067456a^2 - 37363712a + 11483020)x^2$ |
| $(\frac{1}{14640836}(-1592512a^5 + 32285584a^4 - 184207604a^3 + 206506735a^2 - 59636178a - 7448176), \frac{1}{14640836}(991680a^5 - 20629200a^4 + 125893444a^3 - 196900555a^2 + 131178420a - 44230152))$ | $y^2 + \frac{1}{204971704}(-19638720a^5 + 403249552a^4 - 2370786532a^3 + 3116825143a^2 - 1605521436a + 469421936)xy + \frac{1}{409943408}(8679744a^5 - 170629136a^4 + 898285180a^3 - 550217883a^2 - 188995344a + 264298996)y = x^3 + \frac{1}{409943408}(8679744a^5 - 170629136a^4 + 898285180a^3 - 550217883a^2 - 188995344a + 264298996)x^2$ |
| $(\frac{1}{7320418}(-2568192a^5 + 51310416a^4 - 281244856a^3 + 243006141a^2 - 26469532a + 28636578), \frac{1}{3660209}(-3457536a^5 + 69073792a^4 - 378570112a^3 + 327094332a^2 - 35629461a + 31950180))$ | $y^2 + \frac{1}{102485852}(-14220288a^5 + 284159984a^4 - 1557951144a^3 + 1346173359a^2 - 146626498a + 246554436)xy + \frac{1}{25621463}(199680a^5 - 3959424a^4 + 21461824a^3 - 18516864a^2 + 2020510a - 2870755)y = x^3 + \frac{1}{25621463}(199680a^5 - 3959424a^4 + 21461824a^3 - 18516864a^2 + 2020510a - 2870755)x^2$ |

Table 6.9 All non-isomorphic Elliptic Curves obtained from new torsion points of $X_1(14)$ over the number field generated by $64x^6 - 1296x^5 + 7372x^4 - 8275x^3 + 3802x^2 - 848x + 344$

*In this case the point* $(\frac{1}{14640836}(989184a^5 - 19743088a^4 + 108056168a^3 - 93346623a^2 + 10170184a + 22702588), \frac{1}{14640836}(-2767872a^5 + 55269840a^4 - 302706680a^3 + 261523005a^2 - 28490042a - 45357056))$ *gives rise to the elliptic curve*

$$\begin{aligned} y^2 &+ \frac{(-1288704a^5 + 25682224a^4 - 140248904a^3 + 121121919a^2 - 13200949a + 38336784)}{51242926}xy \\ &+ \frac{(-608256a^5 + 11932304a^4 - 63638424a^3 + 54788289a^2 - 5993896a + 1746120)}{102485852}y \\ &= x^3 + \frac{(-608256a^5 + 11932304a^4 - 63638424a^3 + 54788289a^2 - 5993896a + 1746120)}{102485852}x^2 \end{aligned}$$

□

**Remark 6.0.6.** *By* MAGMA*, Rank*$(X_1(14), L)$ *is positive where L is the number field generated the by the polynomial* $x^3 + \frac{1}{3}x^2 - x + 1$*, so we have infinitely many elliptic curves over the number field L with torsion* $\mathbb{Z}/14\mathbb{Z}$*.*

**Remark 6.0.7.** *By* MAGMA*, Rank*$(X_1(14), L)$ *is positive where L is the number field generated the by the polynomial* $x^6 - 4x^5 + 9x^4 + 6x^3 - 3x^2 - 2x + 1$*, so we have infinitely many elliptic curves over the number field L with torsion* $\mathbb{Z}/14\mathbb{Z}$*.*

**Remark 6.0.8.** *By* MAGMA*, Rank*$(X_1(14), L)$ *is positive where L is the number field generated the by the polynomial* $81x^6 - 504x^4 + 784x^2 + 2352$*, so we have infinitely many elliptic curves over the number field L with torsion* $\mathbb{Z}/14\mathbb{Z}$*.*

**Remark 6.0.9.** *By* MAGMA*, Rank*$(X_1(14), L)$ *is positive where L is the number field generated the by the polynomial* $x^6 + x^4 + 2x^3 + x^2 - 2x + 1$*, so we have infinitely many elliptic curves over the number field L with torsion* $\mathbb{Z}/14\mathbb{Z}$*.*

***Case 3:*** $\mathbb{Z}/15\mathbb{Z} \subseteq Tors(E, K)$.

*Consider the following modular curve*

$$X_1(15) : y^2 + xy + y = x^3 + x^2.$$

*We have*

$$\mathbb{Z}/4\mathbb{Z} \simeq Tors(X_1(15), \mathbb{Q}) \subseteq Tors(X_1(15), K).$$

*By Theorem 2.2.8,* $Tors(X_1(15), K)$ *must be one of the following groups:*

$$\mathbb{Z}/n\mathbb{Z},\ n = 4, 8, 12, 16, 20, 24, 28$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z},\ n = 2, 4, 6, 8, 10$$

$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4n\mathbb{Z},\ n = 1, 2$$

**Theorem 6.0.10.** *Let $K$ be a sextic number field. Then*

$$Tors(X_1(15),K) \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z} & \text{if } K \supseteq L_1 := \mathbb{Q}[x]/\langle x^2+\frac{1}{4}x+\frac{1}{4}\rangle, \\ \mathbb{Z}/8\mathbb{Z} & \text{if } K \supseteq L_2 := \mathbb{Q}[x]/\langle x^2-x-1\rangle, \\ \mathbb{Z}/8\mathbb{Z} & \text{if } K \supseteq L_3 := \mathbb{Q}[x]/\langle x^2+x+1\rangle, \\ \mathbb{Z}/4\mathbb{Z} & \text{otherwise.} \end{cases}$$

***Proof:*** *The 3-division polynomial of $X_1(15)$ is*

$$\Psi_4(x) = x^4+\frac{5}{3}x^3+x^2+x+\frac{1}{3}.$$

*Clearly a sextic number field cannot contain a root of degree 4 irreducible polynomial. Hence we cannot obtain $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/24\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$ as torsion subgroup of $X_1(15)$ over a sextic number field.*

*The 5-divison polynomial of $X_1(15)$ is*

$$\Psi_5(x) = x^{12}+5x^{11}+\frac{56}{5}x^{10}+29x^9+66x^8+96x^7+87x^6+\frac{249}{5}x^5+18x^4+2x^3-2x^2-x-\frac{1}{5}.$$

*So, we cannot have $\mathbb{Z}/20\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/20\mathbb{Z}$ as torsion subgroup of $X_1(15)$ over a sextic number field.*

*The 7-divison polynomial of $X_1(15)$ is*

$$\Psi_7(x) = f_{24}.$$

*It is clear that a sextic number field cannot contaion a root of degree 24 irreducible polynomial. Hence, $\mathbb{Z}/28\mathbb{Z}$ cannot occur as torsion subgroup of $X_1(15)$ over a sextic number field.*

*The 16-divison polynomial of $X_1(15)$ is*

$$\Psi_{16}(x) = x(x+1)(x+2)(x^2-x-1)(x^2+\frac{1}{4}x+\frac{1}{4})(x^2+x+1)f_4^{(1)}f_4^{(2)}f_4^{(3)}f_4^{(4)}f_8f_{16}^{(1)}f_{16}^{(2)}f_{64}.$$

*Notice that the number fields generated by the polynomials $x^2-x-1$, $x^2+\frac{1}{4}x+\frac{1}{4}$ and $x^2+x+1$ are not isomorphic.*

*By* MAGMA, *$Tors(X_1(15),L) \simeq \mathbb{Z}/8\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^2-x-1$.*

| Point from $X_1(15)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/15\mathbb{Z}$ |
|---|---|
| $(a,-2a-1)$ | $y^2+\frac{(2a-1)}{2}xy+\frac{(-11a+18)}{2}y=x^3+\frac{(-11a+18)}{2}x^2$ |

Table 6.10 All non-isomorphic Elliptic Curves obtained from new torsion points of $X_1(15)$ over the number field generated by $x^2-x-1$

*By* MAGMA, *$Tors(X_1(15),L)\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^2+\frac{1}{4}x+\frac{1}{4}$.*

| Point from $X_1(15)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/15\mathbb{Z}$ |
|---|---|
| $(-2,-4a)$ | $y^2+(8a+1)xy+(24a+8)y=x^3+(24a+8)x^2$ |

Table 6.11 All non-isomorphic Elliptic Curves obtained from new torsion points of $X_1(15)$ over the number field generated by $x^2+\frac{1}{4}x+\frac{1}{4}$

*By* MAGMA, *$Tors(X_1(15),L)\simeq\mathbb{Z}/8\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^2+x+1$. But in this case, new torsion points do not give rise to an elliptic curve with torsion subgroup $\mathbb{Z}/15\mathbb{Z}$.*

*Hence, $\mathbb{Z}/16\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/16\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$ cannot occur as torsion subgroup of $X_1(15)$ over a sextic number field.*

□

***Case 4:*** $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z}$

*Consider following modular curve*

$$X_1(2,10): y^2=x^3+x^2-x=x(x^2+x-1).$$

*We have*

$$\mathbb{Z}/6\mathbb{Z}\simeq Tors(X_1(2,10),\mathbb{Q})\subseteq Tors(X_1(2,10),K).$$

*By Theorem 2.2.8, $Tors(X_1(2,10),K)$ must be one of the following groups:*

$$\mathbb{Z}/n\mathbb{Z},\ n=6,12,18,24,30$$

$$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2n\mathbb{Z},\ n=3,6,9$$

$$\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3n\mathbb{Z},\ n=2,4$$

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

**Theorem 6.0.11.** *Let $K$ be a sextic number field. Then*

$$Tors(X_1(2,10),K) \simeq \begin{cases} \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z} & \textit{if } K \simeq L := \mathbb{Q}[x]/\langle x^6-6x^5+55x^4-180x^3+655x^2-966x+1641\rangle, \\ \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z} & \textit{if } K \supseteq M := \mathbb{Q}[x]/\langle x^2+x-1\rangle, \\ \mathbb{Z}/6\mathbb{Z} & \textit{otherwise.} \end{cases}$$

***Proof:*** *The 5-division polynomial of $X_1(2,10)$ is*

$$\Psi_5(x) = x^{12}+4x^{11}-\frac{46}{5}x^{10}-16x^9-21x^8-72x^7+12x^6+\frac{304}{5}x^5+7xx^4-28x^3+10x^2+\frac{1}{5}.$$

*So, we cannot obtain $\mathbb{Z}/30\mathbb{Z}$ as a torsion subgroup of $X_1(2,10)$ over a sextic number field. The 4-division polynomial of $X_1(2,10)$ is*

$$\Psi_4(x) = x(x^2+1)(x^2+x-1)f_4.$$

*By* MAGMA, *$Tors(X_1(2,10),L) \simeq \mathbb{Z}/6\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^2+1$.*

*By* MAGMA, *$Tors(X_1(2,10),L) \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^2+x-1$. But new torsion points do not give rise to an elliptic curve with torsion subgroup $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z}$. So, we cannot have a point of order 4. Hence, we cannot obtain $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/24\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$ as torsion subgroup of $X_1(2,10)$ over a sextic number field.*

*The 18-division polynomial of $X_1(2,10)$ is*

$$\Psi_{18}(x) = x(x-1)(x+1)(x^2-4x-1)(x^2+x-1)(x^3-x^2+7x-3)(x^3+\frac{7}{3}x^2+\frac{1}{3}x+\frac{1}{3}) \\ (x^6+8x^5+5x^4-5x^2+8x-1)f_9^{(1)}f_9^{(2)}f_{18}f_{27}^{(1)}f_{27}^{(2)}f_{54}$$

*Notice that the number fields generated by the polynomials $x^2-4x-1$ and $x^2+x-1$ are isomorphic and we already investigated $x^2+x-1$. Also the number fields generated by the polynomials $x^3+\frac{7}{3}x^2+\frac{1}{3}x+\frac{1}{3}$ and $x^3-x^2+7x-3$ are isomorphic. So it is enough to consider just one of them.*

*By* MAGMA, *$Tors(X_1(2,10),L) \simeq \mathbb{Z}/6\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^3-x^2+7x-3$.*

*By* MAGMA, *$Tors(X_1(2,10),L) \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^6+8x^5+5x^4-5x^2+8x-1$. But in this case, new torsion points do not give rise to an elliptic curve with torsion subgroup $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z}$. Also notice that number field $L$ contains the number field generated by the polynomial $x^2+x-1$.*

*Now we need to consider that compositum field generated by the polynomials $x^2+x-1$, $x^3-x^2+7x-3$ and also splitting field of the polynomial $x^3-x^2+7x-3$.*

*The compositum field generated by the polynomials $x^2+x-1$ and $x^3-x^2+7x-3$ is isomorphic the number field generated by the polynomial $x^6+8x^5+5x^4-5x^2+8x-1$.*

*The splitting field of $x^3-x^2+7x-3$ is generated by the polynomial $x^6-6x^5+55x^4-180x^3+655x^2-966x+1641$ and By* MAGMA, *$Tors(X_1(2,10),L) \simeq \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^6-6x^5+55x^4-180x^3+655x^2-966x+1641$.*

| Point from $X_1(2,10)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z}$ |
|---|---|
| $(\frac{1}{60}(a^4-4a^3+46a^2-84a+261), \frac{1}{180}(-2a^5+10a^4-85a^3+215a^2-585a+447))$ | $y^2=x^3+\frac{1}{20}(-a^4+4a^3-29a^2+50a-124)x^2+\frac{1}{400}(43a^4-172a^3+778a^2-1212a+2163)x$ |

Table 6.12 All non-isomorphic Elliptic Curves obtained from new torsion points of $X_1(2,10)$ over the number field generated by $x^6-6x^5+55x^4-180x^3+655x^2-966x+1641$

*Hence $\mathbb{Z}/18\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/18\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ cannot occur as a torsion subgroup of $X_1(2,10)$ over a sextic number field.* □

***Case 5:*** $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$

*Consider following the modular curve*

$$X_1(2,12): y^2 = x^3-x^2+x = x(x^2-x+1).$$

*We have*

$$\mathbb{Z}/4\mathbb{Z} \simeq Tors(X_1(2,12),\mathbb{Q}) \subseteq Tors(X_1(2,12),K).$$

*By Theorem 2.2.8, $Tors(X_1(2,12),K)$ must be one of the following groups:*

$$\mathbb{Z}/n\mathbb{Z},\ n=4,8,12,16,20,24,28$$

$$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2n\mathbb{Z},\ n=2,4,6,8,10$$

$$\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4n\mathbb{Z},\ n=1,2$$

**Theorem 6.0.12.** *Let $K$ be a sextic number field. Then*

$$Tors(X_1(2,12),K) \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z} & \text{if } K \supseteq M_1 := \mathbb{Q}[x]/\langle x^2-x+1\rangle, \\ \mathbb{Z}/8\mathbb{Z} & \text{if } K \supseteq M_2 := \mathbb{Q}[x]/\langle x^2-4x+1\rangle, \\ \mathbb{Z}/8\mathbb{Z} & \text{if } K \supseteq M_3 := \mathbb{Q}[x]/\langle x^2+1\rangle, \\ \mathbb{Z}/4\mathbb{Z} & \text{otherwise.} \end{cases}$$

***Proof:*** *The* 3*-division polynomial of* $X_1(2,12)$ *is*

$$\Psi_4(x) = x^4 - \frac{4}{3}x^3 + 2x^2 - \frac{1}{3}.$$

*Clearly, a sextic number field cannot contaion a root of degree* 4 *irreducible polynomial.So,* $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/24\mathbb{Z}$ *and* $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$ *cannot occur as a torsion subgroup of* $X_1(2,12)$ *over a sextic number field.*

*The* 5*-division polynomial of* $X_1(2,12)$ *is*

$$\Psi_5(x) = f_{12}.$$

*Clearly, a sextic number field cannot contaion a root of degree* 12 *irreducible polynomial.So,* $\mathbb{Z}/20\mathbb{Z}$ *and* $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/20\mathbb{Z}$ *cannot occur as a torsion subgroup of* $X_1(2,12)$ *over a sextic number field.*

*The* 7*-division polynomial of* $X_1(2,12)$ *is*

$$\Psi_7(x) = f_{24}.$$

*Clearly, a sextic number field cannot contaion a root of degree* 24 *irreducible polynomial.So,* $\mathbb{Z}/28\mathbb{Z}$ *cannot occur as a torsion subgroup of* $X_1(2,12)$ *over a sextic number field.*

*The* 16*-division polynomial of* $X_1(2,12)$ *is*

$$\Psi_{16}(x) = x(x-1)(x+1)(x^2-4x+1)(x^2-x+1)(x^2+1)f_4^{(1)}f_4^{(2)}f_8^{(1)}f_8^{(2)}f_8^{(3)}f_8^{(4)}f_{16}f_{64}.$$

*By* MAGMA*,* $Tors(X_1(2,12),L) \simeq \mathbb{Z}/8\mathbb{Z}$ *where* $L$ *is the number field generated by the polynomial* $x^2-4x+1$*. But new torsion points do not give rise to an elliptic curve with torsion subgroup* $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$*.*

*By* MAGMA*,* $Tors(X_1(2,12),L) \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ *where* $L$ *is the number field generated by the polynomial* $x^2-x+1$*.But new torsion points do not give rise to an elliptic curve with torsion subgroup* $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$*.*

*By* MAGMA*, $Tors(X_1(2,12),L) \simeq \mathbb{Z}/8\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^2+1$. But new torsion points do not give rise to an elliptic curve with torsion subgroup $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$.*

*So, we cannot obtain $\mathbb{Z}/16\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/16\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$ as a torsion subgroup $X_1(2,12)$ over a sextic number field.* □

***Case 6:*** $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$

*Consider following the modular curve $X_1(3,3)$ of genus 0. The general equation of the elliptic curve with torsion subgroup $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$, [1], is the following:*

$$\mathcal{E}(3,3): y^2+((z+2)v+(1-z))xy+((z+1)v^2-zv)y = x^3$$

*where $v\in K$, $z=\zeta_3$ and $X_1(3,3)$ is defined over the field $\mathbb{Q}(\zeta_3)$. Then the discriminant is given by*

$$\Delta(3,3) = -27(-vz+v^2(1+z))^4+(-vz+v^2(1+z))^3(1-z+v(2+z))^3.$$

*Notice that $\Delta(3,3)=0$ if and only if $v=0$, $v=1$, $v=\frac{z}{1+z}$ and $v=\frac{(-1+z)^3}{(2+z)^3}$. So other than the points $(0,0)$, $(0,1)$, $(0,\frac{z}{1+z})$ and $(0,\frac{(-1+z)^3}{(2+z)^3})$, we can have an elliptic curve with torsion $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$.*

***Case 7:*** $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$

*Consider following the modular curve $X_1(3,6)$ of genus 0. The general equation of the elliptic curve with torsion subgroup $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$, [1], is the following:*

$$\mathcal{E}(3,6): y^2+(t+2)xy+(-t(t+1))y = x^3+(-t(t+1))x^2$$

*where $t=\frac{4v^2+6v+3}{v^3}$, $v\in K$ and and $X_1(3,6)$ is defined over the field $\mathbb{Q}(\zeta_3)$. Then the discriminant is given by*

$$\begin{aligned}\Delta(3,6) = -27t^4(t+1)^4+8t^3(t+2)^3(t+1)^3+t^3\left((t+2)^2-4t(t+1)\right)^2(t+1)^3 \\ -9t^3(t+2)\left((t+2)^2-4t(t+1)\right)(t+1)^3.\end{aligned}$$

*Notice that $\Delta(3,6)=0$ if and only if $v=-1$, $v=-\frac{3}{2}$, $v=\frac{1}{4}\left(-3-i\sqrt{3}\right)$, $v=\frac{1}{4}\left(-3+i\sqrt{3}\right)$, $v=\frac{1}{2}\left(-3-i\sqrt{3}\right)$ and $v=\frac{1}{2}\left(-3+i\sqrt{3}\right)$. So other than the points $(0,v)$, where $v$ is the root of $\Delta(3,6)$, we can have an elliptic curve with torsion $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$.*

***Case 8:*** $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/9\mathbb{Z}$

*Consider following the modular curve*

$$X_1(3,9) : y^2 + y = x^3$$

*We have*

$$\mathbb{Z}/3\mathbb{Z} \simeq Tors(X_1(3,9), \mathbb{Q}) \subseteq Tors(X_1(3,9), K).$$

*By Theorem 2.2.8, $Tors(X_1(3,9), K)$ must be one of the following groups:*

$$\mathbb{Z}/n\mathbb{Z},\ n = 3, 6, 9, 12, 15, 18, 21, 24, 27, 30$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z},\ n = 3, 6, , 9$$

$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3n\mathbb{Z},\ n = 1, 2, 3, 4$$

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

**Theorem 6.0.13.** *Let $K$ be a sextic number field. Then*

$$Tors(X_1(3,9), K) \simeq \begin{cases} \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & \text{if } K \supseteq M_1 := \mathbb{Q}[x]/\langle x^2 - x + 1\rangle, \\ \mathbb{Z}/6\mathbb{Z} & \text{if } K \supseteq M_2 := \mathbb{Q}[x]/\langle x^3 + \frac{1}{4}\rangle, \\ \mathbb{Z}/9\mathbb{Z} & \text{if } K \supseteq M_3 := \mathbb{Q}[x]/\langle x^3 - 3x^2 + 1\rangle, \\ \mathbb{Z}/6\mathbb{Z} & \text{if } K \simeq N_1 := \mathbb{Q}[x]/\langle x^6 + 5x^3 - \frac{1}{2}\rangle, \\ \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} & \text{if } K \simeq N_2 := \mathbb{Q}[x]/\langle x^6 - 3x^5 + 12x^4 + 11x^3 + 6x^2 + 3x + 1\rangle, \\ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} & \text{if } K \simeq N_3 := \mathbb{Q}[x]/\langle x^6 + 3x^5 + 9x^4 + 2x^3 + 3x^2 + 1\rangle, \\ \mathbb{Z}/3\mathbb{Z} & \text{otherwise.} \end{cases}$$

***Proof:*** *The 5-division polynomial of $X_1(3,9)$ is*

$$\Psi_5(x) = f_{12}.$$

*Clearly, a sextic number field cannot contain a root of degree 12 polynomial. So, we cannot have $\mathbb{Z}/15\mathbb{Z}$ and $\mathbb{Z}/30\mathbb{Z}$ as a torsion subgroup of $X_(3,9)$ over a sextic number field.*

*The 4-division polynomial of $X_1(3,9)$ is*

$$\Psi_4(x) = (x^3 + \frac{1}{4})(x^6 + 5x^3 - \frac{1}{2}).$$

*By* MAGMA, *$Tors(X_1(3,9), L) \simeq \mathbb{Z}/6\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^3 + 1/4$. But new torsion points do not give rise to an elliptic curve with torsion subgroup $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$, since an elliptic curve cannot have $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ as torsion subgroup over cubic number field.*

*By* MAGMA, *$Tors(X_1(3,9),L) \simeq \mathbb{Z}/6\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^6+5x^3-\frac{1}{2}$. However, new points do not give rise to an elliptic curve with torsion subgroup $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/9\mathbb{Z}$, even we have a positive rank we cannot obtain an elliptic curve with torsion subgroup $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/9\mathbb{Z}$ over $L$ since $L$ does not contain $\zeta_3$. So, we could not obtain a 4-torsion point. Hence we cannot obtain $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/24\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$ as a torsion subgroup of $X_1(3,9)$ over a sextic number field.*

*The* 3*-division polynomial of $X_1(3,9)$ is*

$$\Psi_3(x) = x(x+1)(x^2-x+1).$$

*By* MAGMA, *$Tors(X_1(3,9),L) \simeq \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^2-x+1$. However, new points do not give rise to an elliptic curve with torsion subgroup $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/9\mathbb{Z}$,since an elliptic curve cannot have $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/9\mathbb{Z}$ as torsion subgroup over quadratic number field.*

*The* 6*-division polynomial of $X_1(3,9)$ is*

$$\Psi_6(x) = x(x+1)(x^2-x+1)(x^3-2)(x^3+\frac{1}{4})(x^3+3x^2-3x+1)$$
$$(x^6-3x^5+12x^4+11x^3+6x^2+3x+1).$$

*Notice that the number fields generated by polynomials $x^3-2$, $x^3+\frac{1}{4}$ and $x^3+3x^2-3x+1$ are isomorphic. By* MAGMA, *$Tors(X_1(3,9),L) \simeq \mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^6-3x^5+12x^4+11x^3+6x^2+3x+1$.*

| Point from $X_1(3,9)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/9\mathbb{Z}$ |
|---|---|
| $(\frac{1}{9}(a^5-4a^4+16a^3-2a^2-a+4), \frac{1}{3}(a^5-3a^4+12a^3+10a^2+3a))$ | $y^2+\frac{1}{3}(72a^5-221a^4+860a^3+789a^2+154a-34)xy+\frac{1}{3}(1410a^5-4327a^4+16838a^3+15465a^2+3014a-739)y = x^3+\frac{1}{3}(1410a^5-4327a^4+16838a^3+15465a^2+3014a-739)x^2$ |

Table 6.13 All non-isomorphic Elliptic Curves obtained from new torsion points of $X_1(3,9)$ over the number field generated by $x^6-3x^5+12x^4+11x^3+6x^2+3x+1$

*We also need to investigate compositum field generatet by the polyomials $x^2-x+1$ and $x^3+1/4$, which is the field generated by the polynomial $16x^6-48x^5+96x^4-104x^3+84x^2-60x+25$. But it is easy to notice that this compositum field is isomorphic to the field generated by the polynomial $x^6-3x^5+12x^4+11x^3+6x^2+3x+1$.*

*So we cannot obtain $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ as a torsion subgroup of $X_1(3,9)$ over a sextic number field.*

*The 9-division polynomial of $X_1(3,9)$ is*

$$\Psi_9(x) = x(x+1)(x^2-x+1)(x^3-3x^2+1)(x^6+3x^5+9x^4+2x^3+3x^2+1)f_{18}$$

*By* MAGMA*, $Tors(X_1(3,9),L)\simeq\mathbb{Z}/9\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^3-3x^2+1$. Notice that $L$ does not contain $\zeta_3$, so new points does not give rise to an elliptic curve over $L$.*

*By* MAGMA*, $Tors(X_1(3,9),L)\simeq\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/9\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^6+3x^5+9x^4+2x^3+3x^2+1$.*

| Point from $X_1(3,9)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/9\mathbb{Z}$ |
|---|---|
| $(\frac{1}{3}(-a^4-4a^3-12a^2-10a-4), \frac{1}{3}(4a^5+12a^4+35a^3+4a^2-10))$ | $y^2+\frac{1}{3}(-14a^5-42a^4-120a^3-14a^2-18)xy+\frac{1}{3}(-89a^5-267a^4-763a^3-89a^2-136)y = x^3+\frac{1}{3}(-89a^5-267a^4-763a^3-89a^2-136)x^2$ |

Table 6.14 All non-isomorphic Elliptic Curves obtained from new torsion points of $X_1(3,9)$ over the number field generated by $x^6+3x^5+9x^4+2x^3+3x^2+1$

*We also need to investigate compositum field generated by the polyomials $x^2-x+1$ and $x^3-3x^2+1$, which is the field generated by the polynomial $x^6-9x^5+30x^4-47x^3+45x^2-30x+19$. But it is easy to notice that this compositum field is isomorphic to the field generated by the polynomial $x^6+3x^5+9x^4+2x^3+3x^2+1$*

*The 7-division polynomial of $X_1(3,9)$ is*

$$\Psi_7(x) = (x^6-\frac{1}{7}x^3+\frac{1}{7})f_{18}.$$

*By* MAGMA*, $Tors(X_1(3,9),L)\simeq\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^6-\frac{1}{7}x^3+\frac{1}{7}$. Notice that $L$ contains the number field generated by the polynomial $x^2-x+1$ and in this case $L$ contains $\zeta_3$. But new points do not give rise to an elliptic curve with torsion subgroup $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/9\mathbb{Z}$.*

*But we could not obtain a 7-torsion point, hence we cannot have $\mathbb{Z}/21\mathbb{Z}$ as a torsion subgroup of $X_1(3,9)$ over a sextic number field.*

*The* 18*-division polynomial of* $X_1(3,9)$ *is*

$$\Psi_{18}(x) = x(x+1)(x^2-x+1)(x^3-3x^2+1)(x^3-2)(x^3+1/4)(x^3+3x^2-3x+1)$$
$$(x^6-3x^5+12x^4+11x^3+6x^2+3x+1)(x^6+3x^5+9x^4+2x^3+3x^2+1)f_9^{(1)}f_9^{(2)}f_{18}^{(1)}f_{18}^{(2)}f_{27}f_{54}$$

*and the* 27*-division polynomial of* $X_1(3,9)$ *is*

$$\Psi_{27}(x) = x(x+1)(x^2-x+1)(x^3-3x^2+1)(x^6+3x^5+9x^4+2x^3+3x^2+1)f_9f_{18}f_{27}f_{54}f_{81}.$$

*Notice that we already investigated all the necessary polynomial in* $\Psi_{18}(x)$ *and* $\Psi_{27}(x)$ *when we are working with other division polynomials. Hence, we cannot obtain* $\mathbb{Z}/18\mathbb{Z}$, $\mathbb{Z}/27\mathbb{Z}$ *and* $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/18\mathbb{Z}$ *as a subgroup of* $X_1(3,9)$ *over a sextic number field.* □

***Case 9:*** $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$

*Consider following the modular curve* $X_1(4,4)$ *of genus* 0.

*The general equation of the elliptic curve with torsion subgroup* $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$, *[1], is the following:*

$$\mathcal{E}(4,4): y^2+xy+(-t)y = x^3+(-t)x^2$$

*where* $t = \frac{(1-v)(v^2-2v+2)}{2v^4}$, $v \in K$ *and* $X_1(4,4)$ *is defined over the field* $\mathbb{Q}(\zeta_4)$. *Then the discriminant is given by*

$$\Delta(4,4) = -27t^4+(1-4t)^2t^3-9(1-4t)t^3+8t^3.$$

*Notice that* $\Delta(4,4) = 0$ *if and only if* $v = 1$, $v = 2$, $v = 1-i$ *and* $v = 1+i$. *So other than the points* $(0,1)$, $(0,2)$, $(0,1-i)$ *and* $(0,1+i)$ *we can have an elliptic curve with torsion* $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$.

***Case 10:*** $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$

*Consider following the modular curve*

$$X_1(4,8): y^2 = x^3-x.$$

*We have*

$$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z} \simeq Tors(X_1(4,8),\mathbb{Q}) \subseteq Tors(X_1(4,8),K).$$

*By Theorem 2.2.8,* $Tors(X_1(4,8),K)$ *must be one of the following groups:*

$$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2n\mathbb{Z},\ n = 1,...,10$$

$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4n\mathbb{Z},\ n = 1,2$$

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

**Theorem 6.0.14.** *Let $K$ be a sextic number field. Then*

$$Tors(X_1(4,8),K) \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} & \textit{if } K \supseteq M_1 := \mathbb{Q}[x]/\langle x^2-2x-1\rangle, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} & \textit{if } K \supseteq M_2 := \mathbb{Q}[x]/\langle x^2+1\rangle, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \textit{otherwise.} \end{cases}$$

***Proof:*** *The 3-division polynomial of $X_1(4,8)$ is*

$$\Psi_3(x) = x^4 - 2x^2 - \frac{1}{3}.$$

*A sextic number field cannot contain a root of degree 4 polynomial. So, we cannot obtain $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ as torsion subgroup of $X_1(4,8)$ over a sextic number field.*

*The 5-division polynomial of $X_1(4,8)$ is*

$$\Psi_3(x) = (x^4 - \frac{2}{5}x^2 + \frac{1}{5})f_8.$$

*A sextic number field cannot contain a root of degree 4 and 8 polynomial. So, we cannot obtain $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$ as torsion subgroup of $X_1(4,8)$ over a sextic number field.*

*The 8-division polynomial of $X_1(4,8)$ is*

$$\Psi_8(x) = x(x-1)(x+1)(x^2-2x-1)(x^2+1)(x^2+2x-1)f_8^{(1)}f_8^{(2)}f_8^{(3)}.$$

*Notice that the number fields generated by the polynomials $x^2-2x-1$ and $x^2+2x-1$ are isomorphic. So, it is enough to consider only one of them. By* MAGMA, *$Tors(X_1(4,8),L) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^2-2x-1$.*

*By* MAGMA, *$Tors(X_1(4,8),L) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^2+1$.*

*So, we cannot have $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ as torsion subgroup of $X_1(4,8)$ over a sextic number field.*

*The 7-division polynomial of $X_1(4,8)$ is*

$$\Psi_7(x) = f_{24}.$$

*A sextic number field cannot contain a root of degree 24 polynomial. Hence, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$ cannot occur as a torsion subgroup of $X_1(4,8)$ over a sextic number field.*

***Case 11:*** $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$

*Consider following the modular curve*

$$X_1(6,6) : y^2 = x^3 + 1.$$

*We have*

$$\mathbb{Z}/6\mathbb{Z} \simeq Tors(X_1(6,6),\mathbb{Q}) \subseteq Tors(X_1(6,6),K).$$

*By Theorem 2.2.8, $Tors(X_1(6,6),K)$ must be one of the following groups:*

$$\mathbb{Z}/n\mathbb{Z},\ n = 6,12,18,24,30$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z},\ n = 3,6,9$$

$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$$

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

**Theorem 6.0.15.** *Let $K$ be a sextic number field. Then*

$$Tors(X_1(6,6),K) \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} & \text{if } K \supseteq L := \mathbb{Q}[x]/\langle x^2 - x + 1\rangle, \\ \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} & \text{if } K \simeq M := \mathbb{Q}[x]/\langle x^6 - 6x^5 + 36x^4 + 8x^3 - 24x^2 + 16\rangle, \\ \mathbb{Z}/6\mathbb{Z} & \text{otherwise.} \end{cases}$$

***Proof:****The 4-division polynomial of $X_1(6,6)$ is*

$$\Psi_4(x) = (x+1)(x^2 - x + 1)(x^2 + 2x - 2)f_4.$$

*By* MAGMA*, we obtain that $Tors(X_1(6,6),L) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ where $L$ is the number field is generated by the polynomial $x^2 - x + 1$.*

*By* MAGMA*, $Tors(X_1(6,6),L) \simeq \mathbb{Z}/6\mathbb{Z}$ where $L$ is the number field generated by the polynomial $x^2 + 2x - 2$.*

*So we cannot obtain a 4-torsion point. Thus $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/24\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ cannot occur as a torsion subgroup of $X_1(6,6)$ over a sextic number* *field.*

*The* 5*-division polynomial of* $X_1(6,6)$ *is*

$$\Psi_5(x) = f_{12}.$$

*Clearly, a sextic number field cannot contain a root of degree* 12 *polynomial. Hence we cannot have* $\mathbb{Z}/30\mathbb{Z}$ *as a torsion subgroup of* $X_1(6,6)$ *over a sextic number field.*

*The* 18*-division polynomial of* $X_1(6,6)$ *is*

$$\Psi_{18}(x) = x(x-2)(x+1)(x^2-x+1)(x^2+2x+4)(x^3+4)(x^3+6x^2+4)$$
$$(x^6-6x^5+36x^4+8x^3-24x^2+16)f_9^{(1)}f_9^{(2)}f_{18}f_{27}^{(1)}f_{27}^{(2)}f_{54}.$$

*Notice that the number fields generated by the polynomials* $x^2-x+1$ *and* $x^2+2x+4$ *are isomorphic and we already examined the polynomial* $x^2-x+1$*. Also Notice that the number fields generated by the polynomials* $x^3+6x^2+4$ *and* $x^3+4$ *are isomorphic.*

*By* MAGMA*,* $Tors(X_1(6,6),L) \simeq \mathbb{Z}/6\mathbb{Z}$ *where* $L$ *is the number field generated by the polynomial* $x^3+4$*.*

*We also need to investigate the splitting field of* $x^3+4$ *and the compositum field of* $x^3+4$ *and* $x^2-x+1$*. But these two fields are isomorphic to the number field generated by the polynomial* $x^6-6x^5+36x^4+8x^3-24x^2+16$*.*

*By* MAGMA*,* $Tors(X_1(6,6),L) \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ *where* $L$ *is the number field generated by the polynomial* $x^6-6x^5+36x^4+8x^3-24x^2+16$*.*

| Point from $X_1(6,6)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ |
|---|---|
| $(\frac{1}{36}(a^4 - 8a^3 + 48a^2 - 56a - 32), \frac{1}{12}(a^4-6a^3+36a^2+4a-12))$ | $y^2+\frac{4}{3}xy+\frac{2}{9}y = x^3+\frac{2}{9}x^2$ |

Table 6.15 All non-isomorphic Elliptic Curves obtained from new torsion points of $X_1(6,6)$ over the number field generated by $x^6-6x^5+36x^4+8x^3-24x^2+16$

*So,* $\mathbb{Z}/18\mathbb{Z}$*,* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$ *and* $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ *cannot occur as torsion subgroup of* $X_1(6,6)$ *over a sextic number field.* □

# 7. Torsion Subgroups over Number Fields with Smallest Discriminant

*In the following table we list the 2 cubic number fields with different Galois group and smallest discriminant. In the table, D is the discriminant of the field, G its Galois group, and the last column is the generating polynomial of field $K_i$ where $1 \le i \le 2$.*

## 7.1 Cubic Number Fields

| Field | D | G | Polynomial |
|---|---|---|---|
| $K_1$ | $-23$ | $S_3$ | $x^3-x^2+1$ |
| $K_2$ | 49 | $C_3$ | $x^3-x^2-2x+1$ |

Table 7.1 Cubic Number Fields with Smallest Discriminant

*We investigate possible torsion groups over the above fields.*

*In this chapter for the computation of torsion of Jacobian over a number field we use the* MAGMA *code by Samir Siksek [2].*

*The results in this section can be found in [22].*

**Theorem 7.1.1.** *The torsion of an elliptic curve over $K_1$ is isomorphic to one of the following groups:*

$$\mathbb{Z}/m\mathbb{Z},\ m=1,...,10,12$$

$$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2m\mathbb{Z},\ m=1,...,4,6.$$

***Proof:*** *We already have all the torsion subgroups occuring over $\mathbb{Q}$.*

***Genus 1***

*Consider the following modular curve*

$$X_1(11) : y^2 - y = x^3 - x^2.$$

*By our computations we obtain that* $X_1(11)(K_1) \simeq \mathbb{Z}/5\mathbb{Z} \simeq X_1(11)(\mathbb{Q})$ *and all the points of* $X_1(11)(K_1)$ *are cusps. Hence we cannot obtain an elliptic curves with torsion* $\mathbb{Z}/11\mathbb{Z}$ *over* $K_1$.

*Consider the following modular curve*

$$X_1(14) : y^2 + xy + y = x^3 - x.$$

*By our computations we obtain that* $X_1(14)(K_1) \simeq \mathbb{Z}/6\mathbb{Z} \simeq X_1(14)(\mathbb{Q})$ *and all the points of* $X_1(14)(K_1)$ *are cusps. Hence we cannot obtain an elliptic curves with torsion* $\mathbb{Z}/14\mathbb{Z}$ *over* $K_1$

*Consider the following modular curve*

$$X_1(15) : y^2 + xy + y = x^3 + x^2.$$

*By our computations we obtain that* $X_1(15)(K_1) \simeq \mathbb{Z}/4\mathbb{Z} \simeq X_1(15)(\mathbb{Q})$ *and all the points of* $X_1(15)(K_1)$ *are cusps. Hence we cannot obtain an elliptic curves with torsion* $\mathbb{Z}/15\mathbb{Z}$ *over* $K_1$

*Consider the following modular curve*

$$X_1(2,10) : y^2 = x^3 + x^2 - x.$$

*By our computations we obtain that* $X_1(2,10)(K_1) \simeq \mathbb{Z}/6\mathbb{Z} \simeq X_1(2,10)(\mathbb{Q})$ *and all the points of* $X_1(2,10)(K_1)$ *are cusps. Hence we cannot obtain an elliptic curves with torsion* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ *over* $K_1$.

*Consider the following modular curve*

$$X_1(2,12) : y^2 = x^3 - x^2 + x.$$

*By our computations we obtain that* $X_1(2,12)(K_1) \simeq \mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ *where* $(a^2 - a + 1, a^2 - 2a + 1)$ *is the point with infinite order. So we can have an elliptic curve over* $K_1$ *with torsion subgroup* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$.

***Genus 2***

*For genus 2 curves we check, Jacobian of the curve over the number field and whether there is no growth in torsion and rank. We conclude that all points are cusps over the number field, since none of the points on the curve cannot give an elliptic curve with desired torsion over $\mathbb{Q}$.*

*Consider the following modular curve*

$$X_1(13): y^2 = x^6 - 2x^5 + x^4 - 2x^3 + 6x^2 - 4x + 1.$$

*By* MAGMA, $Tors(J_1(13)(K_1)) \simeq \mathbb{Z}/19\mathbb{Z}$ *and* $Rank(J_1(13)(K_1)) = 0$. *Since there is no growth in torsion and rank is* $0$, *we can say that all the points on* $X_1(13)$ *are cusps.*

*Consider the following modular curve*

$$X_1(16): y^2 = x^5 + 2x^4 + 2x^2 - x.$$

*By* MAGMA, $Tors(J_1(16)(K_1)) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ *and* $Rank(J_1(16)(K_1)) = 0$. *Since there is no growth in torsion and rank is* $0$, *we can say that all the points on* $X_1(16)$ *are cusps.*

*Consider the following modular curve*

$$X_1(18): y^2 = x^6 + 2x^5 + 5x^4 + 10x^3 + 10x^2 + 4x + 1.$$

*By* MAGMA, $Tors(J_1(18)(K_1)) \simeq \mathbb{Z}/21\mathbb{Z}$ *and* $Rank(J_1(18)(K_1)) = 0$. *Since there is no growth in torsion and rank is* $0$, *we can say that all the points on* $X_1(18)$ *are cusps.*

***Higher genus Curves***

*Since we cannot obtain* $\mathbb{Z}/14\mathbb{Z}$ *as a torsion subgroup of an elliptic curve over* $K_1$, *it is not possible to obtain* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$ *as a torsion subgroup of an elliptic curve over* $K_1$.

*We cannot use above methods for* $X_1(20)$ *since it is a non-hyperelliptic curve of genus* $3$. *In this case we will use*

$$X_0(20): y^2 = x^3 + x^2 + 4x + 4$$

*and show that there is no* $20$*-cycle over* $K_1$. *By* MAGMA,
$X_0(20)(K_1) \simeq X_0(20)(\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$.

*By [24],* $X_0(20)$ *has* $6$ *rational cusps. Hence all the points on* $X_0(20)(K_1)$ *are* *cusps.*

**Theorem 7.1.2.** *The torsion of an elliptic curve over $K_2$ is isomorphic to one of the following groups:*

$$\mathbb{Z}/m\mathbb{Z},\ m = 1,...,10,12,13,14,18$$

$$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2m\mathbb{Z},\ m = 1,...,4.$$

***Proof:*** *We already have all the torsion subgroups occuring over $\mathbb{Q}$.*

***Genus 1***

*Consider the following modular curve*

$$X_1(11): y^2 - y = x^3 - x^2.$$

*By our computations we obtain that $X_1(11)(K_2) \simeq \mathbb{Z}/5\mathbb{Z} \simeq X_1(11)(\mathbb{Q})$ and all the points of $X_1(11)(K_2)$ are cusps. Hence we cannot obtain an elliptic curves with torsion $\mathbb{Z}/11\mathbb{Z}$ over $K_2$.*

*Consider the following modular curve*

$$X_1(14): y^2 + xy + y = x^3 - x.$$

*By our computations we obtain that $X_1(14)(K_1) \simeq \mathbb{Z}/18\mathbb{Z}$. Notice that the number fields generated by the polynomials $x^3 - x^2 - 2x + 1$ and $x^3 - 2x^2 - x + 1$ are isomorphic. We already obtain elliptic curves over $K_2$ with torsion subgroup $\mathbb{Z}/14\mathbb{Z}$, which is*

$$E^1_{14}: y^2 + \frac{1}{7}(9a^2 - 13a + 1)xy + \frac{1}{7}(8a^2 - 4a - 19)y = x^3 + \frac{1}{7}7(8a^2 - 4a - 19)x^2$$

$$E^2_{14}: y^2 + \frac{1}{7}(3a^2 + 5a + 5)xy + \frac{1}{7}(8a^2 + 7a - 4)y = x^3 + \frac{1}{7}(8a^2 + 7a - 4)x^2$$

*Consider the following modular curve*

$$X_1(15): y^2 + xy + y = x^3 + x^2.$$

*By our computations we obtain that $X_1(15)(K_2) \simeq \mathbb{Z}/4\mathbb{Z} \simeq X_1(15)(\mathbb{Q})$ and all the points of $X_1(15)(K_2)$ are cusps. Hence we cannot obtain an elliptic curves with torsion $\mathbb{Z}/15\mathbb{Z}$ over $K_2$*

*Consider the following modular curve*

$$X_1(2,10): y^2 = x^3 + x^2 - x.$$

*By our computations we obtain that* $X_1(2,10)(K_2) \simeq \mathbb{Z}/6\mathbb{Z} \simeq X_1(2,10)(\mathbb{Q})$ *and all the points of* $X_1(2,10)(K_2)$ *are cusps. Hence we cannot obtain an elliptic curves with torsion* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ *over* $K_2$.

*Consider the following modular curve*

$$X_1(2,12): y^2 = x^3 - x^2 + x.$$

*By our computations we obtain that* $X_1(2,12)(K_2) \simeq \mathbb{Z}/4\mathbb{Z} \simeq X_1(2,12)(\mathbb{Q})$ *and all the points of* $X_1(2,12)(K_2)$ *are cusps. Hence we cannot obtain an elliptic curves with torsion* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ *over* $K_2$.

***Genus 2***

$Tors(J_1(13)(K_2)) \simeq \mathbb{Z}/19\mathbb{Z}$ *and* $0 < Rank(J_1(13)(K_2)) \leq 2$. *In this case we can easily find a point on* $X_1(13)$ *over the number field* $K_2$ *that gives an elliptic curve with torsion subgroup* $\mathbb{Z}/13\mathbb{Z}$.

| Point from $X_1(13)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/13\mathbb{Z}$ |
|---|---|
| $(a^2-a-1, 2a^2-6)$ | $y^2+(4a^2-2a-8)xy+(20a^2-11a-45)y = x^3+(20a^2-11a-45)x^2$ |

Table 7.2 Elliptic curve obtained from points on $X_1(13)$ over the number field $K_2$

*By* MAGMA, $Tors(J_1(16)(K_1)) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ *and* $Rank(J_1(16)(K_1)) = 0$. *Since there is no growth in torsion and rank is* 0, *we can say that all the points on* $X_1(16)$ *are cusps.*

$Tors(J_1(18)(K_2)) \simeq \mathbb{Z}/21\mathbb{Z}$ *and* $0 < Rank(J_1(18)(K_2)) \leq 2$. *In this case we can easily find a point on* $X_1(18)$ *over the number field* $K_2$ *that gives an elliptic curve with torsion subgroup* $\mathbb{Z}/18\mathbb{Z}$.

| Point from $X_1(18)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/18\mathbb{Z}$ |
|---|---|
| $(-a^2+1, 3a+3)$ | $y^2+(-7a^2+6a+13)xy+(-a^2+9a-13)y = x^3+(-a^2+9a-13)x^2$ |

Table 7.3 Elliptic curve obtained from points on $X_1(18)$ over the number field $K_2$

***Higher genus Curves***

*Since we can only obtain two elliptic curves with the torsion subgroup* $\mathbb{Z}/14\mathbb{Z}$ *over* $K_2$, *which are* $E^1_{14}$ *and* $E^2_{14}$, *we need to check the elliptic curves* $E^1_{14}$ *and* $E^2_{14}$ *above* *to find another 2-torsion point. But By* MAGMA*, we obtain that there does not exist another 2-torsion point on $E_{14}^1$ and $E_{14}^2$ . So, it is not possible to obtain $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$ as a torsion subgroup of an elliptic curve over $K_2$.*

*We cannot use above methods for $X_1(20)$ since it is a non-hyperelliptic curve of genus 3. In this case we will use*

$$X_0(20) : y^2 = x^3 + x^2 + 4x + 4$$

*and show that there is no 20-cycle over $K_1$. By* MAGMA*,*
*$X_0(20)(K_1) \simeq X_0(20)(\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$.*

*By [24], $X_0(20)$ has 6 rational cusps. Hence all the points on $X_0(20)(K_1)$ are cusps.*

## 7.2 Quartic Number Fields

*In the following table we list the* 5 *quartic number fields with different Galois group and smallest discriminant. In the table, $D$ is the discriminant of the field, $G$ its Galois group, and the last column is the generating polynomial of field $K_i$ where* $1 \leq i \leq 5$.

| Field | D | G | Polynomial |
|---|---|---|---|
| $K_1$ | 125 | $C_4$ | $x^4 - x^3 + x^2 - x + 1$ |
| $K_2$ | 144 | $V_4$ | $x^4 - x^2 + 1$ |
| $K_3$ | 117 | $D_4$ | $x^4 - x^3 - x^2 + x + 1$ |
| $K_4$ | 3136 | $A_4$ | $x^4 - 2x^3 + 2x^2 + 2$ |
| $K_5$ | 229 | $S_4$ | $x^4 - x + 1$ |

Table 7.4 Quartic Number Fields with Smallest Discriminant

*We investigate possible torsion groups over the above fields.*

*For this section, we assume that no torsion groups occur over the quartic number fields other than these in Theorem 1.0.4.*

*In this section we will analyze the modular curves for each field according to their genus, because although we always get a conclusion for small genus curves, this was not possible for curves with large genus.*

**Remark 7.2.1.** *We could not find any method to check the existence of $K_i$-rational points for the modular curves $X_1(17)$, $X_1(21)$ and $X_1(22)$ over the number field $K_i$ where $i = 1, ..., 5$.*

**Theorem 7.2.2.** *The torsion of an elliptic curve over $K_1$ is isomorphic to one of the following groups:*

$$\mathbb{Z}/m\mathbb{Z},\ m = 1, ..., 10, 12, 15, 16$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z},\ m = 1, ..., 4$$

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

***Proof:*** *We already have all the torsion subgroups occuring over $\mathbb{Q}$.*

***Genus 0***

*Since $K_1$ does not contain $\zeta_3$ and $\zeta_4$, $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ cannot occur as a torsion subgroup of an elliptic curve over $K_1$.*

*Notice that $K_1$ contains $\zeta_5$, so it is enough to find one elliptic curve with torsion $\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$ over $K_1$.*

| Point from $X_1(5,5)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$ |
|---|---|
| $(0,\zeta_5)$ | $y^2+\frac{1}{22}(-8\zeta_5^3+5\zeta_5^2-8\zeta_5+24)xy+\frac{1}{22}(-8\zeta_5^3+5\zeta_5^2-8\zeta_5+2)y=x^3+\frac{1}{22}(-8\zeta_5^3+5\zeta_5^2-8\zeta_5+2)x^2$ |

Table 7.5 Elliptic curve obtained from points on $X_1(5,5)$ over the number field $K_1$

### ***Genus 1***

*Consider the following modular curve*

$$X_1(11): y^2-y=x^3-x^2.$$

*By our computations we obtain that $X_1(11)(K_1)\simeq\mathbb{Z}/5\mathbb{Z}\simeq X_1(11)(\mathbb{Q})$ and all the points of $X_1(11)(K_1)$ are cusps. Hence we cannot obtain an elliptic curves with torsion $\mathbb{Z}/11\mathbb{Z}$ over $K_1$.*

*Consider the following modular curve*

$$X_1(14): y^2+xy+y=x^3-x.$$

*By our computations we obtain that $X_1(14)(K_1)\simeq\mathbb{Z}/6\mathbb{Z}\simeq X_1(14)(\mathbb{Q})$ and all the points of $X_1(14)(K_1)$ are cusps. Hence we cannot obtain an elliptic curves with torsion $\mathbb{Z}/14\mathbb{Z}$ over $K_1$*

*Consider the following modular curve*

$$X_1(15): y^2+xy+y=x^3+x^2.$$

*By our computations we obtain that $X_1(15)(K_1)\simeq\mathbb{Z}/16\mathbb{Z}$. Notice that the number fields generated by the polynomials $x^4-x^3+x^2-x+1$ and $x^4+3x^3+4x^2+2x+1$ are isomorphic. We already obtain elliptic curves over $K_1$ with torsion subgroup $\mathbb{Z}/15\mathbb{Z}$, which are*

$$y^2+(-10a^3+10a^2-5)xy+(-94a^3+94a^2-58)y=x^3+(-94a^3+94a^2-58)x^2,$$

$$y^2+(-2a^3+5a^2-5a+3)xy+(3a^3+5a^2-13a+10)y=x^3+(3a^3+5a^2-13a+10)x^2.$$

*Consider the following modular curve*

$$X_1(2,10): y^2=x^3+x^2-x.$$

*By our computations we obtain that $X_1(2,10)(K_1)\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ Notice that $K_1$ contains the number field generated by the polynomial $x^2-4x-1$. But all the new points from torsion subgroup are cusps.*

*Consider the following modular curve*

$$X_1(2,12): y^2=x^3-x^2+x.$$

*By our computations we obtain that $X_1(2,12)(K_1)\simeq\mathbb{Z}/4\mathbb{Z}\simeq X_1(2,12)(\mathbb{Q})$ and all the points of $X_1(2,12)(K_1)$ are cusps. Hence we cannot obtain an elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$ over $K_1$.*

*Consider the following modular curve*

$$X_1(3,9): y^2+y=x^3.$$

*By our computations we obtain that $X_1(3,9)(K_1)\simeq\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$ where $(a^3-a^2,a^3-a^2)$ is the point with infinite order. Even rank is positive, since $K_1$ does not contain $\zeta_3$, we cannot have an elliptic curve over $K_1$ with torsion subgroup $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/9\mathbb{Z}$.*

*Consider the following modular curve*

$$X_1(4,8): y^2=x^3-x.$$

*By our computations we obtain that $X_1(4,8)(K_1)\simeq\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ where $(a^3-a^2,-a^3+a^2)$ is the point with infinite order. Even rank is positive, since $K_1$ does not contain $\zeta_4$, we cannot have an elliptic curve over $K_1$ with torsion subgroup $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$.*

*Consider the following modular curve*

$$X_1(6,6): y^2=x^3+1.$$

*By our computations we obtain that $X_1(6,6)(K_1)\simeq\mathbb{Z}/6\mathbb{Z}\simeq X_1(6,6)(\mathbb{Q})$ and all the points of $X_1(6,6)(K_1)$ are cusps. Hence we cannot obtain an elliptic curves with torsion $\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ over $K_1$*

### *Genus 2*

*By* MAGMA*,* $Tors(J_1(13)(K_1)) \simeq \mathbb{Z}/19\mathbb{Z}$ *and* $Rank(J_1(13)(K_1)) = 0$*. Since there is no growth in torsion and rank is* 0*, we can say that all the points on* $X_1(13)$ *are cusps.*

$Tors(J_1(16)(K_1)) \simeq \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ *and* $0 < Rank(J_1(16)(K_1)) \leq 2$*. In this case we can easily find a point on* $X_1(16)$ *over the number field* $K_1$ *that gives an elliptic curve with torsion subgroup* $\mathbb{Z}/16\mathbb{Z}$*.*

| Point from $X_1(16)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/16\mathbb{Z}$ |
|---|---|
| $(2a^3-2a^2-3, 16a^3+4a^2+12a-6)$ | $y^2+(2a^3+3a^2+3a+3)xy+(-3a^3-5a^2-5a-3)y = x^3+(-3a^3-5a^2-5a-3)x^2$ |

Table 7.6 Elliptic curve obtained from points on $X_1(16)$ over the number field $K_1$

*By* MAGMA*,* $Tors(J_1(18)(K_1)) \simeq \mathbb{Z}/21\mathbb{Z}$ *and* $Rank(J_1(18)(K_1)) = 0$*. Since there is no growth in torsion and rank is* 0*, we can say that all the points on* $X_1(18)$ *are cusps.*

### *Higher genus Curves*

*Since we cannot obtain* 14*-torsion over* $K_1$*,obviously* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$ *cannot occur over* $K_1$*.*

*Since we cannot obtain* 18*-torsion over* $K_1$*,obviously* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$ *cannot occur over* $K_1$*.*

*Since* $\mathbb{Z}/16\mathbb{Z}$ *occur as a torsion subgroup of an elliptic curve over* $K_1$*, we cannot use same argument for* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$*. Also we could not find any method to check its existence over* $K_1$*.*

*We cannot use above methods for* $X_1(20)$ *since it is a non-hyperelliptic curve of genus* 3*. In this case we will use*

$$X_0(20) : y^2 = x^3 + x^2 + 4x + 4$$

*and show that there is no* 20*-cycle over* $K_1$*. By* MAGMA*,*
$X_0(20)(K_1) \simeq X_0(20)(\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$*.*

*By [24],* $X_0(20)$ *has* 6 *rational cusps. Hence all the points on* $X_0(20)(K_1)$ *are cusps. Now consider*

$$X_0(24) : y^2 = x^3 - x^2 - 4x + 4.$$

*We will show that there is no 24-cycle over $K_1$. By* MAGMA,
$X_0(24)(K_1) \simeq X_0(24)(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

*By [24], $X_0(24)$ has 8 rational cusps. Hence all the points on $X_0(24)(K_1)$ are cusps.*

**Theorem 7.2.3.** *The torsion of an elliptic curve over $K_2$ is isomorphic to one of the following groups:*

$$\mathbb{Z}/m\mathbb{Z},\ m = 1, ..., 10, 12, 14, 15$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z},\ m = 1, ..., 4$$

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

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

***Proof:*** *We already have all the torsion subgroups occuring over $\mathbb{Q}$.*

***Genus 0***

*Since $K_2$ does not contain $\zeta_5$, $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ cannot occur as a torsion subgroup of an elliptic curve over $K_2$.*

*Notice that $K_2$ contains $\zeta_3$, so it is enough to find one elliptic curve with torsion $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ over $K_2$.*

| Point from $X_1(3,3)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ |
|---|---|
| $(0, \zeta_3)$ | $y^2 + y = x^3$ |

Table 7.7 Elliptic curve obtained from points on $X_1(3,3)$ over the number field $K_2$

| Point from $X_1(3,6)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ |
|---|---|
| $(0, \zeta_3)$ | $y^2 + (2\zeta_3 + 1)xy + (6\zeta_3 + 4)y = x^3 + (6\zeta_3 + 4)x^2$ |

Table 7.8 Elliptic curve obtained from points on $X_1(3,6)$ over the number field $K_2$

*Notice that $K_2$ contains $\zeta_4$, so it is enough to find one elliptic curve with torsion $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ over $K_2$.*

| Point from $X_1(4,4)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ |
|---|---|
| $(0,\zeta_4)$ | $y^2+xy+\frac{1}{2}(3\zeta_4+1)y=x^3+\frac{1}{2}(3\zeta_4+1)x^2$ |

Table 7.9 Elliptic curve obtained from points on $X_1(4,4)$ over the number field $K_2$

***Genus 1***

*Consider the following modular curve*

$$X_1(11): y^2-y=x^3-x^2.$$

*By our computations we obtain that* $X_1(11)(K_2)\simeq\mathbb{Z}/5\mathbb{Z}\simeq X_1(11)(\mathbb{Q})$ *and all the points of* $X_1(11)(K_1)$ *are cusps. Hence we cannot obtain an elliptic curves with torsion* $\mathbb{Z}/11\mathbb{Z}$ *over* $K_2$*.*

*Consider the following modular curve*

$$X_1(14): y^2+xy+y=x^3-x.$$

*By our computations we obtain that* $X_1(14)(K_2)\simeq\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ *where* $(-a^3,a^3-a^2-a)$ *is the point with infinite order. So we can have an elliptic curve over* $K_2$ *with torsion subgroup* $\mathbb{Z}/14\mathbb{Z}$*.*

*Consider the following modular curve*

$$X_1(15): y^2+xy+y=x^3+x^2.$$

*By our computations we obtain that* $X_1(15)(K_2)\simeq\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$ *where* $(a^3-a-1,-a^3-a^2)$ *is the point with infinite order. So we can have an elliptic curve over* $K_2$ *with torsion subgroup* $\mathbb{Z}/15\mathbb{Z}$*.*

*Consider the following modular curve*

$$X_1(2,10): y^2=x^3+x^2-x.$$

*By our computations we obtain that* $X_1(2,10)(K_2)\simeq\mathbb{Z}/6\mathbb{Z}\simeq X_1(2,10)(\mathbb{Q})$ *and all the points of* $X_1(2,10)(K_2)$ *are cusps. Hence we cannot obtain an elliptic curves with torsion* $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z}$ *over* $K_2$*.*

*Consider the following modular curve*

$$X_1(2,12): y^2 = x^3 - x^2 + x.$$

*By our computations we obtain that* $X_1(2,12)(K_2) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. *Notice that the number fields generated by the polynomials* $x^4 - x^2 + 1$ *and* $x^4 - 2x^3 + 5x^2 - 4x + 1$ *are isomorphic. We already saw that new torsion points do not give rise to an elliptic curve in the previous chapter.*

*Consider the following modular curve*

$$X_1(3,9): y^2 + y = x^3.$$

*By our computations we obtain that* $X_1(3,9)(K_2) \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. *But new points do not give rise to an elliptic curve with torsion subgroup* $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$.

*Consider the following modular curve*

$$X_1(4,8): y^2 = x^3 - x.$$

*By our computations we obtain that* $X_1(4,8)(K_2) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. *Notice that the number field generated by the polynomial* $x^4 - x^2 + 1$ *contains the number field generated by the polynomial* $x^2 + 1$. *All the new points from torsion subgroup are cusps. So, new torsion points do not give rise to an elliptic curve with desired torsion.*

*Consider the following modular curve*

$$X_1(6,6): y^2 = x^3 + 1.$$

*By our computations we obtain that* $X_1(6,6)(K_2) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. *So,* $K_2$ *contains number field generated by the polynomial* $x^2 - x + 1$. *Even* $K_2$ *does contain* $\zeta_6$, *new points from torsion are cusps. Clearly, new torsion points do not give rise to an elliptic curve with desired torsion.*

### *Genus 2*

*By* MAGMA, $Tors(J_1(13)(K_2)) \simeq \mathbb{Z}/19\mathbb{Z}$ *and* $Rank(J_1(13)(K_2)) = 0$. *Since there is no growth in torsion and rank is* $0$, *we can say that all the points on* $X_1(13)$ *are cusps.*

*By* MAGMA, $Tors(J_1(16)(K_2)) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ *and* $Rank(J_1(16)(K_2)) = 0$.

*By* MAGMA*, $Tors(J_1(18)(K_2)) \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/21\mathbb{Z}$ and $Rank(J_1(18)(K_2)) = 0$.*

*Since there is a growth in torsion for some cases, we cannot say anything about their existence over $K_2$.*

***Higher genus Curves***

*By* MAGMA*, $X_0(20)(K_2) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.*

*By* MAGMA*, $X_0(24)(K_2) \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.*

*We could not obtain any useful information with this method, but we figure out a method useful for $X_1(20)(K_2)$ and $X_1(24)(K_2)$.*

*As $X_1(4n)$ is a cover of $X_1(2,2n)$, if $Y_1(2,2n) = \emptyset$ then $Y_1(4n) = \emptyset$. In our case we have $Y_1(2,10) = \emptyset$ and $Y_1(2,12) = \emptyset$, so we can say $Y_1(20) = \emptyset$ and $Y_1(24) = \emptyset$. Thus we cannot have $\mathbb{Z}/20\mathbb{Z}$ and $\mathbb{Z}/24\mathbb{Z}$ as torsion subgroup of an elliptic curve over $K_2$.*

*Since $\mathbb{Z}/14\mathbb{Z}$ occurs as a torsion subgroup of an elliptic curve over $K_2$, we cannot say $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$ occurs or not.*

*Similarly, since we do not have information for $\mathbb{Z}/16\mathbb{Z}$ and $\mathbb{Z}/18\mathbb{Z}$, we also cannot decide $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$ occur or not.*

**Theorem 7.2.4.** *The torsion of an elliptic curve over $K_3$ is isomorphic to one of the following groups:*

$$\mathbb{Z}/m\mathbb{Z},\ m = 1, ..., 13$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z},\ m = 1, ..., 5$$

$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3m\mathbb{Z},\ m = 1, 2.$$

***Proof:*** *We already have all the torsion subgroups occuring over $\mathbb{Q}$.*

***Genus 0***

*Since $K_3$ does not contain $\zeta_4$ and $\zeta_5$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ cannot occur as a torsion subgroup of an elliptic curve over $K_3$.*

*Notice that $K_3$ contains $\zeta_3$, so it is enough to find one elliptic curve with torsion $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ over $K_3$.*

| Point from $X_1(3,3)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ |
|---|---|
| $(0,\zeta_3)$ | $y^2+y=x^3$ |

Table 7.10 Elliptic curve obtained from points on $X_1(3,3)$ over the number field $K_3$

| Point from $X_1(3,6)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ |
|---|---|
| $(0,\zeta_3)$ | $y^2+(2\zeta_3+1)xy+(6\zeta_3+4)y=x^3+(6\zeta_3+4)x^2$ |

Table 7.11 Elliptic curve obtained from points on $X_1(3,6)$ over the number field $K_3$

***Genus 1***

*Consider the following modular curve*

$$X_1(11): y^2-y=x^3-x^2.$$

*By our computations we obtain that $X_1(11)(K_3) \simeq \mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ where $(-a^3+2a^2-1, a^3-a^2-a+2)$ is the point with infinite order. So we can have an elliptic curve over $K_3$ with torsion subgroup $\mathbb{Z}/11\mathbb{Z}$.*

*Consider the following modular curve*

$$X_1(14): y^2+xy+y=x^3-x.$$

*By our computations we obtain that $X_1(14)(K_3) \simeq \mathbb{Z}/6\mathbb{Z} \simeq X_1(14)(\mathbb{Q})$ and all the points of $X_1(14)(K_3)$ are cusps. Hence we cannot obtain an elliptic curves with torsion $\mathbb{Z}/14\mathbb{Z}$ over $K_3$*

*Consider the following modular curve*

$$X_1(15): y^2+xy+y=x^3+x^2.$$

*By our computations we obtain that $X_1(15)(K_3) \simeq \mathbb{Z}/8\mathbb{Z}$. Notice that $K_3$ contains the number field generated by the polynomial $x^2+x+1$, but in the previous chapter we obtain that new torsion points does not give rise to elliptic curves with the torsion subgroup $\mathbb{Z}/15\mathbb{Z}$. Hence we cannot obtain an elliptic curves with torsion $\mathbb{Z}/15\mathbb{Z}$ over $K_3$*

*Consider the following modular curve*

$$X_1(2,10) : y^2 = x^3 + x^2 - x.$$

*By our computations we obtain that* $X_1(2,10)(K_3) \simeq \mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ *where* $(2a^3 - 3a^2 + 2, 3a^3 - 5a^2 + a + 2)$ *is the point with infinite order. So we can have an elliptic curve over* $K_3$ *with torsion subgroup* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$.

*Consider the following modular curve*

$$X_1(2,12) : y^2 = x^3 - x^2 + x.$$

*By our computations we obtain that* $X_1(2,12)(K_3) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. *Notice that the number field* $K_3$ *contains the number field generated by the polynomial* $x^2 - x + 1$ *and all the points are cusps.*

*Consider the following modular curve*

$$X_1(3,9) : y^2 + y = x^3.$$

*By our computations we obtain that* $X_1(3,9)(K_3) \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. *But new points do not give rise to an elliptic curve with torsion subgroup* $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$

*Consider the following modular curve*

$$X_1(4,8) : y^2 = x^3 - x.$$

*By our computations we obtain that* $X_1(4,8)(K_3) \simeq \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *where* $(-a, a^2 - a - 1)$ *is the point with infinite order. Even rank is positive, since* $K_3$ *does not contain* $\zeta_4$, *we cannot have an elliptic curve over* $K_3$ *with torsion subgroup* $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.

*Consider the following modular curve*

$$X_1(6,6) : y^2 = x^3 + 1.$$

*By our computations we obtain that* $X_1(6,6)(K_3) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.*So,* $K_3$ *contains number field generated by the polynomial* $x^2 - x + 1$. *Even* $K_3$ *does contain* $\zeta_6$, *new points from torsion are cusps. Clearly, new torsion points do not give rise to an elliptic curve with desired torsion.*

***Genus 2***

*By* MAGMA, $Tors(J_1(13)(K_3)) \simeq \mathbb{Z}/57\mathbb{Z}$ *and* $Rank(J_1(13)(K_3)) = 0$. *In this case* *we can easily find a point on $X_1(13)$ over the number field $K_3$ that gives an elliptic curve with torsion subgroup $\mathbb{Z}/13\mathbb{Z}$.*

| Point from $X_1(13)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/13\mathbb{Z}$ |
|---|---|
| $(a^3-a^2+1, a^3-3a^2+2)$ | $y^2+(2a^3-4a^2+2a+2)xy+(7a^3-12a^2+a+8)y = x^3+(7a^3-12a^2+a+8)x^2$ |

Table 7.12 Elliptic curve obtained from points on $X_1(13)$ over the number field $K_3$

*By* MAGMA, $Tors(J_1(16)(K_3)) \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z}$ *and* $Rank(J_1(16)(K_3)) = 0$. *Since there is no growth in torsion and rank is* 0, *we can say that all the points on* $X_1(16)$ *are cusps.*

*By* MAGMA, $Tors(J_1(18)(K_3)) \simeq \mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/21\mathbb{Z}$ *and* $Rank(J_1(18)(K_3)) = 0$. *Since there is growth in this case we cannot decide its occurrence.*

***Higher genus Curves***

*Since we cannot obtain* 14*-torsion over* $K_3$,*obviously* $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/14\mathbb{Z}$ *cannot occur over* $K_3$.

*Since we cannot obtain* 16*-torsion over* $K_3$,*obviously* $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/16\mathbb{Z}$ *cannot occur over* $K_3$.

*We cannot use same argument for* $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/18\mathbb{Z}$, *since we do not have information about* $X_1(18)$.

*By* MAGMA, $X_0(20)(K_3) \simeq \mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$. *Since rank is positive we cannot decide its occurrence over* $K_3$.

*Now consider*

$$X_0(24): y^2 = x^3 - x^2 - 4x + 4.$$

*We will show that there is no* 24*-cycle over* $K_3$. *By* MAGMA, $X_0(24)(K_3) \simeq X_0(24)(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$.

*By [24],* $X_0(24)$ *has* 8 *rational cusps. Hence all the points on* $X_0(24)(K_3)$ *are cusps.*

**Theorem 7.2.5.** *The torsion of an elliptic curve over* $K_4$ *is isomorphic to one of the following groups:*

$$\mathbb{Z}/m\mathbb{Z},\ m = 1,\dots,10,12$$

$$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2m\mathbb{Z},\ m = 1,\dots,5.$$

***Proof:*** *We already have all the torsion subgroups occuring over* $\mathbb{Q}$.

***Genus 0***

*Since* $K_4$ *does not contain* $\zeta_3$, $\zeta_4$ *and* $\zeta_5$, $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ *and* $\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$ *cannot occur as a torsion subgroup of an elliptic curve over* $K_4$.

***Genus 1***

*Consider the following modular curve*

$$X_1(11): y^2 - y = x^3 - x^2.$$

*By our computations we obtain that* $X_1(11)(K_4) \simeq \mathbb{Z}/5\mathbb{Z} \simeq X_1(11)(\mathbb{Q})$ *and all the points of* $X_1(11)(K_4)$ *are cusps. Hence we cannot obtain an elliptic curves with torsion* $\mathbb{Z}/11\mathbb{Z}$ *over* $K_4$.

*Consider the following modular curve*

$$X_1(14): y^2 + xy + y = x^3 - x.$$

*By our computations we obtain that* $X_1(14)(K_4) \simeq \mathbb{Z}/6\mathbb{Z} \simeq X_1(14)(\mathbb{Q})$ *and all the points of* $X_1(14)(K_4)$ *are cusps. Hence we cannot obtain an elliptic curves with torsion* $\mathbb{Z}/14\mathbb{Z}$ *over* $K_4$.

*Consider the following modular curve*

$$X_1(15): y^2 + xy + y = x^3 + x^2.$$

*By our computations we obtain that* $X_1(15)(K_4) \simeq \mathbb{Z}/4\mathbb{Z} \simeq X_1(15)(\mathbb{Q})$ *and all the points of* $X_1(15)(K_4)$ *are cusps. Hence we cannot obtain an elliptic curves with torsion* $\mathbb{Z}/15\mathbb{Z}$ *over* $K_4$.

*Consider the following modular curve*

$$X_1(2,10): y^2 = x^3 + x^2 - x.$$

*By our computations we obtain that* $X_1(2,10)(K_4) \simeq \mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ *where* $(\frac{1}{2809}(714a^3 - 730a^2 - 340a + 1139), \frac{1}{148877}(34976a^3 - 34312a^2 - 25216a + 13125))$ *is the point with infinite order. So we can have an elliptic curve over* $K_4$ *with torsion subgroup* $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z}$.

*Consider the following modular curve*

$$X_1(2,12) : y^2 = x^3 - x^2 + x.$$

*By our computations we obtain that* $X_1(2,12)(K_4) \simeq \mathbb{Z}/4\mathbb{Z} \simeq X_1(2,12)(\mathbb{Q})$ *and all the points of* $X_1(2,12)(K_4)$ *are cusps. Hence we cannot obtain an elliptic curves with torsion* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ *over* $K_4$*.*

*Consider the following modular curve*

$$X_1(3,9) : y^2 + y = x^3.$$

*By our computations we obtain that* $X_1(3,9)(K_4) \simeq \mathbb{Z}/3\mathbb{Z} \simeq X_1(3,9)(\mathbb{Q})$ *and all the points of* $X_1(3,9)(K_4)$ *are cusps. Hence we cannot obtain an elliptic curves with torsion* $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ *over* $K_4$*.*

*Consider the following modular curve*

$$X_1(4,8) : y^2 = x^3 - x.$$

*By our computations we obtain that* $X_1(4,8)(K_4) \simeq \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ *where* $(\frac{80a^3-164a^2+152a+41}{81}, \frac{-686a^3+2192a^2-2972a+424}{729})$ *is the point with infinite order. Even rank is positive, since* $K_4$ *does not contain* $\zeta_4$*, we cannot have an elliptic curve over* $K_4$ *with torsion subgroup* $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$*.*

*Consider the following modular curve*

$$X_1(6,6) : y^2 = x^3 + 1.$$

*By our computations we obtain that* $X_1(6,6)(K_4) \simeq \mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ *where* $(-a^3 + 2a^2 + 2, -2a^3 + 4a^2 + 2a + 3)$ *is the point with infinite order. Even rank is positive, since* $K_4$ *does not contain* $\zeta_6$*, we cannot have an elliptic curve over* $K_4$ *with torsion subgroup* $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$*.*

***Genus 2***

*By* MAGMA*,* $Tors(J_1(13)(K_4)) \simeq \mathbb{Z}/19\mathbb{Z}$ *and* $Rank(J_1(13)(K_4)) \leq 2$*.*

*By* MAGMA*,* $Tors(J_1(16)(K_4)) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ *and* $Rank(J_1(16)(K_4)) \leq 2$*.*

*By* MAGMA*,* $Tors(J_1(18)(K_4)) \simeq \mathbb{Z}/21\mathbb{Z}$ *and* $Rank(J_1(18)(K_4)) \leq 4$*.*

*Since we could not obtain lower bound* $Rank(J_1(13)(K_4))$*,* $Rank(J_1(16)(K_4))$ *and* $Rank(J_1(18)(K_4))$*, we cannot decide existence of* $\mathbb{Z}/13\mathbb{Z}$*,* $\mathbb{Z}/16\mathbb{Z}$ *and* $\mathbb{Z}/18\mathbb{Z}$ *over*

*$K_4$.*

***Higher genus Curves***

*Since we cannot obtain 14-torsion over $K_4$,obviously $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/14\mathbb{Z}$ cannot occur over $K_4$. But we cannot use same argument for $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/16\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/18\mathbb{Z}$ ,since we do not have information about $X_1(16)$ and $X_1(18)$.*

*By* MAGMA*, $X_0(20)(K_4)\simeq\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$. Since rank is positive we cannot decide its occurrence over $K_4$.*

*Now consider*

$$X_0(24): y^2 = x^3 - x^2 - 4x + 4.$$

*We will show that there is no 24-cycle over $K_4$. By* MAGMA*,
$X_0(24)(K_4)\simeq X_0(24)(\mathbb{Q})\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$.*

*By [24], $X_0(24)$ has 8 rational cusps. Hence all the points on $X_0(24)(K_4)$ are cusps.*

**Theorem 7.2.6.** *The torsion of an elliptic curve over $K_5$ is isomorphic to one of the following groups:*

$$\mathbb{Z}/m\mathbb{Z},\ m = 1,...,10,12$$

$$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2m\mathbb{Z},\ m = 1,...,4,6.$$

***Proof:*** *We already have all the torsion subgroups occuring over $\mathbb{Q}$.*

***Genus 0***

*Since $K_5$ does not contain $\zeta_3$, $\zeta_4$ and $\zeta_5$, $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$ cannot occur as a torsion subgroup of an elliptic curve over $K_5$.*

***Genus 1***

*Consider the following modular curve*

$$X_1(11): y^2 - y = x^3 - x^2.$$

*By our computations we obtain that $X_1(11)(K_5)\simeq\mathbb{Z}/5\mathbb{Z}\simeq X_1(11)(\mathbb{Q})$ and all the points of $X_1(11)(K_5)$ are cusps. Hence we cannot obtain an elliptic curves with torsion $\mathbb{Z}/11\mathbb{Z}$ over $K_5$.*

*Consider the following modular curve*

$$X_1(14): y^2 + xy + y = x^3 - x.$$

*By our computations we obtain that* $X_1(14)(K_5) \simeq \mathbb{Z}/6\mathbb{Z} \simeq X_1(14)(\mathbb{Q})$ *and all the points of* $X_1(14)(K_5)$ *are cusps. Hence we cannot obtain an elliptic curves with torsion* $\mathbb{Z}/14\mathbb{Z}$ *over* $K_5$.

*Consider the following modular curve*

$$X_1(15): y^2 + xy + y = x^3 + x^2.$$

*By our computations we obtain that* $X_1(15)(K_5) \simeq \mathbb{Z}/4\mathbb{Z} \simeq X_1(15)(\mathbb{Q})$ *and all the points of* $X_1(15)(K_5)$ *are cusps. Hence we cannot obtain an elliptic curves with torsion* $\mathbb{Z}/15\mathbb{Z}$ *over* $K_5$.

*Consider the following modular curve*

$$X_1(2,10): y^2 = x^3 + x^2 - x.$$

*By our computations we obtain that* $X_1(2,10)(K_5) \simeq \mathbb{Z}/6\mathbb{Z} \simeq X_1(2,10)(\mathbb{Q})$ *and all the points of* $X_1(2,10)(K_5)$ *are cusps. Hence we cannot obtain an elliptic curves with torsion* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ *over* $K_5$.

*Consider the following modular curve*

$$X_1(2,12): y^2 = x^3 - x^2 + x.$$

*By our computations we obtain that* $X_1(2,12)(K_5) \simeq \mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ *where* $(a^3 - 1, a^3 + a^2 + a)$ *is the point with infinite order. So we can have an elliptic curve over* $K_5$ *with torsion subgroup* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$.

*Consider the following modular curve*

$$X_1(3,9): y^2 + y = x^3.$$

*By our computations we obtain that* $X_1(3,9)(K_5) \simeq \mathbb{Z}/3\mathbb{Z} \simeq X_1(3,9)(\mathbb{Q})$ *and all the points of* $X_1(3,9)(K_5)$ *are cusps. Hence we cannot obtain an elliptic curve with torsion* $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ *over* $K_5$

*Consider the following modular curve*

$$X_1(4,8): y^2 = x^3 - x.$$

*By our computations we obtain that $X_1(4,8)(K_5) \simeq \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ where $(a^3+a^2+a-1, -2a^3-a^2+2)$ is the point with infinite order. Even rank is positive, since $K_5$ does not contain $\zeta_4$, we cannot have an elliptic curve over $K_5$ with torsion subgroup $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.*

*Consider the following modular curve*

$$X_1(6,6) : y^2 = x^3+1.$$

*By our computations we obtain that $X_1(6,6)(K_5) \simeq \mathbb{Z}/6\mathbb{Z} \simeq X_1(6,6)(\mathbb{Q})$ and all the points of $X_1(6,6)(K_5)$ are cusps. Hence we cannot obtain an elliptic curve with torsion $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ over $K_5$*

***Genus 2***

*By* MAGMA*, $Tors(J_1(13)(K_5)) \simeq \mathbb{Z}/19\mathbb{Z}$ and $Rank(J_1(13)(K_5)) = 0$. Since there is no growth in torsion and rank is $0$, we can say that all the points on $X_1(13)$ are cusps.*

*By* MAGMA*, $Tors(J_1(16)(K_5)) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ and $Rank(J_1(16)(K_5)) = 0$. Since there is no growth in torsion and rank is $0$, we can say that all the points on $X_1(16)$ are cusps.*

*By* MAGMA*, $Tors(J_1(18)(K_5)) \simeq \mathbb{Z}/21\mathbb{Z}$ and $Rank(J_1(18)(K_5)) = 0$. Since there is no growth in torsion and rank is $0$, we can say that all the points on $X_1(18)$ are cusps.*

***Higher genus Curves***

*Since we cannot obtain $14$-torsion over $K_5$,obviously $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$ cannot occur over $K_5$.*

*Since we cannot obtain $16$-torsion over $K_5$,obviously $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$ cannot occur over $K_5$.*

*Since we cannot obtain $18$-torsion over $K_5$,obviously $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$ cannot occur over $K_5$.*

*We cannot use above methods for $X_1(20)$ since it is a non-hyperelliptic curve of genus $3$. In this case we will use*

$$X_0(20) : y^2 = x^3+x^2+4x+4$$

*and show that there is no $20$-cycle over $K_5$. By* MAGMA*, $X_0(20)(K_5) \simeq X_0(20)(\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$.*

*By [24], $X_0(20)$ has 6 rational cusps. Hence all the points on $X_0(20)(K_5)$ are cusps.*

*By* MAGMA*, $X_0(24)(K_5) \simeq \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Since rank is positive we cannot decide existence of $\mathbb{Z}/24\mathbb{Z}$ over $K_5$.*

### 7.3 Quintic Number Fields

*In the following table we list the* 5 *quintic number fields with different Galois group and smallest discriminant. In the table, $D$ is the discriminant of the field, $G$ its Galois group, and the last column is the generating polynomial of field $K_i$ where* $1 \leq i \leq 5$.

| Field | D | G | Polynomial |
|---|---|---|---|
| $K_1$ | 1609 | $S_5$ | $x^5 - x^3 - x^2 + x + 1$ |
| $K_2$ | 2209 | $D_5$ | $x^5 - 2x^4 + 2x^3 - x^2 + 1$ |
| $K_3$ | 35152 | $F_5$ | $x^5 - x^4 + 2x^3 - 4x^2 + x - 1$ |
| $K_4$ | 18496 | $A_5$ | $x^5 - x^4 + 2x^2 - 2x + 2$ |
| $K_5$ | 14641 | $C_5$ | $x^5 - x^4 - 4x^3 + 3x^2 + 3x - 1$ |

Table 7.13 Quintic Number Fields with Smallest Discriminant

*We investigate possible torsion groups over the above field.*

*In this chapter for the computation of torsion of Jacobian we use the* MAGMA *code of Samir Siksek and the code can be found at website.*

*For this section, we assume that no torsion groups occur over the quintic number field other than these in Theorem 2.1.7.*

*In this section we will analyze the modular curves for each field according to their genus, because although we always get a conclusion for small genus curves, this was not possible for curves with large genus.*

**Remark 7.3.1.** *We could not find any method to check the existence of $K_i$-rational points for the modular curves $X_1(17)$, $X_1(19)$, $X_1(21)$, $X_1(22)$ and $X_1(25)$ over the number field $K_i$ where $i = 1,...,5$.*

**Theorem 7.3.2.** *The torsion of an elliptic curve over $K_1$ is isomorphic to one of the following groups:*

$$\mathbb{Z}/m\mathbb{Z},\ m = 1,...,10,12,13,14,15$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z},\ m = 1,...,4.$$

***Proof:*** *We already have all the torsion subgroups occuring over $\mathbb{Q}$.*

***Genus 1***

*Consider the following modular curve*

$$X_1(11): y^2 - y = x^3 - x^2.$$

*By our computations we obtain that* $X_1(11)(K_1) \simeq \mathbb{Z}/5\mathbb{Z} \simeq X_1(11)(\mathbb{Q})$ *and all the points of* $X_1(11)(K_1)$ *are cusps. Hence we cannot obtain an elliptic curves with torsion* $\mathbb{Z}/11\mathbb{Z}$ *over* $K_1$*.*

*Consider the following modular curve*

$$X_1(14): y^2 + xy + y = x^3 - x.$$

*By our computations we obtain that* $X_1(14)(K_1) \simeq \mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ *where* $(-a, -a^4 + a^2 + a - 1)$ *is the point with infinite order. So we can have an elliptic curve over* $K_1$ *with torsion subgroup* $\mathbb{Z}/14\mathbb{Z}$*.*

*Consider the following modular curve*

$$X_1(15): y^2 + xy + y = x^3 + x^2.$$

*By our computations we obtain that* $X_1(15)(K_1) \simeq \mathbb{Z}^2 \times \mathbb{Z}/4\mathbb{Z}$ *where* $(a^4 - a, -a^3 + a + 1)$ *and* $(3a^4 - 2a^3 - 2a^2 - 2a + 4, -9a^4 + 6a^3 + 5a^2 + 6a - 13)$ *are the points with infinite order. So we can have an elliptic curve over* $K_1$ *with torsion subgroup* $\mathbb{Z}/15\mathbb{Z}$*.*

*Consider the following modular curve*

$$X_1(2,10): y^2 = x^3 + x^2 - x.$$

*By our computations we obtain that* $X_1(2,10)(K_1) \simeq \mathbb{Z}/6\mathbb{Z} \simeq X_1(2,10)(\mathbb{Q})$ *and all the points of* $X_1(2,10)(K_1)$ *are cusps. Hence we cannot obtain an elliptic curves with torsion* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ *over* $K_1$*.*

*Consider the following modular curve*

$$X_1(2,12): y^2 = x^3 - x^2 + x.$$

*By our computations we obtain that* $X_1(2,12)(K_1) \simeq \mathbb{Z}/4\mathbb{Z} \simeq X_1(2,12)(\mathbb{Q})$ *and all the points of* $X_1(2,12)(K_1)$ *are cusps. Hence we cannot obtain an elliptic curves with torsion* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ *over* $K_1$*.*

***Genus 2***

*By* MAGMA*,* $Tors(J_1(13)(K_1)) \simeq \mathbb{Z}/19\mathbb{Z}$ *and* $0 < Rank(J_1(13)(K_1)) \leq 2$*. In this* *case we can easily find a point on $X_1(13)$ over the number field $K_1$ that gives an elliptic curve with torsion subgroup $\mathbb{Z}/13\mathbb{Z}$.*

| Point from $X_1(13)$ | Corresponding Elliptic Curve with torsion $\mathbb{Z}/13\mathbb{Z}$ |
|---|---|
| $(a^2, a^3-a^2+a+1)$ | $y^2+(a^4-a+2)xy+(5a^4-3a^3-2a^2-3a+7)y = x^3 + (5a^4-3a^3-2a^2-3a+7)x^2$ |

Table 7.14 Elliptic curve obtained from points on $X_1(13)$ over the number field $K_1$

*By* MAGMA, $Tors(J_1(16)(K_1)) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ *and* $Rank(J_1(16)(K_1)) = 0$. *Since there is no growth in torsion and rank is* $0$, *we can say that all the points on* $X_1(16)$ *are cusps.*

*By* MAGMA, $Tors(J_1(18)(K_1)) \simeq \mathbb{Z}/21\mathbb{Z}$ *and* $Rank(J_1(18)(K_1)) = 0$. *Since there is no growth in torsion and rank is* $0$, *we can say that all the points on* $X_1(18)$ *are cusps.*

***Higher genus Curves***

*Since we cannot obtain* $16$*-torsion over* $K_1$,*obviously* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$ *cannot occur over* $K_1$.

*Since* $\mathbb{Z}/14\mathbb{Z}$ *occur as a torsion subgroup of an elliptic curve over* $K_1$, *we cannot use same argument for* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$. *Also we could not find any other method to check that it occurs or not over* $K_1$. *We cannot use above methods for* $X_1(20)$ *since it is a non-hyperelliptic curve of genus* $3$. *In this case we will use*

$$X_0(20) : y^2 = x^3 + x^2 + 4x + 4$$

*and show that there is no* $20$*-cycle over* $K_1$. *By* MAGMA, $X_0(20)(K_1) \simeq X_0(20)(\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$. *By [24],* $X_0(20)$ *has* $6$ *rational cusps. Hence all the points on* $X_0(20)(K_1)$ *are cusps.*

*Now consider*

$$X_0(24) : y^2 = x^3 - x^2 - 4x + 4.$$

*We will show that there is no* $24$*-cycle over* $K_1$. *By* MAGMA, $X_0(24)(K_1) \simeq X_0(24)(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. *By [24],* $X_0(24)$ *has* $8$ *rational cusps. Hence all the points on* $X_0(24)(K_1)$ *are cusps.*

**Theorem 7.3.3.** *The torsion of an elliptic curve over* $K_2$ *is isomorphic to one of the following groups:*

$$\mathbb{Z}/m\mathbb{Z},\ m = 1, \ldots, 10, 12, 14$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z},\ m = 1,...,4,6.$$

***Proof:*** *We already have all the torsion subgroups occuring over $\mathbb{Q}$.*

***Genus 1***

*Consider the following modular curve*

$$X_1(11) : y^2 - y = x^3 - x^2.$$

*By our computations we obtain that $X_1(11)(K_2) \simeq \mathbb{Z}/5\mathbb{Z} \simeq X_1(11)(\mathbb{Q})$ and all the points of $X_1(11)(K_2)$ are cusps. Hence we cannot obtain an elliptic curves with torsion $\mathbb{Z}/11\mathbb{Z}$ over $K_2$.*

*Consider the following modular curve*

$$X_1(14) : y^2 + xy + y = x^3 - x.$$

*By our computations we obtain that $X_1(14)(K_2) \simeq \mathbb{Z}^2 \times \mathbb{Z}/6\mathbb{Z}$ where $(-a^4 + 2a^3 - a^2, a^4 - a^3 - a^2 - a)$ and $(a^3 - a^2 + 1, a^4 - 3a^3 + 3a^2 - 2)$ are the points with infinite order. So we can have an elliptic curve over $K_2$ with torsion subgroup $\mathbb{Z}/14\mathbb{Z}$.*

*Consider the following modular curve*

$$X_1(15) : y^2 + xy + y = x^3 + x^2.$$

*By our computations we obtain that $X_1(15)(K_2) \simeq \mathbb{Z}/4\mathbb{Z} \simeq X_1(15)(\mathbb{Q})$ and all the points of $X_1(15)(K_2)$ are cusps. Hence we cannot obtain an elliptic curves with torsion $\mathbb{Z}/15\mathbb{Z}$ over $K_2$.*

*Consider the following modular curve*

$$X_1(2,10) : y^2 = x^3 + x^2 - x.$$

*By our computations we obtain that $X_1(2,10)(K_2) \simeq \mathbb{Z}/6\mathbb{Z} \simeq X_1(2,10)(\mathbb{Q})$ and all the points of $X_1(2,10)(K_2)$ are cusps. Hence we cannot obtain an elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ over $K_2$.*

*Consider the following modular curve*

$$X_1(2,12) : y^2 = x^3 - x^2 + x.$$

*By our computations we obtain that $X_1(2,12)(K_2) \simeq \mathbb{Z}^2 \times \mathbb{Z}/4\mathbb{Z}$ where*

*$(2a^2-2a+1,-2a+3)$ and $(a^4-a^3+a^2,-a^4+a^3+1)$ are the points with infinite order. So we can have an elliptic curve over $K_2$ with torsion subgroup $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$.*

***Genus 2***

*By* MAGMA, *$Tors(J_1(13)(K_2))\simeq\mathbb{Z}/19\mathbb{Z}$ and $Rank(J_1(13)(K_2))=0$. Since there is no growth in torsion and rank is 0, we can say that all the points on $X_1(13)$ are cusps.*

*By* MAGMA, *$Tors(J_1(16)(K_2))\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z}$ and $Rank(J_1(16)(K_2))=0$. Since there is no growth in torsion and rank is 0, we can say that all the points on $X_1(16)$ are cusps.*

*By* MAGMA, *$Tors(J_1(18)(K_2))\simeq\mathbb{Z}/21\mathbb{Z}$ and $Rank(J_1(18)(K_2))=0$. Since there is no growth in torsion and rank is 0, we can say that all the points on $X_1(18)$ are cusps.*

***Higher genus Curves***

*Since we cannot obtain 16-torsion over $K_2$,obviously $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/16\mathbb{Z}$ cannot occur over $K_2$.*

*Since $\mathbb{Z}/14\mathbb{Z}$ occur as a torsion subgroup of an elliptic curve over $K_2$, we cannot use same argument for $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/14\mathbb{Z}$. Also we could not find any other method to check its existence over $K_2$.*

*We cannot use above methods for $X_1(20)$ since it is a non-hyperelliptic curve of genus 3. In this case we will use*

$$X_0(20): y^2=x^3+x^2+4x+4$$

*and show that there is no 20-cycle over $K_2$. By* MAGMA, *$X_0(20)(K_2)\simeq X_0(20)(\mathbb{Q})\simeq\mathbb{Z}/6\mathbb{Z}$. By [24], $X_0(20)$ has 6 rational cusps. Hence all the points on $X_0(20)(K_2)$ are cusps.*

*By* MAGMA, *$X_0(24)(K_2)\simeq\mathbb{Z}^2\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$. Since rank is positive we cannot decide its existence over $K_2$.*

**Theorem 7.3.4.** *The torsion of an elliptic curve over $K_3$ is isomorphic to one of the following groups:*

$$\mathbb{Z}/m\mathbb{Z},\ m=1,...,12,14,15$$

$$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2m\mathbb{Z},\ m=1,...,6.$$

***Proof:*** *We already have all the torsion subgroups occuring over $\mathbb{Q}$.*

***Genus 1***

*By our computations we obtain that $X_1(11)(K_3) \simeq \mathbb{Z}\times\mathbb{Z}/5\mathbb{Z}$ where*

$$(\frac{1}{10082}(-14a^4+1397a^3-3725a^2+6161a+5289),\\ \frac{1}{715822}(177601a^4-125712a^3+16421a^2-103362a+477684))$$

*is the point with infinite order. So we can have an elliptic curve over $K_3$ with torsion subgroup $\mathbb{Z}/11\mathbb{Z}$.*

*By our computations we obtain that $X_1(14)(K_3) \simeq \mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ where*

$$(\frac{1}{1681}(445a^4-1432a^3+1199a^2+275a+685),\\ \frac{1}{68921}(2505a^4+115823a^3-170020a^2+32316a-66576))$$

*is the point with infinite order. So we can have an elliptic curve over $K_3$ with torsion subgroup $\mathbb{Z}/14\mathbb{Z}$.*

*By our computations we obtain that $X_1(15)(K_3) \simeq \mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ where $\left(\frac{1}{578}(-131a^4+481a^3-133a^2+1261a-74), \frac{1}{9826}(3163a^4+4557a^3+14522a^2+10119a-3969)\right)$ is the point with infinite order. So we can have an elliptic curve over $K_3$ with torsion subgroup $\mathbb{Z}/15\mathbb{Z}$.*

*By our computations we obtain that $X_1(2,10)(K_3) \simeq \mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ where $\left(\frac{1}{1225}(619a^4-78a^3+871a^2-1032a-279), \frac{1}{42875}(20586a^4+8993a^3+42669a^2-30183a-23476)\right)$ is the point with infinite order. So we can have an elliptic curve over $K_3$ with torsion subgroup $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z}$.*

*By our computations we obtain that $X_1(2,12)(K_3) \simeq \mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ where $\left(4a^4-9a^3+11a^2-23a+20, -29a^4+46a^3-64a^2+136a-76\right)$ is the point with infinite order. So we can have an elliptic curve over $K_3$ with torsion subgroup $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$.*

***Genus 2***

*By* MAGMA, *$Tors(J_1(13)(K_3)) \simeq \mathbb{Z}/19\mathbb{Z}$ and $Rank(J_1(13)(K_3)) = 0$. Since there is no growth in torsion and rank is* 0, *we can say that all the points on $X_1(13)$ are cusps.*

*By* MAGMA, *$Tors(J_1(16)(K_3)) \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z}$ and $Rank(J_1(16)(K_3)) \leq 2$.*

*By* MAGMA*, $Tors(J_1(18)(K_3)) \simeq \mathbb{Z}/21\mathbb{Z}$ and $Rank(J_1(18)(K_3)) \leq 2$.*

*Since we could not obtain lower bound $Rank(J_1(16)(K_2))$ and $Rank(J_1(18)(K_2))$, we cannot decide existence of $\mathbb{Z}/16\mathbb{Z}$ and $\mathbb{Z}/18\mathbb{Z}$ over $K_3$.*

***Higher genus Curves***

*We cannot say anything about existence of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$ ,since we do not have information about $X_1(14)$ and $X_1(16)$.*

*By* MAGMA*, $X_0(20)(K_3) \simeq \mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Since rank is positive we cannot decide existence $\mathbb{Z}/20\mathbb{Z}$ over $K_3$.*

*By* MAGMA*, $X_0(24)(K_3) \simeq \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Since rank is positive we cannot decide existence $\mathbb{Z}/24\mathbb{Z}$ over $K_3$.*

**Theorem 7.3.5.** *The torsion of an elliptic curve over $K_4$ is isomorphic to one of the following groups:*

$$\mathbb{Z}/m\mathbb{Z},\ m = 1, ..., 10, 12, 15$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z},\ m = 1, ..., 5.$$

***Proof:*** *We already have all the torsion subgroups occuring over $\mathbb{Q}$.*

***Genus 1***

*By our computations we obtain that $X_1(11)(K_4) \simeq \mathbb{Z}/5\mathbb{Z} \simeq X_1(11)(\mathbb{Q})$ and all the points of $X_1(11)(K_4)$ are cusps. Hence we cannot obtain an elliptic curves with torsion $\mathbb{Z}/11\mathbb{Z}$ over $K_4$.*

*By our computations we obtain that $X_1(14)(K_4) \simeq \mathbb{Z}/6\mathbb{Z} \simeq X_1(14)(\mathbb{Q})$ and all the points of $X_1(14)(K_4)$ are cusps. Hence we cannot obtain an elliptic curves with torsion $\mathbb{Z}/14\mathbb{Z}$ over $K_4$.*

*By our computations we obtain that $X_1(15)(K_4) \simeq \mathbb{Z}^2 \times \mathbb{Z}/4\mathbb{Z}$ where $(a^4 - a^3 + a^2, -a^4 + 3a^3 - 5a^2 + 4a - 3)$ and $\left(\frac{1}{4}(a^4 + 2), \frac{1}{8}(-5a^4 + 2a^3 + 2a^2 - 10)\right)$ are the points with infinite order. So we can have an elliptic curve over $K_4$ with torsion subgroup $\mathbb{Z}/15\mathbb{Z}$.*

*By our computations we obtain that $X_1(2,10)(K_4) \simeq \mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ where $(a^3 + 1, a^4 + 2a - 1)$ is the point with infinite order. So we can have an elliptic curve over $K_4$ with torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$.*

*By our computations we obtain that $X_1(2,12)(K_4) \simeq \mathbb{Z}/4\mathbb{Z} \simeq X_1(2,12)(\mathbb{Q})$ and all the points of $X_1(2,12)(K_4)$ are cusps. Hence we cannot obtain an elliptic curves* *with torsion $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$ over $K_4$.*

***Genus 2***

*By* MAGMA*, $Tors(J_1(13)(K_4))\simeq\mathbb{Z}/19\mathbb{Z}$ and $Rank(J_1(13)(K_4))=0$. Since there is no growth in torsion and rank is $0$, we can say that all the points on $X_1(13)$ are cusps.*

*By* MAGMA*, $Tors(J_1(16)(K_4))\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z}$ and $Rank(J_1(16)(K_4))=0$. Since there is no growth in torsion and rank is $0$, we can say that all the points on $X_1(16)$ are cusps.*

*By* MAGMA*, $Tors(J_1(18)(K_4))\simeq\mathbb{Z}/21\mathbb{Z}$ and $Rank(J_1(18)(K_4))=0$. Since there is no growth in torsion and rank is $0$, we can say that all the points on $X_1(18)$ are cusps.*

***Higher genus Curves***

*Since we cannot obtain $14$-torsion over $K_4$,obviously $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/14\mathbb{Z}$ cannot occur over $K_4$.*

*Since we cannot obtain $16$-torsion over $K_4$,obviously $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/16\mathbb{Z}$ cannot occur over $K_4$.*

*By* MAGMA*, $X_0(20)(K_4)\simeq\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$. Since rank is positive, we cannot decide existence $\mathbb{Z}/20\mathbb{Z}$ over $K_4$.*

*Now consider*

$$X_0(24):y^2=x^3-x^2-4x+4.$$

*We will show that there is no $24$-cycle over $K_4$. By* MAGMA*, $X_0(24)(K_4)\simeq X_0(24)(\mathbb{Q})\simeq\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$. By [24], $X_0(24)$ has $8$ rational cusps. Hence all the points on $X_0(24)(K_4)$ are cusps.*

**Theorem 7.3.6.** *The torsion of an elliptic curve over $K_5$ is isomorphic to one of the following groups:*

$$\mathbb{Z}/m\mathbb{Z},\ m=1,...,12$$

$$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2m\mathbb{Z},\ m=1,...,4.$$

***Proof:*** *We already have all the torsion subgroups occuring over $\mathbb{Q}$.*

***Genus 1***

*By our computations we obtain that $X_1(11)(K_5) \simeq \mathbb{Z}/25\mathbb{Z}$. In this case we obtain following* 3 *non-isomoprhic elliptic curves over $K_5$ with torsion subgroup $\mathbb{Z}/15\mathbb{Z}$.*

$$\begin{aligned} y^2+(-4a^4+11a^3-3a^2-8a+3)xy+(-652a^4+1739a^3-321a^2-1380a+383)y \\ = x^3+(-155a^4+411a^3-73a^2-325a+90)x^2, \end{aligned}$$

$$\begin{aligned} &y^2+(501a^4-918a^3-1241a^2+2537a-605)xy+(-7687269a^4+14074083a^3+19055905a^2 \\ &-38894025a+9252517)y = x^3+(-484791a^4+887570a^3+1201744a^2-2452818a+583502)x^2, \end{aligned}$$

$$\begin{aligned} y^2+(4a^4-8a^3-8a^2+22a-10)xy+(-739a^4+1329a^3+1869a^2-3669a+788)y \\ = x^3+(-180a^4+318a^3+464a^2-877a+168)x^2. \end{aligned}$$

*By our computations we obtain that $X_1(14)(K_5) \simeq \mathbb{Z}/6\mathbb{Z} \simeq X_1(14)(\mathbb{Q})$ and all the points of $X_1(14)(K_5)$ are cusps. Hence we cannot obtain an elliptic curves with torsion $\mathbb{Z}/14\mathbb{Z}$ over $K_5$.*

*By our computations we obtain that $X_1(15)(K_5) \simeq \mathbb{Z}/4\mathbb{Z} \simeq X_1(15)(\mathbb{Q})$ and all the points of $X_1(15)(K_5)$ are cusps. Hence we cannot obtain an elliptic curves with torsion $\mathbb{Z}/15\mathbb{Z}$ over $K_5$.*

*By our computations we obtain that $X_1(2,10)(K_5) \simeq \mathbb{Z}/6\mathbb{Z} \simeq X_1(2,10)(\mathbb{Q})$ and all the points of $X_1(2,10)(K_5)$ are cusps. Hence we cannot obtain an elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ over $K_5$.*

*By our computations we obtain that $X_1(2,12)(K_5) \simeq \mathbb{Z}/4\mathbb{Z} \simeq X_1(2,12)(\mathbb{Q})$ and all the points of $X_1(2,12)(K_5)$ are cusps. Hence we cannot obtain an elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ over $K_5$.*

***Genus 2***

*By* MAGMA, *$Tors(J_1(13)(K_5)) \simeq \mathbb{Z}/19\mathbb{Z}$ and $Rank(J_1(13)(K_5)) = 0$. Since there is no growth in torsion and rank is* 0, *we can say that all the points on $X_1(13)$ are cusps.*

*By* MAGMA, *$Tors(J_1(16)(K_5)) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ and $Rank(J_1(16)(K_5)) = 0$. Since there is no growth in torsion and rank is* 0, *we can say that all the points on $X_1(16)$ are cusps.*

*By* MAGMA, *$Tors(J_1(18)(K_5)) \simeq \mathbb{Z}/21\mathbb{Z}$ and $Rank(J_1(18)(K_5)) = 0$. Since there is no growth in torsion and rank is* 0, *we can say that all the points on $X_1(18)$ are* *cusps.*

***Higher genus Curves***

*Since we cannot obtain* $14$*-torsion over* $K_4$*,obviously* $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/14\mathbb{Z}$ *cannot occur over* $K_4$*.*

*Since we cannot obtain* $16$*-torsion over* $K_4$*,obviously* $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/16\mathbb{Z}$ *cannot occur over* $K_4$*.*

*We cannot use above methods for* $X_1(20)$ *since it is a non-hyperelliptic curve of genus* $3$*. In this case we will use*

$$X_0(20) : y^2 = x^3 + x^2 + 4x + 4$$

*and show that there is no* $20$*-cycle over* $K_5$*. By* MAGMA*,*
$X_0(20)(K_5) \simeq X_0(20)(\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$*.*

*By [24],* $X_0(20)$ *has* $6$ *rational cusps. Hence all the points on* $X_0(20)(K_5)$ *are cusps.*

*Now consider*

$$X_0(24) : y^2 = x^3 - x^2 - 4x + 4.$$

*We will show that there is no* $24$*-cycle over* $K_5$*. By* MAGMA*,*
$X_0(24)(K_5) \simeq X_0(24)(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$*.*

*By [24],* $X_0(24)$ *has* $8$ *rational cusps. Hence all the points on* $X_0(24)(K_5)$ *are cusps.*

# BIBLIOGRAPHY

[1] Andrew v. sutherland. https://math.mit.edu/~drew/. Accessed: 2023-10-17.

[2] Samir siksek. https://homepages.warwick.ac.uk/staff/S.Siksek/progs/chabnf/g2-jac.m. Accessed: 2023-10-17.

[3] H. Baaziz. Equations for the modular curve x1(n) and models of elliptic curves with torsion points. Math. Comput., 79:2371–2386, 2010. URL https://api.semanticscholar.org/CorpusID:5656324.

[4] W. Bosma, J. J. Cannon, and C. Playoust. The magma algebra system i: The user language. J. Symb. Comput., 24:235–265, 1997. URL https://api.semanticscholar.org/CorpusID:17976479.

[5] H. B. Daniels and E. González-Jiménez. On the torsion of rational elliptic curves over sextic fields. Math. Comput., 89:411–435, 2018. URL https://api.semanticscholar.org/CorpusID:52037385.

[6] M. Derickx and A. Sutherland. Torsion subgroups of elliptic curves over quintic and sextic number fields. Proceedings of the American Mathematical Society, 145(10):4233–4245, 2017.

[7] M. Derickx, A. Etropolski, M. van Hoeij, J. S. Morrow, and D. Zureick-Brown. Sporadic cubic torsion. Algebra & Number Theory, 2020. URL https://api.semanticscholar.org/CorpusID:220830727.

[8] G. Faltings. Endlichkeitssätze für abelsche varietäten über zahlkörpern. Inventiones mathematicae, 73:349–366, 1983. URL https://api.semanticscholar.org/CorpusID:121049418.

[9] S. D. Galbraith. Equations for modular curves. 1996. URL https://api.semanticscholar.org/CorpusID:117979661.

[10] E. González-Jiménez. Complete classification of the torsion structures of rational elliptic curves over quintic number fields. Journal of Algebra, 478: 484–505, 2016. URL https://api.semanticscholar.org/CorpusID:5559913.

[11] E. González-Jiménez and Á. Lozano-Robledo. On the torsion of rational elliptic curves over quartic fields. Math. Comput., 87:1457–1478, 2016. URL https://api.semanticscholar.org/CorpusID:3760150.

[12] E. González-Jiménez, F. Najman, and J. M. Tornero. Torsion of rational elliptic curves over cubic fields. The Rocky Mountain Journal of Mathematics, 46(6):1899–1917, 2016.

[13] D. Jeon. Defining equations of certain modular curves. 2013. URL https://api.semanticscholar.org/CorpusID:123674429.

[14] *D. Jeon, C. H. Kim, and A. Schweizer. On the torsion of elliptic curves over cubic number fields.* Acta Arithmetica*, 113:291–301, 2004. URL https://api.semanticscholar.org/CorpusID:55416029.*

[15] *J. W. Jones and D. P. Roberts. A database of number fields.* Lms Journal of Computation and Mathematics*, 17:595–618, 2014. URL https://api.semanticscholar.org/CorpusID:119148870.*

[16] *S. Kamienny. Torsion points on elliptic curves and q-coefficients of modular forms.* Inventiones mathematicae*, 109:221–229, 1992. URL https://api.semanticscholar.org/CorpusID:118750444.*

[17] *M. A. Kenku and F. Momose. Torsion points on elliptic curves defined over quadratic fields.* Nagoya Mathematical Journal*, 109:125 – 149, 1975. URL https://api.semanticscholar.org/CorpusID:16816807.*

[18] *D. S. Kubert. Universal bounds on the torsion of elliptic curves.* Proceedings of The London Mathematical Society*, pages 193–237, 1976. URL https://api.semanticscholar.org/CorpusID:122966249.*

[19] *Q. Liu and D. J. Lorenzini. New points on curves.* arXiv: Number Theory*, 2017. URL https://api.semanticscholar.org/CorpusID:85550568.*

[20] *B. Mazur. Modular curves and the eisenstein ideal.* Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, 47:33–186, 1977. URL https://api.semanticscholar.org/CorpusID:122609075.*

[21] *B. Mazur and D. Goldfeld. Rational isogenies of prime degree.* Inventiones mathematicae*, 44:129–162, 1978. URL https://api.semanticscholar.org/CorpusID:121987166.*

[22] *F. Najman. Torsion of elliptic curves over cubic fields.* Journal of Number Theory*, 132:26–36, 2011. URL https://api.semanticscholar.org/CorpusID:8732125.*

[23] *F. Najman. Torsion of rational elliptic curves over cubic fields and sporadic points on $x_1(n)$.* Mathematical Research Letters*, 23(1):245–272, 2016. ISSN 1073-2780. doi: 10.4310/MRL.2016.v23.n1.a12.*

[24] *A. P. Ogg. Rational points on certain elliptic modular curves. Vol. XXIV: 221–231, 1973.*

[25] *F. P. Rabarison. Structure de torsion des courbes elliptiques sur les corps quadratiques.* Acta Arithmetica*, 144:17–52, 2010. URL https://api.semanticscholar.org/CorpusID:123097183.*

[26] *M. A. Reichert. Explicit determination of nontrivial torsion structures of elliptic curves over quadratic number fields.* Mathematics of Computation*, 46: 637–658, 1986. URL https://api.semanticscholar.org/CorpusID:121647015.*

[27] *F. N. Sheldon Kamienny. Torsion groups of elliptic curves over quadratic fields.* Acta Arithmetica*, 152(3):291–305, 2012. URL http://eudml.org/doc/279075.*

*[28] J. H. Silverman. The arithmetic of elliptic curves. In* Graduate texts in mathematics*, 1986. URL https://api.semanticscholar.org/CorpusID:117121125.*

*[29] Y. Yang. Defining equations of modular curves.* Advances in Mathematics*, 204:481–508, 2006. URL https://api.semanticscholar.org/CorpusID:55340273.*