university of groningen

faculty of science and engineering

Elliptic curves with $\mathbb{Q}$-rational points of order n

Bachelor's Project Mathematics

July 7, 2023

Student: L. Wiersema

First supervisor: Dr. P. Kılıçer

Second supervisor: Prof. J. Top

Abstract

We give an overview of the basic concepts of elliptic curves. We use the Tate normal form of the equation of an elliptic curve to classify all elliptic curves over $\mathbb{Q}$ with a rational torsion point of given order greater than 3 up to isomorphism. We give the definition of the division polynomials and look at their uses in the context of elliptic curves. We give a proof of the non-existence of an elliptic curve over $\mathbb{Q}$ with a rational torsion point of order 11.

Contents

Preface

The study of elliptic curves constitutes a major area of current research within the field of mathematics, especially in number theory. It combines concepts from algebra, number theory and geometry. Elliptic curves have many applications in mathematics. For example, elliptic curves were used to prove Fermat's Last Theorem, and elliptic curves over finite fields can be used in the field of cryptography.

In Section 1, we define elliptic curves and the group law on them. We also look at some important results regarding the group structures of elliptic curves. In particular, we cover Mazur's theorem about the torsion subgroup of elliptic curves over the rational numbers.
In Section 2, we cover isomorphisms between elliptic curves in the Weierstrass normal form. We also define some invariants associated to elliptic curves.
In Section 3, we find conditions on the coefficients of the equation of an elliptic curve for which the elliptic curve has a point of order 2 or 3. We also look at some families of curves with points of order 2 or 3.
In Section 4, we define the Tate normal form of an elliptic curve, and show how we can use them to classify elliptic curves over $\mathbb{Q}$ with a point of a particular order greater than 3 up to isomorphism. In Section 5, we find these families of elliptic curves.
In Section 6, we define the sequence of polynomials called the division polynomials and cover some of their uses in the context of elliptic curves. We also explain how they can be used to write an algorithm to find elliptic curves with trivial torsion subgroup.
Finally, in Section 7, we give a proof of the fact that there are no elliptic curves over $\mathbb{Q}$ with a rational torsion point of order 11. In this section, we use some concepts from algebraic number theory.

Acknowledgements

I want to thank my supervisors Pınar Kılıçer and Jaap Top for all of their support and feedback.
I want to thank Remco de Jong, Milène Mandeville, Stef Nomden and Tijmen van der Ree for their input and suggestions.
Finally, I want to thank my family, for supporting me and always being there.

1 Elliptic curves

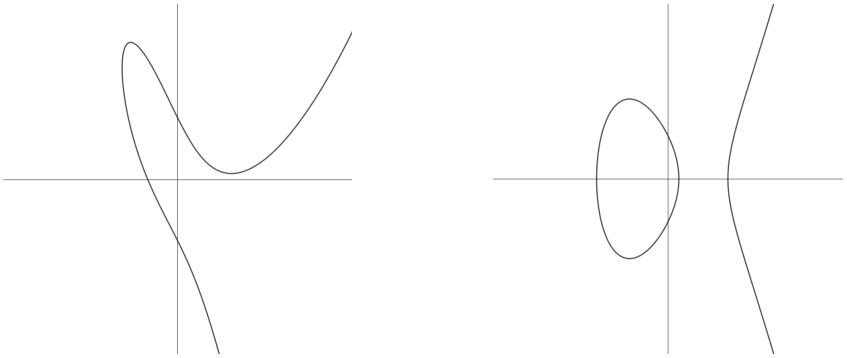
In this section, we explain the basic ideas of elliptic curves.

Definition 1.1 (Elliptic Curves)**.** An elliptic curve $E = E(K)$ over a field K is a non-singular plane algebraic curve. In other words, it is the set of all points $(x, y) \in K^2$ that satisfy the equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.1}$$

for some $a_1, a_2, a_3, a_4, a_6 \in K$, together with the 'point at infinity' O which lies on every vertical line. An explanation of this point can be found in Section 1.1. An equation of the form (1.1) is said to be in the Weierstrass normal form. We also denote the right-hand side of (1.1) by $f(x)$.

The curve given by (1.1) has to be non-singular. We discuss what this means in Section 1.3.
In Figure 1, some examples of elliptic curves over $\mathbb{R}$ are shown.



(a) $y^2 + 4xy = x^3 - 3x^2 + 6$ (b) $y^2 = x^3 - 7x + 3$

Figure 1: Examples of elliptic curves over $\mathbb{R}$.

1.1 The projective plane

This section is based on [Was08] and [Hus04].

To understand the meaning of the 'point at infinity' O, we need to know some basic projective geometry. Let K be a field. The projective plane $\mathbb{P}^2_K$ over K is a projective space given by equivalence classes of triples (x, y, z), where x, y and z are in K and at least one of x, y and z is non-zero. We say that two triples (x_1, y_1, z_1) and (x_2, y_2, z_2) are equivalent if there exists a non-zero $\lambda \in K$ such that $(x_1, y_1, z_1) = (\lambda x_2, \lambda y_2, \lambda z_2)$. We denote this equivalence by $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$. The equivalence classes are denoted by $(x : y : z)$, and they are called points in the projective plane.

Lemma 1.2 (Projective lines)**.** *The following statements are true.*

- *Let $(a : b : c)$ and $(\alpha : \beta : \gamma)$ be two distinct points in $\mathbb{P}^2_K$. Then there is a unique line through these two points, given by*

$$\det\left(\begin{bmatrix} x & y & z \\ a & b & c \\ \alpha & \beta & \gamma \end{bmatrix}\right) = 0.$$

- *Two lines $ux + vy + wz = 0$ and $u'x + v'y + w'z = 0$ in $\mathbb{P}^2_K$ coincide if and only if their coefficients satisfy $(u : v : w) = (u' : v' : w')$.*

- *Two distinct lines in $\mathbb{P}^2_K$ intersect in exactly one point.*

We omit the proof of this lemma.

On the projective plane, we can make a distinction between "finite points" and "points at infinity". If $z \neq 0$, we can always write $(x : y : z) = (\frac{x}{z} : \frac{y}{z} : 1)$. Such points are called "finite points".
If $z = 0$ however, we can think of dividing by z as giving ∞ in the x- or y-coordinate. Therefore, we call points of the form $(x : y : 0)$ the "points at infinity".

In the context of projective geometry, we call the plane K^2 the affine plane. We can include the affine plane K^2 in the projective plane $\mathbb{P}^2_K$ using the map

$$(x, y) \mapsto (x : y : 1).$$

In other words, the affine plane can be identified with the set of finite points of the projective plane.

1.2 Homogeneous polynomials

This section is based on [Was08].

A polynomial $F(x, y, z)$ over a field K is called homogeneous of degree n if every monomial term of F is of the form $a \cdot x^i y^j z^k$, where $a \in K$ and $i + j + k = n$. In this case F has the property that $F(\lambda x, \lambda y, \lambda z) = \lambda^n F(x, y, z)$ for all $\lambda \in K$. Therefore, if $(x_1, y_1, z_1) \sim (x_2, y_2, z_2)$, we have $F(x_1, y_1, z_1) = 0 \iff F(x_2, y_2, z_2) = 0$. This means that a zero of F in the projective plane $\mathbb{P}^2_K$ is independent of the choice of representative, and hence the set of zeros of F in $\mathbb{P}^2_K$ is well-defined.

We can make any polynomial homogeneous by inserting the appropriate powers of z. Doing this may allow us to find more solutions to equations by including the points at infinity in their solution domain.

Example 1.3. We can find an intersection point of two distinct vertical lines. Consider the vertical lines $x = a$ and $x = b$, where $a, b \in K$ and $a \neq b$. These lines do not intersect in the affine plane. We can make both lines homogeneous of order 1 by inserting a factor z on the right hand side. We obtain equations $x = az$ and $x = bz$, respectively. We can find solutions at infinity by setting $z = 0$. In this case, we find that there is only one intersection, for $x = 0$ and $z = 0$. We need that $y \neq 0$, so we get that the only solution is $(0 : 1 : 0)$.

Let E be an elliptic curve over K given by the polynomial equation

$$y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0. \tag{1.2}$$

By substituting the appropriate powers of z into (1.2), we can turn this polynomial into a homogeneous polynomial of degree 3:

$$y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3 = 0. \tag{1.3}$$

The points (x, y) on the curve in the affine plane correspond to the finite points $(x : y : 1)$ on the curve in the projective plane. To find points on this curve that lie at infinity, we set $z = 0$ in (1.3) and we obtain:

$$-x^3 = 0.$$

The only solution to this equation is $x = 0$. We can conclude that the only point at infinity that lies on the curve is $(0 : 1 : 0)$. As we found in Example 1.3, this is the unique point that lies on all vertical lines. This is the point that we call O.

For most purposes of this text, it provides no advantage to work with projective coordinates. For this reason, we use affine coordinates to denote points on E and treat the point at infinity O as a special point, unless specified otherwise.

1.3 The group law

This section is based on [Hus04].

Consider an elliptic curve E over a field K given by an equation in Weierstrass normal form (1.1). The plane curve given by (1.1) has to be non-singular. In this section, we explain what it means for a curve to be non-singular. We also show that, since the plane curve given by (1.1) is non-singular, we can define an algebraic structure on E called the chord-tangent law. We can then use the chord-tangent law to define a group law on $E(K)$.

Consider a cubic curve C over a field K given by the homogeneous equation

$$F(x, y, z) = y^2z + a_1xyz + a_3yz^2 - x^3 - a_2x^2z - a_4xz^2 - a_6z^3 = 0. \tag{1.4}$$

Definition 1.4 (Non-singular curve)**.** A plane algebraic curve given by (1.4) is non-singular if there is no point on the curve where all partial derivatives of $F(x, y, z)$ vanish simultaneously.

Whether a cubic curve is non-singular depends on the coefficients of the equation that defines it. We can make this condition on the coefficients more explicit.

For ease of notation, we define the following coefficients associated to the curve given by (1.4):

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= a_1a_3 + 2a_4, \\ b_6 &= a_3^2 + 4a_6, \\ b_8 &= a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2. \end{aligned} \tag{1.5}$$

These coefficients are related by

$$4b_8 = b_2b_6 - b_4^2.$$

Using this notation, we can define a quantity associated to the cubic curve called the discriminant.

Definition 1.5 (Discriminant)**.** Let C be the cubic curve over a field K given by (1.4). With notation as above, the discriminant Δ of C is defined as

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6. \tag{1.6}$$

We can use the discriminant to determine whether a cubic curve is non-singular.

Theorem 1.6. *A plane algebraic curve given by* (1.4) *is non-singular if and only if its discriminant* Δ *as given by* (1.6) *is non-zero.*

A curve of the form (1.1) is an elliptic curve precisely when it is non-singular.

Proposition 1.7. *Let K be a field. Let L be a line and let C be a cubic curve in $\mathbb{P}^2_K$. Suppose L intersects C in two K-rational points, counting multiplicities. Then, there is a third K-rational intersection point.*

Proof. Let the line L be given by $ax + by + cz = 0$ and let the cubic C be given by $F(x, y, z) = 0$, where $F(x, y, z)$ is a homogeneous polynomial. We can use the equation for L to eliminate one variable in the third-order equation of the cubic.

For intersections off the line $z = 0$, we can find a polynomial equation in the x-coordinate or in the y-coordinate of the intersection points. Thus, the intersection points are rational if and only if the roots of the cubic equation are rational.

Henceforth, it is sufficient to prove the following algebraic statement: if a cubic polynomial with rational coefficients has two rational roots, then the third root is rational. This is a well-known result from algebra. □

Another way to phrase Proposition 1.7 in the context of elliptic curves is: if P and Q are points on an elliptic curve E, then the line through P and Q intersects E in a third point R. This is the idea behind the following geometric construction, called the chord-tangent law.

Definition 1.8 (Chord-tangent law)**.** Let E be an elliptic curve over a field K given by (1.1).
Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points on E. If $P_1 \neq P_2$, let L be the line through P_1 and P_2. If $P_1 = P_2$, let L be the tangent line to E at P_1. By Proposition 1.7, the line L intersects E in a third point, counting multiplicities, which we denote by $R(P_1, P_2)$. If L is vertical, the third point is the point at infinity O, which is on every vertical line.

The chord-tangent law is not a group law on $E(K)$. However, we can use it to define a more sophisticated construction on $E(K)$ which is. The following proposition is also used in this construction.

Proposition 1.9 (Inverse)**.** *Suppose (x, y) is a point in $E(K)$. Then $(x, -y - a_1x - a_3)$ is also a point in $E(K)$. We call this point the inverse of (x, y) and denote it by $-(x, y)$.*

Proof. Since (x, y) has coordinates in K, clearly $(x, -y - a_1x - a_3)$ also has coordinates in K. Therefore, it is sufficient to show that $(x, -y - a_1x - a_3)$ is in $E(K)$.
We know that (x, y) satisfies the equation (1.1), since (x, y) is in $E(K)$. We can verify that the point $(x, -y - a_1x - a_3)$ also satisfies (1.1) by a direct computation:

$$(-y - a_1x - a_3)^2 + a_1x(-y - a_1x - a_3) + a_3(-y - a_1x - a_3) = y^2 + a_1xy + a_3y = f(x).$$

This concludes the proof. □

Remark 1.10 (Symmetry line)**.** If the characteristic of the field K is different from 2, it follows from Proposition 1.9 that E has vertical symmetry around the line given by

$$y = -\frac{a_1 x + a_3}{2}. \tag{1.7}$$

We call this the symmetry line of E.

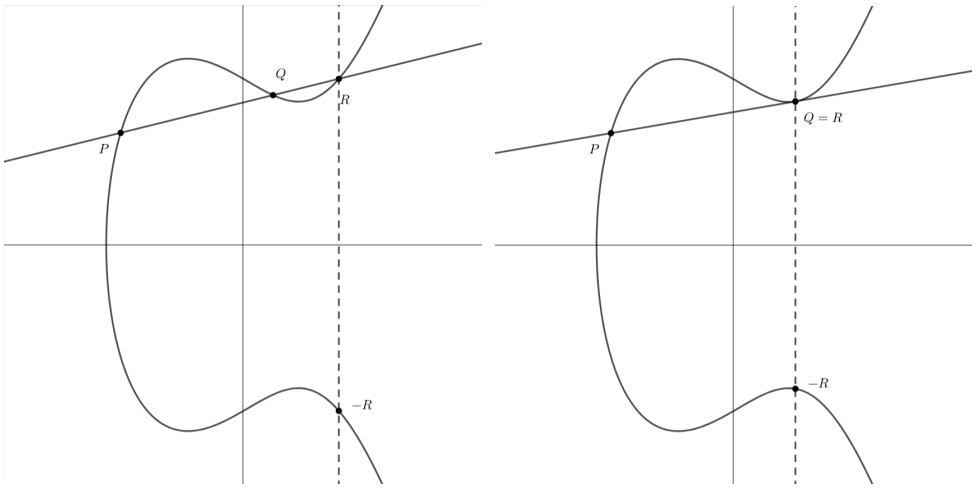
Recall from Subsection 1.2 that O is the point $(0 : 1 : 0)$, which is the unique point that lies on every vertical line. Since $(0 : -1 : 0) = (0 : 1 : 0)$, we can say that the "top" and "bottom" of every vertical line is the same. Therefore, $-O = O$. In addition, the line through O and a finite point $P = (x, y)$ on E is always vertical, so the third point on this line is always $-P$. Since O is the only point at infinity on E, we say that the third point through O and O is O itself.

With the chord-tangent law and the notion of inverse in mind, we can define the group law on $E(K)$.

Definition 1.11 (Group law)**.** The group law on $E(K)$ is defined using the chord-tangent law. For any points P_1 and P_2 in $E(K)$, we define

$$P_1 + P_2 = -R(P_1, P_2).$$

The identity element is O. The inverse of a point P_1 is $-P_1$. The group law as defined above is associative, but the proof of this is omitted. A proof can be found in [Hus04, Chapter 3.1, theorem 1.2]. Some illustrative examples of the construction of the group law are depicted in Figure 2.



(a) P, Q and R distinct (b) $Q = R$

(c) $P = Q$ (d) $Q = -P$

Figure 2: Examples of the construction of the group law, where $R := R(P, Q)$.

Remark 1.12. Assume P, Q and R are distinct K-rational points on an elliptic curve E. By the definition of the group law, the three points lie on a line if and only if

$$P + Q + R = O.$$

Notation 1.13 (Multiples)**.** Assume P is a point in $E(K)$. For any positive integer n, it is conventional to denote the sum

$$\underbrace{P + P + \cdots + P}_{n \text{ times}}$$

by nP. By associativity, the inverse of nP is equal to n times the inverse of P, i.e. $-(nP) = n(-P)$. Therefore, this point is denoted by $-nP$.

Remark 1.14 (Tangent lines)**.** The tangent line to E at a point (x, y) can be found using formal differentiation of equation (1.1). We consider $y = y(x)$ and differentiate both sides with respect to x:

$$\begin{aligned} \tfrac{\mathrm{d}}{\mathrm{d}x}\left(y(x)^2 + a_1 x y(x) + a_3 y(x)\right) &= f'(x) \\ 2y(x)y'(x) + a_1 y(x) + a_1 x y'(x) + a_3 y'(x) &= f'(x) \\ (2y(x) + a_1 x + a_3)y'(x) &= f'(x) - a_1 y(x). \end{aligned}$$

If (x, y) is such that $2y + a_1 x + a_3 = 0$, then by Proposition 1.9 the point (x, y) is equal to its inverse, i.e. $-(x, y) = (x, y)$. This means that $(x, y) + (x, y) = O$, so $-O = O$ is on the tangent line to E at (x, y). Henceforth, the tangent line at (x, y) is vertical. If the characteristic of K is different from 2, this happens if and only if (x, y) is on the symmetry line (1.7). Otherwise, we get that the slope of the tangent line is

$$y'(x, y) = \frac{f'(x) - a_1 y}{2y + a_1 x + a_3}. \tag{1.8}$$

Let P and Q be points in $E(K)$, and let L be the line through P and Q. If L is not vertical, it can be represented by an equation $y = \lambda x + \beta$. The x-coordinate of $R(P, Q)$ can be found by substituting the expression $y = \lambda x + \beta$ into (1.1) and solving the resulting cubic polynomial for x. Using the fact that x_1 and x_2 are roots of this polynomial, we can find the root decomposition of this polynomial. This also gives us the third root.

Remark 1.15 (Formulas for addition)**.** Let E be the elliptic curve over a field K given by (1.1).
Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points on E, and let L be the line through P_1 and P_2 as defined in 1.8. Here, we give computations of the group law to find the coordinates of the point $P_1 + P_2$ explicitly.

1. If $x_1 \neq x_2$: the line L is given by $y = \lambda x + \beta$, where $\lambda = (y_2 - y_1)/(x_2 - x_1)$ and $\beta = y_1 - \lambda x_1$.
2. If $x_1 = x_2$ but $y_1 \neq y_2$: the line L is the vertical line given by $x = x_1$.
3. If $P_1 = P_2$ and $2y_1 + a_1 x_1 + a_3 = 0$: the line L is the tangent line to E at P_1, which is the vertical line $x = x_1$.
4. If $P_1 = P_2$ and $2y_1 + a_1 x_1 + a_3 \neq 0$: the line L is the tangent line to E at P_1, given by $y = \lambda x + \beta$, where $\lambda = y'(x_1, y_1)$ and $\beta = y_1 - \lambda x_1$.

In cases 2 and 3, the line L is vertical and hence we have $R(P_1, P_2) = O$.
In cases 1 and 4, we use the chord-tangent law to find the third point $R(P_1, P_2)$. This point has coordinates (x_3, y_3), where

$$\begin{aligned} x_3 &= \lambda^2 + \lambda a_1 - a_2 - x_1 - x_2, \\ y_3 &= \lambda x_3 + \beta. \end{aligned} \tag{1.9}$$

Finally, we have $P_1 + P_2 = -R(P_1, P_2)$, so

$$P_1 + P_2 = (x_3, -y_3 - a_1 x_3 - a_3). \tag{1.10}$$

1.4 The group structure

In this section, we give some important results regarding the structure of the group on elliptic curve.

Definition 1.16 (Torsion points and order)**.** Assume P is a K-rational point on an elliptic curve E. If there exists a positive integer n such that $nP = O$, we say that P is a torsion point of $E(K)$. The group of all torsion points of $E(K)$ is called the torsion subgroup of $E(K)$ and is denoted by $\mathrm{Tor}\,(E(K))$. If P is a torsion point, the smallest positive integer m such that $mP = O$ is called the order of P.

It has been shown that the torsion subgroup of an elliptic curve over the field $\mathbb{Q}$ of rational numbers can only have one of few possible structures. The following result was shown by Mazur [Maz77].

Theorem 1.17 (Mazur)**.** *Let E be an elliptic curve over $\mathbb{Q}$. Then, $\mathrm{Tor}\,(E(\mathbb{Q}))$ is isomorphic to either*

$$\mathbb{Z}/m\mathbb{Z} \quad \text{for } m = 1, 2, \ldots, 10, 12$$

or

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

In particular, this means that the order of a $\mathbb{Q}$-rational torsion point on E must be in $\{1, 2, \ldots, 10, 12\}$.

The following theorem by Mordell is an important result about the torsion group of an elliptic curve over $\mathbb{Q}$ [Mor22].

Theorem 1.18 (Mordell)**.** *Let E be an elliptic curve over $\mathbb{Q}$. Then the group $E(\mathbb{Q})$ is a finitely generated abelian group.*

We omit the proof, as it is beyond the scope of this paper.

The possible structures of finitely generated abelian groups are all known.

Theorem 1.19 (Fundamental theorem of finitely generated abelian groups)**.** *Let G be a finitely generated abelian group. Then G is isomorphic to*

$$\mathrm{Tor}(G) \times \mathbb{Z}^r$$

for some unique finite non-negative integer r. The number r is called the rank of G.

We omit the proof, as it is beyond the scope of this paper.

By Theorems 1.18 and 1.19, we can always write

$$E(\mathbb{Q}) \cong \mathrm{Tor}(E(\mathbb{Q})) \times \mathbb{Z}^r$$

for some unique finite non-negative integer r, depending on E.

2 Isomorphisms

This section is based on [Hus04].

We can define isomorphisms between elliptic curves and some quantities associated to them.

2.1 Isomorphisms between elliptic curves

We can define maps between elliptic curves with equations in the Weierstrass normal form by means of a change of variables.

Definition 2.1 (Admissible change of variables)**.** An admissible change of variables in the equation of an elliptic curve is one of the form

$$x = u^2\overline{x} + r \text{ and } y = u^3\overline{y} + su^2\overline{x} + t, \tag{2.1}$$

where $u, r, s, t \in K$ and $u \neq 0$.

An admissible change of variables as in (2.1) yields a new form of the equation in variables $\overline{x}$ and $\overline{y}$:

$$\overline{y}^2 + \overline{a}_1\overline{x}\overline{y} + \overline{a}_3\overline{y} = \overline{x}^3 + \overline{a}_2\overline{x}^2 + \overline{a}_4\overline{x} + \overline{a}_6, \tag{2.2}$$

where the coefficients are given by

$$\begin{aligned} u\overline{a}_1 &= a_1 + 2s, \\ u^2\overline{a}_2 &= a_2 - sa_1 + 3r - s^2, \\ u^3\overline{a}_3 &= a_3 + ra_1 + 2t, \\ u^4\overline{a}_4 &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st, \\ u^6\overline{a}_6 &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - rta_1 - t^2. \end{aligned} \tag{2.3}$$

This equation represents the same curve in different coordinates. We can define a new curve $\overline{E}$ by

$$\overline{E}: \ y^2 + \overline{a}_1xy + \overline{a}_3y = x^3 + \overline{a}_2x^2 + \overline{a}_4x + \overline{a}_6.$$

This curve $\overline{E}$ is isomorphic to E. Among other things, this means that the group $\overline{E}(K)$ is isomorphic to $E(K)$. The isomorphism $\phi : \overline{E} \to E$ is such that the functions x, y on E composed with ϕ are related to the functions $\overline{x}$, $\overline{y}$ on $\overline{E}$ by

$$x\phi = u^2\overline{x} + r \text{ and } y\phi = u^3\overline{y} + su^2\overline{x} + t. \tag{2.4}$$

It can be shown that inverting an admissible change of variables and composing two admissible changes of variables also yields an admissible change of variables.

Theorem 2.2. *Any isomorphism between two elliptic curves with equations in the Weierstrass normal form is given by an admissible change of variables.*

The proof of this theorem is omitted.

2.2 Associated quantities

To help classify elliptic curves up to isomorphism, we associate some quantities to the equation in the Weierstrass normal form (1.1) of an elliptic curve E over a field K. Recall the b_i-coefficients (1.5) and discriminant (1.6) associated to such a curve.

Remark 2.3. If two elliptic curves E and $\overline{E}$ are isomorphic with isomorphism $\phi : \overline{E} \to E$ given by (2.4), then the coefficients b_i associated with E and $\overline{b}_i$ associated with $\overline{E}$ are related as follows:

$$\begin{aligned} u^2\overline{b}_2 &= b_2 + 12r, \\ u^4\overline{b}_4 &= b_4 + rb_2 + 6r^2, \\ u^6\overline{b}_6 &= b_6 + 2rb_4 + r^2b_2 + 4r^3, \\ u^8\overline{b}_8 &= b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4. \end{aligned}$$

Consequently, the discriminants Δ of E and $\overline{\Delta}$ of $\overline{E}$ are related by

$$u^{12}\overline{\Delta} = \Delta.$$

Remark 2.4. If the characteristic of the field K is different from 2, then we can use the admissible change of variables

$$x = \overline{x} \text{ and } y = \overline{y} - \frac{a_1 x + a_3}{2}$$

to change the Weierstrass normal form into

$$\overline{y}^2 = \overline{x}^3 + \frac{b_2}{4}\overline{x}^2 + \frac{b_4}{2}\overline{x} + \frac{b_6}{4}. \tag{2.5}$$

Next, we define the coefficients

$$\begin{aligned} c_4 &= b_2^2 - 24b_4, \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6. \end{aligned}$$

With notation as above, if the characteristic of K is different from 2 and 3, we can rewrite the discriminant as

$$\Delta = \frac{c_4^3 - c_6^2}{12^3}.$$

Definition 2.5 (j-invariant)**.** For an elliptic curve E, we define the j-invariant of E as

$$j(E) = j = \frac{c_4^3}{\Delta}.$$

In fields of characteristic different from 2 and 3, we can also write

$$j = 12^3 \frac{c_4^3}{c_4^3 - c_6^2}.$$

Remark 2.6. Under a change of variables as in 2.3, the c_i-coefficients associated with E and the $\overline{c}_i$-coefficients associated with $\overline{E}$ are related by

$$\begin{aligned} u^4\overline{c}_4 &= c_4, \\ u^6\overline{c}_6 &= c_6. \end{aligned}$$

Consequently, we have $j(E) = j(\overline{E})$. Indeed, the j-invariant is an invariant of an elliptic curve E up to isomorphism.

Remark 2.7. If the characteristic of the field K is different from 2 and 3, then we can use the admissible change of variables

$$\overline{x} = \hat{x} - \frac{b_2}{12} \text{ and } \overline{y} = \hat{y}$$

to change the form (2.5) into

$$\hat{y} = \hat{x}^3 - \frac{c_4}{48}\hat{x} - \frac{c_6}{864}.$$

An equation of the form

$$y^2 = x^3 + Ax + B \tag{2.6}$$

has discriminant

$$\Delta = -16\left(4A^3 + 27B^2\right). \tag{2.7}$$

3 Curves with points of order 2 or 3

This section is based on [Hus04].

First, we want to classify elliptic curves which have points of order 2 or 3. In this section, let E be an elliptic curve given by (1.1).

3.1 Curves with points of order 2

A point $P = (x, y)$ on E has order 2 if and only if $P = -P$ and $P \neq O$, i.e. if and only if the coordinates of P satisfy

$$2y + a_1 x + a_3 = 0.$$

Using similar arguments as in Remark 2.4, we can find the x-coordinates of these points by solving the equation

$$4x^3 + b_2 x^2 + 2b_4 x + b_6 = 0.$$

This equation can have zero, one or three distinct solutions in K. Hence, the number of points of order 2 on an elliptic curve can be 0, 1 or 3.
If the characteristic of K is different from 2 and 3, we can use an admissible change of variables to put the equation of the curve into the form

$$y^2 = x^3 + Ax + B,$$

as explained in Remarks 2.4 and 2.7. Then, the symmetry line as in (1.7) is given by $y = 0$, so we can find the possible x-coordinates of points of order 2 by solving

$$x^3 + Ax + B = 0.$$

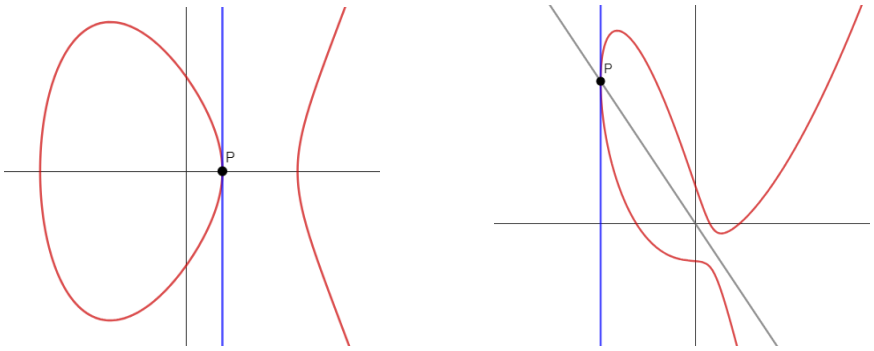


Figure 3: Examples of elliptic curves with points of order 2

3.2 The Legendre family

As an example of elliptic curves with points of order 2, we briefly discuss the Legendre family of elliptic curves.

Definition 3.1 (The Legendre family)**.** Let K be a field of characteristic not equal to 2. The Legendre family is the family of elliptic curves E_λ over K of the form

$$y^2 = x(x-1)(x-\lambda), \tag{3.1}$$

where $\lambda \in K$.

A straightforward computation shows that the discriminant of an elliptic curve E_λ of this family is

$$\Delta_\lambda = 16\lambda^2(\lambda-1)^2.$$

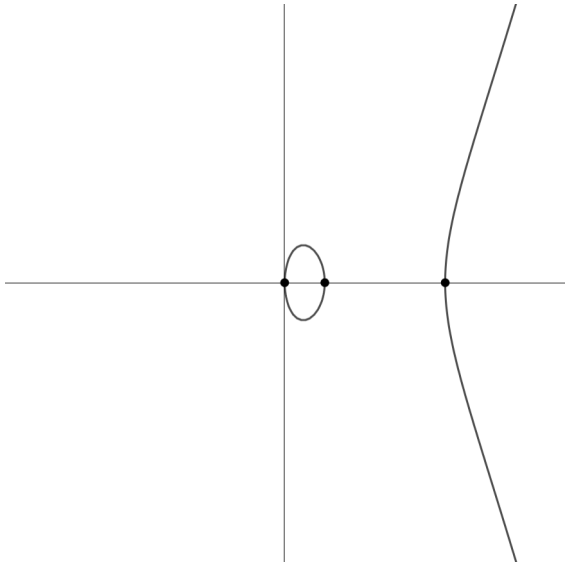


Figure 4: The curve E_4

For $\lambda \in K \setminus \{0, 1\}$, the curve (3.1) is non-singular. Any elliptic curve E_λ has exactly 3 points of order 2, namely $(0, 0)$, $(1, 0)$, and $(\lambda, 0)$.

We can expand the equation (3.1) of E_λ to obtain

$$y^2 = x^3 - (\lambda + 1)x^2 + \lambda x.$$

If the characteristic of K is also different from 3, we can use the admissible change of variables

$$x = \tfrac{1}{9}\overline{x} + \tfrac{1}{3}(\lambda + 1) \text{ and } y = \tfrac{1}{27}\overline{y}$$

in order to obtain the isomorphic curve $\overline{E}_\lambda$ in Weierstrass normal form:

$$y^2 = x^3 - 27(\lambda^2 - \lambda + 1)x - 27(2\lambda^3 - 3\lambda^2 - 3\lambda + 2).$$

The points of order 2 are mapped to the following points under this change of variables:

$$(0, 0) \mapsto (-3\lambda - 3, 0);$$
$$(1, 0) \mapsto (6 - 3\lambda, 0);$$
$$(\lambda, 0) \mapsto (6\lambda - 3, 0).$$

3.3 Curves with points of order 3

A point P on E has order 3 if and only if $2P = -P$ and $P \neq O$. Using the chord-tangent law, this means that the third point on the tangent line to E at P must be P itself; the tangent line is not vertical and only intersects the curve at P. We aim to show that points of order 3 are exactly the inflection points of E.

In order to study inflection points, we need to define the second derivative of y with respect to x. An inflection point is a point where this second derivative is zero. Before, we found using formal differentiation that

$$(2y + a_1x + a_3)y' = f'(x) - a_1y,$$

where we consider $y = y(x)$ as a function of x. Using formal differentiation again, we find

$$(2y' + a_1)y' + (2y + a_1x + a_3)y'' = f''(x) - a_1y'.$$

For points that are not on the symmetry line, we can rewrite this equation to obtain an expression for y'':

$$y''(x, y) = \frac{f''(x) - 2y'(y' + a_1)}{2y + a_1x + a_3}. \tag{3.2}$$

Proposition 3.2. *A finite point $P = (x_1, y_1)$ on E is of order 3 if and only if $y''(x_1, y_1) = 0$.*

Proof. We aim to show that both of these statements are equivalent with

$$3x_1 = \lambda^2 + \lambda a_1 - a_2,$$

where $\lambda = y'(x_1, y_1)$ is the slope of the tangent line to E at P.
Suppose $P = (x_1, y_1)$ on E is a point of order 3. In particular, this means that the tangent line to P at E is not vertical, so $\lambda = y'(x_1, y_1)$ is well-defined. Using formulas (1.9) and (1.10), we find that

$$2P = (x_3, -y_3 - a_1x_3 - a_3),$$

where

$$\begin{aligned} x_3 &= \lambda^2 + \lambda a_1 - a_2 - 2x_1, \\ y_3 &= \lambda x_3 + \beta. \end{aligned}$$

Since P is of order 3, we have that $2P = -P = (x_1, -y_1 - a_1x_1 - a_3)$. By equating the coordinates of $2P$ and $-P$, we get the system

$$\begin{cases} \lambda^2 + \lambda a_1 - a_2 - 2x_1 = x_1, \\ -\lambda x_3 - \beta - a_1x_3 - a_3 = -y_1 - a_1x_1 - a_3. \end{cases} \tag{3.3}$$

The point (x_1, y_1) is of order 3 if and only if its coordinates satisfy (3.3). Further rewriting the system, we get

$$\begin{cases} 3x_1 = \lambda^2 + \lambda a_1 - a_2, & \text{(3.4a)} \\ y_1 = \lambda x_3 + \beta. & \text{(3.4b)} \end{cases}$$

Since the tangent line to E at P is given by $y = \lambda x + \beta$ and P is on this line, we know that $y_1 = \lambda x_1 + \beta$. Therefore, we know that $x_1 = x_3$ if and only if $y_1 = \lambda x_3 + \beta$, hence equations (3.4a) and (3.4b) are equivalent. We get that the point (x_1, y_1) is of order 3 if and only if

$$3x_1 = \lambda^2 + \lambda a_1 - a_2,$$

which is what we wanted to show.

Now, suppose that $P = (x_1, y_1)$ is a point on E such that $y''(x_1, y_1)$ is well-defined and $y''(x_1, y_1) = 0$. Let us denote $\lambda = y'(x_1, y_1)$. If we plug $(x, y) = (x_1, y - 1)$ into (3.2), we get

$$y''(x_1, y_1) = \frac{f''(x_1) - 2\lambda(\lambda + a_1)}{2y_1 + a_1x_1 + a_3}.$$

We can compute $f''(x) = 6x + 2a_2$. We get that $y''(x_1, y_1) = 0$ if and only if

$$6x_1 + 2a_2 - 2\lambda(\lambda + a_1) = 0.$$

Rewriting this equation, we get that $y''(x_1, y_1) = 0$ if and only if

$$3x_1 = \lambda^2 + \lambda a_1 - a_2,$$

which is what we wanted to show.
Finally, we can conclude that a point (x_1, y_1) on E is of order 3 if and only if $y''(x_1, y_1) = 0$. □

Solving $y''(x, y) = 0$ is equivalent to solving

$$f''(x) - 2y'(x, y)(y'(x, y) + a_1) = 0.$$

If we expand this expression and substitute

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

this equation reduces to the fourth degree polynomial equation

$$3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8 = 0, \tag{3.5}$$

where b_2, b_4, b_6 and b_8 are defined as in (1.5). Since this polynomial in x is of degree 4, there can be at most 4 distinct solutions. If P is a point of order 3, then $-P$ is a distinct point of order 3. Therefore, there can be at most 8 distinct points of order 3 on an elliptic curve.
If the characteristic of K is not equal to 2 or 3, we can use an admissible change of variables to put the equation of the curve in the form

$$y^2 = x^3 + Ax + B,$$

as in Remarks 2.4 and 2.7. In this case, equation (3.5) reads as

$$3x^4 + 6Ax^2 + 12Bx - A^2 = 0.$$

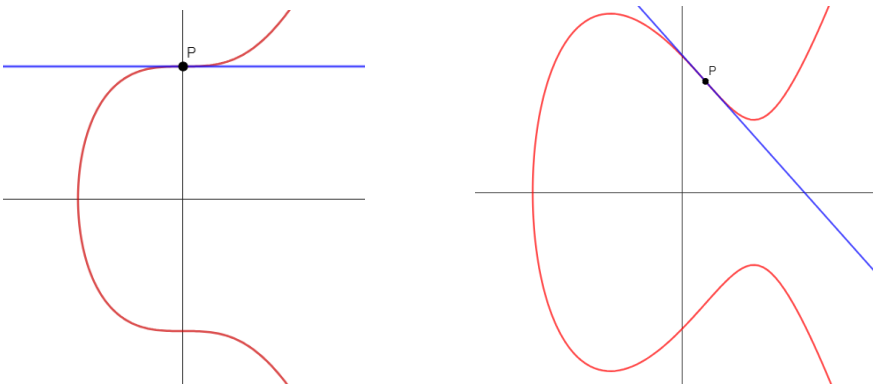


Figure 5: Examples of elliptic curves with points of order 3

We can show that the number of points of order 3 on an elliptic curve can only be 0, 2 or 8.

Proposition 3.3. *Let E be an elliptic curve over a field K. Suppose P_1 and P_2 are two points on E of order 3 with distinct x-coordinates. Then, the set $\{P_1, P_2\}$ is a basis of the set of all points on E of order dividing 3, and there are 8 distinct points of order 3.*

Proof. It is shown above that there can be at most 8 different points of order 3 on E.
Suppose Q is a point of order 3. In particular, Q is not of order 2, so $Q \neq -Q$. We have $Q \neq O$, so $-Q \neq O$. We also have $2(-Q) = -(2Q) = -(-Q) = Q \neq O$. Since $3(-Q) = -(3Q) = -O = O$, it follows that $-Q$ is a distinct point of order 3.
Therefore, it follows that there can be at most 4 pairs of points of order 3 with the same x-coordinates. We already have 2 such pairs: $\{\pm P_1\}$ and $\{\pm P_2\}$. We know that these are distinct since we assumed P_1 and P_2 have distinct x-coordinates. Now, we need to show that $\{\pm(P_1 + P_2)\}$ and $\{\pm(P_1 - P_2)\}$ are two distinct pairs of points of order 3.
We have

$$\begin{aligned} P_1 + P_2 = O &\iff P_2 = -P_1, \\ P_1 + P_2 = P_1 &\iff P_2 = O, \\ P_1 + P_2 = -P_1 &\iff P_1 = P_2, \\ P_1 + P_2 = P_2 &\iff P_1 = 0, \\ P_1 + P_2 = -P_2 &\iff P_1 = P_2. \end{aligned}$$

By assumption, we have $P_1, P_2 \neq O$ and $P_1 \notin \{\pm P_2\}$, so $P_1 + P_2 \notin \{O, \pm P_1, \pm P_2\}$. It follows that $-(P_1 + P_2)$ is also not in this set. Since $3(P_1 + P_2) = 3P_1 + 3P_2 = O + O = O$, the set $\{\pm(P_1 + P_2)\}$ is a new pair of points of order 3.

Similarly, we have

$$\begin{aligned} P_1 - P_2 = O &\iff P_1 = P_2, \\ P_1 - P_2 = P_1 &\iff P_2 = O, \\ P_1 - P_2 = -P_1 &\iff P_2 = -P_1, \\ P_1 - P_2 = P_2 &\iff P_1 = -P_2, \\ P_1 - P_2 = -P_2 &\iff P_1 = 0, \\ P_1 - P_2 = P_1 + P_2 &\iff P_2 = O, \\ P_1 - P_2 = -(P_1 + P_2) &\iff P_1 = O. \end{aligned}$$

By assumption, we have $P_1, P_2 \neq O$ and $P_1 \notin \{\pm P_2\}$, so $P_1 - P_2 \notin \{O, \pm P_1, \pm P_2\}$. It follows that $-(P_1 - P_2)$ is also not in this set. Since $3(P_1 - P_2) = 3P_1 - 3P_2 = O - O = O$, the set $\{\pm(P_1 - P_2)\}$ is a new pair of points of order 3.
Now, we have 8 distinct points of order 3. Thus, the set spanned by $\{P_1, P_2\}$ is equal to the set of all points on E of order dividing 3. This concludes the proof. □

3.4 The Hessian family

As an example of elliptic curves with points of order 3, we briefly discuss the Hessian family of elliptic curves and an adaptation of this family.

Definition 3.4 (The Hessian family)**.** Let K be a field of characteristic different from 3. The Hessian family is the family of elliptic curves E_α over K of the form

$$y^2 + \alpha xy + y = x^3, \tag{3.6}$$

where $\alpha \in K$.

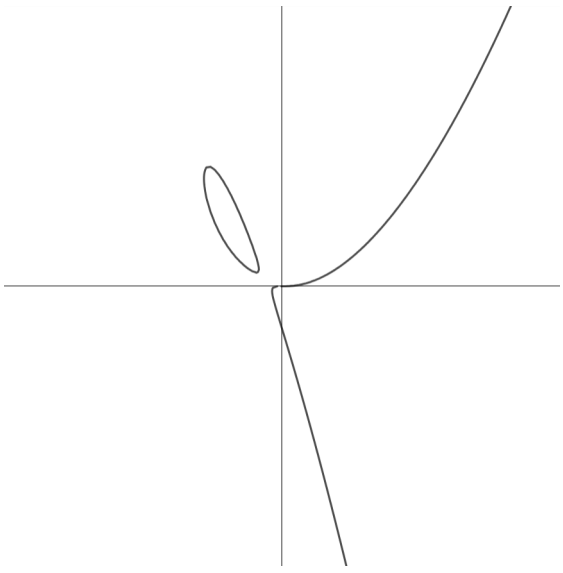


Figure 6: The curve $E_{3.3}$ over $\mathbb{R}$

A straightforward computation shows that the discriminant of E_α is given by

$$\Delta_\alpha = \alpha^3 - 27.$$

Hence, we see that the curve (3.6) is non-singular whenever $\alpha \notin 3\mu_3$, where μ_3 is the set of roots of $x^3 - 1$ in K.
This family is constructed in such a way that the point $(0, 0)$ is a torsion point of order 3 on every elliptic curve of the family. This can easily be verified by plugging $(x, y) = (0, 0)$ into (3.6), (1.8) and (3.2) and

using Proposition 3.2.
More generally, we can look at elliptic curves $E(a_1, a_3)$ given by an equation of the form

$$y^2 + a_1xy + a_3y = x^3. \tag{3.7}$$

Every such curve has the point $(0, 0)$ on it. A straightforward computation of the discriminant yields

$$\Delta(a_1, a_3) = a_3^3(a_1^3 - 27a_3).$$

We find that the curve (3.7) is non-singular if and only if $a_3 \neq 0$ and $a_1 \notin 3\sqrt[3]{a_3}\mu_3$. It can again be easily verified that on elliptic curves of this form, the point $(0, 0)$ is of order 3.
If a line $y = \lambda x + \beta$ has a double intersection point with an elliptic curve E, then this line is the tangent line to E at this point. Moreover, if this line has a triple intersection point, it is the tangent line at this point and does not intersect the curve in any other point. By the group law, this point must be of order 3, because we get $2P = -P$.
We want to find conditions on a_1 and a_3 such that the line $y = x + u$ has a triple intersection in a point $(v, v + u)$ for $v \neq 0$ on $E(a_1, a_3)$. To solve this, we have to solve the equation

$$x^3 - (x + u)^2 - (a_1x + a_3)(x + u) = (x - v)^3.$$

By comparing the coefficients of the powers of x, we get the system of equations

$$\begin{cases} 3v = a_1 + 1 & \text{(3.8a)} \\ -3v^2 = 2u + a_1u + a_3 & \text{(3.8b)} \\ v^3 = u^2 + a_3u. & \text{(3.8c)} \end{cases}$$

By multiplying equation (3.8b) by u and subtracting this from equation (3.8c), we obtain

$$v^3 + 3uv^2 = -(a_1 + 1)u^2.$$

Substituting $a_1 + 1 = 3v$ and rewriting, we get

$$v^3 + 3uv^2 + 3vu^2 = 0$$

or equivalently

$$(v + u)^3 = u^3.$$

We want to find solutions for $v \neq 0$, so we also need to assume $u \neq 0$. Thus, we find

$$\left(\frac{v + u}{u}\right)^3 = 1.$$

Since $v \neq 0$, we get $(v + u)/u \neq 1$, so we must have $(v + u)/u \in \mu_3 \setminus \{1\}$. If the field K is such that $\mu_3 = \{1\}$, then this construction is not possible. For the remainder of this section, we assume that K contains three distinct third roots of unity, so $\mu_3 \setminus \{1\}$ is not empty. Then we can also assume that $(v + u)/(u) = \rho \in \mu_3$, where ρ is a third root of unity different from 1. An important property of ρ is that

$$\rho^2 + \rho + 1 = 0.$$

Now, we have $v + u = \rho u$, so

$$v = (\rho - 1)u$$

and

$$u = (\rho - 1)^{-1}v.$$

We have that

$$(\rho - 1)(\rho^2 - 1) = 3,$$

so

$$(\rho - 1)^{-1} = \tfrac{1}{3}(\rho^2 - 1).$$

By rewriting $\rho^2 + \rho + 1 = 0$, we find $\rho^2 - 1 = -\rho - 2$, so we can also write

$$(\rho - 1)^{-1} = -\tfrac{1}{3}(\rho + 2).$$

Hence,

$$u = -\tfrac{1}{3}(\rho + 2)v$$

and

$$u + v = \left(1 - \tfrac{1}{3}(\rho + 2)\right) v = \tfrac{1}{3}(1 - \rho)v.$$

We can substitute the above expression of u in terms of v into system (3.8) to find expressions for a_1 and a_3 in terms of v:

$$\begin{cases} 3v = a_1 + 1 & \text{(3.9a)} \\ -3v^2 = -\tfrac{1}{3}(a_1 + 2)(\rho + 2)v + a_3 & \text{(3.9b)} \\ v^3 = \tfrac{1}{9}(\rho + 2)^2 v^2 - \tfrac{1}{3}a_3(\rho + 2)v. & \text{(3.9c)} \end{cases}$$

Equation (3.9a) gives

$$a_1(v) = 3v - 1.$$

After substituting this into equation (3.9b), we can rewrite equations (3.9b) and (3.9c) to find that they are equivalent. They can both be rewritten to obtain

$$a_3(v) = (\rho - 1)v^2 + \tfrac{1}{3}(\rho + 2)v.$$

Thus, for any $v \in K$ for which $\Delta_v := \Delta(a_1(v), a_3(v)) \neq 0$, we get that the elliptic curve E_v given by

$$y^2 + a_1(v)xy + a_3(v)y = x^3$$

has distinct points of order 3

$$P_1 := (0, 0) \text{ and } P_2 := (v, \tfrac{1}{3}(1 - \rho)v).$$

By Proposition 3.3, since we have two points of order 3 with distinct x-coordinates, we can find all points of order 3: $\{P_1, P_2\}$ is a basis for the set of points of order dividing 3. The full set is

$$\{O, \pm P_1, \pm P_2, \pm(P_1 + P_2), \pm(P_1 - P_2)\}.$$

4 Tate normal form

This section is based on [Hus04].

We can use an admissible change of variables to put the equation for an elliptic curve in a different form. In this section, we take a look at the Tate normal form and its applications.

Definition 4.1 (Tate normal form)**.** The Tate normal form of an elliptic curve E over a field K is

$$E = E(b, c) : \ y^2 + (1 - c)xy - by = x^3 - bx^2, \tag{4.1}$$

where $b, c \in K$.

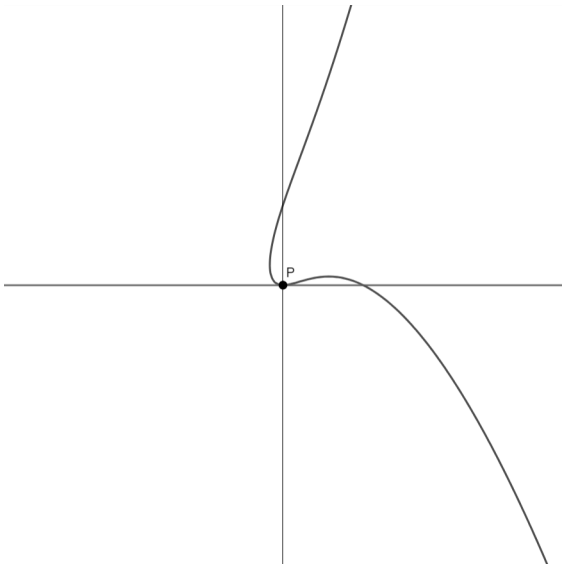


Figure 7: The curve $E(2, 4)$

Using the expression (1.6) for the discriminant, we can compute the discriminant in terms of b and c:

$$\Delta(b, c) = (1 - c)^4 b^3 - (1 - c)^3 b^3 - 8(1 - c)^2 b^4 + 36(1 - c)b^4 - 27b^4 + 16b^5. \tag{4.2}$$

In particular, we see that we need $b \neq 0$.

An elliptic curve E in Tate normal form always contains the point $(0, 0)$, and the tangent line at $(0, 0)$ is horizontal. This means that the point $(0, 0)$ is not of order 2.

As is shown in Section 3.3, a point P on E is a point of order 3 only if its x-coordinate is a root of polynomial (3.5). Hence, the point $(0, 0)$ is of order 3 only if 0 is a root of this polynomial. This is equivalent to the condition $b_8 = 0$, where b_8 is defined as in (1.5). For a curve $E = E(b, c)$ in Tate normal form, we have $b_8 = -b^3$. Since we assume $b \neq 0$, we have $b_8 \neq 0$ and hence $(0, 0)$ can not have order 3.

It is relatively easy to compute multiples of P on a curve in Tate normal form. Over the base field $\mathbb{Q}$, we can use this to find necessary and sufficient conditions on the parameters b and c for which P has a particular order. This is done in section 5. In combination with the following result, this allows us to classify all elliptic curves over $\mathbb{Q}$ with a point of finite order greater than 3. The proof is adapted from [Hus04, Chapter 4.4].

Theorem 4.2. *Every elliptic curve over a field K with a point of order $n > 3$ is isomorphic to a curve in Tate normal form for which the point $(0, 0)$ has order n.*

Proof. Suppose we have an elliptic curve E over a field K given by

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

Suppose (x_1, y_1) is a K-rational point on E which has order greater than 3. First, we want to use an admissible change of variables $x = u^2\overline{x} + r$ and $y = u^3\overline{y} + su^2\overline{x} + t$ so that we get an equation of the form

$$y^2 + \overline{a}_1xy + \overline{a}_3y = x^3 + \overline{a}_2x^2 \tag{4.3}$$

and the point (x_1, y_1) gets mapped to the point $(0, 0)$. Without loss of generality, we can choose $u = 1$. We have to find values of r, t and s for which we get an equation of the form (4.3) and (x_1, y_1) gets mapped to $(0, 0)$.

The point (x_1, y_1) gets mapped to the point $(x_1 - r, y_1 - s(x_1 - r) - t)$. Clearly, we need $r = x_1$ and $t = y_1$ to set this point equal to $(0, 0)$.

We can verify that this choice of r and t guarantees that $\overline{a}_6 = 0$. By plugging in $r = x_1$ and $t = y_1$ into (2.3), we find that

$$\overline{a}_6 = a_6 + a_4x_1 + a_2x_1^2 + x_1^3 - a_3y_1 - a_1x_1y_1 - y_1^2.$$

Since (x_1, y_1) is on E, we know that

$$y_1^2 + a_1x_1y_1 + a_3y_1 = x_1^3 + a_2x_1^2 + a_4x_1 + a_6,$$

so indeed $\overline{a}_6 = 0$.

By plugging $r = x_1$, $t = y_1$ into (2.3), we find

$$\overline{a}_4 = a_4 - sa_3 + 2a_2x_2 - a_1(y_1 + sx_1) + 3x_1^2 - 2sy_1.$$

In order to find s, we set $\overline{a}_4$ equal to 0 and solve for s:

$$a_4 - sa_3 + 2a_2x_2 - a_1(y_1 + sx_1) + 3x_1^2 - 2sy_1 = 0.$$

We rearrange the terms to get all factors of s on one side:

$$s(2y_1 + a_1x_1 + a_3) = 3x_1^2 + 2a_2x_1 + a_4 - a_1y_1.$$

We assumed (x_1, y_1) has order greater than 3, so $2y_1 + a_1x_1 + a_3 \neq 0$. Therefore, we get

$$s = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3},$$

which is equal to the slope of the tangent line to E at (x_1, y_1), as is shown in Remark 1.14.

For these choices of r, t and s, we get the isomorphic curve given by the equation

$$y^2 + \overline{a}_1xy + \overline{a}_3y = x^3 + \overline{a}_2x^2,$$

where

$$\begin{aligned}
\overline{a}_1 &= a_1 + 2s, \\
\overline{a}_2 &= -s^2 - a_1s + 3x_1 + a_2, \\
\overline{a}_3 &= 2y_1 + a_1x_1 + a_3.
\end{aligned}$$

By our arguments above, $\overline{a}_3 \neq 0$. Since s is the slope of the tangent line to E at (x_1, y_1), we know by Proposition 3.2 that $\overline{a}_2 = 0$ if and only if (x_1, y_1) has order 3. Since we assumed that (x_1, y_1) has order greater than 3, we have $\overline{a}_2 \neq 0$.

Now, to put this equation into Tate normal form, we need to make the coefficients of y and x^2 equal. To do this, we use the admissible change of variables $\overline{x} = (\overline{a}_3/\overline{a}_2)^2\tilde{x}$, $\overline{y} = (\overline{a}_3/\overline{a}_2)^3\tilde{y}$. Using (2.3), we get coefficients

$$\begin{aligned}
\tilde{a}_1 &= \frac{\overline{a}_1\overline{a}_2}{\overline{a}_3}, \\
\tilde{a}_2 &= \frac{\overline{a}_2^3}{\overline{a}_3^2}, \\
\tilde{a}_3 &= \frac{\overline{a}_2^3}{\overline{a}_3^2}.
\end{aligned}$$

Finally, we define

$$\begin{aligned}
b &= -\tilde{a}_2 = -\tilde{a}_3, \\
c &= 1 - \tilde{a}_1,
\end{aligned}$$

so we get the form

$$y^2 + (1 - c)xy - by = x^3 - bx^2.$$

This concludes the proof. □

5 Curves with points of order n

This section is based on [Hus04, Chapter 4.4], except where specified otherwise. We provide the details of the computations.

Using the Tate normal form of an elliptic curve, we can find families consisting of all elliptic curves over $\mathbb{Q}$ in Tate normal form for which the point $P = (0, 0)$ has a given order $n \in \{4, 5, \ldots, 10, 12\}$. By Theorem 4.2, these families contain all curves with a point of given order $n \in \{4, 5, \ldots, 10, 12\}$ up to isomorphism.

Similar computations for more general cases have been done by other authors. For instance, in [Sut11], these computations are performed for elliptic curves over finite fields for order $n \leq 50$. In [Rei86], these computations are performed for elliptic curves over quadratic extensions of $\mathbb{Q}$.

There are two ways to define the families of elliptic curves with a point of given order n. The first method is to find necessary and sufficient conditions on the parameters b and c for which the curve given by (4.1) is in a particular family. This method is useful for checking whether a given curve with an equation in Tate normal form is in one of the families.

The second method is to reparametrize the curve in a single variable. This is done by defining b and c in terms of a new independent parameter α. This method is useful for constructing curves in a particular family. The required computations for this method are similar to those of the first method.

For the first method, we need b and c to satisfy a polynomial equation $f_n(b, c) = 0$ and $\Delta(b, c) \neq 0$, where $\Delta(b, c)$ is defined as in (4.2). The polynomial $f_n(b, c)$ depends on n, and we aim to compute the explicit form of this polynomial for $n \in \{4, 5, \ldots, 10, 12\}$. We also aim to show that we can express both b and c in terms of a single parameter. We use this for the second method.

5.1 Multiples of P

We can compute multiples of P on $E(b, c)$ in terms of b and c using the group law:

$$\begin{aligned} P &= (0, 0), & 2P &= (b, bc), & 3P &= (c, b - c), \\ -P &= (0, b), & -2P &= (b, 0), & -3P &= (c, c^2). \end{aligned}$$

If $c \neq 0$, we can denote $d := \frac{b}{c}$ and we can compute

$$\begin{aligned} 4P &= \left(d(d-1), d^2(c - d + 1)\right), \\ -4P &= \left(d(d-1), d(d-1)^2\right). \end{aligned}$$

If we also have $c \neq b$, we can denote $e := \frac{c}{d-1}$ and we can compute

$$\begin{aligned} 5P &= \left(de(e-1), de^2(d - e)\right), \\ -5P &= \left(de(e-1), d^2e(e-1)^2\right). \end{aligned}$$

If additionally $c^2 \neq b - c$, then $e \neq 1$ and we can denote $g := \frac{e(d-e)}{e-1}$. For ease of notation, additionally denote $\ell := g^2 + (1 - c)g + b - de(e - 1)$. Then, we get

$$\begin{aligned} 6P &= (\ell, -(g + 1 - c) \cdot \ell + b), \\ -6P &= (\ell, g \cdot \ell). \end{aligned}$$

We can use these expressions to find $f_n(b, c)$ explicitly for our desired values of n.

5.2 Order 4

Since P can not be of order 2, we know that P is of order 4 if and only if $4P = O$, or equivalently, $2P = -2P$. Using Section 5.1, this condition reduces to

$$bc = 0.$$

Since we require $b \neq 0$, we must have $c = 0$. Hence, we find

$$f_4(b, c) = c. \tag{5.1}$$

We can parametrize b and c in terms of a single new variable α. In this case, we can simply put

$$\begin{aligned} b_4(\alpha) &= \alpha, \\ c_4(\alpha) &= 0. \end{aligned}$$

Plugging in $b = b_4(\alpha)$ and $c = c_4(\alpha)$ into (4.2) yields

$$\Delta_4(\alpha) = \alpha^4(1 + 16\alpha).$$

Hence, curves of this family are non-singular for $\alpha \neq 0, -\frac{1}{16}$.

The family of elliptic curves with a point of order 4 is precisely given by

$$E_4(\alpha) : \; y^2 + xy - \alpha y = x^3 - \alpha x^2,$$

where $\alpha \neq 0, -\frac{1}{16}$.

5.3 Order 5

Going forward, we understand that P can only be of order n if P is not of order m for $m < n$. Therefore, we assume that b and c do not satisfy the conditions for which P has lower order, i.e. we assume that b and c are such that $f_m(b, c) \neq 0$ for $m < n$.
In particular, we assume that $b \neq 0$ and $c \neq 0$, so $d = \frac{b}{c}$ is well-defined and non-zero.
The point P is of order 5 if and only if $5P = O$, or equivalently, $3P = -2P$. Using Section 5.1, this condition reduces to the system of equations

$$\begin{cases} c & = b, \\ b - c & = 0. \end{cases}$$

These equations are equivalent. We find

$$f_5(b, c) = b - c. \tag{5.2}$$

We can parametrize b and c in terms of a single new variable α. In this case, we can simply put

$$\begin{aligned} b_5(\alpha) &= \alpha, \\ c_5(\alpha) &= \alpha. \end{aligned}$$

Plugging in $b = b_5(\alpha)$ and $c = c_5(\alpha)$ into (4.2) yields

$$\Delta_5(\alpha) = \alpha^5(\alpha^2 - 11\alpha - 1).$$

It can be easily verified that $\alpha^2 - 11\alpha - 1$ has no rational zeros, so curves of this family are non-singular for all $\alpha \neq 0$.

The family of elliptic curves with a point of order 5 is precisely given by

$$E_5(\alpha) : \; y^2 + (1 - \alpha)xy - \alpha y = x^3 - \alpha x^2,$$

where $\alpha \neq 0$.

5.4 Order 6

Going forward, we assume P is not of order 4 or 5, so $c \neq 0$ and $b \neq c$. This means that $e = \frac{c}{d-1}$ is well-defined and non-zero.
Since the point P can not have order 2 or 3, it has order 6 if and only if $6P = 0$, which holds if and only if $3P = -3P$. Using Section 5.1, this condition reduces to the equation

$$b - c = c^2.$$

Hence, we find

$$f_6(b, c) = c^2 + c - b. \tag{5.3}$$

We can parametrize b and c in terms of a single new variable α. In this case, we can put

$$\begin{aligned} b_6(\alpha) &= \alpha^2 + \alpha, \\ c_6(\alpha) &= \alpha. \end{aligned}$$

Plugging in $b = b_6(\alpha)$ and $c = c_6(\alpha)$ into 4.2 yields

$$\Delta_6(\alpha) = \alpha^6(\alpha+1)^3(9\alpha+1).$$

Thus, curves of this family are non-singular for $\alpha \neq 0, -1, -\frac{1}{9}$.

The family of elliptic curves with a point of order 6 is precisely given by

$$E_6(\alpha):\ y^2 + (1-\alpha)xy - (\alpha^2+\alpha)y = x^3 - (\alpha^2+\alpha)x^2,$$

where $\alpha \neq 0, -1, -\frac{1}{9}$.

5.5 Order 7

The point P has order 7 if and only if $7P = 0$, or equivalently, $4P = -3P$. Using Section 5.1, this condition reduces to the system of equations

$$\begin{cases} c &= d(d-1), \\ c^2 &= d^2(c-d+1). \end{cases}$$

Notice that the first equation implies the second: if $c = d(d-1)$, then

$$\begin{aligned} d^2(c-d+1) &= d^2(d(d-1)-d+1) \\ &= d^2(d^2-2d+1) \\ &= d^2(d-1)^2 \\ &= c^2. \end{aligned}$$

Hence, the first equation is sufficient. We can rewrite this equation to obtain a polynomial in terms of b and c:

$$\begin{aligned} c = d(d-1) &\iff c = \tfrac{b}{c}\left(\tfrac{b}{c} - 1\right) \\ &\iff c^3 = b(b-c) \\ &\iff c^3 + bc - b^2 = 0. \end{aligned}$$

Thus, we find

$$f_7(b,c) = c^3 + bc - b^2. \tag{5.4}$$

We can parametrize b and c in terms of a single new variable α. In this case, we can redefine d to be an independent parameter and set $\alpha = d$. Using (...) and the fact that $b = cd$, we find:

$$\begin{aligned} b_7(\alpha) &= \alpha^2(\alpha-1), \\ c_7(\alpha) &= \alpha(\alpha-1). \end{aligned}$$

Plugging in $b = b_7(\alpha)$ and $c = c_7(\alpha)$ into 4.2 yields:

$$\Delta_7(\alpha) = \alpha^7(\alpha-1)^7(\alpha^3 - 8\alpha^2 + 5\alpha + 1).$$

The cubic $\alpha^3 - 8\alpha^2 + 5\alpha + 1$ has no rational zeros. Thus, curves of this family are non-singular for $\alpha \neq 0, 1$, or equivalently $b \neq 0$ and $c \neq 0, b$.

The family of elliptic curves with a point of order 7 is precisely given by

$$E_7(\alpha):\ y^2 + (1-\alpha(\alpha-1))xy - \alpha^2(\alpha-1)y = x^3 - \alpha^2(\alpha-1)x^2,$$

where $\alpha \neq 0, 1$.

5.6 Order 8

We assume that the parameters b and c are such that the point P is not of order 4. Since P can not have order 2, the point P has order 8 if and only if $8P = O$, or equivalently, $4P = -4P$. Using Section 5.1, this condition reduces to the equation

$$d^2(c - d + 1) = d(d - 1)^2.$$

Since we assume $b \neq 0$, we get $d \neq 0$ and we can divide both sides by d to obtain

$$d(c - d + 1) = (d - 1)^2.$$

We rewrite the equation:

$$\begin{aligned} d(c - d + 1) = (d - 1)^2 &\iff cd - d^2 + d = d^2 - 2d + 1 \\ &\iff cd = 2d^2 - 3d + 1 \\ &\iff b = (d - 1)(2d - 1) \\ &\iff bc^2 = (b - c)(2b - c) \\ &\iff bc^2 = 2b^2 - 3bc + c^2 \\ &\iff 2b^2 + (1 - b)c^2 - 3bc = 0. \end{aligned} \tag{5.5}$$

Hence, we find

$$f_8(b, c) = 2b^2 + (1 - b)c^2 - 3bc. \tag{5.6}$$

We can parametrize b and c in terms of a single new variable α. In this case, we can redefine d to be an independent parameter and set $\alpha = d$. Using equation (5.5) and the fact that $c = \frac{b}{d}$, we can define:

$$\begin{aligned} b_8(\alpha) &= (\alpha - 1)(2\alpha - 1), \\ c_8(\alpha) &= \frac{(\alpha - 1)(2\alpha - 1)}{\alpha}. \end{aligned}$$

Plugging in $b = b_8(\alpha)$ and $c = c_8(\alpha)$ into 4.2 yields:

$$\Delta_8(\alpha) = \alpha^{-4}(1 - 2\alpha)^4(\alpha - 1)^8(8(\alpha - 1)\alpha + 1).$$

Note that $8(\alpha - 1)\alpha + 1$ does not have rational zeros. Therefore, curves of this family are non-singular for $\alpha \neq 0, 1, \frac{1}{2}$, or equivalently $b \neq 0$, $c \neq 0$, $c \neq 2b$, $c \neq b$.

The family of elliptic curves with a point of order 8 is precisely given by

$$E_8(\alpha) : \; y^2 + (1 - c_8(\alpha))xy - b_8(\alpha)y = x^3 - b_8(\alpha)x^2,$$

where $\alpha \neq 0, 1, \frac{1}{2}$.

5.7 Order 9

Since P can not have order 3, the point P has order 9 if and only if $9P = 0$, or equivalently, $5P = -4P$. Using Section 5.1, this condition reduces to the system of equations

$$\begin{cases} de(e - 1) &= d(d - 1), \\ de^2(d - e) &= d(d - 1)^2. \end{cases}$$

Since $d \neq 0$ by assumption, this is equivalent to

$$\begin{cases} e(e - 1) &= d - 1, \\ e^2(d - e) &= (d - 1)^2. \end{cases}$$

Notice that the first equation implies the second: if $e(e - 1) = d - 1$, then

$$\begin{aligned} e^2(d - e) &= e^2(-(e - 1) - 1 + d) \\ &= -e^2(e - 1) + e^2(d - 1) \\ &= -e(d - 1) + e^2(d - 1) \\ &= e(e - 1)(d - 1) \\ &= (d - 1)^2. \end{aligned}$$

Hence, the first equation is sufficient. We can rewrite this equation to obtain a polynomial in terms of b and c:

$$\begin{aligned} e(e-1) = d-1 &\iff d = e^2 - e + 1 \\ &\iff d(d-1)^2 = c^2 - c(d-1) + (d-1)^2 \\ &\iff b(b-c)^2 = c^5 - c^3(b-c) + c(b-c)^2 \\ &\iff c^5 - c^3(b-c) - (b-c)^3 = 0. \end{aligned}$$

Thus, we find

$$f_9(b,c) = c^5 - c^3(b-c) - (b-c)^3. \tag{5.7}$$

We can express c in terms of d and e as

$$\begin{aligned} c &= (d-1)e \\ &= de - e \\ &= (e^2 - e + 1)e - e \\ &= e^3 - e^2. \end{aligned}$$

Using $b = cd$, we get

$$b = (e^3 - e^2)(e^2 - e + 1).$$

We can parametrize b and c in terms of a single new variable α. In this case, we can redefine e to be an independent parameter and set $\alpha = e$:

$$\begin{aligned} b_9(\alpha) &= (\alpha^3 - \alpha^2)(\alpha^2 - \alpha + 1), \\ c_9(\alpha) &= \alpha^3 - \alpha^2. \end{aligned}$$

Plugging in $b = b_9(\alpha)$ and $c = c_9(\alpha)$ into 4.2 yields:

$$\Delta_9(\alpha) = \alpha^9(\alpha-1)^9(\alpha^2 - \alpha + 1)^3(\alpha^3 - 6\alpha^2 + 3\alpha + 1).$$

The cubic $\alpha^3 - 6\alpha^2 + 3\alpha + 1$ has no rational zeros. Thus, curves of this family are non-singular for $\alpha \neq 0, 1$, or equivalently $b \neq 0, c^2 + c$, $c \neq 0, b$.

The family of elliptic curves with a point of order 9 is precisely given by

$$E_9(\alpha):\ y^2 + (1 - c_9(\alpha))xy - b_9(\alpha)y = x^3 - b_9(\alpha)x^2,$$

where $\alpha \neq 0, 1$.

5.8 Order 10

We assume that the parameters b and c are such that P does not have order 5. Since P can not have order 2, the point P has order 10 if and only if $10P = O$, or equivalently, $5P = -5P$. Using Section 5.1, this condition reduces to the equation

$$de^2(d-e) = d^2e(e-1)^2.$$

Since we assume that d and e are well-defined and non-zero, we can divide both sides by de to get

$$e(d-e) = d(e-1)^2.$$

We rewrite the equation:

$$\begin{aligned} e(d-e) = d(e-1)^2 &\iff de - e^2 = de^2 - 2de + d \\ &\iff (d+1)e^2 - 3de + d = 0. \end{aligned} \tag{5.8}$$

We can rewrite (5.8) in terms of b and c:

$$\begin{aligned} (d+1)e^2 - 3de + d = 0 &\iff (d+1)c^2 - 3cd(d-1) + d(d-1)^2 = 0 \\ &\iff \left(\tfrac{b}{c} + 1\right)c^2 - 3c\tfrac{b}{c}\left(\tfrac{b}{c} - 1\right) + \tfrac{b}{c}\left(\tfrac{b}{c} - 1\right)^2 = 0 \\ &\iff bc + c^2 - 3\tfrac{b^2}{c} + 3b + \tfrac{b^3}{c^3} - 2\tfrac{b^2}{c^2} + \tfrac{b}{c} = 0 \\ &\iff bc^4 + c^5 - 3b^2c^2 + 3bc^3 + b^3 - 2b^2c + bc^2 = 0. \end{aligned}$$

Hence, we find

$$f_{10}(b,c) = c^5 + bc^4 + 3bc^3 + b(1-3b)c^2 - 2b^2c + b^3. \tag{5.9}$$

We can also rewrite (5.8) to obtain an expression for d in terms of e:

$$\begin{aligned}(d+1)e^2 - 3de + d = 0 &\iff (e^2 - 3e + 1)d + e^2 = 0 \\ &\iff d = -\frac{e^2}{e^2 - 3e + 1}.\end{aligned}$$

Note that $e^2 - 3e + 1$ has no rational zeros, so this is a well-defined fraction. This allows us to find expressions for b and c in terms of e:

$$\begin{aligned}c &= (d-1)e \\ &= de - e \\ &= -\frac{e^3}{e^2 - 3e + 1} - e \\ &= -\frac{2e^3 - 3e^2 + e}{e^2 - 3e + 1},\end{aligned}$$

and

$$b = cd \tag{5.10}$$

$$= \frac{e^3(2e^2 - 3e + 1)}{(e^2 - 3e + 1)^2}. \tag{5.11}$$

We can parametrize b and c in terms of a single new variable α. In this case, we can redefine e to be an independent parameter and set $\alpha = e$:

$$\begin{aligned}c_{10}(\alpha) &= -\frac{2\alpha^3 - 3\alpha^2 + \alpha}{\alpha^2 - 3\alpha + 1}, \\ b_{10}(\alpha) &= \frac{\alpha^3(2\alpha^2 - 3\alpha + 1)}{(\alpha^2 - 3\alpha + 1)^2}.\end{aligned}$$

Plugging in $b = b_{10}(\alpha)$ and $c = c_{10}(\alpha)$ into 4.2 yields:

$$\Delta_{10}(\alpha) = \frac{\left(4\alpha^2 - 2\alpha - 1\right)(2\alpha - 1)^5 (\alpha - 1)^{10} \alpha^{10}}{(\alpha^2 - 3\alpha + 1)^{10}}$$

This equation is derived using SageMath [The23]. The quadratic terms $4\alpha^2 - 2\alpha - 1$ and $\alpha^2 - 3\alpha + 1$ have no rational roots, so these terms can not be zero. Thus, curves of this family are non-singular for $\alpha \neq 0, 1, \frac{1}{2}$. We can obtain conditions for b and c by substituting back $e = \alpha$.

- Rewriting $e \neq 0$ yields $c \neq 0$.
- Rewriting $e \neq 1$ yields $c^2 + c - b \neq 0$.
- Rewriting $e \neq \frac{1}{2}$ yields $2c^2 + c - b \neq 0$.
- For e to be well-defined, we need $d \neq 1$, so $b \neq c$

Thus, curves of this family are non-singular for $b \neq 0, c, c^2 + c, 2c^2 + c$, and $c \neq 0$.

The family of elliptic curves with a point of order 10 is precisely given by

$$E_{10}(\alpha):\ y^2 + (1 - c_{10}(\alpha))xy - b_{10}(\alpha)y = x^3 - b_{10}(\alpha)x^2,$$

where $\alpha \neq 0, 1, \frac{1}{2}$.

5.9 Order 12

This section is based on results from [GAT00]. We provide the details of the computations.

We assume that the parameters b and c are such that P does not have order 4 or 6. Since P can not have order 2 or 3, the point P has order 12 if and only if $12P = O$, or equivalently, $6P = -6P$. Using Section 5.1, this condition reduces to the equation

$$g \cdot \ell = -(g + 1 - c) \cdot \ell + b$$

or equivalently

$$(2g + 1 - c) \cdot \ell = b.$$

Using SageMath [The23], we find that this is equivalent to

$$\left(c^6 + (b+1)c^4 - 5bc^3 + (10b^2 - b^3)c^2 - 9b^3c + 3b^4\right) \cdot \frac{c}{(c^2 - b + c)^3} = 0.$$

By assumption, we have $c \neq 0$ and $c^2 + c - b \neq 0$, so we can reduce this to

$$c^6 + (b+1)c^4 - 5bc^3 + (10b^2 - b^3)c^2 - 9b^3c + 3b^4 = 0. \tag{5.12}$$

Therefore, we get

$$f_{12}(b, c) = c^6 + (b+1)\,c^4 + 3b^4 - 9b^3c - 5bc^3 - \left(b^3 - 10b^2\right)c^2. \tag{5.13}$$

Using SageMath [The23], we can also write (5.12) in terms of d and e:

$$\left(e^2 + 3d^2 + 1 - d^2e - de - 3d\right) \cdot (d-1)^6 \cdot e^4 = 0.$$

By assumption, $d \neq 1$ and $e \neq 0$, so we find the equivalent equation

$$e^2 + 3d^2 + 1 - d^2e - de - 3d = 0. \tag{5.14}$$

Since we assume that P is not of order 6, we have $c^2 \neq b - c$ and hence $e \neq 1$. Therefore, we can define $f := \frac{e-d}{e-1}$.
By substituting $d = (1-e)f + e$ into (5.14), we can use SageMath [The23] to rewrite the equation into

$$\left(e(f-1)^2 - 3f^2 + 3f - 1\right)(e-1)^2 = 0.$$

Note that $e \neq 1$ and $f \neq 1$ by assumption. Therefore, we can rewrite this equation to find

$$e = \frac{3f^2 - 3f + 1}{(f-1)^2}.$$

We can find d in terms of f in a similar way. First, we write e in terms of d and f.

$$\begin{aligned} f = \frac{e-d}{e-1} &\iff (e-1)f = e - d \\ &\iff e(f-1) = f - d \\ &\iff e = \frac{f-d}{f-1}. \end{aligned}$$

Now, we substitute this into (5.14) and use SageMath [The23] to find the equivalent equation

$$\left(d(f-1) + 2f^2 - 2f + 1\right) \cdot \frac{(d-1)^2}{(f-1)^2} = 0.$$

Since $d \neq 1$ and $f \neq 1$ by assumption, we find

$$d = \frac{-2f^2 + 2f - 1}{f - 1}.$$

Now, we can write b and c in terms of f:

$$c = de - e = \frac{(3f^2 - 3f + 1)(f - 2f^2)}{(f-1)^3},$$
$$b = cd = c \cdot \frac{-2f^2 + 2f - 1}{f - 1}.$$

We can parametrize b and c in terms of a single new variable α. In this case, we can redefine f to be an independent parameter and set $\alpha = f$:

$$b_{12}(\alpha) = \frac{(-2\alpha^2 + 2\alpha - 1)(3\alpha^2 - 3\alpha + 1)(\alpha - 2\alpha^2)}{(\alpha-1)^4},$$
$$c_{12}(\alpha) = \frac{(3\alpha^2 - 3\alpha + 1)(\alpha - 2\alpha^2)}{(\alpha-1)^3}.$$

Plugging in $b = b_{12}(\alpha)$ and $c = c_{12}(\alpha)$ into 4.2 yields:

$$\Delta_{12}(\alpha) = \frac{\left(6\alpha^2 - 6\alpha + 1\right)\left(3\alpha^2 - 3\alpha + 1\right)^4\left(2\alpha^2 - 2\alpha + 1\right)^3(2\alpha - 1)^6\,\alpha^{12}}{(\alpha-1)^{24}}.$$

This equation is derived using SageMath [The23]. The quadratic terms $6\alpha^2 - 6\alpha + 1$, $3\alpha^2 - 3\alpha + 1$ and $2\alpha^2 - 2\alpha + 1$ have no rational roots, so these terms can not be zero. Thus, curves of this family are non-singular for $\alpha \neq 0, 1, \frac{1}{2}$. By substituting back $f = \alpha$, we can rewrite these conditions to find conditions on b and c.

- Rewriting $f \neq 1$ yields $b \neq c$.
- Rewriting $f \neq 0$ yields $c^3 + bc - b^2 \neq 0$.
- Rewriting $f \neq \frac{1}{2}$ yields $c^3 - c^2 + 3bc - 2b^2 \neq 0$.
- For f to be well-defined, we need $e \neq 1$, so $b \neq c^2 + c$.

The family of elliptic curves with a point of order 12 is precisely given by

$$E_{12}(\alpha):\ y^2 + (1 - c_{12}(\alpha))xy - b_{12}(\alpha)y = x^3 - b_{12}(\alpha)x^2,$$

where $\alpha \neq 0, 1, \frac{1}{2}$.

5.10 Table

The table below summarizes the results from this section.

Order n	$b_n(\alpha)$	$c_n(\alpha)$	Conditions on α
4	α	0	$\alpha \neq 0, -\frac{1}{16}$
5	α	α	$\alpha \neq 0$
6	$\alpha(\alpha+1)$	α	$\alpha \neq 0, -1, -\frac{1}{9}$
7	$\alpha^2(\alpha-1)$	$\alpha(\alpha-1)$	$\alpha \neq 0, 1$
8	$(\alpha-1)(2\alpha-1)$	$b_8(\alpha)/\alpha$	$\alpha \neq 0, 1, \frac{1}{2}$
9	$c_9(\alpha)(\alpha^2 - \alpha + 1)$	$\alpha^2(\alpha-1)$	$\alpha \neq 0, 1$
10	$c_{10}(\alpha)\left(-\frac{\alpha^2}{\alpha^2-3\alpha+1}\right)$	$-\frac{2\alpha^3-3\alpha^2+\alpha}{\alpha^2-3\alpha+1}$	$\alpha \neq 0, 1, \frac{1}{2}$
12	$c_{12}(\alpha)\left(-\frac{2\alpha^2-2\alpha+1}{\alpha-1}\right)$	$\frac{(3\alpha^2-3\alpha+1)(\alpha-2\alpha^2)}{(\alpha-1)^3}$	$\alpha \neq 0, 1, \frac{1}{2}$

6 Division polynomials

This section is based on [Was08, Chapter 3.2].

In section 3, we found polynomials whose rational roots are the x-coordinates of potential points of order 2 or 3. In this section, we generalize this concept to points of any order. In this section, we consider an elliptic curve E over $\mathbb{Q}$ given by equation (2.6).

First, we define the division polynomials corresponding to E.

Definition 6.1 (Division polynomials)**.** The division polynomials are a sequence of recursively defined polynomials in $\mathbb{Z}[x, y, A, B]$. The n-th division polynomial is denoted by ψ_n. The sequence is defined as follows:

$$\begin{aligned}
\psi_0 &= 0;\\
\psi_1 &= 1;\\
\psi_2 &= 2y;\\
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2;\\
\psi_4 &= 4y\left(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3\right);\\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \quad \text{for } m \geq 2;\\
\psi_{2m} &= (2y)^{-1}\psi_m\left(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2\right) \quad \text{for } m \geq 3.
\end{aligned} \tag{6.1}$$

In practice, we take A and B to be the coefficients of the equation (2.6) and we substitute the expression $y^2 = x^3 + Ax + B$ to eliminate even powers of y when possible.

Lemma 6.2. *Let $m \geq 0$ be a non-negative integer. If we fix A and B and substitute $y^2 = x^3 + Ax + B$, then we get*

$$\begin{aligned}
\psi_{2m+1} &\in \mathbb{Q}[x],\\
\psi_{2m} &\in 2y\mathbb{Q}[x].
\end{aligned}$$

Additionally, for any non-negative integer $n \geq 0$, we get

$$\psi_n^2 \in \mathbb{Q}[x].$$

The proof is omitted.

Notation 6.3. For notational convenience, we define the following polynomials for any integer $n \geq 2$:

$$\phi_n = x\psi_n^2 - \psi_{n+1}\psi_{n-1}, \tag{6.2}$$

$$\omega_n = (4y)^{-1}\left(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2\right). \tag{6.3}$$

6.1 Torsion points

The division polynomials can be used to compute the multiples of rational points P on E.

Theorem 6.4 (Multiples on E)**.** *Let $P = (x, y)$ be a rational point on E. Then for any integer $n \geq 2$ such that $\psi_n(x, y) \neq 0$, we have*

$$nP = \left(\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x, y)}{\psi_n^3(x, y)}\right). \tag{6.4}$$

The proof of this theorem is beyond the scope of this text and is omitted.

Since the point nP is in $E(\mathbb{Q})$, the coordinates of nP given by (6.4) must satisfy (2.6):

$$\left(\frac{\omega_n(x, y)}{\psi_n^3(x, y)}\right)^2 = \left(\frac{\phi_n(x)}{\psi_n^2(x)}\right)^3 + A\left(\frac{\phi_n(x)}{\psi_n^2(x)}\right) + B. \tag{6.5}$$

If we multiply both sides of equation (6.5) by $\psi_n^6(x)$, we find

$$\omega_n^2(x, y) = \phi_n^3(x) + A\phi_n(x)\psi_n^4(x) + B\psi_n^6(x). \tag{6.6}$$

If $\psi_n(x,y)$ and $\omega_n(x,y)$ are both 0, then equation (6.6) implies that $\phi_n(x)$ must also be 0. However, it is shown in [Cas49, lemma 2] that $\psi_n(x,y)$ and $\phi_n(x)$ can not have common zeros. Henceforth, $\psi_n(x,y)$ and $\omega_n(x,y)$ can not have common zeros.

One could ask the question, what happens if $\psi_n(x,y) = 0$? Clearly, the multiple nP must be defined, but the equations in (6.4) do not seem to be well-defined in this case. In order to understand what happens in this scenario, we need to consider these equations in projective coordinates. An explanation of this can be found in Sections 1.1 and 1.2.

If $\psi_n(x,y) \neq 0$, we can write the point nP in projective coordinates as

$$nP = \left(\frac{\phi_n(x)}{\psi_n^2(x)} : \frac{\omega_n(x,y)}{\psi_n^3(x,y)} : 1 \right).$$

We can multiply every coordinate by $\psi_n^3(x,y)$ to find

$$nP = \left(\phi_n(x)\psi_n(x,y) : \omega_n(x,y) : \psi_n^3(x,y) \right). \tag{6.7}$$

Notice that the representative $\left(\phi_n(x)\psi_n(x,y),\, \omega_n(x,y),\, \psi_n^3(x,y)\right)$ is well-defined even if $\psi_n(x,y) = 0$. In fact, if $\psi_n(x,y) = 0$, we find that

$$nP = (0 : \omega_n(x,y) : 0).$$

As argued before, $\omega_n(x,y)$ and $\psi_n(x,y)$ do not have common zeros, which means that this is a well-defined point. Thus, we obtain

$$nP = (0:1:0).$$

In other words, if $\psi_n(x,y) = 0$, then nP is the point at infinity O. This leads us to the following result.

Corollary 6.5 (Roots of division polynomials)**.** *Let $P = (x,y)$ be a rational point on E. Let $n \geq 2$ be an integer.*

1. *If $\psi_n(x,y) = 0$, then $nP = O$ and hence P has order dividing n.*
2. *Conversely, if P has order dividing n, then (x,y) is a zero of ψ_n and hence x is a root of ψ_n^2.*

Proof. The proof of the first statement is given above.
Assume that P has order dividing n. Then $nP = O = (0:1:0)$ in projective coordinates. We know that nP is also given by (6.7). By comparing the coordinates, we find that $\psi_n(x,y)$ must be zero. Hence, (x,y) is a zero of ψ_n. By Lemma 6.2, we can substitute the expression $y^2 = x^3 + Ax + B$ into ψ_n^2 if applicable to get $\psi_n^2 \in \mathbb{Q}[x]$. It follows that $\psi_n^2(x)$ must also be zero. This concludes the proof. □

Remark 6.6 (Finding torsion points)**.** Using Corollary 6.5, we can find all torsion points on E.
First, we find all rational roots of $\psi_n^2(x)$. Then, we find the corresponding y-values by plugging these values of x into (2.6) and solving for y. If we get a rational y-value, we have found a point on E with order dividing n.
In order to check for a given point $P = (x,y)$ whether it has order precisely n, we can compute mP using (6.4) for all $m \geq 2$ dividing n, where we understand mP to be O if $\psi_m(x,y) = 0$. The smallest value of m for which $mP = O$ is the order of P.
In order to find all points of order exactly n, we can also find all zeros of ψ_m for m dividing n. The $\mathbb{Q}$-rational zeros of ψ_n that do not occur as a zero of any of the ψ_m correspond to points of order n.

6.2 Trivial torsion group

Using the method described in Remark 6.6, we can find some elliptic curves over $\mathbb{Q}$ that have trivial torsion group. We wrote a program in SageMath [The23] to do this. The program works as follows. It loops over elliptic curves given an equation of the form (2.6), where the parameters A and B are integers within specified ranges.

By Mazur's theorem 1.17, every non-trivial torsion point on E has an order in $\{2,3,\ldots,10,12\}$. If P is a torsion point on E whose order n is composite, then for any prime p dividing n, the torsion point $\frac{n}{p}P$ has order p. Thus, if the torsion group of E is non-trivial, it contains a torsion point whose order is a prime number in $\{2,3,\ldots,10,12\}$, i.e. one of the primes $\{2,3,5,7\}$. Therefore, in order to check whether

a curve has trivial torsion group, it is sufficient to show that there are no points with order 2, 3, 5 or 7 on this curve.

For each combination of values of A and B, the program checks whether the discriminant of the corresponding curve is non-zero. If the discriminant is non-zero, it finds the rational roots of division polynomials ψ_3, ψ_5 and ψ_7 and the polynomial $x^3 + Ax + B$, which corresponds to ψ_2 as we show in section 3.1.

If the program finds a rational root r of one of the aforementioned polynomials, it finds the rational roots of the equation $y^2 = r^3 + Ar + B$ in y. If there are none, the program continues. If there is a rational solution, this means there is a non-trivial torsion point on E. In this case, the program begins the procedure again for the next values of A and B.

If the program finds that there are no non-trivial torsion points, it returns the values of A and B and begins the procedure again for the next values of A and B. If all combinations of values of A and B have been analyzed, it ends.

Remark 6.7. The algorithm described above is not necessarily the most efficient. Since we assume the parameters A and B to be integers, it is possible to find all possible values of the y-coordinate of torsion points using a result called the Nagell-Lutz Theorem 7.7. The above procedure, however, is easier to modify to include non-integer rational values for A and B.

We ran the algorithm for all values of A and B in $\{-20, -19, \dots, 20\}$. For 1676 of the 1681 combinations, the discriminant is non-zero. Of these 1676 elliptic curves, 1494 have trivial torsion group. For example, the elliptic curves with the following equations have trivial torsion group:

$$y^2 = x^3 - 19x + 13;$$
$$y^2 = x^3 - 11x - 11;$$
$$y^2 = x^3 + 5x + 7;$$
$$y^2 = x^3 + 8x + 5.$$

Interestingly, a relatively large number of elliptic curves has trivial torsion group. This is, in fact, not a coincidence.

Denote the elliptic curve over $\mathbb{Q}$ with equation $y^2 = x^3 + Ax + B$ by $E_{(A,B)}$. For $M \in \mathbb{Z}$, $M > 0$, define the following sets:

$$\mathcal{C}(M) := \{(A, B) \in \mathbb{Z} \mid 4A^3 + 27B^2 \neq 0,\ |A|, |B| \leq M\},$$
$$\mathcal{T}(M) := \{(A, B) \in \mathcal{C}(M) \mid \operatorname{Tor}\left(E_{(A,B)}\right) \neq \{O\}\}.$$

Then we have the following result from [GJT10].

Theorem 6.8. *With the notation as above:*

$$\lim_{M \to \infty} \frac{|\mathcal{T}(M)|}{|\mathcal{C}(M)|} = 0.$$

In other words, an elliptic curve $E_{(A,B)}$ with $|A|, |B| \leq M$ arbitrarily chosen is more likely to have a trivial torsion group for larger values of M.

7 Non-existence of torsion points of order 11

By Mazur's theorem 1.17, we know that an elliptic curve E over $\mathbb{Q}$ can only have rational torsion points with order in $\{1, 2, \ldots, 10, 12\}$. In particular, such a curve can not have a rational torsion point of order 11. This fact was already known before Mazur's theorem. The aim of this section is to show a proof of this fact. This section is adapted from the proof by I. Kiming [Kim03]. We provide additional details.

Theorem 7.1. *(Billing-Mahler, cf. [BM40]) An elliptic curve E over $\mathbb{Q}$ does not have a rational torsion point of order* 11*.*

Proof. This prove uses several intermediate results. Consider the following facts:

- Fact 1: If there exists an elliptic curve over $\mathbb{Q}$ with a rational torsion point of order 11, then the cubic curve C over $\mathbb{Q}$ given by
$$u^2v - u^2w + uw^2 - v^2w = 0 \tag{7.1}$$
has more than 5 rational points.
- Fact 2: Let C be the cubic curve over $\mathbb{Q}$ given by (7.1) and let E be the elliptic curve over $\mathbb{Q}$ given by the homogeneous equation
$$y^2z = x^3 - 4x^2z + 16z^3. \tag{7.2}$$
Then, there exists a bijection between $C(\mathbb{Q})$ and $E(\mathbb{Q})$.
- Fact 3: The elliptic curve E over $\mathbb{Q}$ given by (7.2) has exactly 5 rational points.

The proofs of these facts can be found in subsections 7.1, 7.2 and 7.3, respectively.
Facts 2 and 3 together imply that the cubic curve C over $\mathbb{Q}$ given by (7.1) has exactly 5 rational points. By fact 1, this means that there can not exist an elliptic curve over $\mathbb{Q}$ with a point of order 11. This concludes the proof. □

The proofs of Facts 1 and 2 use mostly algebraic and geometrical arguments. The proof of Fact 3 uses results from algebraic number theory. The relevant background information on algebraic number theory is discussed in Appendix A.

7.1 Cubic curve C

In this section, we prove the following proposition.

Proposition 7.2 (Fact 1)**.** *If there exists an elliptic curve over $\mathbb{Q}$ with a rational torsion point of order* 11*, then the cubic curve C over $\mathbb{Q}$ given by* (7.1) *has more than* 5 *rational points.*

Proof. Assume E is an elliptic curve over $\mathbb{Q}$ with the rational point $\widetilde{P}$ of order 11. In this proof, we consider all points to be in the projective plane $\mathbb{P}^2_{\mathbb{Q}}$. For any integer $i \in \mathbb{Z}$, denote $\widetilde{P}_i := i \cdot \widetilde{P}$. Since $\widetilde{P}$ is of order 11, we have

$$\widetilde{P}_i = \widetilde{P}_j \iff i \equiv j \mod 11.$$

Henceforth, three points $\widetilde{P}_i$, $\widetilde{P}_j$ and $\widetilde{P}_k$ are on a line in $\mathbb{P}^2_{\mathbb{Q}}$ if and only if the indices i, j, and k add up to a multiple of 11. In other words,

$$\widetilde{P}_i + \widetilde{P}_j + \widetilde{P}_k = O \iff i + j + k \equiv 0 \mod 11. \tag{7.3}$$

Denote $\widetilde{P} = (a : b : c)$ and $\widetilde{P}_2 = (\alpha : \beta : \gamma)$. We have $\widetilde{P}_0 = O = (0 : 1 : 0)$. By (7.3), these three points are not on a line. Therefore, the points $(0, 1, 0)$, (a, b, c) and (α, β, γ) in $\mathbb{Q}^3$ are linearly independent. We can define an invertible linear map ϕ from $\mathbb{Q}^3$ into itself by

$$\begin{aligned} \phi :\ & \mathbb{Q}^3 \to \mathbb{Q}^3 \\ (0,1,0) &\mapsto (0,1,0) =: P'_0, \\ (a,b,c) &\mapsto (1,0,0) =: P'_1, \\ (\alpha,\beta,\gamma) &\mapsto (0,0,1) =: P'_2. \end{aligned}$$

Denote $P_i' := \phi(\widetilde{P}_i)$. We can consider the map ϕ as a bijective map from $\mathbb{P}^2_{\mathbb{Q}}$ into itself. As such it maps lines to lines, so Lemma 7.3 implies that P_i', P_j' and P_k' are on a line if and only if $i+j+k \equiv 0 \mod 11$.

In particular, the point P_3' is not on the line through P_0' and P_1'. This line is given by $z = 0$ by Lemma 1.2. Therefore, if we denote $P_3' = (u, v, w)$, we know that $w \neq 0$. Similarly, P_3' is not on the line through P_0' and P_2' given by $x = 0$ or the line through P_1' and P_2' given by $y = 0$, so $u \neq 0$ and $v \neq 0$ as well.

Since all of the coordinates of P_3' are non-zero, we can use a change of variables to normalize the point P_3' to $(1, 1, 1)$. To be precise, we consider the invertible linear map ψ of $\mathbb{Q}^3$ into itself, given by

$$\begin{aligned} \psi :\ & \mathbb{Q}^3 \to \mathbb{Q}^3 \\ & (x, y, z) \mapsto (u^{-1}x, v^{-1}y, w^{-1}z). \end{aligned}$$

We can consider this map ψ to be a bijection from $\mathbb{P}^2_{\mathbb{Q}}$ into itself. As such, it maps lines to lines, and it fixes the projective points $(1 : 0 : 0)$, $(0 : 1 : 0)$ and $(0 : 0 : 1)$.

Denote $P_i := \psi(P_i') = \psi(\phi(\widetilde{P}_i))$ for $i \in \mathbb{Z}$. Then we have

$$P_0 = (0 : 1 : 0), \tag{7.4}$$
$$P_1 = (1 : 0 : 0), \tag{7.5}$$
$$P_2 = (0 : 0 : 1), \tag{7.6}$$
$$P_3 = (1 : 1 : 1). \tag{7.7}$$

Similar to before, we have

$$P_i = P_j \iff i \equiv j \mod 11 \tag{7.8}$$

and P_i, P_j and P_k are on a line if and only if $i + j + k \equiv 0 \mod 11$.

Using these facts and Lemma 1.2, we can prove the following lemma:

Lemma 7.3. *In the above setting we have*

$$P_{-3} = (1 : 0 : 1). \tag{7.9}$$

Additionally, if we denote

$$P_4 = (x_1 : x_2 : x_3), \tag{7.10}$$

where $x_i \in \mathbb{Q}$, then the coordinates of P_4 satisfy the equation

$$x_1^2x_2 - x_1^2x_3 + x_1x_3^2 - x_2^2x_3 = 0. \tag{7.11}$$

Proof. If $i \not\equiv j \mod 11$, there exists a unique line through P_i and P_j, which we denote by $L_{i,j}$. Lemma 1.2 tells us how to find the equation for $L_{i,j}$ given the coordinates of P_i and P_j. Furthermore, if k, i, j, m, n are integers satisfying $k + i + j \equiv k + m + n \equiv 0 \mod 11$, then we can conclude that P_k is on the intersection between $P_{i,j}$ and $P_{m,n}$.

First, we find some restrictions on the values of x_1, x_2 and x_3. By (7.8), we know that P_4 is distinct from P_0, P_1, P_2 and P_3. In particular, this means that at most one of x_1, x_2 and x_3 can be equal to 0.

In order to find the coordinates of P_{-3}, we construct lines through points of which we know the coordinates already, and find the coordinates of their intersections. First, using equalities (7.4), (7.5), (7.6) and (7.7), we compute the equations of the following lines:

$$L_{0,1} : z = 0; \tag{7.12}$$
$$L_{0,2} : x = 0; \tag{7.13}$$
$$L_{0,3} : x - z = 0; \tag{7.14}$$
$$L_{1,2} : y = 0; \tag{7.15}$$
$$L_{1,4} : x_3y - x_2z = 0; \tag{7.16}$$
$$L_{2,3} : x - y = 0. \tag{7.17}$$

Note: if $x_2 = 0$, then $x_3 \neq 0$, which implies that $L_{1,4} = L_{1,2}$. This implies that P_1, P_2 and P_4 are on a line, but $1 + 2 + 4 \not\equiv 0 \mod 11$, so this is a contradiction. Hence, $x_2 \neq 0$. Similarly, $x_3 \neq 0$ since P_0, P_1 and P_4 are not on a line.

We know that P_0, P_1 and P_3 are not on a line, since $0+1+3 \not\equiv 0 \mod 11$. Hence, $L_{0,3}$ and $L_{1,2}$ are distinct lines. Since $-3+0+3 \equiv -3+1+2 \equiv 0 \mod 11$, the point P_{-3} is the unique point of intersection between $L_{0,3}$ and $L_{1,2}$. Combining (7.14) and (7.15), we find:

$$P_{-3} = (1:0:1),$$

which is what we wanted to show.

Next, in order to establish equation (7.11), we aim to find an expression the coordinates of P_5 in terms of x_1, x_2 and x_3. Since $2+4+5 \equiv 0 \mod 11$, the points P_2, P_4 and P_5 are on a line. The relation between the coordinates of these points then gives us the desired equation.

First, we need to find expressions for the coordinates of the points P_{-1}, P_{-2} and P_{-5} in terms of x_1, x_2 and x_3. Combining (7.9) and (7.10), we can find the equation of the line $L_{-3,4}$:

$$L_{-3,4}: \ -x_2x + (x_1 - x_3)y + x_2z = 0. \tag{7.18}$$

We know that $x_2 \neq 0$ and $x_3 \neq 0$. If $x_1 = x_3$, then $L_{-3,4} = L_{0,3}$, which implies that P_0, P_3 and P_4 are on a line. However, since $0+3+4 \not\equiv 0 \mod 11$, this is a contradiction. Hence, $x_1 \neq x_3$.

The point P_{-1} is the unique point of intersection between $L_{0,1}$ and $L_{-3,4}$. By combining (7.12) and (7.18), we find:

$$P_{-1} = (x_1 - x_3 : x_2 : 0). \tag{7.19}$$

Since $x_1 - x_3 \neq 0$ and $x_2 \neq 0$, this is a well-defined point which is distinct from any of the previously defined points. By combining (7.19) and (7.7), we can find the equation of the line $L_{-1,3}$:

$$L_{-1,3}: \ x_2x - (x_1 - x_3)y + (x_1 - x_2 - x_3)z = 0. \tag{7.20}$$

Note: if $x_1 - x_3 = x_2$, then $L_{-1,3} = L_{2,3}$. This implies that P_{-1}, P_2 and P_3 are on a line. However, we can compute $-1+2+3 \not\equiv 0 \mod 11$, so this is a contradiction. Hence, $x_1 - x_3 \neq x_2$.

The point P_{-2} is the unique point of intersection between $L_{0,2}$ and $L_{-1,3}$. By combining (7.13) and (7.20), we find:

$$P_{-2} = (0 : x_1 - x_2 - x_3 : x_1 - x_3). \tag{7.21}$$

Since $x_1 - x_3 \neq 0$, $x_1 - x_3 \neq x_2$ and $x_2 \neq 0$, this is a well-defined point which is distinct from any of the previously defined points. By combining (7.21) and (7.9), we can find the equation of the line $L_{-2,-3}$:

$$L_{-2,-3}: \ (x_1 - x_2 - x_3)x + (x_1 - x_3)y - (x_1 - x_2 - x_3)z = 0. \tag{7.22}$$

The point P_{-5} is the unique point of intersection between $L_{1,4}$ and $L_{2,3}$. By combining (7.16) and (7.17), we find:

$$P_{-5} = (x_2 : x_2 : x_3). \tag{7.23}$$

Note: since $-5 \not\equiv 3 \mod 11$, we have that $P_{-5} \neq P_3$, so $x_2 \neq x_3$.

By combining (7.4) and (7.23), we can find the equation of the line $L_{0,-5}$:

$$L_{0,-5}: \ x_3x - x_2z = 0. \tag{7.24}$$

The point P_5 is the unique point of intersection between $L_{0,-5}$ and $L_{-2,-3}$. By combining (7.24) and (7.22), we find:

$$P_5 = ((x_1 - x_3)x_2 : -x_1x_2 + x_1x_3 + x_2^2 - x_3^2 : (x_1 - x_3)x_3). \tag{7.25}$$

Note: since $x_1 - x_3 \neq 0$ and $x_2 \neq 0$, this is a well-defined point.

Since $2+4+5 \equiv 0 \mod 11$, the points P_2, P_4 and P_5 lie on a line. Therefore, we find:

$$\det\left(\begin{bmatrix} 0 & 0 & 1 \\ x_1 & x_2 & x_3 \\ (x_1 - x_3)x_2 & -x_1x_2 + x_1x_3 + x_2^2 - x_3^2 & (x_1 - x_3)x_3 \end{bmatrix}\right) = 0.$$

This is equivalent to

$$x_1^2 - x_1^2x_3 + x_1x_3^2 - x_2^2x_3 = 0,$$

which is what we wanted to show. This concludes the proof. □

Let C be the cubic curve over $\mathbb{Q}$ given by (7.1). A straightforward computation verifies that all of P_0, P_1, P_2, P_3 and P_{-3} are rational points on C. By Lemma 7.3, P_4 is also a rational point on C. By (7.8), all of these points are mutually distinct. Henceforth, there are more than 5 distinct rational points on C. This concludes the proof. □

7.2 Curves C and E

Consider the cubic curve C given by (7.1) and the elliptic curve E given by the homogeneous equation (7.2). Define the sets A and B as

$$\begin{aligned} A &:= \{(u : v : w) \in C(\mathbb{Q}) \mid uv \neq 0\}, \\ B &:= \{(x : y : z) \in E(\mathbb{Q}) \mid x(y + 4z) \neq 0\}. \end{aligned} \tag{7.26}$$

The proof of the following proposition is a special case of an algorithm developed by T. Nagell [Nag28].

Proposition 7.4. *Let C, E, A and B be as above.*
The map f defined by

$$f(u : v : w) = (4uv : 8v^2 - 4uw : uw)$$

maps points in A to points in B.
The map g defined by

$$g(x : y : z) = (2x^2 : x(y + 4z) : 4z(y + 4z))$$

maps points in B to points in A.
Moreover, if we consider $f : A \to B$ and $g : B \to A$, then

$$\begin{aligned} g \circ f &= \mathrm{id}_A, \\ f \circ g &= \mathrm{id}_B . \end{aligned}$$

Henceforth, there is a bijection between A and B.

Proof. First, we show that f maps points in A to points in B. Let $(u : v : w)$ be a point in A. Then $uv \neq 0$. Since $A \subset C(\mathbb{Q})$, we know that u, v and w satisfy (7.1). Therefore, we also have $w \neq 0$, since otherwise (7.1) would imply $u^2v = 0$ and hence $uv = 0$, which is a contradiction. We can hence put

$$V := \frac{v}{u}, \quad W := \frac{w}{u}, \quad t := \frac{V}{W}.$$

Using (7.1), we find that

$$\begin{aligned} t^2W^3 - W^2 + (1 - t)W &= V^2W - W^2 + W - V \\ &= u^{-3}\left(v^2w - w^2u + wu^2 - vu^2\right) \\ &= 0. \end{aligned}$$

Since $w \neq 0$, we have $W \neq 0$, so we can obtain the equality

$$t^2W^2 - W + (1 - t) = 0. \tag{7.27}$$

Put

$$R := 1 - 4t^2(1 - t).$$

Using the quadratic formula on (7.27), we find

$$W \in \left\{ \frac{1 \pm \sqrt{R}}{2t^2} \right\}.$$

We can rewrite this to obtain

$$2t^2W - 1 \in \left\{ \pm\sqrt{R} \right\}. \tag{7.28}$$

Put

$$x := 4t, \quad y := 4(2t^2W - 1).$$

By (7.28), we know

$$(2t^2W - 1)^2 \in \left\{ \left(\pm\sqrt{R} \right)^2 \right\} = \{R\},$$

so

$$y^2 = 4^2 R.$$

Therefore, we see that x and y satisfy

$$\begin{aligned} y^2 &= 4^2 R \\ &= (4t)^3 - 4 \cdot (4t)^2 + 16 \\ &= x^3 - 4x^2 + 16. \end{aligned}$$

Hence, the point $(x : y : 1) = (4uv : 8v^2 - 4uw : uw) = f(u : v : w)$ is in $E(\mathbb{Q})$. To show that this point is in B, it is sufficient to show that $x \neq 0$ and $y + 4 \neq 0$.
By assumption, we have $V \neq 0$ and $W \neq 0$, so $t \neq 0$. Since $x = 4t$, it follows that $x \neq 0$. It also follows that $2t^2W - 1 \neq -1$, so $y = 4(2t^2W - 1) \neq -4$, so $y + 4 \neq 0$. This shows that f maps points in A to points in B.

Secondly, we show that g maps points in B to points in A. Let $(x : y : z)$ be a point in B. Put

$$u := 2x^2, \quad v := x(y + 4z), \quad w := 4z(y + 4z).$$

By assumption, $x(y + 4z) \neq 0$, so the point $(u : v : w)$ is on the projective plane. We also have $x \neq 0$, so both $u \neq 0$ and $v \neq 0$, so $uv \neq 0$. Thus, if $(u : v : w)$ is in $C(\mathbb{Q})$, then it is A. The fact that $(u : v : w)$ is in $C(\mathbb{Q})$ follows from a straightforward computation:

$$\begin{aligned} u^2v - u^2w + uw^2 - v^2w &= 4x^5(y + 4z) - 16x^4z(y + 4z) + 32x^2z^2(y + 4z)^2 - 4x^2z(y + 4z)^3 \\ &= 4x^2(y + 4z) \cdot \left(x^3 - 4x^2z + 8z^2(y + 4z) - z(y + 4z)^2 \right) \\ &= 4x^2(y + 4z) \cdot \left(x^3 - 4x^2z + 16z^3 - y^2z \right). \end{aligned}$$

Since $(x : y : z)$ is in $E(\mathbb{Q})$, we know from (7.2) that $x^3 - 4x^2z + 16z^3 - y^2z = 0$, so in fact

$$u^2v - u^2w + uw^2 - v^2w = 0.$$

This shows that g maps points in B to points in A.

Finally, we consider $f : A \to B$ and $g : B \to A$ and show that $g \circ f = \mathrm{id}_A$ and $f \circ g = \mathrm{id}_B$.
Let $(u : v : w)$ be an arbitrary point in A. In particular, this means that $uv^2 \neq 0$. We have

$$\begin{aligned} (g \circ f)(u : v : w) &= g(4uv : 8v^2 - 4uw : uw) \\ &= (32u^2v^2 : 4uv(8v^2 - 4uw + 4uw) : 4uw(8v^2 - 4uw + 4uw)) \\ &= (32uv^2 \cdot u : 32uv^2 \cdot v : 32uv^2 \cdot w) \\ &= (u : v : w). \end{aligned}$$

Since $(u : v : w)$ was chosen arbitrarily, this works for all elements of A. Hence, $g \circ f = \mathrm{id}_A$.
Let $(x : y : z)$ be an arbitrary point in B. In particular, this means that $x^2(y + 4z) \neq 0$. We have

$$\begin{aligned} (f \circ g)(x : y : z) &= f(2x^2 : x(y + 4z) : 4z(y + 4z)) \\ &= (8x^3(y + 4z) : 8x^2(y + 4z)^2 - 32x^2z(y + 4z) : 8x^2z(y + 4z)) \\ &= (8x^2(y + 4z) \cdot x : 8x^2(y + 4z) \cdot (y + 4z - 4z) : 8x^2(y + 4z) \cdot z) \\ &= (x : y : z). \end{aligned}$$

Since $(x : y : z)$ was chosen arbitrarily, this works for all elements of B. Hence, $f \circ g = \mathrm{id}_B$.
This concludes the proof. □

Using this result, we can prove the following proposition.

Proposition 7.5 (Fact 2)**.** *Let C be the cubic curve over $\mathbb{Q}$ given by* (7.1) *and let E be the elliptic curve over $\mathbb{Q}$ given by* (7.2)*. Then, there exists a bijection between $C(\mathbb{Q})$ and $E(\mathbb{Q})$.*

Proof. Define the sets A and B as in (7.26). By Proposition 7.4, there exists a bijection between A and B. Therefore, it is sufficient to show that there exists a bijection between $C(\mathbb{Q}) \setminus A$ and $E(\mathbb{Q}) \setminus B$. In fact, we can show that $C(\mathbb{Q}) \setminus A$ and $E(\mathbb{Q}) \setminus B$ are both finite sets with exactly 4 elements, which implies the existence of a bijection between them.

First, we find all points in $C(\mathbb{Q})$ which are not in A. Assume $(u : v : w) \in C(\mathbb{Q}) \setminus A$. Then $uv = 0$.

- If $u = 0$, then v and w must satisfy
$$v^2 w = 0,$$
so $v = 0$ or $w = 0$. Since u, v and w can not all be 0, we find that the points in $C(\mathbb{Q})$ satisfying $u = 0$ are $(0 : 0 : 1)$ and $(0 : 1 : 0)$.
- if $v = 0$, then u and w must satisfy
$$uw(w - u) = 0,$$
so $u = 0$, $w = 0$, or $w = u \neq 0$. Since u, v and w can not all be 0, we find that the points in $C(\mathbb{Q})$ satisfying $v = 0$ are $(0 : 0 : 1)$, $(1 : 0 : 0)$ and $(1 : 0 : 1)$.

Thus, $C(\mathbb{Q}) \setminus A = \{(1 : 0 : 0), (0 : 1 : 0), (0 : 0 : 1), (1 : 0 : 1)\}$ is a set containing exactly 4 elements.

Secondly, we find all points in $E(\mathbb{Q})$ which are not in B. Assume $(x : y : z) \in E(\mathbb{Q}) \setminus B$. Then $x(y + 4z) = 0$.

- If $x = 0$, then y and z must satisfy
$$y^2 z = 16z^3.$$
Since x, y and z can not all be 0, we find either $z = 0$, $y = 4z$ or $y = -4z$. Hence, the points in $E(\mathbb{Q})$ satisfying $x = 0$ are $(0 : 1 : 0)$, $(0 : 4 : 1)$ and $(0 : -4 : 1)$.
- If $y = -4z$, then x and z must satisfy
$$x^3 - 4x^2 z = 0.$$
Since x, y and z can not all be 0, we find either $x = 0$ or $x = 4z$. Hence, the points in $E(\mathbb{Q})$ satisfying $y + 4z = 0$ are $(0 : -4 : 1)$ and $(4 : -4 : 1)$.

Thus, $E(\mathbb{Q}) \setminus B = \{(0 : 1 : 0), (0 : 4 : 1), (0 : -4 : 1), (4, -4, 1)\}$ is a set containing exactly 4 elements. By our previous arguments, this concludes the proof. □

7.3 Elliptic curve E

Consider the elliptic curve E given by (7.2). In this section, we consider the Weierstrass normal form of this equation, which is given by

$$y^2 = x^3 - 4x^2 + 16. \tag{7.29}$$

The aim of this section is to prove the following proposition.

Proposition 7.6 (Fact 3)**.** *Let E be the curve given by* (7.29)*. Then $|E(\mathbb{Q})| = 5$.*

To prove this proposition, we show that $E(\mathbb{Q})$ has exactly 5 torsion points using the Nagell-Lutz theorem, and we show that $E(\mathbb{Q})$ has no free part using arguments from algebraic number theory.

7.3.1 The torsion group of E

The following result is used in this section [Was08, theorem 8.7].

Theorem 7.7 (Nagell-Lutz Theorem)**.** *Let E' be a non-singular elliptic curve over $\mathbb{Q}$ which has an equation in Weierstrass normal form given by*

$$y^2 = x^3 + ax^2 + bx + c$$

with $a, b, c \in \mathbb{Z}$. We can write the discriminant D of the polynomial on the right-hand side as

$$D = -4a^3 c + a^2 b^2 + 18abc - 4b^3 - 27c^2. \tag{7.30}$$

Suppose $P = (x, y)$ is a $\mathbb{Q}$-rational point on E' of finite order. The coordinates of P must satisfy both of the following properties:

- *the coordinates x and y are both integers;*
- *either $y = 0$ or y^2 divides D.*

The proof of this theorem is beyond the scope of this paper and is omitted.

The following result is used in this section.

Theorem 7.8 (Rational root theorem)**.** *Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial with integer coefficients and $a_0, a_n \neq 0$. Suppose f has a rational root $\frac{p}{q}$, where $p, q \in \mathbb{Z}$ and $\gcd(p, q) = 1$. Then q divides a_n and p divides a_0.*

We can use the Nagell-Lutz theorem 7.7 and the rational root theorem 7.8 to find all torsion points of $E(\mathbb{Q})$.

Lemma 7.9 (Torsion points of $E(\mathbb{Q})$)**.** *Let E be the elliptic curve given by* (7.29)*.*
Then $\mathrm{Tor}(E(\mathbb{Q})) = \{O, (0,4), (0,-4), (4,4), (4,-4)\}$ and the point $(0,4)$ is a generator for this group.

Proof. The equation for E is of the form $y^2 = x^3 + ax^2 + bx + c$ with $a, b, c \in \mathbb{Z}$, so we can use the Nagell-Lutz theorem.
Substituting $a = -4$, $b = 0$ and $c = 16$ into (7.30), we find

$$\begin{aligned} D &= -4 \cdot (-4)^3 \cdot 16 - 27 \cdot 16^2 \\ &= 16^2 \cdot (16 - 27) \\ &= -11 \cdot 16^2. \end{aligned}$$

Suppose $(x, y) \in \mathrm{Tor}(E(\mathbb{Q}))$. By the Nagell-Lutz theorem, we know that x and y must be integers and either $y = 0$ or y^2 divides $D = -11 \cdot 16^2$. Note that y^2 divides D if and only if y divides 16. Hence, we have $y^2 \in \{0, 1, 4, 16, 64, 256\}$. The x-coordinate must satisfy

$$x^3 - 4x^2 + 16 - y^2 = 0.$$

Using Theorem 7.8, we can find the rational roots of this polynomial for the aforementioned values of y^2. Fix a value of y^2. If the polynomial $x^3 - 4x^2 + 16 - y^2$ has a rational root $x = p/q$, where p and q are coprime integers, then p must divide $16 - y^2$ and q must divide 1. Without loss of generality, we can assume $q = 1$. We need to check for all possible values of p whether it gives a root. We use SageMath [The23] to do these computations and omit them here.

We find that the polynomial only has rational roots for $y^2 = 16$. In this case, the roots are $x = 0$ and $x = 4$. Henceforth, the torsion points of $E(\mathbb{Q})$ are exactly O, $(0,4)$, $(0,-4)$, $(4,4)$ and $(4,-4)$.

We can use the chord-tangent law to show that $(0,4)$ generates the torsion group. The tangent line to E at $(0,4)$ is given by $y = \lambda x + \beta$, where $\beta = 4$ and $\lambda = \frac{f'(0)}{8} = \frac{3 \cdot 0^2 - 8 \cdot 0}{8} = 0$. Then by (1.9), we have

$$\begin{aligned} x_3 &= 4, \\ y_3 &= 4. \end{aligned}$$

Hence, by (1.10), we have

$$2 \cdot (0,4) = (4,-4).$$

Next, we can compute $3 \cdot (0,4) = 2 \cdot (0,4) + (0,4) = (4,-4) + (0,4)$. The line through $(4,-4)$ and $(0,4)$ is given by $y = -2x + 4$. Then by (1.9), we have

$$\begin{aligned} x_3 &= 4 + 4 - 4 = 4, \\ y_3 &= -2 \cdot 4 + 4 = -4. \end{aligned}$$

Thus, by (1.10), we have

$$3 \cdot (0,4) = (4,4) = -(2 \cdot (0,4)).$$

Then

$$\begin{aligned} 4 \cdot (0,4) &= 3 \cdot (0,4) + (0,4) \\ &= -2 \cdot (0,4) + (0,4) \\ &= -(0,4) = (0,-4), \end{aligned}$$

and hence

$$\begin{aligned} 5 \cdot (0,4) &= 4 \cdot (0,4) + (0,4) \\ &= -(0,4) + (0,4) \\ &= O. \end{aligned}$$

So indeed, $(0,4)$ generates the torsion group. □

Recall from section 1 that we can write

$$E(\mathbb{Q}) \cong \mathrm{Tor}(E(\mathbb{Q})) \times \mathbb{Z}^r$$

for some unique finite non-negative integer r. By Lemma 7.9

$$\mathrm{Tor}(E(\mathbb{Q})) \cong \mathbb{Z}/5\mathbb{Z}.$$

In order to show that $E(\mathbb{Q})$ has exactly 5 points, it is therefore sufficient to show that $r = 0$. Finding the rank of an elliptic curve, however, is not an easy task. We use algebraic number theory to find the rank of $E(\mathbb{Q})$. In order to do this, we consider the fields obtained by appending roots of $f(x) = x^3 - 4x^2 + 16$ to $\mathbb{Q}$. Therefore, we need to know more about the roots of f.

7.3.2 Roots of f

The aim of this section is to find whether the roots $\theta_1, \theta_2, \theta_3$ of the polynomial $f(x) = x^3 - 4x^2 + 16$ are rational, real and irrational, or complex. To this purpose, we use the following theorem.

Theorem 7.10. *Let f be a polynomial over $\mathbb{C}$ given by*

$$f(x) = x^3 + ax^2 + bx + c,$$

where $a, b, c \in \mathbb{R}$. Let the discriminant D of f be given by (7.30). We have the following.

- *If $D > 0$, then f has 3 distinct real roots.*
- *If $D < 0$, then f has 1 real root and 2 non-real complex conjugate roots.*
- *If $D = 0$ and $a^2 = 3b$, then f has 1 real root with multiplicity 3.*
- *If $D = 0$ and $a^2 \neq 3b$, then f has 2 distinct real roots, of which 1 with multiplicity 2.*

Additionally, D is related to the roots r_1, r_2, r_3 of f by

$$D = (r_1 - r_2)^2 (r_1 - r_3)^2 (r_2 - r_3)^2.$$

In this case, we have

$$D = -11 \cdot 16^2,$$

as we computed in the proof of 7.9. Hence, by Theorem 7.10, f has 1 real root $\theta_1 =: \theta$ and 2 non-real complex conjugate roots θ_2 and θ_3.

We need to know whether the real root θ is rational. To this purpose, we use the rational root theorem 7.8 to find whether f has a rational root. By the rational root theorem, if f has a rational root $\frac{p}{q}$ with $p, q \in \mathbb{Z}$ and $\gcd(p, q) = 1$, then q divides 1 and p divides 16. Thus, if f has a rational root, it must be in $\{\pm 1, \pm 2, \pm 4, \pm 8, \pm 16\}$. We can substitute these values for x to find whether f has a rational root. We compute

$$\begin{aligned} f(1) &= 13, & f(-1) &= 11, \\ f(2) &= 8, & f(-2) &= -8, \\ f(4) &= 16, & f(-4) &= -112, \\ f(8) &= 272, & f(-8) &= -752, \\ f(16) &= 3088, & f(-16) &= -5104. \end{aligned}$$

We conclude that f has no rational roots. Hence, θ is real and irrational.

By factoring f, we can find expressions for θ_2 and θ_3 in terms of θ_1. A computation verifies that

$$x^3 - 4x^2 + 16 = (x - \theta_1)(x^2 + (\theta_1 - 4)x + \theta_1(\theta_1 - 4)).$$

We see that θ_2 and θ_3 are the roots of $x^2 + (\theta_1 - 4)x + \theta_1(\theta_1 - 4)$. Using the quadratic formula, we can put

$$\theta_2 := \frac{4 - \theta_1 + \sqrt{-3\theta_1^2 + 8\theta_1 + 16}}{2}, \quad \theta_3 := \frac{4 - \theta_1 - \sqrt{-3\theta_1^2 + 8\theta_1 + 16}}{2}.$$

7.3.3 The rank of E

In this section, we use definitions and results from Appendix A freely.
Define the polynomial f by

$$f(x) = x^3 - 4x^2 + 16.$$

In section 7.3.2 we find that f has 1 irrational real root, which we denote by θ, and 2 non-real complex conjugate roots, which we denote by θ_2 and θ_3. Since f has degree 3 and does not have any roots in $\mathbb{Q}$, we know that it is irreducible over $\mathbb{Q}$. Therefore, f is the minimal polynomial of θ over $\mathbb{Q}$.

Consider the number field

$$K := \mathbb{Q}(\theta).$$

Since we can substitute $\theta^3 = 4\theta^2 - 16$, any element of K can be written uniquely in the form

$$p_0 + p_1\theta + p_2\theta^2$$

for some rational numbers p_0, p_1, p_2. Using SageMath [The23], we find that $\{1, \theta/2, \theta^2/4\}$ is an integral basis of K.

We know that K has 1 real embedding and 2 complex embeddings. The only roots of 1 in K are -1 and 1, since θ is real. By Theorem A.28, the group of units U of O_K is equal to the direct product $W \times V$, where $W = \{1, -1\}$ and V is a free abelian group of rank $1 + 1 - 1 = 1$, i.e. $V = \left\{\eta^k \mid k \in \mathbb{Z}\right\}$ for some fundamental unit η of O_K. Using SageMath [The23], we find that we can choose $\eta := 1 - \frac{\theta}{2}$.

Consider the map

$$\mu : E(\mathbb{Q}) \to K^\times / \left(K^\times\right)^2$$

defined by

$$\begin{aligned} \mu(O) &= 1 \mod \left(K^\times\right)^2, \\ \mu(x, y) &= (x - \theta) \mod \left(K^\times\right)^2. \end{aligned}$$

The following result is adapted from [Cas91].

Lemma 7.11. *The map μ is a group homomorphism.*

Proof. It is sufficient to show that $\mu(P_1 + P_2) = \mu(P_1)\mu(P_2)$ for any P_1, $P_2 \in E(\mathbb{Q})$. We consider three distinct cases.

- Assume $P_2 = O$. Then

$$\begin{aligned} \mu(P_1 + O) &= \mu(P_1) \\ &= \mu(P_1) \cdot \left(1 \mod \left(K^\times\right)^2\right) \\ &= \mu(P_1)\mu(O). \end{aligned}$$

- Assume $P_1 = (x_1, y_1) \neq O$ and $P_2 = -P_1$. Then P_1 and P_2 have the same x-coordinate, so

$$\begin{aligned} \mu(P_1 + (-P_1)) &= \mu(O) \\ &= 1 \mod \left(K^\times\right)^2 \\ &= (x_1 - \theta)^2 \mod \left(K^\times\right)^2 \\ &= \mu(P_1)\mu(-P_1). \end{aligned}$$

- Assume $P_1 = (x_1, y_1) \neq O$, $P_2 = (x_2, y_2) \neq O$ and $P_2 \neq P_1$. Let $P_3 = (x_3, y_3) := -(P_1 + P_2)$, so P_1, P_2 and P_3 lie on a line $y = \lambda x + \beta$ for some λ, $\beta \in \mathbb{Q}$. Then we must have that

$$f(x) - (\lambda x + \beta)^2 = (x - x_1)(x - x_2)(x - x_3).$$

If we replace x by θ, we find

$$(x_1 - \theta)(x_2 - \theta)(x_3 - \theta) = (\lambda\theta + \beta)^2.$$

Since θ is not rational, we know that x_1, x_2 and x_3 are not equal to θ, so in particular $x_1 - \theta$ and $x_2 - \theta$ have an inverse in $K^\times$. Hence, we find

$$x_3 - \theta = (x_1 - \theta)^{-1}(x_2 - \theta)^{-1}(\lambda\theta + \beta)^2.$$

Since $-P_3$ has the same x-coordinate as P_3, we have that

$$\begin{aligned}
\mu(P_1 + P_2) &= \mu(-P_3) \\
&= (x_3 - \theta) \mod \left(K^\times\right)^2 \\
&= (x_1 - \theta)^{-1}(x_2 - \theta)^{-1}(\lambda\theta + \beta)^2 \mod \left(K^\times\right)^2 \\
&= (x_1 - \theta)^{-1}(x_2 - \theta)^{-1} \mod \left(K^\times\right)^2 \\
&= (x_1 - \theta)^{-1}(x_2 - \theta)^{-1} \cdot (x_1 - \theta)^2(x_2 - \theta)^2 \mod \left(K^\times\right)^2 \\
&= (x_1 - \theta)(x_2 - \theta) \mod \left(K^\times\right)^2 \\
&= \mu(P_1)\mu(P_2).
\end{aligned}$$

Hence, $\mu(P_1 + P_2) = \mu(P_1)\mu(P_2)$ for all P_1, $P_2 \in E(\mathbb{Q})$. This concludes the proof. □

The following result is from [Cas91].

Lemma 7.12. *The kernel of μ is $2E(\mathbb{Q})$.*

Proof. The fact that $2E(\mathbb{Q}) \subset \ker(\mu)$ follows from Lemma 7.11: let $P_2 \in 2E(\mathbb{Q})$ be arbitrary. Then, there exists a point $P_1 \in E(\mathbb{Q})$ such that $P_2 = P_1 + P_1$. Then, by Lemma 7.11:

$$\begin{aligned}
\mu(P_2) &= \mu(P_1 + P_1) \\
&= \mu(P_1)^2 \\
&= 1 \mod \left(K^\times\right)^2.
\end{aligned}$$

Hence, $P_2 \in \ker(\mu)$. Since P_2 was chosen arbitrarily, this holds for all elements of $2E(\mathbb{Q})$. This proves that $2E(\mathbb{Q}) \subset \ker(\mu)$.

In the following, we show that $\ker(\mu) \subset 2E(\mathbb{Q})$. Together with the fact that $2E(\mathbb{Q}) \subset \ker(\mu)$, this implies that $\ker(\mu) = 2E(\mathbb{Q})$.
By definition of μ, we have $O \in \ker(\mu)$. We have $O = 2O$, so $O \in 2E(\mathbb{Q})$. Let $P_1 = (x_1, y_1) \in \ker(\mu) \setminus \{O\}$ be arbitrary. Then $\mu(x_1, y_1) = (x_1 - \theta) \mod \left(K^\times\right)^2 = 1 \mod \left(K^\times\right)^2$, so we can write

$$x_1 - \theta = \left(p_2\theta^2 + p_1\theta + p_0\right)^2$$

for some p_0, p_1, $p_2 \in \mathbb{Q}$, not all zero.

Assume for contradiction that $p_2 = 0$. In this case, we can rewrite the above equation to obtain

$$p_1^2\theta^2 + (2p_0p_1 + 1)\theta + (p_0^2 - x_1) = 0.$$

Since p_0, p_1, $x_1 \in \mathbb{Q}$, this implies that θ is the root of a polynomial over $\mathbb{Q}$ of degree 2. However, this contradicts the fact that $f(x) = x^3 - 4x^2 + 16$ is the minimal polynomial of θ over $\mathbb{Q}$, as f has degree 3. Hence, by contradiction, we find that $p_2 \neq 0$.

We claim that it is possible to find rational numbers s_0, s_1, r_0, r_1, where r_0 and r_1 are not both equal to 0, such that

$$(s_1\theta + s_0)(p_2\theta^2 + p_1\theta + p_0) = r_1\theta + r_0.$$

Substituting $\theta^3 = 4\theta^2 - 16$, we get

$$\begin{aligned}(s_1\theta + s_0)(p_2\theta^2 + p_1\theta + p_0) &= s_1p_2\theta^3 + (s_0p_2 + s_1p_1)\theta^2 + (s_1p_0 + s_0p_1)\theta + s_0p_0 \\ &= (s_0p_2 + s_1p_1 + 4s_1p_2)\theta^2 + (s_1p_0 + s_0p_1)\theta + s_0p_0 - 16s_1p_2.\end{aligned}$$

Since $p_2 \neq 0$, we can choose $s_1 = -1$, $s_0 = \frac{p_1}{p_2} + 4$, $r_1 = \frac{p_1^2}{p_2} + 4p_1 - p_0$, $r_0 = \frac{p_0p_1}{p_2} + 4p_0 + 16p_2$. Note that r_1 and r_0 can not both be equal to 0, since K is a domain and neither of $s_1\theta + s_0$ and $p_2\theta^2 + p_1\theta + p_0$ is equal to 0. For these values, we get

$$(s_0 - \theta)^2(p_2\theta^2 + p_1\theta + p_0)^2 = (r_1\theta + r_0)^2$$

and hence

$$(s_0 - \theta)^2(x_1 - \theta) = (r_1\theta + r_0)^2$$

so

$$(\theta - x_1)(s_0 - \theta)^2 + (r_1\theta + r_0)^2 = 0.$$

This means that θ is a root of the polynomial

$$(x - x_1)(s_0 - x)^2 + (r_1x + r_0)^2.$$

This is a monic polynomial of degree 3 over $\mathbb{Q}$. Therefore, this polynomial must be equal to the minimal polynomial f of θ over $\mathbb{Q}$:

$$f(x) = (x - x_1)(s_0 - x)^2 + (r_1x + r_0)^2.$$

We can rewrite this to

$$f(x) - (r_1x + r_0)^2 = (x - x_1)(s_0 - x)^2,$$

which means that the line $y = r_1x + r_0$ intersects E twice in the point (s_0, t), where $t = r_1s_0 + r_0 \in \mathbb{Q}$, and once in either $(x_1, y_1) = P_1$ or $(x_1, -y_1) = -P_1$. This means that either $P_1 = 2(s_0, t)$ or $P_1 = 2(-(s_0, t))$, and (s_0, t) and $-(s_0, t)$ are both in $E(\mathbb{Q})$, so $P_1 \in 2E(\mathbb{Q})$. Since P_1 was chosen arbitrarily, we find that $\ker(\mu) \subset 2E(\mathbb{Q})$.

By our previous arguments, this concludes the proof. □

We know that $E(\mathbb{Q}) \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}^r$ for some non-negative integer r. By the homomorphism theorem, we also have

$$\begin{aligned}\operatorname{Im}(\mu) &\cong E(\mathbb{Q})/\ker(\mu) \\ &= E(\mathbb{Q})/2E(\mathbb{Q}) \\ &\cong (\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}^r)/(2\mathbb{Z}/5\mathbb{Z} \times 2\mathbb{Z}^r) \\ &\cong (\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}^r)/(\mathbb{Z}/5\mathbb{Z} \times 2\mathbb{Z}^r) \\ &\cong \mathbb{Z}^r/2\mathbb{Z}^r \\ &\cong (\mathbb{Z}/2\mathbb{Z})^r.\end{aligned}$$

Henceforth, showing that $r = 0$ is equivalent to showing that the image of μ is trivial.

In what follows, we make use of the following lemma.

Lemma 7.13. *Let $(x, y) \in E(\mathbb{Q})$ be arbitrary. We can write*

$$x = \frac{r}{t^2}, \quad y = \frac{s}{t^3}$$

for some integers r, s, $t \in \mathbb{Z}$ such that $\gcd(r, t) = \gcd(s, t) = 1$.

Proof. By assumption, $x, y \in \mathbb{Q}$, so we can write

$$x = \frac{a}{b}, \quad y = \frac{c}{d}$$

for some $a, b, c, d \in \mathbb{Z}$ with $\gcd(a, b) = \gcd(c, d) = 1$. Without loss of generality, adjusting a and c if necessary, we may assume that b and d are positive. We can write

$$\begin{aligned} x^3 + k_2x^2 + k_1x + k_0 &= \frac{a^3}{b^3} + k_2\frac{a^2}{b^2} + k_1\frac{a}{b} + k_0 \\ &= \frac{a^3 + k_2a^2b + k_1ab^2 + k_0b^3}{b^3} \end{aligned}$$

and

$$y^2 = \frac{c^2}{d^2}.$$

Since (x, y) is in $E(\mathbb{Q})$, we have

$$\frac{c^2}{d^2} = \frac{a^3 + k_2a^2b + k_1ab^2 + k_0b^3}{b^3}$$

and hence

$$b^3c^2 = d^2(a^3 + k_2a^2b + k_1ab^2 + k_0b^3).$$

First, we know that d^2 divides b^3c^2. Since $\gcd(c^2, d^2) = \gcd(c, d)^2 = 1$, this implies that d^2 divides b^3.

Secondly, we know that b^3 divides $d^2(a^3 + k_2a^2b + k_1ab^2 + k_0b^3)$. Assume for contradiction that

$$\gcd(b^3, a^3 + k_2a^2b + k_1ab^2 + k_0b^3) = \delta > 1.$$

Write the prime decomposition of b

$$b = \prod_{i=1}^{m} p_i^{\alpha_i}$$

for distinct primes p_i and integer exponents $\alpha_i \geq 1$. In this notation, we can write

$$b^3 = \prod_{i=1}^{m} p_i^{3\alpha_i}.$$

Since δ divides b^3, there exist distinct $i_1, i_2, \ldots, i_u \in \{1, 2, \ldots, m\}$ and $v_1, v_2, \ldots, v_u \in \mathbb{Z}$ which satisfy the inequality $1 \leq v_j \leq 3\alpha_{i_j}$ for all $1 \leq j \leq u$ such that

$$\delta = \prod_{j=1}^{u} p_{i_j}^{v_j}.$$

Define

$$\varepsilon := \prod_{j=1}^{u} p_{i_j}.$$

We see that ϵ divides both b and δ. We assumed that $\delta > 1$, so $\epsilon > 1$ as well. Since ε divides δ, it also divides $a^3 + k_2a^2b + k_1ab^2 + k_0b^3$. Since ε divides b, this implies that it divides a^3. Since all exponents in the prime decomposition of ε are 1, this implies that ε divides a. Henceforth, ε divides $\gcd(a, b)$. However, since $\varepsilon > 1$, this contradicts with our assumption that $\gcd(a, b) = 1$. Hence, by contradiction, we get that $\gcd(b^3, a^3 + k_2a^2b + k_1ab^2 + k_0b^3) = 1$.

Therefore, we find that b^3 divides d^2. Since d^2 also divides b^3, this means that $\left|b^3\right| = \left|d^2\right|$. We assumed that b and d are both positive, so in fact $b^3 = d^2$.

Write the prime decompositions of b and d as

$$b = \prod_{i=1}^{m} p_i^{\alpha_i},$$

$$d = \prod_{j=1}^{n} q_j^{\beta_j},$$

where $p_1, p_2, \ldots, p_m$ are mutually distinct primes, $q_1, q_2, \ldots, q_n$ are mutually distinct primes, and the exponents $\alpha_i, \beta_j \geq 1$ are integers for all $1 \leq i \leq m$ and $1 \leq j \leq n$. In this notation, we have

$$\prod_{i=1}^{m} p_i^{3\alpha_i} = \prod_{j=1}^{n} q_j^{2\beta_j}.$$

Since the prime decomposition of a number is unique, this must mean that $m = n$ and the sets of primes $\{p_1, p_2, \ldots, p_m\}$ and $\{q_1, q_2, \ldots, q_n\}$ are equal. Without loss of generality, we may assume $p_i = q_i$ for all $1 \leq i \leq m$. This means that $3\alpha_i = 2\beta_i$ for all $1 \leq i \leq m$. This means that all α_i are even, so we can write $\alpha_i = 2\gamma_i$ for $1 \leq i \leq m$. We can also write $\beta_i = 3\gamma_i$ for $1 \leq i \leq m$. We see that

$$b = \left(\prod_{i=1}^{m} p_i^{\gamma_i} \right)^2,$$
$$d = \left(\prod_{i=1}^{m} p_i^{\gamma_i} \right)^3.$$

Define

$$t := \prod_{i=1}^{m} p_i^{\gamma_i}.$$

We have $b = t^2$ and $d = t^3$, so

$$x = \frac{a}{t^2}, \quad y = \frac{c}{t^3}.$$

It is clear that $\gcd(a, t) = \gcd(c, t) = 1$, since $\gcd(a, t)$ divides $\gcd(a, t^2)$ which is $\gcd(a, b) = 1$ and $\gcd(c, t)$ divides $\gcd(c, t^3)$ which is $\gcd(c, d) = 1$. Hence, we can put $r := a$ and $s := c$. This concludes the proof. □

Next, we wish to show by contradiction that the image of μ is trivial. Assume for contradiction that there exists a point $(x, y) \in E(\mathbb{Q})$ such that $\mu(x, y) = (x - \theta) \mod (K^\times)^2 \neq 1 \mod (K^\times)^2$, i.e. $x - \theta$ is not a square in $(K^\times)^2$. By Lemma 7.13, we can write

$$x = \frac{r}{t^2}, \quad y = \frac{s}{t^3}$$

for some integers r, s, $t \in \mathbb{Z}$ such that $\gcd(r, t) = \gcd(s, t) = 1$. Since $\mathbb{Z} \subset K$, we can write

$$\begin{aligned}(x - \theta) \mod \left(K^\times\right)^2 &= t^2(x - \theta) \mod \left(K^\times\right)^2 \\ &= (r - t^2\theta) \mod \left(K^\times\right)^2.\end{aligned}$$

Let O_K denote the ring of integers of K. Since r and t are integers, we know $r - t^2\theta$ is an algebraic integer, so $r - t^2\theta \in O_K$. By corollary A.15, the ideal $(r - t^2\theta)O_K$ has a unique decomposition into non-zero prime ideals of O_K. Write

$$(r - t^2\theta)O_K = \prod_{j=1}^{\ell} \left(\mathfrak{p}_j'\right)^{b_j},$$

where ℓ is some positive integer, the $\mathfrak{p}_j'$ are mutually distinct non-zero prime ideals of O_K and the exponents $b_j \in \mathbb{Z}$ are positive.

We already computed that the discriminant of f is $-11 \cdot 16^2 = -2^8 \cdot 11$. Using SageMath [The23], we can compute the discriminants of O_K and O_L:

$$\operatorname{disc}(O_K) = -44 = -2^2 \cdot 11;$$
$$\operatorname{disc}(O_L) = -21296 = -2^4 \cdot 11^3.$$

We see that f, O_K and O_L have the same prime divisors with different exponents. We can use this to prove the following theorem.

Theorem 7.14. *Let K, L, O_K and O_L be as above. Let $\mathfrak{p}$ be a non-zero prime ideal of O_K. If $\mathfrak{p}$ is ramified in O_L, then $\mathfrak{p}$ divides either $2O_K$ or $11O_K$.*

Proof. Assume $\mathfrak{p}$ is a non-zero prime ideal of O_K that is ramified in O_L. We know that K is a field extension of $\mathbb{Q}$, and $O_{\mathbb{Q}} = \mathbb{Z}$. By Theorem A.18, $\mathfrak{p}$ lies over a unique prime ideal of $\mathbb{Z}$, which is of the form $p\mathbb{Z}$ for some prime number p. By Theorem A.17, this means that $\mathfrak{p}$ divides $(p\mathbb{Z})O_K = pO_K$. It is sufficient to show that p is either 2 or 11.

Since $\mathfrak{p}$ divides pO_K, we also have that $\mathfrak{p}O_L$ divides $(pO_K)O_L = pO_L$. By assumption, $\mathfrak{p}$ is ramified in O_L, so $\mathfrak{p}O_L$ is not square-free, hence pO_L is not square-free. This means that $p\mathbb{Z}$ is ramified in O_L. By Theorem A.20, this means that p divides $\operatorname{disc}(O_L)$. As we showed above, the only primes dividing the discriminant $\operatorname{disc}(O_L)$ are 2 and 11, so p must be either 2 or 11. By the arguments above, this concludes the proof. □

The following theorem provides more information about the exponents b_j in the prime ideal decomposition of $(r - t^2\theta)O_K$.

Theorem 7.15. *Let everything be as described above. If a non-zero prime ideal $\mathfrak{p}'_j$ does not divide $2O_K$ or $11O_K$ then the exponent b_j is even.*

Proof. Assume $\mathfrak{p}'_j$ is a non-zero prime ideal of O_K that does not divide $2O_K$ or $11O_K$. By Theorem 7.14, the ideal $\mathfrak{p}'_j$ is not ramified in O_L. Hence, $\mathfrak{p}'_j O_L$ is a product of distinct non-zero prime ideals in O_L.

Assume for contradiction that b_j is odd. We aim to show that this implies that every non-zero prime ideal of O_L dividing $\mathfrak{p}'_j O_L$ divides at least one of the ideals $(\theta_a - \theta_b)O_L$, where $a, b \in \{1, 2, 3\}$ are distinct.

By Lemma 7.13, we can write $x = \frac{r}{t^2}$ and $y = \frac{s}{t^3}$ for some integers r, s, $t \in \mathbb{Z}$ such that $\gcd(r, t) = 1$ and $\gcd(s, t) = 1$. Since (x, y) lies on E, and $f(x) = (x - \theta_1)(x - \theta_2)(x - \theta_3)$, we have

$$s^2 = (r - t^2\theta_1)(r - t^2\theta_2)(r - t^2\theta_3).$$

Let $\mathfrak{q}$ be a prime ideal of O_L that divides $\mathfrak{p}'_j O_L$. By Theorem A.18, $\mathfrak{q}$ only lies over the prime ideal $\mathfrak{p}'_j$ in O_K, so it does not divide $\mathfrak{p}'_k O_L$ for $k \neq j$. Since $\mathfrak{p}'_j$ is not ramified in O_L, this means that the largest power of $\mathfrak{q}$ that divides $(r - t^2\theta_1)O_L$ is $\mathfrak{q}^1$.

Since $\mathfrak{p}'_j$ divides $(r - t^2\theta_1)O_K$, $\mathfrak{q}$ divides $(r - t^2\theta_1)O_L$. Therefore, it also divides $s^2 O_L$, which is equal to $(sO_L)^2$. Consider the unique non-zero prime ideal factorization of sO_L in O_L. The square of this factorization is the unique non-zero prime ideal factorization of $(sO_L)^2$. Therefore, every non-zero prime ideal that divides $(sO_L)^2$ must occur in this factorization as an even power. In particular, $\mathfrak{q}$ occurs in the factorization of $(s^2 O_L)$ as an even power.

Since $\mathfrak{q}^2$ divides $(sO_L)^2$, but $\mathfrak{q}^2$ does not divide $(r - t^2\theta_1)O_L$, it must be true that $\mathfrak{q}$ divides $(r - t^2\theta_k)O_L$ for at least one $k \in \{2, 3\}$.

Since $\mathfrak{q}$ divides $(r - t^2\theta_1)O_L$ and $(r - t^2\theta_k)O_L$, it divides $\mathfrak{h} := (r - t^2\theta_1, r - t^2\theta_k)O_L$. We have

$$\begin{aligned} -1 \cdot (r - t^2\theta_1) + 1 \cdot (r - t^2\theta_k) &= (\theta_1 - \theta_k)t^2 \in \mathfrak{h}; \\ -\theta_k \cdot (r - t^2\theta_1) + \theta_1 \cdot (r - t^2\theta_k) &= (\theta_1 - \theta_k)r \in \mathfrak{h}. \end{aligned}$$

Since $\gcd(r, t) = 1$, we have $\gcd(r, t^2) = 1$. Therefore, we can use Bézout's theorem to conclude that there exist integers u, v such that $u \cdot r + v \cdot t^2 = 1$. Henceforth,

$$u \cdot (\theta_1 - \theta_k)r + v \cdot (\theta_1 - \theta_k)t^2 = (\theta_1 - \theta_k) \in \mathfrak{h}.$$

By Theorem A.12, $\mathfrak{h}$ divides the ideal $(\theta_1 - \theta_k)O_L$. Since $\mathfrak{q}$ divides $\mathfrak{h}$, it also divides $(\theta_1 - \theta_k)O_L$. Since the ideal $\mathfrak{q}$ was chosen arbitrarily, this means that every non-zero prime ideal of O_L that divides $\mathfrak{p}'_j O_L$ divides at least one of the ideals $(\theta_1 - \theta_2)O_L$ and $(\theta_1 - \theta_3)O_L$.

By Theorem 7.10, we can write

$$\operatorname{disc}(f) = (\theta_1 - \theta_2)^2(\theta_1 - \theta_3)^2(\theta_2 - \theta_3)^2.$$

Since each prime ideal divisor of $\mathfrak{p}'_j O_L$ divides at least one of the ideals $(\theta_1 - \theta_2)O_L$ and $(\theta_1 - \theta_3)O_L$, we have that $\mathfrak{p}'_j O_L$ divides $\operatorname{disc}(f)O_L$. We found that $\operatorname{disc}(f) = -2^8 \cdot 11$. By Theorem A.18, there is a unique prime number p such that $\mathfrak{p}'_j O_K$ divides pO_K. Therefore, also $\mathfrak{p}'_j O_L \mid pO_L$.

By assumption, p is not equal to 2 or 11. Since p is a prime number, we know $\gcd(p, -2^8 \cdot 11) = 1$. By Bézout's theorem, there exist integers u and v such that $u \cdot p + v \cdot (-2^8 \cdot 11) = 1$. Since u and v are in O_L

as well, we know that $1 \in pO_L + (-2^8 \cdot 11)O_L$ and hence $pO_L + (-2^8 \cdot 11)O_L = O_L$. Since $\mathfrak{p}_j' O_L$ divides both pO_L and $(-2^8 \cdot 11)O_L$, it also divides $pO_L + (-2^8 \cdot 11)O_L = O_L$. This means that $\mathfrak{p}_j' O_L = O_L$.

By Theorem A.18, there is a non-zero prime ideal Q of O_L which lies over $\mathfrak{p}_j' O_K$. By Theorem A.17, this means that Q divides $\mathfrak{p}_j' O_L = O_L$., so $Q = O_L$.

Theorem A.17 also implies that $\mathfrak{p}_j' O_K = Q \cap O_K = O_L \cap O_K = O_K$. However, this contradicts the assumption that $\mathfrak{p}_j'$ does not divide $2O_K$ or $11O_K$, as O_K divides both. Hence, by contradiction, b_j can not be odd, so it must be even. This concludes the proof. □

As a consequence of Theorem 7.15, the only non-zero prime ideals of O_K that that could divide the ideal $(r - t^2\theta)O_K$ and have an odd exponent in its decomposition are the primes that divide $2O_K$ or $11O_K$. Therefore, we can write

$$(r - t^2\theta)O_K = \left(\prod_{i=1}^{k} \mathfrak{p}_i^{a_i}\right) \mathfrak{A}^2,$$

where k is some positive integer, the $\mathfrak{p}_i$ are mutually distinct non-zero prime ideals of O_K dividing $2O_K$ or $11O_K$, exponents $a_i \in \{0, 1\}$ for all i, and $\mathfrak{A}$ is an ideal of O_K. We use the convention $\mathfrak{p}^0 = O_K$ for any ideal $\mathfrak{p}$ of O_K.

We need to know the prime ideal decomposition of $2O_K$ and $11O_K$. Recall that $\{1, \theta/2, \theta^2/4\}$ is an integral basis for K. This means that $O_K = \mathbb{Z}[\theta/2]$, so O_K is monogenic. Therefore, we can use Theorem A.16.

The minimal polynomial of $\theta/2$ can be found by a direct computation. We have

$$\begin{aligned}\left(\frac{\theta}{3}\right)^2 &= \frac{\theta^3}{8} \\ &= \frac{4\theta^2 - 16}{8} \\ &= 2\left(\frac{\theta}{2}\right)^2 - 2.\end{aligned}$$

Thus, the minimal polynomial of $\theta/2$ is

$$g(x) = x^3 - 2x^2 + 2.$$

We use Theorem A.16.

We reduce $g(x)$ modulo 2. We immediately get

$$x^3 - 2x^2 + 2 \equiv x^3 \mod 2.$$

We find that

$$2O_K = ((2, \theta/2)O_K)^3.$$

Denote $\mathfrak{p} := (2, \theta/2)O_K$.

We reduce $g(x)$ modulo 11. By computing $g(x) \mod 11$ and $g'(x) \mod 11$ for $0 \leq x \leq 10$, we find that

$$x^3 - 2x^2 + 2 \equiv (x - 5)^2(x - 3) \mod 11.$$

Hence

$$11O_K = ((11, \theta/2 - 5)O_K)^2(11, \theta/2 - 3)O_K.$$

Denote $\mathfrak{q} := (11, \theta/2 - 5)O_K$ and $\mathfrak{r} := (11, \theta/2 - 3)O_K$.

So we have

$$(r - t^2\theta)O_K = \mathfrak{p}^{a_1}\mathfrak{q}^{a_2}\mathfrak{r}^{a_3}\mathfrak{A}^2$$

where $a_1, a_2, a_3 \in \{0, 1\}$.

Using Theorems A.23 and A.24, we can compute the ideal norms of $\mathfrak{p}$, $\mathfrak{q}$ and $\mathfrak{r}$.

Recall that $2O_K = \mathfrak{p}^3$. By Theorem A.23,

$$\begin{aligned}\mathrm{N}_{\mathbb{Q}}^{K}(\mathfrak{p})^3 &= \mathrm{N}_{\mathbb{Q}}^{K}\left(\mathfrak{p}^3\right)\\ &= \mathrm{N}_{\mathbb{Q}}^{K}(2O_K).\end{aligned}$$

By Theorem A.24,

$$\mathrm{N}_{\mathbb{Q}}^{K}(2O_K) = |\sigma_1(2)\sigma_2(2)\sigma_3(2)|.$$

Since $2 \in \mathbb{Q}$ and each embedding of K fixes $\mathbb{Q}$,

$$\mathrm{N}_{\mathbb{Q}}^{K}(2) = |2 \cdot 2 \cdot 2| = 8.$$

Thus,

$$\mathrm{N}_{\mathbb{Q}}^{K}(\mathfrak{p})^3 = 8.$$

Since the ideal norm of a non-zero ideal is a positive integer, we find

$$\mathrm{N}_{\mathbb{Q}}^{K}(\mathfrak{p}) = 2.$$

Recall that $11O_K = \mathfrak{q}^2\mathfrak{r}$. Similar to above, we have

$$\begin{aligned}\mathrm{N}_{\mathbb{Q}}^{K}(\mathfrak{q})^2\,\mathrm{N}_{\mathbb{Q}}^{K}(\mathfrak{r}) &= \mathrm{N}_{\mathbb{Q}}^{K}(\mathfrak{q}^2\mathfrak{r})\\ &= \mathrm{N}_{\mathbb{Q}}^{K}(11O_K)\\ &= |\sigma_1(11)\sigma_2(11)\sigma_3(11)|\\ &= 11^3.\end{aligned}$$

Since $\mathfrak{q}$ and $\mathfrak{r}$ are not equal to O_K, their norms are strictly greater than 1. Henceforth, we find that

$$\begin{aligned}\mathrm{N}_{\mathbb{Q}}^{K}(\mathfrak{q}) &= 11,\\ \mathrm{N}_{\mathbb{Q}}^{K}(\mathfrak{r}) &= 11.\end{aligned}$$

We can use Theorem A.24 to compute the norm of $(r - t^2\theta)O_K$.

$$\begin{aligned}\mathrm{N}_{\mathbb{Q}}^{K}\left(\left(r - t^2\theta\right)O_K\right) &= \left|\mathrm{N}_{\mathbb{Q}}^{K}(r - t^2\theta)\right|\\ &= \left|\sigma_1(r - t^2\theta)\sigma_2(r - t^2\theta)\sigma_3(r - t^2\theta)\right|\\ &= \left|(r - t^2\theta_1)(r - t^2\theta_2)(r - t^2\theta_3)\right|\\ &= \left|t^6(x - \theta_1)(x - \theta_2)(x - \theta_3)\right|\\ &= \left|t^6 f(x)\right|\\ &= \left|t^6 y^2\right|\\ &= s^2.\end{aligned}$$

We also have

$$\begin{aligned}\mathrm{N}_{\mathbb{Q}}^{K}\left(\left(r - t^2\theta\right)O_K\right) &= \mathrm{N}_{\mathbb{Q}}^{K}\left(\mathfrak{p}^{a_1}\mathfrak{q}^{a_2}\mathfrak{r}^{a_3}\mathfrak{A}^2\right)\\ &= \mathrm{N}_{\mathbb{Q}}^{K}(\mathfrak{p})^{a_1}\,\mathrm{N}_{\mathbb{Q}}^{K}(\mathfrak{q})^{a_2}\,\mathrm{N}_{\mathbb{Q}}^{K}(\mathfrak{r})^{a_3}\,\mathrm{N}_{\mathbb{Q}}^{K}(\mathfrak{A})^2\\ &= 2^{a_1} \cdot 11^{a_2+a_3} \cdot \mathrm{N}_{\mathbb{Q}}^{K}(\mathfrak{A})^2.\end{aligned}$$

Comparing these values yields the equation

$$s^2 = 2^{a_1} \cdot 11^{a_2+a_3} \cdot \mathrm{N}_{\mathbb{Q}}^{K}(\mathfrak{A})^2.$$

From this equation, it follows that the term $2^{a_1} \cdot 11^{a_2+a_3}$ must be a square. Therefore, we need $a_1 = 0$ and $a_2 = a_3$. We aim to show that a_2 and a_3 must in fact also be 0.

Lemma 7.16. *Let everything be as above. The exponents a_2 and a_3 are both equal to 0.*

Proof. We have $a_2, a_3 \in \{0, 1\}$ and $a_2 = a_3$. Thus, there are only two possibilities: either $a_2 = a_3 = 1$ or $a_2 = a_3 = 0$. Assume for contradiction that $a_2 = a_3 = 1$. This means that $\mathfrak{q}\mathfrak{r}$ divides $(r - t^2\theta)O_K$. Since $\mathfrak{q}^2\mathfrak{r} = 11O_K$, we have

$$11O_K \;\Big|\; \mathfrak{q}^2\mathfrak{r}^2 \;\Big|\; ((r - t^2\theta)O_K)^2 = (r^2 - 2rt^2\theta + t^4\theta^2)O_K.$$

This means that $r^2 - 2rt^2\theta + t^4\theta^2 \in 11O_K$, so

$$r^2 - 2rt^2\theta + t^4\theta^2 = 11p_0 + 11p_1\frac{\theta}{2} + 11p_2\frac{\theta^2}{4}$$

for some $p_0, p_1, p_2 \in \mathbb{Z}$. This implies

$$r^2 = 11p_0, \quad 4t^4 = 11p_2.$$

Since 11 is a prime number, r and t are integers and 4 and 11 are coprime, this implies

$$11 \;\Big|\; r, \quad 11 \;\Big|\; t.$$

However, this contradicts $\gcd(r, t) = 1$. Therefore, by contradiction, a_2 and a_3 must both be 0. This concludes the proof. □

Therefore, we can write

$$(r - t^2\theta)O_K = \mathfrak{A}^2$$

for some ideal $\mathfrak{A}$ of O_K. We aim to show that $\mathfrak{A}$ is a principal ideal. Then, we can write $\mathfrak{A} = AO_K$, and hence $(r - t^2\theta)O_K = A^2O_K$. We can then find a relation between $r - t^2\theta$ and A^2, which gives us equations that r and t^2 have to satisfy. From these equations, we can arrive at a contradiction.

Lemma 7.17. *Let O_K be as above. Then, O_K is a PID.*

Proof. We can compute Minkowski's bound for K. The number of complex embeddings of K is equal to the number of non-real of roots of f, which is 2. The discriminant of K is -44. The degree of K over $\mathbb{Q}$ is 3. Plugging this into (A.1), we obtain

$$\begin{aligned} M_K &= \sqrt{|-44|}\left(\frac{4}{\pi}\right)^1 \frac{3!}{3^3} \\ &= 2\sqrt{11} \cdot \frac{4}{\pi} \cdot \frac{6}{27} \\ &= \frac{\sqrt{11}}{\pi} \cdot \frac{16}{9} \approx 1.88. \end{aligned}$$

Thus, by Theorem A.27, every ideal class of K contains an ideal of norm 1. Since the only ideal of O_K that has norm 1 is O_K itself, there is only one ideal class. Hence, the class number of K is 1. By Proposition A.26, this means that every ideal of O_K is principal, so O_K is a PID. □

By Lemma 7.17, we can write

$$\mathfrak{A} = AO_K$$

for some $A \in O_K$. Therefore,

$$(r - t^2\theta)O_K = A^2O_K,$$

so

$$r - t^2\theta = u \cdot A^2$$

for some unit u of O_K. Note that u can not be a square in K, since $r - t^2\theta$ is not a square in K by assumption. Recall that every unit of O_K is of the form $\pm\eta^k$ for $\eta = 1 - \frac{\theta}{2}$ and some $k \in \mathbb{Z}$. Without loss of generality, possibly adjusting A if necessary, we may assume $u \in \{-1, \eta, -\eta\}$. By comparing the

possible values of the norm of $u \cdot A^2$ to the norm of $r - t^2\theta$, we aim to show that u must be equal to η. This then gives us equations that r and t^2 have to satisfy.

Recall that the norm of the element $r - t^2\theta$ is equal to s^2. We therefore have

$$s^2 = \mathrm{N}_{\mathbb{Q}}^K(r - t^2\theta) = \mathrm{N}_{\mathbb{Q}}^K(u \cdot A^2) = \mathrm{N}_{\mathbb{Q}}^K(u) \cdot \mathrm{N}_{\mathbb{Q}}^K(A)^2.$$

By Theorem A.5, we have $\mathrm{N}_{\mathbb{Q}}^K(A)^2 > 0$, so we need $\mathrm{N}_{\mathbb{Q}}^K(u) > 0$. We can compute the norms of -1, η and $-\eta$. We find

$$\mathrm{N}_{\mathbb{Q}}^K(-1) = (-1)^3 = -1.$$

Recall that we defined θ_2 and θ_3 in terms of θ_1 as

$$\theta_2 = \frac{4 - \theta_1 + \sqrt{-3\theta_1^2 + 8\theta_1 + 16}}{2}, \quad \theta_3 = \frac{4 - \theta_1 - \sqrt{-3\theta_1^2 + 8\theta_1 + 16}}{2}.$$

One can compute

$$\begin{aligned} \theta_2 + \theta_3 &= 4 - \theta_1; \\ \theta_2\theta_3 &= \theta_1^2 - 4\theta_1. \end{aligned}$$

We compute

$$\begin{aligned} \mathrm{N}_{\mathbb{Q}}^K(\eta) &= \prod_{i=1}^{3} \sigma_i \left(1 - \frac{\theta}{2}\right) \\ &= \left(1 - \frac{\theta_1}{2}\right)\left(1 - \frac{\theta_2}{2}\right)\left(1 - \frac{\theta_3}{2}\right) \\ &= \left(1 - \frac{\theta_1}{2}\right)\left(1 - \left(\frac{\theta_2 + \theta_3}{2}\right) + \frac{\theta_2\theta_3}{4}\right) \\ &= \left(1 - \frac{\theta_1}{2}\right)\left(1 - \frac{4 - \theta_1}{2} + \frac{\theta_1^2 - 4\theta_1}{4}\right) \\ &= \left(1 - \frac{\theta_1}{2}\right)\left(-1 - \frac{\theta_1}{2} + \frac{\theta_1^2}{4}\right) \\ &= -1 + \frac{\theta_1^2}{2} - \frac{\theta_1^3}{8} \\ &= -1 + \frac{\theta_1^2}{2} - \frac{4\theta_1^2 - 16}{8} \\ &= 1. \end{aligned}$$

It follows that

$$\mathrm{N}_{\mathbb{Q}}^K(-\eta) = \mathrm{N}_{\mathbb{Q}}^K(-1) \cdot \mathrm{N}_{\mathbb{Q}}^K(\eta) = -1.$$

We require $\mathrm{N}_{\mathbb{Q}}^K(u) > 0$, so the only option is $u = \eta$. Hence, we conclude that $r - t^2\theta = \eta \cdot A^2$ for some $A \in O_K$. By writing out this equality in terms of θ, we can obtain equations that r and t^2 have to satisfy. These equations imply that r and t must both be even, which contradicts our assumption that $\gcd(r, t) = 1$. This implies that there is no non-torsion rational point on E.

We have

$$r - t^2\theta = \eta A^2.$$

Thus,

$$\eta(r - t^2\theta) = \eta^2 A^2 = (\eta A)^2.$$

Denote

$$\eta A = p_0 + p_1\frac{\theta}{2} + p_2\frac{\theta^2}{4}.$$

We have

$$\eta(r - t^2\theta) = \left(p_0 + p_1\frac{\theta}{2} + p_2\frac{\theta^2}{4}\right)^2. \tag{7.31}$$

If we write out the left-hand side of equation (7.31), we get

$$\begin{aligned}\eta(r - t^2\theta) &= \left(1 - \frac{\theta}{2}\right)(1 - t^2\theta) \\ &= r - \left(r + 2t^2\right)\frac{\theta}{2} + 2t^2\frac{\theta^2}{4}.\end{aligned} \tag{7.32}$$

If we write out the right-hand side of equation (7.31), we get

$$\begin{aligned}\left(p_0 + p_1\frac{\theta}{2} + p_2\frac{\theta^2}{4}\right)^2 &= p_0^2 + 2p_0p_1\frac{\theta}{2} + \left(2p_0p_2 + p_1^2\right)\frac{\theta^2}{4} + p_1p_2\frac{\theta^3}{4} + p_2^2\frac{\theta^4}{16} \\ &= p_0^2 + 2p_0p_1\frac{\theta}{2} + \left(2p_0p_2 + p_1^2\right)\frac{\theta^2}{4} + p_1p_2\frac{4\theta^2 - 16}{4} + p_2^2\frac{16\theta^2 - 16\theta - 64}{16} \\ &= \left(p_0^2 - p_1p_2 - 4p_2^2\right) + \left(2p_0p_1 - 2p_2^2\right)\frac{\theta}{2} + \left(2p_0p_2 + p_1^2 + 4p_1p_2 + 4p_2^2\right)\frac{\theta^2}{4}.\end{aligned} \tag{7.33}$$

Comparing the coefficients of equations (7.32) and (7.33), we obtain the system of equations

$$\begin{cases} r = p_0^2 - 4p_1p_2 - 4p_2^2, & \text{(7.34a)} \\ -r - 2t^2 = 2p_0p_1 - 2p_2^2, & \text{(7.34b)} \\ 2t^2 = 2p_0p_2 + p_1^2 + 4p_1p_2 + 4p_2^2. & \text{(7.34c)} \end{cases}$$

Equation (7.34b) implies that r is even. Therefore equation (7.34a) implies that p_0 is even. Also, equation (7.34c) implies that p_1 must be even. Since p_0 and p_1 are even, the right-hand side of equation (7.34c) is divisible by 4. Therefore, so must the left-hand side be. Since $2t^2$ is divisible by 4, we must have that t^2 is even, so t is even. In conclusion, both r and t must be even. But this contradicts our assumption that $\gcd(r, t) = 1$.

Therefore, by contradiction, every point (x, y) on $E(\mathbb{Q})$ must satisfy $\mu(x, y) = 1 \mod (K^\times)^2$. By our previous arguments, this proves that μ has trivial image, and hence the rank of $E(\mathbb{Q})$ is 0. By Lemma 7.9, this proves the following fact.

Proposition 7.18 (Fact 3)**.** *Let E be the elliptic curve over $\mathbb{Q}$ given by*

$$y^2 = x^3 - 4x^2 + 16.$$

The group $E(\mathbb{Q})$ consists of exactly 5 distinct points.

This concludes the proof of Theorem 7.1.

Conclusion

In this paper, we covered the basic concepts of elliptic curves. We showed the group law and some results regarding the group structures of elliptic curves. One of these results was Mazur's theorem, which is a central result for this text.
We covered isomorphisms between elliptic curves that preserve the Weierstrass normal form of the equation, and defined some invariant quantities.
We found conditions for the coefficients of the equation in the Weierstrass normal form of an elliptic curve for which the curve has points of order 2 or 3. For fields of characteristic different from 2, we found that points of order 2 lie on a line, which we call the symmetry line. We found that points of order 3 are rational inflection points of the curve. We also looked at the Legendre family and the Hessian family of elliptic curves, which contain curves with a point of order 2 or 3, respectively.
We defined the Tate normal form of an equation of an elliptic curve. We showed that any elliptic curve over $\mathbb{Q}$ with a rational torsion point of order n greater than 3 is isomorphic to an elliptic curve with an equation in Tate normal form, where $(0, 0)$ has order n. We used this to classify all elliptic curves over $\mathbb{Q}$ with such a torsion point up to isomorphism. We found conditions on the parameters of the equation in Tate normal form for which the point $(0, 0)$ on the associated elliptic curve has order n. We also found families of elliptic curves where $(0, 0)$ has order n defined by a single parameter.
We defined the division polynomials. We stated that they can be used to compute multiples of a point on an elliptic curve and to find points on an elliptic curve with a particular order. We used these results to write an algorithm to find elliptic curves over $\mathbb{Q}$ with trivial torsion group. We related this to a result which states that such curves are ubiquitous.
Finally, we gave a proof of the fact that elliptic curves over $\mathbb{Q}$ can not have a rational torsion point of order 11. For this proof, we covered the basic concepts of algebraic number theory.

A Appendix: Algebraic number theory

This section is based on [Mar18]. The proofs of the results in this section are beyond the scope of this text and are omitted.

A.1 Basic concepts

Definition A.1. The following are central concepts in algebraic number theory.

- A complex number $\alpha \in \mathbb{C}$ is an algebraic integer if α is a root of some monic polynomial wit coefficients in $\mathbb{Z}$.
- The set of all algebraic integers in $\mathbb{C}$ is denoted by $\mathbb{A}$.
- A number field is a subfield of $\mathbb{C}$ which has finite degree over $\mathbb{Q}$.

Proposition A.2. *The following are central results relating to the concepts above.*

- *The set $\mathbb{A}$ is a subring of $\mathbb{C}$.*
- *The only algebraic integers in $\mathbb{Q}$ are the ordinary integers, i.e. $\mathbb{Q} \cap \mathbb{A} = \mathbb{Z}$.*
- *A number field K can always be represented as $\mathbb{Q}[\alpha]$ for some algebraic number α. If α is a root of an irreducible polynomial over $\mathbb{Q}$ of degree n, then the set $\{1, \alpha, \alpha^2, \dots, \alpha^{n-1}\}$ is a basis for $\mathbb{Q}[\alpha]$ as a vector space over $\mathbb{Q}$.*
- *Let $K = \mathbb{Q}[\alpha]$ be a number field of degree n over $\mathbb{Q}$. Then there are exactly n distinct embeddings of K into $\mathbb{C}$. Each embedding $\sigma : K \to \mathbb{C}$ is determined by the image of α under σ: each embedding maps α to one of the conjugates of α, i.e. to one of the roots of the minimal polynomial of α over $\mathbb{Q}$.*

Definition A.3 (Ring of integers)**.** Let K be a number field. Then $O_K := K \cap \mathbb{A}$ is called the ring of integers corresponding to K.

Definition A.4 (Norm of an element)**.** Let K be a number field of degree n over $\mathbb{Q}$. Let $\sigma_1, \dots, \sigma_n$ be the embeddings of K into $\mathbb{C}$. For any element α of K, we define the norm of α over $\mathbb{Q}$ to be

$$\mathrm{N}_{\mathbb{Q}}^{K}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha).$$

It is important to note that the norm is multiplicative since the embeddings are homomorphisms. In other words, for any $\alpha, \beta \in K$, we have

$$\mathrm{N}_{\mathbb{Q}}^{K}(\alpha\beta) = \mathrm{N}_{\mathbb{Q}}^{K}(\alpha) \cdot \mathrm{N}_{\mathbb{Q}}^{K}(\beta).$$

Theorem A.5. *Let K be a number field. Let α be an element of K. Then $\mathrm{N}_{\mathbb{Q}}^{K}(\alpha) \in \mathbb{Q}$.*

Definition A.6 (Discriminant of an n-tuple)**.** Let K be a number field of degree n over $\mathbb{Q}$. Let $\sigma_1, \dots, \sigma_n$ be the embeddings of K into $\mathbb{C}$. Let $\alpha_1, \dots, \alpha_n \in K$ be arbitrary. Let $[\sigma_i(\alpha_j)]$ denote the n by n matrix having $\sigma_i(\alpha_j)$ in the i-th row, j-th column. We define the discriminant of the n-tuple $(\alpha_1, \dots, \alpha_n)$ by

$$\mathrm{disc}(\alpha_1, \dots, \alpha_n) = \left(\det[\sigma_i(\alpha_j)]\right)^2.$$

Note that this definition is independent of the ordering of the σ_i and α_j because of the square.

Proposition A.7. *Let K be a number field of degree n over $\mathbb{Q}$. The discriminant has the following properties.*

- *For any $\alpha_1, \dots, \alpha_n \in K$, the discriminant $\mathrm{disc}(\alpha_1, \dots, \alpha_n)$ is a rational number.*
- *If $\alpha_1, \dots, \alpha_n \in K \cap \mathbb{A}$, i.e. all α_i are algebraic integers, then $\mathrm{disc}(\alpha_1, \dots, \alpha_n)$ is an integer.*
- *Elements $\alpha_1, \dots, \alpha_n \in K$ are linearly dependent over $\mathbb{Q}$ if and only if $\mathrm{disc}(\alpha_1, \dots, \alpha_n) = 0$.*

Theorem A.8 (Integral basis)**.** *Let K be a number field of degree n over $\mathbb{Q}$ and let O_K be the ring of integers of K. Then O_K is a free abelian group of rank n. Equivalently, there exist algebraic integers $\beta_1, \ldots, \beta_n \in O_K$ such that*

$$O_K = \beta_1\mathbb{Z} + \cdots + \beta_n\mathbb{Z}.$$

The set $\{\beta_1, \ldots, \beta_n\}$ is called an integral basis for O_K. It is a basis for O_K over $\mathbb{Z}$ and also a basis for K over $\mathbb{Q}$.

Theorem A.9 (Discriminant of a ring of integers and number field)**.** *Let K be a number field of degree n over $\mathbb{Q}$, O_K the ring of integers of K, $\{\beta_1, \ldots, \beta_n\}$ and $\{\gamma_1, \ldots, \gamma_n\}$ integral bases for O_K. Then*

$$\operatorname{disc}(\beta_1, \ldots, \beta_n) = \operatorname{disc}(\gamma_1, \ldots, \gamma_n).$$

In other words, the discriminant of an integral basis of O_K can be regarded as an invariant of O_K. We also call the discriminant of an integral basis of O_K the discriminant of O_K or the discriminant of K. We denote this by $\operatorname{disc}(O_K)$ *or* $\operatorname{disc}(K)$*, respectively. By A.7,* $\operatorname{disc}(K) \in \mathbb{Z} \setminus \{0\}$.

A.2 Dedekind domains

Definition A.10 (Dedekind domain)**.** A Dedekind domain is an integral domain R such that:

1. every ideal of R is finitely generated;
2. every non-zero prime ideal of R is a maximal ideal;
3. R is integrally closed in its field of fractions

$$K = \left\{ \frac{\alpha}{\beta} \mid \alpha, \beta \in R,\, \beta \neq 0 \right\}.$$

In other words, if $\alpha/\beta \in K$ is a root of some monic polynomial over R, then in fact $\alpha/\beta \in R$.

Theorem A.11. *Every ring of integers is a Dedekind domain.*

Theorem A.12. *Let I be a non-zero ideal in a Dedekind domain R. Let $\alpha \in I$ be a non-zero element. There exists an ideal J of R such that $IJ = \alpha R$.*

This result has some useful corollaries.

Corollary A.13. *Let A, B, C be non-zero ideals in a Dedekind domain R*

- *If $AB = AC$, then $B = C$.*
- *The ideal A divides B if and only if A contains B.*

Theorem A.14. *Every non-zero ideal in a Dedekind domain is uniquely representable as a finite product of non-zero prime ideals.*

By A.11 and A.14, we get the following result.

Corollary A.15. *Every non-zero ideal in a ring of integers is uniquely representable as a finite product of non-zero prime ideals.*

If R is a ring of integers of the form $\mathbb{Z}[\alpha]$ for some algebraic integer α, then we can find the unique factorization of ideals of the form pR with $p \in \mathbb{Z}$ a prime number using the following theorem.

Theorem A.16. *Let R be a monogenic ring of integers, i.e. $R = \mathbb{Z}[\alpha]$ for some algebraic integer α. Let f be the minimal polynomial of α over $\mathbb{Z}$. Let p be a prime number. The unique non-zero prime ideal decomposition of the ideal pR can be found using the following method.*

Reduce the polynomial f modulo p and factor the reduced polynomial as a product of irreducible polynomials modulo p. Write

$$f(x) \equiv g_1(x)^{e_1} \cdots g_m(x)^{e_m} \mod p,$$

where the g_i are mutually distinct irreducible polynomials modulo p and the e_i are positive integers.

The non-zero prime ideal decomposition of the ideal pR is

$$pR = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_m^{e_m},$$

where the e_i are the same as before and each $\mathfrak{p}_i$ is of the form

$$\mathfrak{p}_i = (p, g_i(\alpha))R.$$

A.3 Prime ideals

In this section, let K and L be number fields such that L is a field extension of K. Denote the rings of integers of K and L by O_K and O_L, respectively. The term "prime" will be used to mean "non-zero prime ideal".

Theorem A.17. *Let P be a prime of O_K and let Q be a prime of O_L. The following statements are equivalent:*

1. $Q \mid PO_L$;
2. $Q \supset PO_L$;
3. $Q \supset P$;
4. $Q \cap O_K = P$;
5. $Q \cap K = P$.

When any of the above statements holds, we say that Q lies over P and P lies under Q.

There is a correspondence between the primes of O_K and O_L.

Theorem A.18. *Every prime Q of O_L lies over a unique prime P of O_K. Every prime P of O_K lies under at least one prime Q of O_L. The primes of O_L lying over a given prime P of O_K are the ones which occur in the prime decomposition of PO_L. Hence, there are only finitely many primes of O_L which lie over P.*

Definition A.19 (Ramification)**.** Let P be a prime of O_K. Let $PO_L = Q_1^{e_1} Q_2^{e_2} \cdots Q_r^{e_r}$ be the prime decomposition of PO_L in O_L, where the Q_i are mutually distinct. We say P is ramified in O_L if any of the e_i is greater than 1.

If $K = \mathbb{Q}$, there is a special relation between the discriminant of O_L and the primes of O_K that are ramified in O_L.

Theorem A.20. *Let $K = \mathbb{Q}$, so $O_K = \mathbb{Z}$. A prime ideal of O_K, which is always of the form $p\mathbb{Z}$ for a prime number p, is ramified in O_L if and only if the prime number p divides* $\operatorname{disc}(O_L)$.

A.4 Ideal norm

Let K be a number field with ring of integers O_K. Let I be a non-zero ideal of O_K. We associate a quantity to this ideal, called the ideal norm. It is related to the quotient ring O_K/I.

Proposition A.21. *Let K, O_K and I be as above. The the quotient ring O_K/I is finite.*

Definition A.22 (Ideal norm)**.** Let K be a number field with ring of integers O_K. Let I be a non-zero ideal of O_K. The ideal norm $\mathrm{N}_{\mathbb{Q}}^{K}(I)$ is defined as

$$\mathrm{N}_{\mathbb{Q}}^{K}(I) = |O_K/I|.$$

By convention, the norm of the zero ideal is defined to be 0.

As with the norm of an element, the ideal norm is multiplicative.

Theorem A.23 (Ideal norm is multiplicative)**.** *Let K be a number field and let O_K be its ring of integers. Then for any ideals I and J in O_K,*

$$\mathrm{N}_{\mathbb{Q}}^{K}(IJ) = \mathrm{N}_{\mathbb{Q}}^{K}(I)\,\mathrm{N}_{\mathbb{Q}}^{K}(J).$$

Another useful property of the ideal norm, is that the norm of a principal ideal is related to the norm of its generator.

Theorem A.24 (Ideal norm of a principal ideal)**.** *Let K be a number field and let O_K be its ring of integers. Let $\alpha \in O_K$. For the principal ideal αO_K in O_K, we have*

$$\mathrm{N}_{\mathbb{Q}}^{K}(\alpha O_K) = |\,\mathrm{N}_{\mathbb{Q}}^{K}(\alpha)|.$$

A.5 Ideal classes

We can define an equivalence relation of ideals of a ring of integers.

Definition A.25 (Ideal classes)**.** Let K be a number field. Let O_K be the ring of integers of K. Two non-zero ideals I and J of O_K are said to be equivalent if and only if there exist $\alpha, \beta \in O_K \setminus \{0\}$ such that $\alpha I = \beta J$. This defines an equivalence relation. The equivalence classes corresponding to this relation are called ideal classes of K. The number of ideal classes is called the class number of K.

If the class number of a number field is 1, then its ring of integers is in fact a principal ideal domain [IR90].

Proposition A.26. *Let K be a number field with class number 1. Let O_K be the ring of integers of K. Every ideal of O_K is principal.*

Proof. Clearly, the zero ideal is $0 \cdot O_K$, which is principal. Let I be an arbitrary non-zero ideal of O_K. Since the class number of K is 1, I is in the same equivalence class as the ideal O_K. Hence, there exist non-zero elements α and β in O_K such that $\alpha I = \beta O_K$. This implies that $\beta \in \alpha I$, so $\beta/\alpha \in I$. We have

$$\begin{aligned}(\alpha O_K) \cdot \left(\frac{\beta}{\alpha} O_K\right) &= \beta O_K, \\ (\alpha O_K) \cdot I &= \beta O_K.\end{aligned}$$

By corollary A.13, this means that $I = \beta/\alpha O_K$, so I is principal. Since I was chosen arbitrarily, this concludes the proof. □

There exists a general formula to find the class number of a given number field, but this is beyond the scope of this text. For the purposes of this text, the following result is sufficient [Mar18].

Theorem A.27 (Minkowski's bound)**.** *Let K be a number field of degree n over $\mathbb{Q}$. Let $2s$ be the number of complex embeddings of K into $\mathbb{C}$, i.e. the number of embeddings into $\mathbb{C}$ that do not map K into $\mathbb{R}$. Every ideal class of K contains an integral ideal with ideal norm not exceeding Minkowski's bound*

$$M_K = \sqrt{|\operatorname{disc}(K)|} \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}. \tag{A.1}$$

A.6 Fundamental units

The group of units of a ring of integers has a particular structure.

Theorem A.28 (The unit theorem)**.** *Let K be a number field of degree n over $\mathbb{Q}$ with exactly r real embeddings and $2s$ complex embeddings. Let O_K be the ring of integers of K. Let U be the group of units in O_K. Then U is the direct product $W \times V$ where W is a finite cyclic group consisting of the roots of 1 in K and V is a free abelian group of rank $r + s - 1$.*

The group V as in Theorem A.28 is of the form

$$V = \left\{ u_1^{k_1} u_2^{k_2} \cdots u_{r+s-1}^{k_{r+s-1}} \mid k_i \in \mathbb{Z} \right\}$$

for some set of $r + s - 1$ units $u_1, \ldots, u_{r+s-1}$. Such a set is called a fundamental system of units in O_K. The exponents $k_1, \ldots, k_{r+s-1}$ are uniquely determined for a given member of V.

References

[BM40] G. Billing and K. Mahler. On exceptional points on cubic curves. *J. London Math. Soc. (2)*, 15:32–43, 1940.

[Cas49] J. W. S. Cassels. A note on the division values of $\wp(u)$. *Mathematical Proceedings of the Cambridge Philosophical Society*, 45(2):167–172, 1949.

[Cas91] J. W. S. Cassels. *Lectures on Elliptic Curves*. Cambridge University Press, 1991.

[GAT00] I. García, M. A. Olalla Acosta, and J. M. Tornero. Computing the rational torsion of an elliptic curve using Tate normal form, 2000.

[GJT10] E. González-Jiménez and J. M. Tornero. On the ubiquity of trivial torsion on elliptic curves. *Archiv der Mathematik*, 95(2):135–141, jun 2010.

[Hus04] D. Husemöller. *Elliptic curves*. Springer, 2nd edition, 2004.

[IR90] K. Ireland and M. Rosen. *A classical introduction to modern number theory*. Springer, 2nd edition, 1990.

[Kim03] I. Kiming. There are no points of order 11 on elliptic curves over $\mathbb{Q}$, 2003.

[Mar18] D. A. Marcus. *Number Fields*. Springer, 2nd edition, 2018.

[Maz77] B. Mazur. Modular curves and the Eisenstein ideal. *Publications Mathématiques de l'IHÉS*, 47:33–186, 1977.

[Mor22] L. J. Mordell. On the rational solutions of the indeterminate equations of the third and fourth degrees. *Proc. Camb. Phil. Soc*, 21:179–192, 1922.

[Nag28] T. Nagell. Sur les propriétés arithmétiques des cubiques planes du premier genre. *Acta Math.*, 52:93 – 126, 1928.

[Rei86] M. A. Reichert. Explicit determination of nontrivial torsion structures of elliptic curves over quadratic number fields. *Mathematics of Computation*, 46(174):637–658, 1986.

[Sut11] A. V. Sutherland. Constructing elliptic curves over finite fields with prescribed torsion. *Mathematics of Computation*, 81(278):1131–1147, aug 2011.

[The23] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 7.4)*, 2023. `http://www.sagemath.org`.

[Was08] L. C. Washington. *Elliptic curves: number theory and cryptography*. Chapman and Hall/CRC, 2nd edition, 2008.