University of Luxembourg
Faculty of Science, Technology and Medicine
Department of Mathematics

COUNTING POINTS ON ELLIPTIC CURVES OVER FINITE FIELDS

Author:
Ben Welter (022203560A)

Supervisor:
Dr. F. Baril Boudreau

Undergraduate thesis (12 ECTS) - Academic year 2024/2025

Abstract

Elliptic curves play an important role in number theory and cryptography. This report explores essential aspects of elliptic curves, such as their group structure and their torsion subgroup and isogenies - with particular emphasis on the Frobenius map. Special focus is given to Hasse's bound and division polynomials - both are an essential foundation for the study of René Schoof's algorithm described in [Sch85]. This algorithm, published in 1985, allows the computation of the number of points on an elliptic curve defined over a finite field with a significant time saving to previous approaches. This work provides a detailed analysis of this algorithm: we expand key steps which were only briefly mentioned, and even correct minor mistakes in the original document. To enhance understanding, we complement our report with detailed examples and SageMath-generated illustrations for many of the concepts covered.

Contents

Notation

These are the most used notions in this report.

- K - a field
- $\overline{K}$ - a fixed algebraic closure of a field K
- $\mathbb{N}$ - the set of non-negative integers
- $\mathbb{N}^*$ - the set of all positive integers
- $\mathbb{Z}$ - the set of all integers
- $\mathbb{Z}_{\geq\alpha}$ - the set of all integers such that every β in $\mathbb{Z}_{\geq\alpha}$ is greater or equal than α
- p - a prime number
- $q = p^r$ for p prime and $r \in \mathbb{N}^*$
- $\mathbb{F}_q$ - finite field of cardinality q
- #A - the cardinality of an arbitrary finite set A
- ϕ_q - the q^{th}-Frobenius map
- Ψ_k - the k^{th} division polynomial
- R - a commutative ring
- $R[x]$ - the polynomial ring in x over R
- $R[x_1, \ldots, x_n]$ - the polynomial ring over R in n variables, where $n \in \mathbb{N}^*$
- $\mathrm{char}(R)$ - the characteristic of a ring R
- A^* - A without 0 if A is an additive monoid
- All the code used in this article is written with SageMath [Dev24].

Remark 0.1. If R is a commutative ring with 1 and $f \in R$, then for any integer $n \geq 1$, f^n is the n^{th} fold product of f with itself.

Remark 0.2. If the field over which the elliptic curve is defined is not mentioned, then the elliptic curve is defined over $\overline{K}$.

Introduction

In this report, we tackle Schoof's algorithm. In order to do this, we have to prepare quite a lot of knowledge. This will be built up mainly in Section 1.

The main goal of Section 1 is to prove Hasse's sharp bound. To achieve this, we start by talking about the affine and projective Weierstrass equation which permits us to define the term "elliptic curve". This is followed by a discussion about points on elliptic curves and a visualization of an elliptic curve over a finite field by using SageMath [Dev24]. Having established this, we proceed with the group law on the set of points on elliptic curves, both geometrically and algebraically. Next, we briefly discuss valuation theory, which includes divisors and the Picard group. After this, we cover special maps between elliptic curves, which are called isogenies, like for example the multiplication-by-m map, which lets us define the torsion subgroup. Thereafter we talk about the Frobenius endomorphisms and prove a few properties about it. With all this knowledge, we are finally able to prove the so-called Hasse bound which puts a sharp bound on the number of points of an elliptic curve. We then move on to division polynomials which are used to compute the n^{th} torsion points. This finishes the section about elliptic curves.

The knowledge acquired from Section 1 becomes useful in Section 2 which is fully dedicated to explaining the algorithm described by Schoof in [Sch85, p. 486-490]. We begin with a brief overview of this algorithm, followed by a detailed discussion of all the steps, giving precise explanations.

Appendix A covers projective spaces. We first define what it is and then talk about homogeneous coordinates: coordinates in the projective space. Next, we examine curves, specifically in the projective plane, including the distinction between singular and non-singular curves. For completeness, in Appendix B we include several proofs of the results stated in previous sections. Appendix C contains a few arguments and reasonings that were used multiple times in the discussion of Schoof's algorithm.

1 Elliptic Curves

In this section we discuss different actions on elliptic curves. We begin by defining what are points on elliptic curves. Building on that knowledge, we present the impressive result that their set forms a group. Next, we explore different sorts of maps between elliptic curves. All this work leads to the important result that we can put an upper bound on the number of points of an elliptic curve defined over a finite field $\mathbb{F}_q$.

1.1 Weierstrass equation

An elliptic curve E over a field K is given by a *projective Weierstrass equation* that looks like the following:

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

where $a_1, \ldots, a_6 \in \overline{K}$. This is a homogeneous equation of degree 3 (see Definition A.3). We can also use affine coordinates (see Equation (A.1.1)). By Remark A.5, we substitute $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$ and then the previous equation becomes an *affine Weierstrass equation*:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1.1.1}$$

If $a_1, \ldots, a_6 \in \overline{K}$, then E is an elliptic curve over $\overline{K}$. Furthermore, E is defined over K if $a_1, \ldots, a_6 \in K$.

Remark 1.1. Let E be an elliptic curve defined over a field K satisfying (1.1.1). Then, the *invariant differential* ω (see [Sil09, p. 30] for a definition) associated to (1.1.1) is given by

$$\omega = \frac{dx}{2y + a_1x + a_3}.$$

It is shown in [Sil09, Proposition III.5.1 (p. 76)] that ω is invariant under translation.

We will now see that this Weierstrass equation (1.1.1) can be simplified depending on the value of $\mathrm{char}(K)$.

Proposition 1.1

If $\mathrm{char}(K) \neq 2$, then Equation (1.1.1) can be written as $(y')^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$, where $y' = 2(y + a_1x + a_3)$. In other words, the terms in xy disappear.

This is proven in Appendix B.

Proposition 1.2

If $\mathrm{char}(K) \notin \{2, 3\}$, we can even rewrite Equation (1.1.1) as $y^2 = x^3 + Ax + B$ with $A, B \in \overline{K}$.

This is proven in Appendix B.

An *elliptic curve* E over a field K such that $\text{char}(K) \notin \{2, 3\}$ is given by a Weierstrass equation of the form:

$$E : y^2 = x^3 + Ax + B \tag{1.1.2}$$

where $A, B \in K$.

Let us now compute the discriminant of Expression (1.1.2):

Definition 1.1: Discriminant of a polynomial of degree d

For a polynomial $f \in K[\overline{K}]$ of degree d, the *discriminant* Δ_f is defined as

$$\Delta_f = \frac{(-1)^{d(d-1)/2}}{a_d} Res_x(f, f').$$

(Check [CLO07, Chapter 3: Definition 2 (p. 162-163)] for the meaning of the notion $Res_x(f, f')$)

Proposition 1.3

The discriminant of the polynomial $f(x) = x^3 + Ax + B$ becomes $\Delta_f = -(4A^3 + 27B^2)$.

Proof. See Appendix B. □

Remark 1.2. Silverman [Sil09, (p. 45)] states that the *discriminant* of $f(x) = x^3 + Ax + B$ is $\Delta_f = -16 \times (4A^3 + 27B^2)$. From now on, we will use Silverman's version of the discriminant.

Proposition 1.4: [Sil09, Proposition III.1.4(i) (p. 45)]

E singular (in the sense of Definition A.5) $\iff \Delta_f = 0$

Proof. We need to prove both implications

$\boxed{\implies}$ Let us suppose that E is singular. Then, there exists a singular point $P = (x_0, y_0)$ of E. This means, in light of (1.1.2), that

$$\begin{cases} f(x_0, y_0) = y_0^2 - x_0^3 - ax_0 - b = 0 & (1) \\ \frac{\partial f}{\partial x}(x_0, y_0) = -3x_0^2 - a = 0 & (2) \\ \frac{\partial f}{\partial y}(x_0, y_0) = 2y_0 = 0 & (3) \end{cases}$$

(2) $\implies a = -3x_0^2$ (2')

(2') in (1): $y_0^2 - x_0^3 + 3x_0^3 - b = 0 \iff y_0^2 + 2x_0^3 - b = 0$

(3′) in (1) $\implies 2x_0^3 = b$
Now we can compute the discriminant which concludes the proof. We have

$$\begin{aligned}\Delta &= -16(4A^3 + 27B^2) \\ &= -16\left(4(-3x_0^2)^3 + 27(2x_0^3)^2\right) \\ &= -16\left(-4 \cdot 27x_0^6 + 27 \cdot 4x_0^6\right) \\ &= 0.\end{aligned}$$

$\boxed{\Longleftarrow}$ Now, we suppose $\Delta = 0$. This is only true if $x^3 + Ax + B$ has a double root α. We also know that a root α of a polynomial $P(x)$ is double if and only if $P(x) = 0$ and $P'(x) = 0$ (see [Bar03, p. 16-17]).

$$\begin{aligned}f(\alpha, 0) &= 0^2 - (\alpha^3 + A\alpha + B) = 0, \\ \frac{\partial f}{\partial x}(\alpha, 0) &= -(3\alpha^2 + A) = 0, \\ \frac{\partial f}{\partial y}(\alpha, 0) &= 2 \times 0 = 0.\end{aligned}$$

This point $A = (\alpha, 0)$ verifies the definition of a singular point of E. □

We now show a few examples of what plane curves satisfying a Weierstrass equation can look like over the reals $\mathbb{R}$.

Example 1.1. Define the curves

(a) $y^2 = f_a(x)$, where $f_a = x^3 + x + 4$,

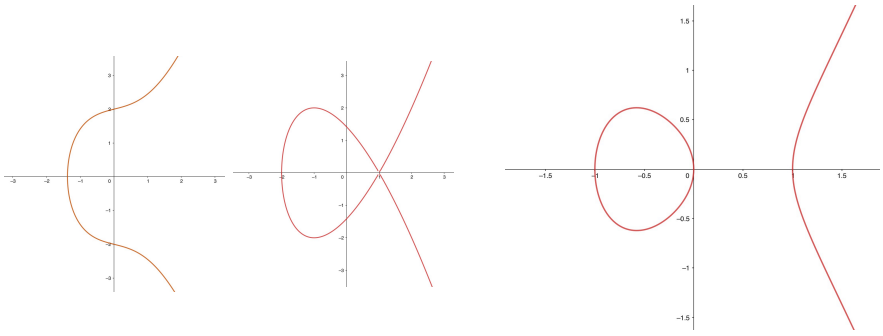
(b) $y^2 = f_b(x)$, where $f_b = x^3 - 3x + 2$,

(c) $y^2 = f_c(x)$, where $f_c = x^3 - x$.

To verify if the curves are singular or not, we compute the discriminants using Remark 1.2.

- $\Delta_{f_a} = -16 \times (4 + 27 \times 4^2) \neq 0$,
- $\Delta_{f_b} = -16 \times (4 \times (-3)^2 + 27 \times 2^2) = 0$,
- $\Delta_{f_c} = -16 \times (4 \times (-1)^3 + 27 \times 0) = 64$.

In conclusion, curves (a) and (c) are elliptic curves, and curve (b) is singular.



(a) $y^2 = x^3 + x + 4$ (b) $y^2 = x^3 - 3x + 2$ (c) $y^2 = x^3 - x$

Figure 1: Depiction of (part of) different plane curves (a), (b), (c).

1.2 Points on elliptic curves

In order to define the group law on the set of points of an elliptic curve, we first need to learn about its points.

Proposition 1.5: [Sil09, included in Proposition III.1.4.(i) (p. 45-46)]

The point $\mathcal{O} = [0 : 1 : 0]$ belongs to any elliptic curve defined by the projective Weierstrass equation: $F(X, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$. In particular it is non-singular. We denote $C : F(X; Y; Z) = 0$.

Proof. We have $\mathcal{O} \in C$ because

$$F(0, 1, 0) = 1^2 \cdot 0 + a_1 \cdot 0 \cdot 1 \cdot 0 + a_3 \cdot 1 \cdot 0^2 - 0^3 - a_2 \cdot 0^2 \cdot 0 - a_4 \cdot 0 \cdot 0^2 - a_6 \cdot 0^3 = 0.$$

Furthermore, $\mathcal{O}$ is nonsingular because

$$\frac{\partial F}{\partial Z}(X, Y, Z) = Y^2 + a_1XY + 2a_3YZ - a_2X^2 - 2a_4XZ - 3a_6Z^2 \implies \frac{\partial F}{\partial Z}(\mathcal{O}) = 1.$$

Since $\frac{\partial F}{\partial Z}(\mathcal{O}) \neq 0$, we conclude that $\mathcal{O}$ is a nonsingular point of C. □

Definition 1.2: K-Rational Points on an elliptic curve

Let K be a field, and let E be an elliptic curve on K. We denote $E(K)$ as the set of *K-rational points* on the elliptic curve E by which we mean

$$E(K) = \{(x, y) \in K \times K \mid y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\},$$

where $\mathcal{O} = [0 : 1 : 0]$ is a point at infinity (in the sense of Definition A.2).

Remark 1.3. What we are doing in Definition 1.2 is an abuse of notation because we mixes affine coordinates (x, y) with the projective point $\mathcal{O}$. In [Sil09, Remark 2.7 (p.10)], the author clarifies that it is common to describe a projective variety by its affine equations, with the understanding that the projective closure is intended. This is why we can write the affine equation $y^2 = x^3 + Ax + B$ and include $\mathcal{O}$ separately, even though $\mathcal{O}$ is part of the projective variety.

The following code allows us to plot an elliptic curve $E : y^2 = x^3 + Ax + B$ over a finite field $\mathbb{F}_p$ where p is prime. It also gives us $\mathbb{F}_p$-rational points on E and returns $\#E(\mathbb{F}_p)$. Explanations can be found in Example 1.2.

```
E = EllipticCurve(GF(p), [A, B])
E.plot(pointsize=30).show()
print(E.points())
print(len(E.points()))
```

Example 1.2. This example uses the previous SageMath code. We can easily calculate $E(\mathbb{F}_p)$ by hand for small prime numbers p. However, when p is large, it becomes very time consuming. We take the elliptic curve $E : y^2 = x^3 + x + 1$ over $\mathbb{F}_p$. Its discriminant equals $-2^4 \cdot 31$. We can discard 2 because we assume that $p \geq 5$. Hence $E/\mathbb{F}_p$ if and only if $p = 31$. We first consider it over $\mathbb{F}_{11}$. In SageMath, we define it like this:

```
E = EllipticCurve(GF(11), [1, 1])
```

The command `E.points()` gives us the coordinates of the points in $E(\mathbb{F}_{11})$.

$$E(\mathbb{F}_{11}) = \left\{ \begin{matrix} [0:1:0], [0:1:1], [0:10:1], [1:5:1], [8:1:1] \\ [1:6:1], [2:0:1], [3:3:1], [3:8:1], [8:9:1] \\ [4:5:1], [4:6:1], [6:5:1], [6:6:1] \end{matrix} \right\}.$$

Now, with the command `len(E.points())`, we get $\#E(\mathbb{F}_{11}) = 14$. We now define the same Weierstrass equation $y^2 = x^3 + x + 1$ over 3 other finite fields $\mathbb{F}_{23}$, $\mathbb{F}_{53}$ and $\mathbb{F}_{101}$ in SageMath. We can easily modify the program to consider this elliptic curve over other finite fields by simply changing GF(11) to GF(p) for $p \in \{23, 53, 101\}$. For example, we get that:

$$\#E(\mathbb{F}_{23}) = 28, \quad \#E(\mathbb{F}_{53}) = 58, \quad \#E(\mathbb{F}_{101}) = 105.$$

The commmand `E.plot().show()` to give us the final plot of E over the four finite fields mentioned before. They look like this:

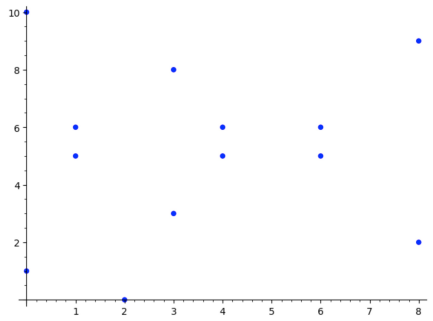


Figure 2: $E(\mathbb{F}_{11})$

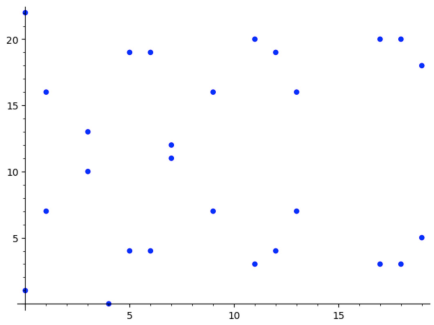


Figure 3: $E(\mathbb{F}_{23})$

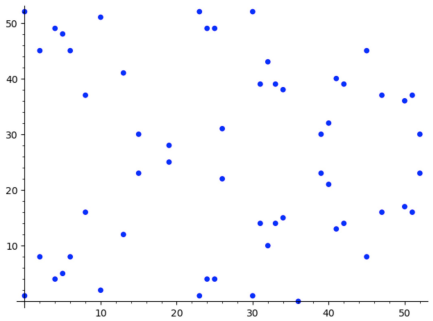


Figure 4: $E(\mathbb{F}_{53})$

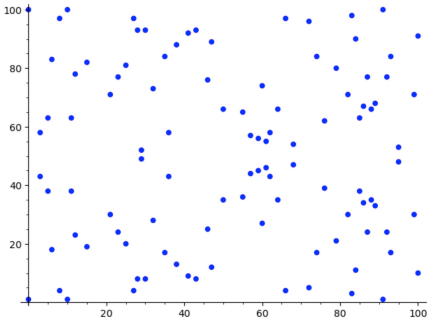


Figure 5: $E(\mathbb{F}_{101})$

Remark 1.4. By looking at Figures 2–5, we see the following.

- Note that the point at infinity is not shown in the Figures 2–5. We realize that we could add a line $y = \frac{q}{2}$ (in the sense of a real line) and we could observe a symmetry across that line. This can be explained by the fact that y^2 is quadratic. So if $(x, y) \in E(\mathbb{F}_q)$, then $(x, -y) \in E(\mathbb{F}_q)$. This results holds for any arbitrary elliptic curve.
- The following observation is specific for the elliptic curve $E : y^2 = x^3 + x + 1$. The point $P = (0, p - 1)$ lies on $E(\mathbb{F}_p)$. This is true because it always satisfies the condition:

$$\begin{aligned} (p-1)^2 &= 1 \\ p^2 - 2p + 1 &= 1 \\ p^2 - 2p &= 0 \\ 0 &\equiv 0 \pmod{p}. \end{aligned}$$

Now, we come to the **main question** of this thesis: What is $\#E(\mathbb{F}_q)$ where $q = p^n$ for p prime and $n \in \mathbb{N}^*$?

Proposition 1.6

Since there are only finitely many elements in a finite field, we can bound from the above the number of $\mathbb{F}_q$-points on an elliptic curve, $\#E(\mathbb{F}_q)$, by $2q+1$.

Proof. Let $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$. For every $x \in \mathbb{F}_q$, we get at most two possible values for y because E is quadratic in y. In total, there are q different $x \in \mathbb{F}_q$. This results in 2q possibilities. We should not forget the point at infinity $O \in E(\mathbb{F}_q)$. That is why $\#E(\mathbb{F}_q) \leq 2q+1$. □

However, a sharper bound was found by Hasse [Has36, p. 206] in 1936. More about this later. Now we are all set up to study about the group law of elliptic curves.

1.3 Group law on points of elliptic curves

A modified version of Bézout's theorem states the following:

Proposition 1.7: [Sch17, Theorem 7.11 (p. 58)]

Let E be an elliptic curve. If $P, Q \in E$ such that $P \neq Q$, then there exists a projective line L through P and Q and a third point $R \in E \cap L$.

Proof. See [Sch17, Theorem 7.11] □

Let us first start with a more geometrical explanation of the group law on the set of points of an elliptic curve. Let $E(K)$ be defined as in Definition 1.2. Now take $P, Q \in E(K)$ and define a line L through P and Q (respectively a tangent line if $P = Q$). By proposition 1.7, the line L meets $E(K)$ at exactly three points: P, Q, and we call the new intersection point R. Now we simply need to reflect the point $R = (x, y)$ across the x-axis and we get a new point $R' = (x, -y)$. We then define the operation $+$ for $P, Q \in E(K)$ as $P + Q = R'$. A picture of the geometrical situation (without worrying about the equations of the objects for the moment) can be seen in Example 1.3.

Remark 1.5. The pair $(E(K), +)$ can be seen as an abelian group with neutral element $\mathcal{O}$, which means that it satisfies the following axioms:

1. Neutral element: $\exists \mathcal{O} \in E(K)$ such that $A + \mathcal{O} = \mathcal{O} + A = A, \quad \forall A \in E(K)$
2. Inverse: $\forall A \in E(K), \exists (-A) \in E(K)$ such that $A + (-A) = (-A) + A = E$
3. Associativity: $(A + B) + C = A + (B + C), \quad \forall A, B, C \in E(K)$
4. Commutativity: $\forall A, B \in E(K), A + B = B + A$

A geometric proof of this group law can be found in [Sch17, (p. 70-84)].

Remark 1.6. Let E be an elliptic curve defined over a field K verifying Equation (1.1.2), and let $P = (x, y)$ be in $E(\overline{K})$. Then the inverse of P in Remark 1.5.2 is $-P = (x, -y)$.

We can also define algebraically the group law on an elliptic curve E.

Proposition 1.8: Addition formulas

Take an elliptic curve over a field K such that $\mathrm{char}(K)$ is not equal to 2 or 3. Let $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E(K)$ and m the slope of the line going through P_1 and P_2. Then the following hold:

(i) If $P_1 = \mathcal{O}$, then $P_1 + P_2 = P_2$.

(ii) If $P_2 = \mathcal{O}$, then $P_1 + P_2 = P_1$.

(iii) If $P_1 = -P_2$, then $P_1 + P_2 = \mathcal{O}$.

(iv) If $x_1 = x_2$ and $y_1 = y_2$ with $y_1 \neq 0$, we define $m \coloneqq \frac{3x_1^2+2ax_1+b}{2y_1}$. We denote $P_1 + P_2$ by $P_3 = (x_3, y_3)$, where $x_3 = m^2 - x_1 - x_2$ and $y_3 = -m(x_3 - x_1) - y_1$.

(v) If $P_1 \neq \pm P_2$ we define $m \coloneqq \frac{y_1-y_2}{x_1-x_2}$. We denote $P_1 + P_2$ by $P_3 = (x_3, y_3)$, where $x_3 = m^2 - x_1 - x_2$ and $y_3 = -m(x_3 - x_1) - y_1$. Then $P + Q = (m^2 - x_1 - x_2, -m(x_3 - x_1) - y_1)$.

For a proof of the group law defined on the set of points of an elliptic curve using these explicit formulas, see [Fri17, (p. 3-8)].

Example 1.3. Take $E : y^2 = x^3 + 1$ over $\mathbb{R}$. The discriminant $\Delta_f = -16 \cdot 31 \neq 0$. We see that $A = (-1, 0)$ and $B = (0, 1)$ are in $E(\mathbb{R})$. Let us calculate $A + B$. The line L going through A and B is defined by $y = x + 1$. Now we want to calculate $L \cap E$. To do this, we solve the following system:

$$\begin{cases} y = x + 1, & (1) \\ y^2 = x^3 + 1. & (2) \end{cases}$$

Replacing (1) in (2), we get

$$\begin{aligned} & (x+1)^2 = x^3 + 1 \\ \iff \quad & x^2 + 2x + 1 = x^3 + 1 \\ \iff \quad & x^3 - x^2 - 2x = 0 \\ \iff \quad & x(x^2 - x - 2) = 0 \\ \iff \quad & x(x-2)(x+1) = 0 \\ \iff \quad & x = 0 \text{ or } x = 2 \text{ or } x = -1. \end{aligned}$$

We see that replacing $x = -1$ and $x = 0$ in (1) results in the points A and B, respectively. So, if $x = 2$, then $y = 2 + 1 = 3$, and $C = (2, 3)$. We can conclude

that $L \cap E = \{(-1,0),(0,1),(2,3)\}$. Now we reflect C along the x-axis and get $A+B = (2,-3)$. The situation is represented by the following picture generated in GeoGebra [Wel25].

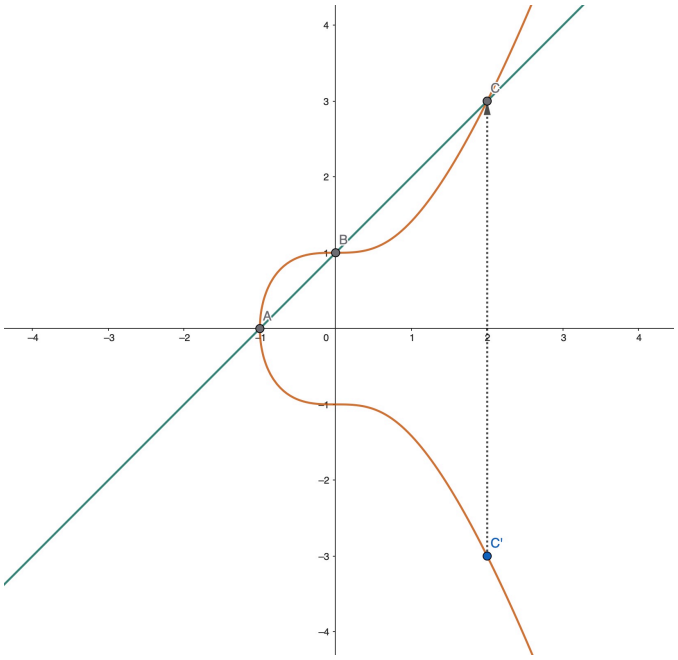


Figure 6: Illustration of the group law on the set of points of an elliptic curve

Now we will treat a special map acting on elliptic curves. (See Definition A.7 which defines maps between curves.)

1.4 Frobenius endomorphism

In this section, we will have a look at the Frobenius map acting on curves.

Definition 1.3: Frobenius map

The q^{th}-*Frobenius map* on $\mathbb{F}_q$ is defined as:

$$\begin{aligned} \phi_q : \mathbb{F}_q &\longrightarrow \mathbb{F}_q \\ x &\longmapsto x^q. \end{aligned}$$

Similarly, we can define the Frobenius map acting between two curves: We define the p^{th}-Frobenius map (for a prime p) as

$$\begin{aligned} \phi_p : C &\longrightarrow C^{(p)} \\ (x_0, x_1, \ldots, x_n) &\longmapsto (x_0^p, x_1^p, \ldots, x_n^p), \end{aligned}$$

where $(x_0, x_1, \ldots, x_n)$ are affine coordinates (see (A.1.1)), and $C^{(p)}$ is the equation of the curve C with coefficients risen to the p^{th} power. Now, the p^{th}-Frobenius map acting on an elliptic curve E over a field K is defined as

$$\begin{aligned} \phi_p : E &\longrightarrow E^{(p)} \\ (x_0, x_1) &\longmapsto (x_0^p, x_1^p) \\ \mathcal{O} &\longmapsto \mathcal{O}. \end{aligned}$$

Let E/K be the elliptic curve defined by

$$E : y^2 = x^3 + Ax + B \tag{1.4.1}$$

over K. We define the curve $E^{(p)}/K$ by the equation

$$E^{(q)}/K : y^2 = x^3 + A^p x + B^p. \tag{1.4.2}$$

We get this form by raising the coefficients of (1.4.1) to the p^{th} power Now by applying the map ϕ_p n time, we have $\phi_q := \phi_{p^n} = \phi_p \circ \phi_p \circ \cdots \circ \phi_p$ (n-times) when $q = p^n$. Then,

$$\begin{aligned} \phi_q : E &\longrightarrow E^{(q)} \\ (x_0, x_1) &\longmapsto (x_0^q, x_1^q) \\ \mathcal{O} &\longmapsto \mathcal{O}. \end{aligned}$$

Let us now consider the case $K = \mathbb{F}_q$:

Remark 1.7. If we now take $E/\mathbb{F}_q$ the elliptic curve defined by $y^2 = x^3 + Ax + B$ such that $A, B \in \mathbb{F}_q$, we get that $A^q = A$ and $B^q = B$ in $\mathbb{F}_q$ (by Euler's theorem). So, we get that the equation of $E^{(q)}/\mathbb{F}_q$ is the same as the one of $E/\mathbb{F}_q$. So, clearly $E = E^{(q)}$. Since the Frobenius map maps $E/\mathbb{F}_q$ to $E/\mathbb{F}_q$, it is actually an endomorphism and we call it Frobenius endomorphism.

Remark 1.8. ϕ_q is an isogeny of degree q by [Sil09, Proposition 2.11 (p. 25)].

Remark 1.9. ϕ_q is injective by [Was08, p. 77].

Proposition 1.9: [Was08, Theorem C.1 (p. 482)]

Let ϕ_q be the q^{th}-Frobenius map. Then the following relation is satisfied: for all $\alpha \in \overline{\mathbb{F}_q}$,

$$\alpha \in \mathbb{F}_q \iff \phi_q(\alpha) = \alpha.$$

Proof. We want to show both implications:
$\boxed{\Longrightarrow}$ Let us first show that if $\alpha \in \mathbb{F}_q$, then $\phi_q(\alpha) = \alpha$.
We know that $\mathbb{F}_q^*$ has order $q-1$. Lagrange's theorem states that every $\alpha \in \mathbb{F}_q^*$ satisfies $\alpha^{q-1} = 1$. Multiplying both sides by α now gives us $\alpha^q = \alpha$. Furthermore, if $\alpha = 0$, we have $\phi_q(0) = 0^q = 0$. So $\forall \alpha \in \mathbb{F}_q$, $\phi_q(\alpha) = \alpha$.
$\boxed{\Longleftarrow}$ Let us now show that if $\phi_q(\alpha) = \alpha$, then $\alpha \in \mathbb{F}_q$.
Let us suppose $f(x) = x^q - x \in \mathbb{F}_q[\alpha]$. Since this polynomial is of degree q, it has

at most q roots in $\mathbb{F}_q$. The derivative of this polynomial is $f'(x) = qx^{q-1} - 1 = -1$ (because $q \equiv 0 \pmod{q}$). So $f'(\alpha)$ has no roots. Hence $f(\alpha)$ does not have a common root with its derivative. So all q roots of $f(x)$ are distinct. By construction of $\mathbb{F}_q$, all elements of $\mathbb{F}_q$ satisfy $x^q = x$. Since f has exactly q distinct roots, and $\mathbb{F}_q$ provides q distinct roots of f. These must be all the roots. Therefore, if $\alpha^q = \alpha$, then α must be one of these q elements of $\mathbb{F}_q$. □

Proposition 1.10: [Was08, Lemma 4.5.2 (p. 99)]

Let $(x, y) \in E(\overline{\mathbb{F}_q})$ and let ϕ_q be the q^{th}-Frobenius map. Then

$$(x, y) \in E(\mathbb{F}_q) \iff \phi_q(x, y) = (x, y).$$

Proof. We want to show both implications:
$\boxed{\Longrightarrow}$ Let us suppose $(x, y) \in E(\mathbb{F}_q)$. Then $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$ and so $(x, y) = (x^q, y^q)$ by Proposition 1.9. Hence $\phi_q(x) = x^q = x$ and $\phi_q(y) = y$. So $\phi_q(x, y) = (x, y)$.
$\boxed{\Longleftarrow}$ Let us suppose $\phi_q(x, y) = (x, y)$. In particular, $\phi_q(x) = x$ and $\phi_q(y) = y$. This implies that $x, y \in \mathbb{F}_q$ by Proposition 1.9. So $(x, y) \in E(\mathbb{F}_q)$ because $(x, y) \in E(\overline{\mathbb{F}_q})$. □

Remark 1.10. For $f(x, y) \in \mathbb{F}_q[x, y] : f(x^q, y^q) = (f(x, y))^q$ because $\mathbb{F}_q$ is perfect and ϕ_q is a ring morphism.

1.5 Valuation theory

Definition 1.4: Divisor

Let E be an elliptic curve defined over a field K. A *divisor* D on E is a formal sum of the form

$$D = \sum_{P \in E(\overline{K})} n_P(P)$$

where

- $n_P \in \mathbb{Z}$ and only finitely many n_P are non-zero, and
- (P) is the symbol associated to each $P \in E(\overline{K})$.

Definition 1.5: Degree of a divisor

The *degree of a divisor* D on E is the integer

$$\deg(D) = \sum_{P \in E(\overline{K})} n_P.$$

Example 1.4. Take $E : y^2 = x^3 + 2x + 1$ over $\mathbb{Q}$ The discriminant $\Delta_f = -944 \neq 0$. We can verify that $P_1 = (0, 1)$ and $P_2 = (1, 2)$ are in $E(\mathbb{Q})$. Then $D = 3 \cdot (P_1) - 2 \cdot (P_2)$ is a divisor on E. Mathematically, we write $D \in Div(E)$. The degree of D is $feg(D) = 3 + (-2) = 1$.

Definition 1.6: Degree-zero Divisors

A divisor $D \in Div(E)$ with $\deg(D) = 0$ is called a *degree-zero divisor*. In that case, we write $D \in Div^0(E)$.

Example 1.5. Take the elliptic curve $E : y^2 = x^3 + 1$ over $\mathbb{Q}$. From Example 1.3, we know $\Delta_f \neq 0$. We can see that $P_1 = (-1, 0)$ and $P_2 = (0, 1) \in E(\mathbb{Q})$. Consider the divisor $D = 4 \cdot (P_1) + 2 \cdot (O) - 6 \cdot (P_2)$. Since $deg(D) = 4 + 2 + (-6) = 0$, we have $D \in Div^0(E)$

Remark 1.11. The set $Div(E)$ of all divisors on $E(\overline{K})$ is the free abelian group on the set $E(\overline{K})$

Definition 1.7: Principal Divisor

A divisor $D \in \mathrm{Div}(E)$ is called *principal* if there exists a rational function $f \in K(E)^*$ such that

$$D = \mathrm{div}(f) = \sum_{P \in E} \mathrm{ord}_P(f)(P).$$

In that case, we write $D \in \mathrm{Prin}(E)$. Here, the notation $\mathrm{ord}_P(f)$ represents the order of vanishing (or the order of poles) of a rational function f at a point P on the elliptic curve E.

Remark 1.12. Principal divisors form a subgroup $Prin(E)$ of $Div(E)$, and in fact also of $Div^0(E)$.

Now, we have all the necessary tools to define the Picard group of E.

Definition 1.8: Picard Group

The *Picard group* (also sometimes called the divisor class group) of an elliptic curve E is denoted by $Pic(E)$ and is defined as the quotient of $Div(E)$ by its subgroup $\mathrm{Prin}(E)$. We also define the Jacobian of E as the quotient group $\mathrm{Pic}^0(E) = \mathrm{Div}^0(E)/\mathrm{Prin}(E)$.

Definition 1.9: Pushforward Map

Let $\phi : E_1 \to E_2$ be a nonconstant map between two curves (see Definition A.7). We define the *pushforward map* induced by ϕ as

$$\phi_* : Pic^0(E_1) \to Pic^0(E_2)$$

$$(D) \mapsto (\phi(D)).$$

Definition 1.10: "Pullback Map"

Let $\phi : E_1 \to E_2$ be a nonconstant morphism between two curves. The *"pullback map"* induced by ϕ is a homomorphism between the Picard groups defined as follows:

$$\phi^* : \mathrm{Pic}^0(E_2) \to \mathrm{Pic}^0(E_1)$$

$$(D) \mapsto (\phi^* D)$$

where for a prime divisor $Q \in E_2$,

$$\phi^* Q = \sum_{P \in \phi^{-1}(Q)} e_\phi(P) \cdot P,$$

and $e_\phi(P)$ is the ramification index of ϕ at P.

For details and explanations of the terms used in Definitions 1.9 and 1.10, see [Sil09, p. 29-30].

1.6 Isogeny

Definition 1.11: Isogeny

Take E_1 and E_2 two elliptic curves. An *isogeny* from E_1 to E_2 is a nonconstant map $\phi : E_1 \to E_2$ satisfying $\phi(0) = 0$.

Let us now look at an example of an isogeny.

Remark 1.13. The *multiplication-by-m map* is an isogeny. It is defined as follows for $m \in \mathbb{N}$:

$$\begin{aligned} [m] : E &\longrightarrow E \\ [m](P) &\longmapsto \underbrace{P + \cdots + P}_{m \text{ times}} \\ [0](P) &\longmapsto \mathcal{O}. \end{aligned}$$

And if $m < 0$, we set $[m](P) = [-m](-P)$.

The map defined in Remark 1.13 allows us to define the torsion subgroup of an elliptic curve.

Definition 1.12: Torsion subgroup

Let E be an elliptic curve and let $m \in \mathbb{N}^*$. The *m-torsion subgroup* of E, denoted by $E[m]$, is the set of points of E of order dividing m. That means

$$E[m] \coloneqq \{P \in E \mid [m]P = \mathcal{O}\}.$$

Proposition 1.11

$E[\ell_1] \cap E[\ell_2] = \{\mathcal{O}\}$ for $\ell_1 \neq \ell_2$

Proposition 1.12: [Sil09, Theorem III.4.8 (p. 71)]

Take E_1 and E_2 two elliptic curves and let $\phi : E_1 \to E_2$ be an isogeny. Then $\phi(P_1 + P_2) = \phi(P_1) + \phi(P_2) \quad \forall P_1, P_2 \in E_1$.

Proof. See [Sil09, Theorem III.4.8]. □

Proposition 1.13: [Sil09, Theorem III.5.2 (p. 77)]

Let E_1 and E_2 be elliptic curves. Let $\phi, \Psi : E_1 \to E_2$ be isogenies and let ω be an invariant differential on E_2. Then

$$(\phi + \Psi)^*\omega = \phi^*\omega + \Psi^*\omega.$$

Proof. See [Sil09, p. 77]. □

Proposition 1.14: [Sil09, Corollary III.5.3 (p. 79)]

Let ω be an invariant differential (see Remark 1.1) on an elliptic curve E and let $m \in \mathbb{Z}$. Then $[m]^*\omega = m\omega$.

Proof. Let us prove the result by induction, starting with the base case:
For $m = 0$, the map $[0]$ is the constant map. So $[0]^*\omega = 0 = 0\omega$.
For $m = 1$, we have that $[1]$ is the identity map. So $[1]^*\omega = 1 \cdot \omega = \omega$.

- We now proceed by ascending induction. We assume the result $[m]^*\omega = m\omega$ holds for some $m \in \mathbb{N}$. Now we want to show that it holds for $m + 1$.

$$\begin{aligned} [m+1] * \omega &= [m]^*\omega + [1]^*\omega && \text{(by Proposition 1.14)} \\ &= m\omega + \omega && \text{(by induction hypothesis)} \\ &= (m+1)\omega, && \text{(factorization of } \omega) \end{aligned}$$

which concludes.

- We still need to prove the proposition for $m \leq 0$. We do this by descending induction. We now assume the result is true for some $m \leq 0$. We have

$$\begin{aligned}
[m-1]^*\omega &= [m]^*\omega + [-1]^*\omega && \text{(by Proposition 1.14)} \\
&= m\omega - \omega && \text{(by induction hypothesis)} \\
&= (m-1)\omega. && \text{(factorizing } \omega\text{)}.
\end{aligned}$$

  So the result holds for $m \leq -1$.

This proves the proposition. □

Proposition 1.15

Let ϕ_q be the q^{th}-Frobenius map. Then for $m, n \in \mathbb{Z}$, the map $m + n\phi_q : E \to F$ is separable (see Definiton A.9) if and only if $p \nmid m$.

Proof. We already know that a map $\varphi : E \to F$ is inseparable if and only if $\varphi^*\omega = 0$. Suppose $\varphi = m + n\phi$ with $m, n \in \mathbb{Z}$. Then $\phi^*\omega = (m + n\phi)^*\omega = m\omega + n\phi^*\omega$ by Propositon 1.14. We compute:

$$\begin{aligned}
\phi^*\omega &= \phi^*\left(\frac{dx}{2y + a_1x + a_3}\right) \\
&= \frac{d(x^q)}{2(y^q) + a_1x^q + a_3} \\
&= \frac{qx^{q-1}}{2(y^q) + a_1x^p + a_3} = 0
\end{aligned}$$

because $q = p^r = 0^r = 0 \pmod p$ (since p divides q). Now by replacing the result into the previous equation,

$$\varphi^*\omega = (m + n\phi)^*\omega = m\omega + n \cdot 0 = m\omega.$$

We have that $\varphi^*\omega = 0 \iff m\omega = 0 \iff p \mid m$. Therefore, φ is inseparable if and only if $p \mid m$. Rewriting this, we get φ is separable if and only if $p \nmid m$. □

Remark 1.14. **Special case for the previous proposition:** Take $m = 1$ and $n = -1$. We get the map $1 - \phi$.

$$(1 - \phi)^*\omega = \omega - \phi^*\omega = \omega - 0 = \omega.$$

Since $\omega \neq 0$, the map $1 - \phi$ is always separable.

Definition 1.13: Dual Isogeny

Let ϕ be an isogeny such that $\phi : E_1 \to E_2$. The *dual isogeny* to ϕ is the unique isogeny $\hat{\phi} : E_2 \to E_1$ such that $\hat{\phi} \circ \phi = [\deg(\phi)]$.

Here are some properties about the dual isogeny which we will use to prove the next proposition.

Properties 1.1. Let $\phi : E_1 \to E_2$ and $\Psi : E_1 \to E_2$ be isogenies.

1. We have $\hat{\phi} \circ \phi = \deg(\phi)$ on E_1.
2. We have $\widehat{\phi + \Psi} = \hat{\phi} + \hat{\Psi}$.
3. We have $[m]\hat{\phi} = \widehat{[m]}\phi, \quad \forall m \in \mathbb{Z}$.

Proof. 1. See [Sil09, Theorem III.6.2.(a) (p. 83-85)].

2. See [Sil09, Theorem III.6.2.(c) (p. 83-85)].

3. Let us prove this statement by induction. We start with the base case. We have $\widehat{[0]} = [0]$ by definition and $\widehat{[1]} = [1]$ because $[1]$ is the identity map.

   - We start by showing the statement is true for $m \geq 0$. We do this by ascending induction. We suppose it is true for $m \in \mathbb{N}$, then we show it is true for $m + 1$. We have

   $$\begin{aligned} \widehat{[m+1]}\phi &= \widehat{[m]}\phi + \widehat{[1]}\phi \quad \text{(Property 2 with } \phi = [m] \text{ and } \Psi = [1]) \\ &= [m]\hat{\phi} + [1]\hat{\phi} \quad \text{(by induction hypothesis)} \\ &= [m+1]\hat{\phi}. \end{aligned}$$

   So the equation is true for $m \geq 0$.

   - Now it remains to prove that the statement is true for $m \leq 0$. We do this by descending induction. Assume it is true for $m \leq 0$, show it is true for $m - 1$. We have

   $$\begin{aligned} \widehat{[m-1]}\phi &= \widehat{[m]}\phi - \widehat{[1]}\phi \quad \text{(Property 2 with } \phi = [m] \text{ and } \Psi = [1]) \\ &= [m]\hat{\phi} - [1]\hat{\phi} \quad \text{(by induction hypothesis)} \\ &= [m-1]\hat{\phi}. \end{aligned}$$

   So the induction is proved.

□

Theorem 1.1. Let E_1 and E_2 two elliptic curves and define the degree map:

$$\deg : Hom(E_1, E_2) \to \mathbb{Z}.$$

$$(\phi : E_1 \to E_2) \mapsto deg(\phi)$$

This map is a positive definite quadratic form.

Proof. In this proof we always take $\phi, \psi \in \mathrm{Hom}(E_1, E_1) \coloneqq End(E_1)$.
We will not prove that the degree map is positive definite. To do this, one proves that

- $deg(\phi) \geq 0 \ \forall \phi \in \mathrm{Hom}(E_1, E_2)$ and,
- $\deg(\phi) = 0 \iff \phi = 0$.

Now we continue the proof by showing that the degree map is a quadratic form, that is

- $\deg(-\phi) = \deg([-1] \circ \phi) = \deg([-1]) \cdot \deg(\phi) = \deg(\phi)$, and
- the mapping

$$\mathrm{Hom}(E_1, E_2) \times \mathrm{Hom}(E_1, E_2) \to \mathbb{R},$$
$$\langle \phi, \psi \rangle \mapsto \deg(\phi + \psi) - \deg(\phi) - \deg(\psi)$$

is bilinear.

To verify this, we use the injection $[\,] : \mathbb{Z} \to \mathrm{End}(E_1)$.

$$\begin{aligned}
\langle \phi, \psi \rangle &= \deg(\phi + \psi) - \deg(\phi) - \deg(\psi) \\
&= \widehat{(\phi + \psi)} \circ (\phi + \psi) - \hat{\phi} \circ \phi - \hat{\psi} \circ \psi && \text{(by Property 1)} \\
&= (\hat{\phi} + \hat{\psi}) \circ (\phi + \psi) - \hat{\phi} \circ \phi - \hat{\psi} \circ \psi && \text{(by Property 3)} \\
&= \hat{\phi} \circ \phi + \hat{\phi} \circ \psi + \hat{\psi} \circ \phi + \hat{\psi} \circ \psi - \hat{\phi} \circ \phi - \hat{\psi} \circ \psi \\
&= \hat{\phi} \circ \psi + \hat{\psi} \circ \phi. && (1.6.1)
\end{aligned}$$

Let us show that (1.6.1) is linear in ϕ. To do this, we need to prove the following two conditions.

- **Additive**: We get

$$\begin{aligned}
[\langle \phi_1 + \phi_2, \psi \rangle] &= \widehat{(\phi_1 + \phi_2)} \circ \psi + \widehat{(\psi)} \circ (\phi_1 + \phi_2) \\
&= \widehat{\phi_1} \circ \psi + \hat{\phi}_2 \circ \psi + \hat{\psi} \circ \phi_1 + \widehat{\psi} \circ \phi_2 \quad \text{(by property 2)} \\
&= [\langle \phi, \psi_1 \rangle] + [\langle \phi, \psi_2 \rangle].
\end{aligned}$$

- **Homogeneity**: We have

$$\begin{aligned}
[\langle n\phi, \psi \rangle] &= (n\hat{\phi}) \circ \psi + \psi \circ (n\phi) \\
&= n\hat{\phi} \circ \psi + n\psi \circ \phi \\
&= n(\hat{\phi} \circ \psi + \psi \circ \phi) \\
&= n[\langle \phi, \psi \rangle].
\end{aligned}$$

So Expression(1.6.1) is linear in ϕ.

Let us now show that (1.6.1) is linear in ψ.

– **Additive**:

$$\begin{aligned}[\langle\phi,\psi_1+\psi_2\rangle] &= \hat{\phi}\circ(\psi_1+\psi_2)+\widehat{(\psi_1+\psi_2)}\circ\phi \\ &= \hat{\phi}\circ\psi_1+\hat{\phi}\circ\psi_2+\widehat{\psi_1}\circ\phi+\widehat{\psi_2}\circ\phi \quad \text{(by Property 1)} \\ &= [\langle\phi,\psi_1\rangle]+[\langle\phi,\psi_2\rangle]\end{aligned}$$

– **Homogeneity**:

$$\begin{aligned}[\langle\phi,n\psi\rangle] &= \hat{\phi}\circ(n\psi)+(n\psi)\circ\phi \\ &= n\hat{\phi}\circ\psi+n\psi\circ\phi \\ &= n(\hat{\phi}\circ\psi+\psi\circ\phi) \\ &= n[\langle\phi,\psi\rangle]\end{aligned}$$

So (1.6.1) is linear in ψ and hence, bilinearity is verified

□

Proposition 1.16: [Sil09, Lemma V.1.2 (p. 138)]

Let G be an abelian group, let $d : G \to \mathbb{Z}$ be a positive definite quadratic form and $|\cdot|$ the usual absolute value on $\mathbb{R}$. Then,

$$|d(\psi-\phi)-d(\psi)-d(\phi)| \le 2\sqrt{d(\psi)d(\phi)} \quad \text{for all } \psi,\phi \in G. \qquad (1.6.2)$$

Proof. Let us define $L(\phi,\psi) = d(\psi-\phi)-d(\phi)-d(\psi)$. We have shown in Theorem 1.1 that this map is bilinear. If $\phi,\psi \in G$ and $m,n \in \mathbb{Z}$ then $n\phi, m\psi \in G$. Hence, $L(n\phi,m\psi) = d(m\psi-n\phi)-d(n\phi)-d(m\psi)$. Rewriting this equation, we get:

$$\begin{aligned}d(m\psi-n\phi) &= d(m\psi)+d(n\phi)+L(m\psi,n\phi) \\ &= m^2d(\psi)+n^2d(\phi)+L(m\psi,n\phi) \qquad (d \text{ is quadratic}) \\ &= m^2d(\psi)+n^2d(\phi)+mnL(\psi,\phi). \qquad (L \text{ is bilinear}) \qquad (1.6.3)\end{aligned}$$

Since d is positive definite, $d(m\psi-n\phi) \ge 0$ where the expression of $d(m\psi-n\phi)$ is given by (1.6.3). Then, we get:

$$m^2d(\psi)+n^2d(\phi)+mnL(\psi,\phi) \ge 0. \qquad (1.6.4)$$

Now, by replacing $m = -L(\psi,\phi)$ and $n = 2d(\psi)$ into (1.6.4), we get:

$$\begin{aligned}0 &\le L^2(\psi,\phi)d(\Psi)+4d^2(\psi)d(\phi)+2d(\psi)(-L(\psi,\phi))L(\psi,\phi) \\ &= \cancel{L^2(\psi,\phi)d(\psi)}+4d^2(\psi)d(\phi)-\cancel{2}L^2(\psi,\phi)d(\psi) \\ &= 4d^2(\psi)d(\phi)-L^2(\psi,\phi)d(\psi) \\ &= d(\psi)[4d(\psi)d(\phi)-L^2(\psi,\phi)]. \qquad (1.6.5)\end{aligned}$$

- If $\psi \neq 0$, then $d(\psi) > 0$ because d is positive definite. So we can divide (1.6.5) by $d(\psi)$ and we get:

$$\begin{aligned} 0 &\leq 4d(\psi)d(\phi) - L^2(\psi,\phi) \\ L^2(\psi,\phi) &\leq 4d(\psi)d(\phi) \\ |L(\psi,\phi)| &\leq 2\sqrt{d(\psi)d(\phi)} && \text{(taking square root)} \\ |d(\psi-\phi) - d(\psi) - d(\phi)| &\leq 2\sqrt{d(\psi)d(\phi)}. && \text{(replacing L)} \end{aligned}$$

- If $\psi = 0$, then $d(\psi) = 0$ because d is positive definite. Replacing $d(\psi) = 0$ into (1.6.2), it becomes:

$$\begin{aligned} &|d(0-\phi) - d(0) - d(\phi)| = |d(-\phi) - d(\phi)| = 0, \\ &2\sqrt{d(\psi)d(\phi)} = 2\sqrt{0 \times d(\phi)} = 0. \end{aligned}$$

□

Remark 1.15. The pair $(\mathrm{Hom}(E_1, E_2), +)$ is an abelian group. Furthermore, in Theorem 1.1 we have shown that the degree map $\deg\colon \mathrm{Hom}(E_1, E_2) \to \mathbb{Z}$ is a positive definite quadratic form. So, the conditions of Proposition 1.16 are verified. This gives us the following special case of Proposition 1.16:

$$|\deg(\phi - \Psi) - deg(\psi) - \deg(\phi)| \leq 2\sqrt{\deg(\psi)deg(\phi)} \quad \forall \phi, \Psi \in \mathrm{Hom}(E_1, E_2).$$

Proposition 1.17: [Sil09, Theorem III.4.10 (p. 72-73)]

Let $\phi : E_1 \to E_2$ be a non-zero isogeny. If ϕ is separable, then $\#\ker(\phi) = \deg(\phi)$.

Proof. See [Sil09, Theorem III.4.10. (p. 72-73)]. □

1.7 Hasse's bound

Proposition 1.18: [Sil09, Theorem V.1.1 (p. 138)]

If E is an elliptic curve defined over a finite field $\mathbb{F}_q$, then

$$|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}.$$

Alternatively, this means that $\#E(\mathbb{F}_q)$ is one of the integers contained in the closed interval $[-2\sqrt{q} + q + 1; 2\sqrt{q} + q + 1]$.

Proof. In Proposition 1.10, we showed that for any point $P \in E(\overline{\mathbb{F}_q})$

$$P \in E(\mathbb{F}_q) \iff \phi_q(P) = P \iff (1 - \phi_q)(P) = 0.$$

Thus, we get that $E(\mathbb{F}_q) = \ker(1-\phi_q)$. In Remark 1.14, we showed that $1-\phi_q$ is a separable map. Applying Proposition 1.17 to $1-\phi_q$ gives $\#ker(1-\phi_q) = \deg(1-\phi_q)$. Hence, Proposition 1.16 yields

$$\begin{aligned}|\#E(\mathbb{F}_q) - 1 - q| &= |\deg(1-\phi_q) - \deg(1) - \deg(\phi_q)| \\ &\leq 2\sqrt{\deg(1)\deg(q)} \\ &= 2\sqrt{1 \cdot q} \\ &= 2\sqrt{q}.\end{aligned}$$

We now get rid of the absolute value in the previous inequation:

$$\begin{aligned}& |\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q} \\ \iff \quad & -2\sqrt{q} \leq \#E(\mathbb{F}_q) - q - 1 \leq 2\sqrt{q} \\ \iff \quad & -2\sqrt{q} + q + 1 \leq \#E(\mathbb{F}_q) \leq 2\sqrt{q} + q + 1.\end{aligned}$$

Since $\#E(\mathbb{F}_q)$ is always an integer, the proof is done. □

The following code gives us a visualization of Hasse's bound depending on the cardinality of the finite field the elliptic curve is defined on. The blue lines give us the values that $\#E(\mathbb{F}_q)$ could take. Note that one can only take the integers in these blue lines.

```
from sage.all import *

def plot_hasse_weil_up_to_q(max_q=1000):
    q_values = [q for q in range(2, max_q+1) if ZZ(q).
                                        is_prime_power()]

    p = Graphics()
    p.set_axes_range(0, max_q + 1, 0, 2*max_q + 2)
    p.axes_labels(['Field size $q$', 'Number of points'])
    p.set_aspect_ratio('automatic')

    for q in q_values:
        lower = q + 1 - 2*sqrt(q)
        upper = q + 1 + 2*sqrt(q)
        p += line([(q, lower), (q, upper)], color='blue', thickness
                                            =1)
        p += point((q, lower), color='red', size=20)
        p += point((q, upper), color='red', size=20)

    q_sym = var('q')
    upper_bound = plot(q_sym + 1 + 2*sqrt(q_sym), (q_sym, 1, max_q)
                                        , color='red', linestyle='--'
                                        )
    lower_bound = plot(q_sym + 1 - 2*sqrt(q_sym), (q_sym, 1, max_q)
                                        , color='red', linestyle='--'
                                        )

    p += upper_bound
    p += lower_bound
    return p
```

```
plot_hasse_weil_up_to_q(100).show(figsize=10, axes=True, frame=True
                                  ,axes_labels=['Field size $q$','
                                  Number of points'])
```

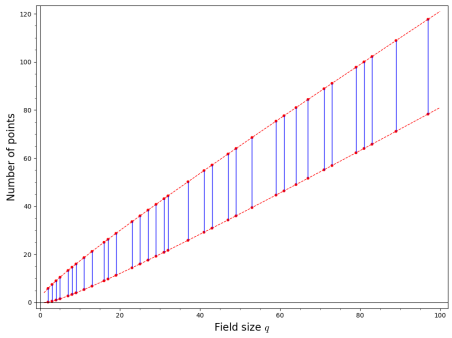


Figure 7: $q < 100$

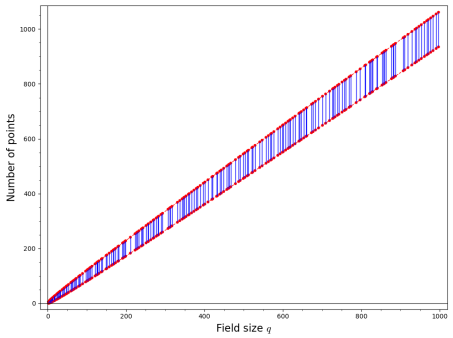


Figure 8: $q < 1000$

Example 1.6. Take the elliptic curve $E : y^2 = x^3 + 2x + 3$ over $\mathbb{F}_7$. We have that $\Delta_E = -16 \cdot (4 \cdot 2^3 + 27 \cdot 3^2) = -4400 \equiv 4 \pmod 7$. Since $\Delta_E \neq 0$, the curve is non-singular. Then Hasse's bound gives us

$$\begin{aligned} & |\#E(\mathbb{F}_7) - 1 - 7| \leq 2\sqrt{7} \\ \implies & |\#E(\mathbb{F}_7) - 8| \leq 2\sqrt{7} \\ \implies & -2\sqrt{7} \leq \#E(\mathbb{F}_7) - 8 \leq 2\sqrt{7} \\ \implies & -2\sqrt{7} + 8 \leq \#E(\mathbb{F}_7) \leq 2\sqrt{7} + 8. \end{aligned}$$

Since $\#E(\mathbb{F}_7)$ is in $\mathbb{N}$, it is an integer in the closed interval $[3, 13]$.

Let us show a naive way to compute $\#E(\mathbb{F}_q)$ for an elliptic curve $E : y^2 = x^3 + Ax + B$ over a finite field $\mathbb{F}_q$. Take $x \in \mathbb{F}_q$ and define the function

$$\chi : \mathbb{F}_q \to \{-1, 0, 1\} :$$

$$\chi(x) = \begin{cases} 1 & \text{if } x \text{ is a square in } \mathbb{F}_q^*, \\ -1 & \text{if } x \text{ is not a square in } \mathbb{F}_q^*, \\ 0 & \text{if } x = 0. \end{cases}$$

We define $\chi(P(x))$ where $P(x) = x^3 + Ax + B$. Now $\forall x \in \mathbb{F}_q^*$, we have

$$1 + \chi(P(x)) = \begin{cases} 2 & \text{if } P(x) \text{ is a square in } \mathbb{F}_q^*, \\ 1 & \text{if } P(x) = 0, \\ 0 & \text{if } P(x) \text{ is not a square in } \mathbb{F}_q^*. \end{cases}$$

For each x, this function $1 + \chi(P(x))$ gives us the amount of points with that specific x. If $P(x) = 0$, then $y = 0$ which gives us the point $(0, 0) \in E(\mathbb{F}_q)$ and

if $P(x)$ is a square, then the points (x, y) and $(x, -y)$ are in $E(\mathbb{F}_q)$ for some y in $\mathbb{F}_q$. So

$$\#E(\mathbb{F}_q) = 1 + \sum_{x \in \mathbb{F}_q} (1 + \chi(P(x))) = 1 + q + \sum_{x \in \mathbb{F}_q} \chi(P(x))$$

because $\sum_{x \in \mathbb{F}_q} 1 = \#\mathbb{F}_q = q$ and we also need to add the point at infinity $O \in E(\mathbb{F}_q)$.

Example 1.7. Let us now comeback to Example 1.6 and compute explicitly $\#E(\mathbb{F}_7)$ with the formula $\#E(\mathbb{F}_q) = 1+q+\sum_{x \in \mathbb{F}_q} \chi(P(x))$. Recall that $f(x) = x^3 + 2x + 3$ and compute $\chi(f(x))$ for all $x \in \mathbb{F}_q$.

$\chi(f(0)) = \chi(3) = -1,$
$\chi(f(1)) = \chi(6) = -1,$
$\chi(f(2)) = 8 + 4 + 3 = \chi(15) = \chi(1) = 1,$
$\chi(f(3)) = 27 + 6 + 3 = \chi(36) = \chi(1) = 1,$
$\chi(f(4)) = \chi(64 + 8 + 3) = \chi(75) = \chi(5) = -1,$
$\chi(f(5)) = \chi(125 + 10 + 3) = \chi(138) = \chi(5) = -1,$
$\chi(f(6)) = \chi(246 + 12 + 3) = \chi(231) = \chi(0) = 0.$

So, the number of points is

$$\#E(\mathbb{F}_7) = 1 + \sum_{x \in \mathbb{F}_q} (1 + \chi(f(x))) = 1 + 7 - 1 - 1 + 1 + 1 - 1 - 1 + 0 = 6.$$

2 Schoof's algorithm

This section consists in going linearly through Schoof's paper [Sch85] and explaining every step and reasoning he did in more details of his algorithm.

2.1 Division polynomials

We now introduce the division polynomials $\Psi_m(x,y) \in \mathbb{F}_q[x,y]$ for $m \in \mathbb{N}^*$. They are used to express the coordinates of the point $[n]P$ in terms of the coordinates of a point P. In the following, I write $\Psi_m(x,y) = \Psi_m$ to simplify the notation. When $\mathrm{char}(\mathbb{F}_q) \notin \{2,3\}$, these polynomials are defined as follows:

$$\begin{aligned}
\Psi_{-1} &= -1,\\
\Psi_0 &= 0,\\
\Psi_1 &= 1,\\
\Psi_2 &= 2y,\\
\Psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2,\\
\Psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3).
\end{aligned}$$

Furthermore, they satisfy the following recurrence relations

$$\forall m \geq 3, \Psi_{2m} = \Psi_m(\Psi_{m+2}\Psi_{m-1}^2 - \Psi_{m-2}\Psi_{m+1}^2)/2y, \tag{2.1.1}$$

$$\forall m \geq 2, \Psi_{2m+1} = \Psi_{m+2}\Psi_m^3 - \Psi_{m+1}^3\Psi_{m-1}. \tag{2.1.2}$$

Remark 2.1. When we forget the previous assumption that $\mathrm{char}(\mathbb{F}_q) \notin \{2,3\}$, the division polynomials can be generalized as follows:

$$\begin{aligned}
\Psi_{-1} &= -1,\\
\Psi_0 &= 0,\\
\Psi_1 &= 1,\\
\Psi_2 &= 2y + a_1x + a_3,\\
\Psi_3 &= 3x^4 + b_2x^3 + 4b_4x^2 + 3b_6x + b_8,\\
\Psi_4 &= (2y + a_1x + a_3)(2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3\\
&\qquad + 10b_8x^2 + (b_2b_8 - b_4b_6)x + b_4b_8 - b_6^2).
\end{aligned}$$

Proposition 2.1: [Sch85, Proposition 2.2 (p. 486)]

Let us take $P = (x,y) \in E(\overline{\mathbb{F}_q})$ and $n \in \mathbb{N}^*$ such that $[n]P \neq 0$. Then,

$$[n]P = \left(x - \frac{\Psi_{n-1}\Psi_{n+1}}{(\Psi_n)^2}, \frac{\Psi_{n+2}(\Psi_{n-1})^2 - \Psi_{n-2}(\Psi_{n+1})^2}{4y(\Psi_n)^3}\right).$$

Proof. See [Sch85, Proposition (2.2.) (p. 486)]. □

Example 2.1. Let us return to Example 1.2. We consider the elliptic curve $E : x^3 + x + 1$ over $\mathbb{F}_{11}$ and take the point $P = (0, 1) \in E(\overline{\mathbb{F}_{11}})$. Here the division polynomials become:

$$\begin{aligned}
\Psi_0 &= 0,\\
\Psi_1 &= 1,\\
\Psi_2 &= 2y = 2,\\
\Psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2 = 3 \cdot 0 + 6 \cdot 1 \cdot 0 + 12 \cdot 1 \cdot 0 - 1^2 = -1,\\
\Psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3)\\
&= 4 \cdot 1(0 + 5 \cdot 1 \cdot 0 + 20 \cdot 1 \cdot 0 - 5 \cdot 1^2 \cdot 0 - 4 \cdot 1 \cdot 1 \cdot 0 - 8 \cdot 1^2 - 1^3)\\
&= 4(0 + 0 + 0 - 0 - 0 - 8 - 1) = 4(-9) = -36 \equiv 8 \pmod{11}.
\end{aligned}$$

Replacing these into Proposition 2.1, we get

$$\begin{aligned}
[2]P &= \left(x - \frac{\Psi_0\Psi_2}{(\Psi_1)^2}, \frac{\Psi_3(\Psi_1)^2 - \Psi_{-1}(\Psi_2)^2}{4y(\Psi_1)^3}\right)\\
&= \left(0 - 1 \cdot 10 \cdot 2^{-2}, 9 \cdot 1 \cdot (4 \cdot 8)^{-1}\right)\\
&= \left(-10 \cdot 4^{-1}, 8 \cdot 32^{-1}\right)\\
&= (-10 \cdot 3, 8 \cdot 10)\\
&= (-30, 80)\\
&\equiv (3, 3) \pmod{11}.
\end{aligned}$$

Definition 2.1: Big $\mathcal{O}$ Notation

Let $\underline{x} \coloneqq (x_1, x_2, \cdots, x_k) \in \mathbb{R}^k$ and let f and g be functions defined on some subset of $\mathbb{R}^k$. Then we say that

$$f(\underline{x}) \text{ is } \mathcal{O}(g(\underline{x})$$

if and only if there exist C in $\mathbb{R}$ and N in $\mathbb{N}$ such that every $n_i \geq N$ and $\mid f(\underline{x}) \mid \leq \mid Cg(\underline{x}) \mid$

Proposition 2.2: [Sil09, variation of Exercise 3.7.(b) (p. 106)]

The division polynomials $\Psi_m(x, y)$, where $m \in \mathbb{N}_{\geq 3}$ can be written in the form

$$\Psi_m = \begin{cases} mx^{\frac{m^2-1}{2}} + \mathcal{O}\left(x^{\frac{m^2-1}{2}-2}\right) & \text{if } m \text{ is odd,}\\ myx^{\frac{m^2-4}{2}} + \mathcal{O}\left(yx^{\frac{m^2-4}{2}-2}\right) & \text{if } m \text{ is even.} \end{cases}$$

Proof. See Appendix B. □

Definition 2.2

Schoof defines the polynomials $f_m(x)$ such that

$$f_m = \begin{cases} \Psi'_m = mx^{\frac{m^2-1}{2}} + \mathcal{O}\left(x^{\frac{m^2-1}{2}-2}\right) & \text{if } m \text{ is odd,} \\ \Psi'_m/y = mx^{\frac{m^2-4}{2}} + \mathcal{O}\left(x^{\frac{m^2-4}{2}-2}\right) & \text{if } m \text{ is even.} \end{cases}$$

Remark 2.2. By looking at Definition 2.2, it becomes clear that

$$\deg(f_m(x)) = \begin{cases} \frac{m^2-1}{2} & \text{if } m \text{ is odd,} \\ \frac{m^2-4}{2} & \text{if } m \text{ is even.} \end{cases}$$

Proposition 2.3: Sch85, Proposition 2.1 (p. 486)]

Let $P = (x, y) \in E(\overline{\mathbb{F}_q})$ such that $P \notin E[2]$. Let $\ell \in \mathbb{Z}_{\geq -1}$. Then $f_\ell(x) = 0 \iff [\ell]P = \mathcal{O}$.

Proof. See [Sch85, p. 486]. □

Note that Proposition 2.3 helps determine the ℓ^{th} torsion point. Concluding from Definition 1.12, P is in $E[\ell]$ when $f_\ell(x) = 0$.

2.2 Summary of Schoof's algorithm

Summary 2.1. Schoof's algorithm consists of the following steps:

1. We will consider $\ell = 3, 5, 7, ..., L$ small prime numbers[†]. Then we need to find L such that $\prod_{\substack{\ell \leq L \\ \ell \neq 2,p}} \ell > 4\sqrt{q}$.[††]
2. We need to compute the Frobenius trace $t \pmod{\ell}$ for sufficiently many (small) primes ℓ.
3. Use the Chinese Remainder Theorem to conclude $t \pmod{\prod_{\substack{\ell \leq L \\ \ell \neq 2,p}} \ell}$.
4. By knowing the Frobenius trace t, we can compute $\#E(\mathbb{F}_q) = q + 1 - t$.

In the following subsections, we present a detailed analysis of the steps presented in Summary 2.1.

[†]We are choosing small prime numbers for computational reasons. Indeed, many computations in this algorithm involve the division polynomials Ψ_m (see Section 2.3). In Remark 2.2, we have discussed the degree of the polynomials f_m which are almost equal to the division polynomials. For a rather small prime $n = 19$, we have already $\deg(f_{19}(x))$=180.

[††]We know that $t = 1 + q - \#E(\mathbb{F}_q)$. By Hasse's bound in Proposition 1.18, we know that $| t | \leq 2\sqrt{q}$. So, the Frobenius trace t is in a closed interval $I = [-2\sqrt{q}, 2\sqrt{q}]$, where the length of I is $4q$.

2.3 How to compute t mod l

In this subsection, we discuss the second step of Schoof's algorithm described in Summary 2.1 [Sch85, p. 486-489].

Proposition 2.4

Let $\phi_\ell \colon T_\ell \to T_\ell$ be the map that induces on the Tate module (for an explanation of the "Tate module" and the symbol $T_\ell(E)$, see [Sil09, p.86-98]). Then, applying the Cayley-Hamilton theorem [HJ13, Theorem 2.4.3.2 (p. 109-110)] gives

$$\phi_\ell^2 - t\phi_\ell + q = 0, \tag{2.3.1}$$

where t is the Frobenius trace.

If we are now looking for $P \in E[\ell]$, Equation (2.3.1) turns into

$$\phi_\ell^2(P) + [q]P \equiv [\tau]\phi_\ell(P) \pmod{\ell}, \tag{2.3.2}$$

where $\tau \equiv t \pmod{\ell}$. We can now compute $t \pmod{\ell}$ by verifying which τ verifies (2.3.2).

Proposition 2.5

The right-hand side of (2.3.2) can be rewritten as

$$[\tau]\phi_\ell(P) = \left(x^q - \left(\frac{\Psi_{\tau-1}\Psi_{\tau+1}}{(\Psi_\tau)^2} \right)^q, \left(\frac{\Psi_{\tau+2}(\Psi_{\tau-1})^2 - \Psi_{\tau-2}(\Psi_{\tau+1})^2}{4y(\Psi_\tau)^3} \right)^q \right). \tag{2.3.3}$$

In particular, when $\tau = 0$, then (2.3.3) becomes: $[0]\phi_\ell(P) = 0$.

Proof. When $\tau = 0$, then by Remark 1.13, we get that $[0]\phi_l(P) = 0$. Furthermore, when $\tau \neq 0$, we conclude as follows. The division polynomials Ψ_k are considered as polynomials in $\mathbb{F}_q[x, y]$. Then $\Psi_k((x^q, y^q)) = (\Psi_k((x, y)))^q$ by Remark 1.7. Let us denote $[\tau]\phi_\ell(P)$ by $(X([\tau]\phi_\ell(P)), Y([\tau]\phi_\ell(P)))$ where

$$X([\tau]\phi_\ell(P)) = x^q - \frac{\Psi_{\tau-1}(x^q, y^q)\,\Psi_{\tau+1}(x^q, y^q)}{(\Psi_\tau\,(x^q, y^q))^2} = x^q - \left(\frac{\Psi_{\tau-1}(x, y)\,\Psi_{\tau+1}(x, y)}{(\Psi_\tau\,(x, y))^2} \right)^q,$$

and

$$\begin{aligned} Y([\tau]\phi_\ell(P)) &= \left(\frac{\Psi_{\tau+2}(x^q, y^q)\,(\Psi_{\tau-1}(x^q, y^q))^2 - \Psi_{\tau-2}(x^q, y^q)\,(\Psi_{\tau+1}\,(x^q, y^q))^2}{4y(\Psi_\tau(x^q, y^q))^3} \right) \\ &= \left(\frac{\Psi_{\tau+2}\,(x, y)\,(\Psi_{\tau-1}\,(x, y))^2 - \Psi_{\tau-2}\,(x, y)\,(\Psi_{\tau+1}\,(x, y))^2}{4y(\Psi_\tau\,(x, y))^3} \right)^q. \end{aligned}$$

□

For the left-hand side of (2.3.1), $[q]P$ is given by Proposition 2.1 and $\phi_\ell^2(P)$ is the q^{th}-Frobenius endomorphism ϕ_q (see Remark 1.7) applied two times to a point P. Furthermore, the term on the right-hand side of (2.3.2), $[\tau]\phi_\ell(P)$, is given by Proposition 2.5. Now that we know all these expressions for the terms in (2.3.2), we can replace them and get:

$$\begin{aligned}&(x^{q^2}; y^{q^2}) + \left(x - \frac{\Psi_{q-1}\Psi_{q+1}}{(\Psi_q)^2}, \frac{\Psi_{q+2}(\Psi_{q-1})^2 - \Psi_{q-2}(\Psi_{q+1})^2}{4y(\Psi_q)^3}\right)\\ &= \begin{cases} 0 & \text{if } r \equiv 0 \pmod{\ell}, \\ \left(x^q - \left(\frac{\Psi_{r-1}\Psi_{r+1}}{\Psi_r^2}\right)^q, \left(\frac{\Psi_{r+2}(\Psi_{r-1})^2 - \Psi_{r-2}(\Psi_{r+1})^2}{4y(\Psi_r)^3}\right)^q\right) & \text{otherwise.}\end{cases}\end{aligned} \tag{2.3.4}$$

Let P be in $E[\ell]$. Then, by Reasoning C.3, Equation (2.3.2) holds if and only if $\phi_\ell^2(P) + [k]P = r\phi_\ell(P)$ where $k \equiv q \pmod{\ell}$.

In order to solve the system (2.3.4), we will sooner or later use the addition formulas from Proposition 1.8 to compute the sum on the left side. Remember that these addition formulas distinguish the cases if the two points P_1 and P_2 that we add are the same, the opposite, or not equal at all. In order to find out if these two points are the same, or the opposite to each other, we verify

$$\phi_\ell^2(P) = \pm[k]P \tag{2.3.5}$$

where $k \equiv q \pmod{\ell}$. Let us denote $\phi_\ell^2(P)$ by $(X(\phi_\ell^2(P)), Y(\phi_\ell^2(P)))$ and $[k]P = (X([k]P), Y([k]P))$. By Reasoning C.4, Equation (2.3.5) holds if

$$X(\phi_\ell^2(P)) = X([k]P), \text{ and} \tag{2.3.6}$$

$$Y(\phi_\ell^2(P)) = \pm Y([k]P) \tag{2.3.7}$$

hold. Now since $[k]P$ is given by Propoosition 2.1 and ϕ_ℓ is given by Remark 1.7, Equation (2.3.6) becomes

$$x^{q^2} = x - \frac{\Psi_{k-1}\Psi_{k+1}}{\Psi_k}. \tag{2.3.8}$$

Equation (2.3.8) exists because the denominator does not vanish by Remark C.2.

Proposition 2.6

By rewriting (2.3.8) using f_k instead of Ψ_k, it transforms into $F_k(x) = 0$ where

$$F_k(x) = \begin{cases} (x^{q^2} - x)(x^3 + Ax + B)f_k^2(x) + f_{k-1}(x)f_{k+1}(x) & \text{if } k \text{ is even,} \\ (x^{q^2} - x)f_k^2(x) - (x^3 + Ax + B)f_{k-1}(x)f_{k+1}(x) & \text{if } k \text{ is odd.}\end{cases}$$

Proof. Since the polynomials $f_k(x)$ from Definition 2.2 depend on the parity of k, we need to consider two cases.
Let k be even (Then $k-1$ and $k+1$ are odd.)
By using the polynomials $f_k(x)$ instead of Ψ_k and choosing a common denominator in Equation (2.3.8), we obtain

$$\begin{aligned} & x^{q^2} = x - \frac{f_{k-1}(x)f_{k+1}(x)}{y^2(f_k(x))^2} \\ \iff & x - \frac{f_{k-1}(x)f_{k+1}(x)}{y^2(f_k(x))^2} - x^{q^2} = 0 \\ \iff & \frac{(x - x^{q^2})y^2(f_k(x))^2 - f_{k-1}(x)f_{k+1}(x)}{y^2(f_k(x))^2} = 0. \end{aligned}$$

Replacing $y^2 = x^3 + Ax + B$ into the previous expression gives

$$\frac{(x^{q^2} - x)(x^3 + Ax + B)(f_k(x))^2 + f_{k-1}(x)f_{k+1}(x)}{(f_k(x))^2(x^3 + Ax + B)} = 0. \tag{2.3.9}$$

Multiplying by the denominator yields

$$(x^{q^2} - x)(x^3 + Ax + B)(f_k(x))^2 + f_{k-2}(x)f_{k+2}(x) = 0.$$

This finishes the case when k is even.

Let k be odd. (Then $k-1$ and $k+1$ are even.)
Using the polynomials $f_k(x)$ instead of Ψ_k and bringing all the terms in (2.3.8) to one side gives

$$x - x^{q^2} - \frac{y^2 f_{k-1}(x)f_{k+1}(x)}{(f_k(x))^2} = 0. \tag{2.3.10}$$

Rewriting the expression (2.3.10) with a common denominator gives us:

$$\frac{(x - x^{q^2})(f_k(x))^2 - y^2 f_{k-1}(x)f_{k+1}(x)}{(f_k(x))^2} = 0. \tag{2.3.11}$$

Multiplying (2.3.11) by its denominator and replacing $y^2 = x^3 + Ax + B$, we obtain

$$(x^{q^2} - x)(f_k(x))^2 - (x^3 + Ax + B) \cdot f_{k-1}(x)f_{k+1}(x) = 0.$$

This finishes the case where k is odd. □

Now we want to compute the greatest common divisor of $F_k(x)$ (from Proposition 2.6) and $f_l(x)$ (from Definition 2.2. We will denote it by $\gcd(F_k(x), f_l(x))$.
Let $\gcd(F_k(x), f_\ell(x)) \neq 1$. Then, by Reasoning C.2, we know that there is a non-zero point $P \in E[\ell]$ satisfying (2.3.5). This is what Schoof defines as case 1 (see [Sch85, p. 488-489] and Section 2.3.1).
Let $\gcd(F_k(x), f_\ell(x)) = 1$. Then, by Reasoning C.2, there is no point $P \in E[\ell]$ such that Equation (2.3.5) is verified. Hence, we know that for each $P \in E[\ell]$, $[q]P \neq \pm\phi_\ell^2(P)$. Schoof calls this case 2 (see [Sch85, p. 489] and Section 2.3.2).

2.3.1 Case 1 [Sch85, p. 488-489]

In this case we know that there is a point $P \in E[\ell]$ such that

$$\phi_\ell^2(P) = \pm[q]P. \tag{2.3.12}$$

By working modulo ℓ, Reasoning C.3 applies and Equation (2.3.12) becomes:

$$\phi_\ell^2(P) \equiv \pm[k]P \pmod{\ell}. \tag{2.3.13}$$

Subcase 1: If $\phi_\ell^2(P) = -[q]P$ (for $P \in E[\ell]$ non-zero), we can replace this into Equation (2.3.1): $\phi_\ell^2(P) - [t]\phi_\ell(P) + [q]P = 0$ and get $[t]\phi_\ell(P) = 0$. This impies

$$[t] = 0 \text{ or } \phi_\ell(P) = 0. \tag{2.3.14}$$

Proposition 2.7

If P is non-zero, then $\phi_\ell(P) \neq 0$.

Proof. Let us suppose that $\phi_\ell(P) = 0$. Clearly, $\phi_\ell(0) = 0$. In Remark 1.9, we stated that the Frobenius endomorphism was injective. Thus $P = 0$. Contradicting that P is non-zero, $\phi_\ell(P) \neq 0$. □

In Equation (2.3.14), we can exclude the case $\phi_\ell(P) = 0$. Now there is only one possibility left in (2.3.14): $[t] = 0$, which implies that $t \equiv 0 \pmod{\ell}$.
Subcase 2: If $\phi_\ell^2(P) = [q]P$, we replace this into (2.3.1) and get:

$$[q]P - [t]\phi_\ell(P) + q[P] = 0 \tag{2.3.15}$$

$$\implies [2q]P - [t]\phi_\ell(P) = 0 \tag{2.3.16}$$

$$\implies \phi_\ell = \frac{2q}{t} \tag{2.3.17}$$

because $t \not\equiv 0 \pmod{\ell}$. Squaring Equation (2.3.17) and multiplying by t^2 yields

$$t^2\phi_\ell^2 = 4q^2. \tag{2.3.18}$$

We are in the subcase where $\phi_\ell^2(P) = [q]P$. Hence (2.3.18) becomes

$$t^2[q]P = [4q^2]P. \tag{2.3.19}$$

Since both maps in Equation (2.3.19) are applied to the same point P, they are equal. Dividing by $2q \not\equiv 0 \pmod{\ell}$ yields

$$2q = \frac{t^2}{2} \tag{2.3.20}$$

Now replacing (2.3.20) into (2.3.16), we get:

$$\begin{aligned}
&\left(\frac{t^2}{2} - t\phi_\ell\right)(P) = 0 \\
\implies &t\left(\frac{t}{2} - \phi_\ell\right)(P) = 0 \\
\implies &\left(\frac{t}{2} - \phi_\ell\right)(P) = 0 \quad \text{because } t \not\equiv 0 \pmod{\ell} \\
\implies &\left(\phi_\ell - \frac{t}{2}\right)(P) = 0.
\end{aligned}$$

We now denote by $w \in \mathbb{F}_\ell$ such that $q \equiv w^2 \pmod{\ell}$. Then (2.3.20) becomes $t^2 = 4w^2 \implies t = \pm 2w$. We now test if there is a point $P \in E[\ell]$ satisfying

$$\phi_\ell(P) = \pm[w]P. \tag{2.3.21}$$

Let us denote $\phi_\ell(P)$ by $(X(\phi_\ell(P)), Y(\phi_\ell(P)))$ and $[w]P = (X([w]P), Y([w]P))$. By Reasoning C.4, solving Equation (2.3.5) means solving

$$X(\phi_\ell(P)) = X([w]P), \text{ and} \tag{2.3.22}$$
$$Y(\phi_\ell(P)) = \pm Y([w]P). \tag{2.3.23}$$

We know the explicit form of each term of (2.3.21): the expression for $[w]P$ is given by Proposition 2.1 and $\phi_\ell(P)$ is the q^{th}-Frobenius endomorphis applied to P. Then Equation (2.3.22)

$$x^q = x - \frac{\Psi_{w-1}(x)\Psi_{w+1}(x)}{(\Psi_w(x))^2}. \tag{2.3.24}$$

Equation (2.3.24) exists because the denominator does not vanish by Remark C.2.

Proposition 2.8

Equation (2.3.24) turns into $G_k(x) = 0$ where

$$G_w(x) = \begin{cases} (x^q - x)(x^3 + Ax + B)f_w^2(x) + f_{w-1}(x)f_{w+1}(x) & \text{if } w \text{ even}, \\ (x^q - x)f_w^2(x) - (x^3 + Ax + B)f_{w-1}(x)f_{w+1}(x) & \text{if } w \text{ odd}. \end{cases}$$

when using the polynomials f_w instead of the Ψ_w's.

Proof. Since the polynomials $f_w(x)$ depend on the parity of w, we need to consider two cases: w even and w odd.

Let w be even. (Then $w - 1$ and $w + 1$ are odd.)

Then rewriting Equation (2.3.24) with f_k instead of Ψ_k yields

$$\begin{aligned} x^q &= x - \frac{f_{w-1}(x)f_{w+1}(x)}{y^2(f_w(x))^2} \\ \iff 0 &= x - \frac{f_{w-1}(x)f_{w+1}(x)}{y^2(f_w(x))^2} - x^q \\ \iff 0 &= \frac{(x-x^q)y^2(f_w(x))^2 - f_{w-1}(x)f_{w+1}(x)}{y^2(f_w(x))^2}. \end{aligned}$$

Replacing $y^2 = x^3 + Ax + B$ into the previous expression gives

$$0 = \frac{(x-x^q)(x^3+Ax+B)(f_k(x))^2 - f_{k-1}(x)f_{k+1}(x)}{y^2(f_k(x))^2}.$$

Multiplying the previous equation by its denominator, we obtain

$$(x^q - x)(x^3 + Ax + B)(f_w(x))^2 + f_{w-1}(x)f_{w+1}(x) = 0.$$

This finishes the case where w is even.

Suppose w is odd. Then $w-1$ and $w+1$ are even and rewriting Equation (2.3.24) with the polynomials f_w from Definition 2.2 gives us

$$x^q = x - \frac{(y \cdot f_{w-1}(x))(y \cdot f_{w+1}(x))}{(f_w(x))^2}.$$

Taking all terms to one side and substituting $y^2 = x^3 + Ax + B$ yields

$$(x^q - x) \cdot ((f_w(x))^2 - (x^3 + Ax + B) \cdot f_{w-1}(x)f_{w+1}(x)) = 0.$$

We multiply the previous expression by its denominator and obtain

$$(x^q - x)(f_w(x))^2 - (x^3 + Ax + B) \cdot f_{w-1}(x)f_{w+1}(x) = 0.$$

This finishes the case when w is odd and concludes the proof. □

We now want to compute $\gcd(G_k(x), f_\ell(x))$, where $f_\ell(x)$ is given by Definition 2.2.
Suppose $\gcd(F_k(x), f_\ell(x)) = 1$. Then, by Reasoning C.2, we get that there is no $P \in E[\ell]$ such that (2.3.21) is verified. Hence, we know that for each $P \in E[\ell]$, $[w]P \neq \pm\phi_\ell(P)$ is verified. Squaring this expression, we are in the case where $\phi_\ell^2(P) = \pm[q]P$. As stated in subcase 1, we now have $t \equiv 0 \pmod{\ell}$.
Let $\gcd(G_k(x), f_\ell(x)) \neq 1$. Then, by Reasoning C.2, we know that there is a non-zero point $P \in E[\ell]$ satisfying (2.3.21).
Now we know that there is $P \in E[\ell]$ such that $\phi_\ell(P) = \pm\omega P$. But we still need to determine the sign. In order to do this, we consider Equation (2.3.23), but only the part

$$Y(\phi_\ell(P)) = Y([w]P), \tag{2.3.25}$$

where $\phi_\ell(P)$ is given by Remark 1.7 and $[\omega]P$ is given by Proposition 2.1. Substituting these values into Equation (2.3.25), we obtain

$$y^q = \frac{\Psi_{w+2}(\Psi_{w-1})^2 - \Psi_{w-2}(\Psi_{w+1})^2}{4y(\Psi_w)^3}. \tag{2.3.26}$$

Equation (2.3.26) exists because the denominator does not vanish by Proposition C.1 and Remark C.2.

Proposition 2.9

Equation (2.3.26) transforms into $H_k(x) = 0$[†], where

$$H_w(x)^{\dagger\dagger} = \begin{cases} 4(x^3+Ax+B)^{\frac{q-1}{2}} f_w^3 - f_{w+2}f_{w-1}^2 + f_{w-2}f_{w+1}^2 & \text{if } w \text{ odd,} \\ 4(x^3+Ax+B)^{\frac{q+3}{2}} f_w^3 - f_{w+2}f_{w-1}^2 + f_{w-2}f_{w+1}^2 & \text{if } w \text{ even} \end{cases}$$

by using f_w instead of Ψ_w

Proof. Since f_w depend on the parity of w, we need to do two cases.

If w is odd, Equation (2.3.26) transforms into

$$y^q = \frac{f_{w+2}(yf_{w-1})^2 - f_{w-2}(yf_{w+1})^2}{4y(f_w)^3}.$$

Taking everything to one side and taking a common denominator yields

$$\frac{y^2\left[-4y^{q-1}(f_w)^3 + f_{w+2}(f_{w-1})^2 - f_{w-2}(f_{w+1})^2\right]}{4y(f_w)^3} = 0.$$

Multiplying by the denominator gives us

$$y^2(-4y^{q-1}(f_w)^3 + f_{w+2}(f_{w-1})^2 - f_{w-2}(f_{w+1})^2) = 0. \tag{2.3.27}$$

Thanks to Proposition C.1 (1), we can divide Equation (2.3.27) by y^2 and for every power of y remaining, we replace $y^2 = x^3 + Ax + B$. We obtain

$$4(x^3+Ax+B)^{\frac{q-1}{2}}(f_w)^3 - f_{w+2}(f_{w-1})^2 + f_{w-2}(f_{w+1})^2 = 0. \tag{2.3.28}$$

This concludes the proof in the odd case.

If w is even, Equation (2.3.26) becomes

$$y^q = \frac{yf_{w+2}(f_{w-1})^2 - yf_{w-2}(f_{w+1})^2}{4y(yf_w)^3}. \tag{2.3.29}$$

[†]In [Sch85, p. 489], the author mistakenly inverted the roles of even and odd.
[††]In [Sch85, p. 489], there are some of the squares missing in the author's equation (18).

As already mentioned, the denominator of Equation (2.3.29) does not vanish. Hence we multiply (2.3.29) by its denominator and get

$$4y^{q+4}(f_w)^3 - yf_{w+2}(f_{w-1})^2 + yf_{w-2}(f_{w+1})^2 = 0.$$

Thanks to Proposition C.1 (1), we can divide Equation (2.3.27) by y and for every power of y remaining, we replace $y^2 = x^3 + Ax + B$. This yields

$$\iff 4(x^3 + Ax + B)^{\frac{q+3}{2}} f_w^3 - f_{w+2}f_{w-1}^2 + f_{w-2}f_{w+1}^2 = 0.$$

This concludes the proof in the even case. □

We want to compute $\gcd(H(x), f_\ell(x))$.

Proposition 2.10

- If $gcd(H(x), f_\ell(x)) \neq 1$, then $t \equiv 2w \pmod{\ell}$.
- If $gcd(H(x), f_\ell(x)) = 1$, then $t \equiv -2w \pmod{\ell}$.

Proof. Suppose $gcd(H(x), f_\ell(x)) \neq 1$. Then, by Reasoning C.2, there exists $P \in E[\ell]$ such that $\phi_\ell(P) = [w]P$. Substituting $\phi_\ell(P) = [w]P$ into (2.3.1), we get

$$\begin{aligned}
&(\phi^2 - [t]\phi + q)P = \mathcal{O} \\
\iff &(q - [tw] + q)P = \mathcal{O} \\
\iff &(-tw + 2q)P = \mathcal{O} \\
\iff &2q = tw \\
\iff &tw = 2w^2 \\
\iff &t = 2w.
\end{aligned}$$

Suppose now that $gcd(H(x), f_\ell(x)) = 1$. Then, by Reasoning C.2 there is no point $P \in E[\ell]$ such that $\phi(P) = [w]P$. But we have seen that there is $P \in E[\ell]$ such that $\phi(P) = \pm[w]P$, hence, we must have that there is $P \in E[\ell]$ such that $\phi(P) = -[w]P$. Now by replacing this into (2.3.1), we get

$$\begin{aligned}
&(\phi^2 - t\phi + q)P = \mathcal{O} \\
\iff &(tw + 2q)P = \mathcal{O} \\
\iff &-2q = tw. \qquad (2.3.30)
\end{aligned}$$

Since we supposed $q \equiv w^2 \pmod{\ell}$, Equation (2.3.30) becomes $t = -2w$. □

2.3.2 Case 2 [Sch85, p. 489]

We now turn to case 2 of Schoof's proof [Sch85, p. 489], where $\phi_\ell^2(P) \neq \pm[q]P$. We want to compute

$$\phi_\ell^2(P) + [q](P) = \tau\phi_\ell(P). \qquad (2.3.31)$$

We start by computing the left-hand side of (2.3.31).

Proposition 2.11

If $\phi_\ell^2(P) \neq \pm[q](P)$, then

$$\begin{aligned}&\phi_\ell^2(P) + [q](P)\\ &= \left(-x^{q^2} - x + \frac{\Psi_{k-1}\Psi_{k+1}}{\Psi_k^2} + \lambda^2, -y^{q^2} - \lambda\left(-2x^{q^2} - x + \frac{\Psi_{k-1}\Psi_{k+1}}{\Psi_k^2} + \lambda^2\right)\right),\end{aligned} \tag{2.3.32}$$

where

$$\lambda = \frac{\Psi_{k+2}\Psi_{k-1}^2 - \Psi_{k-2}\Psi_{k+1}^2 - 4y^{p^2+1}\Psi_k^3}{[\Psi_k^2(x - x^{p^2}) - \Psi_{k-1}\Psi_{k+1}]4y\Psi_k}.$$

Proof. To ease the notation, we denote $\phi_\ell^2(P)$ by $(X(\phi_\ell^2(P)), Y(\phi_\ell^2(P)))$ and $[q]P$ by $(X([q]P), Y([q]P))$. Since $\phi_\ell^2(P) \neq \pm[q](P)$, we use the addition formulas in Proposition 1.8 (v). We have that $[q]P$ is defined by Proposition 2.1 and ϕ_ℓ^2 is given in Remark 1.7. Let us start by computing the slope

$$\lambda = \frac{Y([q]P) - Y(\phi_\ell^2(P))}{X([q]P) - X(\phi_\ell^2(P))}. \tag{2.3.33}$$

This slope exists because $\phi_\ell^2(P) \neq \pm[q](P)$. The numerator of (2.3.33) is

$$\begin{aligned}Y([q]P) - Y(\phi_\ell^2(P)) &= \frac{\Psi_{k+2}\Psi_{k-1}^2 - \Psi_{k-2}\Psi_{k+1}^2}{4y\Psi_k^3} - y^{q^2}\\ &= \frac{\Psi_{k+2}\Psi_{k-1}^2 - \Psi_{k-2}\Psi_{k+1}^2 - 4y^{q^2+1}\Psi_k^3}{4y\Psi_k^3}.\end{aligned}$$

The denominator of (2.3.33) becomes

$$X([q]P) - X(\phi_\ell^2(P)) = x - \frac{\Psi_{k-1}\Psi_{k+1}}{\Psi_k^2} - x^{q^2} = \frac{\Psi_k^2(x - x^{q^2}) - \Psi_{k-1}\Psi_{k+1}}{\Psi_k^2}.$$

We then substitute these two values into (2.3.33) and simplify by Ψ_k^2 to get

$$\begin{aligned}\lambda &= \frac{[\Psi_{k+2}\Psi_{k-1}^2 - \Psi_{k-2}\Psi_{k+1}^2 - 4y^{p^2+1}\Psi_k^3]\boldsymbol{\Psi_k^2}}{[\Psi_k^2(x - x^{p^2}) - \Psi_{k-1}\Psi_{k+1}]4y\boldsymbol{\Psi_k^3}}\\ &= \frac{\Psi_{k+2}\Psi_{k-1}^2 - \Psi_{k-2}\Psi_{k+1}^2 - 4y^{p^2+1}\Psi_k^3}{[\Psi_k^2(x - x^{p^2}) - \Psi_{k-1}\Psi_{k+1}]4y\Psi_k}.\end{aligned} \tag{2.3.34}$$

By the addition formulas in Proposition 1.8 (v), we get the following result[†]:

$$\begin{aligned}
&\phi_\ell^2(P) + [q](P) \\
&= \left(-x^{q^2} - x + \frac{\Psi_{k-1}\Psi_{k+1}}{\Psi_k^2} + \lambda^2, -y^{q^2} - \lambda\left(-x^{q^2} - x + \frac{\Psi_{k-1}\Psi_{k+1}}{\Psi_k^2} + \lambda^2 - x^{q^2}\right)\right) \\
&= \left(-x^{q^2} - x + \frac{\Psi_{k-1}\Psi_{k+1}}{\Psi_k^2} + \lambda^2, -y^{q^2} - \lambda\left(-2x^{q^2} - x + \frac{\Psi_{k-1}\Psi_{k+1}}{\Psi_k^2} + \lambda^2\right)\right).
\end{aligned}$$

□

The λ we defined in Equation (2.3.34) is like in [Sch85, p.489]. Following Schoof, we denote the numerator of λ by α[††] and its denominator by β. That is:

$$\alpha = \Psi_{k+2}\Psi_{k-1}^2 - \Psi_{k-2}\Psi_{k+1}^2 - 4y^{q^2+1}\Psi_k^3, \tag{2.3.35}$$

$$\beta = [\Psi_k^2(x - x^{q^2}) - \Psi_{k-1}\Psi_{k+1}]4y\Psi_k. \tag{2.3.36}$$

This finishes the computation for the left-hand side of Equation (2.3.31).

Remark 2.3. We already computed the right-hand side of (2.3.31) more explicitly in Proposition 2.5 and got:

$$[\tau]\phi_\ell(P) = \left(\left(x - \frac{\Psi_{r-1}\Psi_{r+1}}{(\Psi_r)^2}\right)^q, \left(\frac{\Psi_{r+2}(\Psi_{r-1})^2 - \Psi_{r-2}(\Psi_{r+1})^2}{4y(\Psi_r)^3}\right)^q\right). \tag{2.3.37}$$

Write $[\tau]\phi_\ell(P) = (X([\tau]\phi_\ell(P)), Y([\tau]\phi_\ell(P)))$.

Now we replace the explicit expressions for the left-hand side (2.3.32) and the right-hand side (2.3.37) into (2.3.31). We get

$$X([\tau]\phi_\ell(P)) = -(x^{q^2} + x) + \lambda^2 + \frac{\Psi_{k-1}\Psi_{k+1}}{\Psi_k^2}, \tag{2.3.38}$$

$$Y([\tau]\phi_\ell(P)) = -\frac{\alpha}{\beta}\left(-2x^{q^2} - x + \frac{\Psi_{k-1}\Psi_{k+1}}{\Psi_k^2} + \frac{\alpha^2}{\beta^2}\right) - y^{q^2}. \tag{2.3.39}$$

Proposition 2.12

Equation (2.3.38) can be rewritten as

$$\Psi_r^{2q}\left[\beta^2\left[\Psi_{k-1}\Psi_{k+1} - \Psi_k^2(x^{q^2} + x + x^q)\right] + \alpha^2\Psi_k^2\right] + \beta^2\Psi_k^2(\Psi_{r-1}\Psi_{r+1})^q = 0.$$

Proof. Taking the common denominator on the left, respectively on right side of Equation (2.3.38) gives us

$$\frac{-\beta^2\Psi_k^2(x^{q^2} + x) + \alpha^2\Psi_k^2 + \beta^2\Psi_{k-1}\Psi_{k+1}}{\beta^2\Psi_k^2} = \frac{\Psi_r^{2q}x^q - (\Psi_{r-1}\Psi_{r+1})^q}{\Psi_r^{2q}}.$$

[†]In [Sch85, p. 489], the author forgot the term λ^2 in the y-coordinates.

[††]Note that in the definition of α in [Sch85, p. 489], one should correct the second term of the formula for α replacing Ψ_{k-1} with Ψ_{k-2}.

Since the denominators do not vanish, the terms all exist and we can multiply the previous equation by $\beta^2\Psi_k^2\Psi_r^{2q}$ to get

$$\Psi_r^{2q}\left[-\beta^2\Psi_k^2(x^{q^2}+x)+\alpha^2\Psi_k^2+\beta^2\Psi_{k-1}\Psi_{k+1}\right]=\beta^2\Psi_k^2\left[\Psi_r^{2q}x^q-\Psi_{r-1}^q\Psi_{r+1}^q\right].$$

Expanding the right-hand side of the previous equation yields

$$\boldsymbol{\Psi_r^{2q}}\left[-\beta^2\Psi_k^2(x^{q^2}+x)+\alpha^2\Psi_k^2+\beta^2\Psi_{k-1}\Psi_{k+1}\right]=\beta^2\Psi_k^2\boldsymbol{\Psi_r^{2q}}x^q-\beta^2\Psi_k^2\Psi_{r-1}^q\Psi_{r+1}^q.$$

In the previous expression, we can factor out the common term Ψ_r^{2q} to obtain

$$\begin{aligned}&\Psi_r^{2q}\left[-\beta^{\mathbf{2}}\Psi_k^2x^q-\beta^{\mathbf{2}}\Psi_k^2(x^{q^2}+x)+\alpha^2\Psi_k^2+\beta^2\Psi_{k-1}\Psi_{k+1}\right]\\&+\beta^{\mathbf{2}}\Psi_k^{2q}(\Psi_{r-1}\Psi_{r+1})^q=0.\end{aligned}$$

Again, factoring the common β^2 from the relevant terms in the previous equation yields

$$\Psi_r^{2q}\left[\beta^2\left[\Psi_{k-1}\Psi_{k+1}-\boldsymbol{\Psi_k^2}(x^{q^2}+x)-\boldsymbol{\Psi_k^2}x^q\right]+\alpha^2\Psi_k^2\right]+\beta^2\Psi_k^2\Psi_{r-1}^q\Psi_{r+1}^q=0.$$

By factorizing Ψ_k^2 in the previous equation, we obtain[†]:

$$\Psi_r^{2q}\left[\beta^2\left[\Psi_{k-1}\Psi_{k+1}-\Psi_k^2(x^{q^2}+x+x^q)\right]+\alpha^2\Psi_k^2\right]+\beta^2\Psi_k^2(\Psi_{r-1}\Psi_{r+1})^q=0. \tag{2.3.40}$$

□

Remark 2.4. The equation $\phi_\ell^2(P)+[k]P=-[\tau]\phi_\ell(P)$ can also be rewritten in the form (2.3.40).

Let $P(x,y)$ be the left-hand side of Equation (2.3.40). If we now replace all the division polynomials in $P(x,y)$ by the polynomials defined in Definition 2.2, we end up with a new polynomial $P'(x)$ which only depends on x.
We now want to compute $\gcd(P'(x),f_\ell(x))$. Recall that $P'(x)$ comes from Equation (2.3.32) for the x-coordinates.

Proposition 2.13

- If $\gcd(P'(x),f_\ell(x))=1$, we need to try for the next τ.
- If $\gcd(P'(x),f_\ell(x))\neq 1$, then $t\equiv\pm\tau \pmod{\ell}$.

Proof.
- If $\gcd(P'(x),f_\ell(x))=1$, there is no $P\in E[\ell]$ such that Equation (2.3.2) is verified. We cannot conclude and need to try the next τ.

[†]In [Sch85, p. 489], the term Ψ_k should be squared.

- If $\gcd(P'(x), f_\ell(x)) \neq 1$, we have that there is a point in $E[\ell]$ satisfying $P'(x)$, which is a rewriting of Equation (2.3.1). So we already know that $t \equiv \pm\tau \pmod{\ell}$ and we proceed with the algorithm.

□

Remark 2.5. We now know that either $\phi_\ell^2(P) + [k]P = [\tau]\phi_\ell(P)$, or $\phi_\ell^2(P) + [k]P = -[\tau]\phi_\ell(P)$ holds.

Let us check if there is $P \in E[\ell]$ that verifies $\phi_l^2(P) + [k]P = [\tau]\phi_l(P)$. We do this by verifying if Equation (2.3.39) holds.

Proposition 2.14

Equation (2.3.39) can be written as

$$4^q y^q (\Psi_r)^{3q} \left[\alpha[\Psi_k^2\beta^2(2x^{q^2} + x) - \beta^2\Psi_{k+1}\Psi_{k-1} - \alpha^2\Psi_k^2] - y^{q^2}\beta^3\Psi_k^2\right] - \beta^3\Psi_k^2[\Psi_{r+2}(\Psi_{r-1})^2 - \Psi_{r-2}(\Psi_{r+1})^2] = 0.$$

Proof. Let us first consider the left-hand side of Equation (2.3.39) and take a common denominator. We obtain

$$\begin{aligned} &- \frac{\alpha}{\beta}\left(\frac{\Psi_k^2\beta^2(-2x^{q^2} - x) + \beta^2\Psi_{k+1}\Psi_{k-1} + \alpha^2\Psi_k^2}{\beta^2\Psi_k^2}\right) - \frac{y^{q^2}\beta^3\Psi_k^2}{\beta^3\Psi_k^2} \\ &= \frac{-\alpha[-\Psi_k^2\beta^2(2x^{q^2} + x) + \beta^2\Psi_{k+1}\Psi_{k-1} + \alpha^2\Psi_k^2] - y^{q^2}\beta^3\Psi_k^2}{\beta^2\Psi_k^2} \\ &= \frac{\alpha[\Psi_k^2\beta^2(2x^{q^2} + x) - \beta^2\Psi_{k+1}\Psi_{k-1} - \alpha^2\Psi_k^2] - y^{q^2}\beta^3\Psi_k^2}{\beta^2\Psi_k^2}. \end{aligned}$$

Multiplying Equation (2.3.39) by $4^q y^q (\Psi_r)^{3q}\beta^3\Psi_k^2$ yields

$$\begin{aligned} &4^q y^q (\Psi_r)^{3q}\left[\alpha[\Psi_k^2\beta^2(2x^{q^2} + x) - \beta^2\Psi_{k+1}\Psi_{k-1} - \alpha^2\Psi_k^2] - y^{q^2}\cdot\beta^3\Psi_k^2\right] \\ &= \beta^3\Psi_k^2[\Psi_{r+2}(\Psi_{r-1})^2 - \Psi_{r-2}(\Psi_{r+1})^2]. \end{aligned}$$

Now putting everything to one side in the previous equation gives us[†]:

$$\begin{aligned} &4^q y^q (\Psi_r)^{3q}\left[\alpha[\Psi_k^2\beta^2(2x^{q^2} + x) - \beta^2\Psi_{k+1}\Psi_{k-1} - \alpha^2\Psi_k^2] - y^{q^2}\cdot\beta^3\Psi_k^2\right] \\ &- \beta^3\Psi_k^2[\Psi_{r+2}(\Psi_{r-1})^2 - \Psi_{r-2}(\Psi_{r+1})^2] = 0. \end{aligned} \tag{2.3.40}$$

□

Schoof stops here, but in fact there is a bit more to say. We need to substitute the division polynomials in Equation (2.3.40) by the polynomials f_k defined in

[†]This expression is completely different than the original one in Schoof's paper [Sch85, p. 489] because the author carried on with the mistake mentioned on page 39 of this report.

Definition 2.2. This way, Equation (2.3.40) has no more dependency on y. Since these polynomials f_k depend on the parity of k and τ, we need to consider 4 different cases for this step:

(i) when k and τ are even,

(ii) when k and τ are even,

(iii) when k is even and τ is odd,

(iv) when k is odd and τ is even.

We will illustrate these cases by computing one of them, namely case (i). The three other cases work similarly.
First, we need to realize that α (2.3.35) and β (2.3.36) in Equation (2.3.40) also depend on the parity of k. We address them first and obtain

$$\begin{aligned}\alpha_{\text{even}} &\coloneqq yf_{k+2}(f_{k-1})^2 - yf_{k-2}(f_{k+1})^2 - 4y^{p^2+1}(yf_k)^3 \\ &= y\left[f_{k+2}(f_{k-1})^2 - f_{k-2}(f_{k+1})^2 - 4y^{p^2+3}(f_k)^3\right],\end{aligned}$$

and

$$\begin{aligned}\beta_{\text{even}} &\coloneqq [(yf_k)^2(x - x^{p^2}) - f_{k-1}f_{k+1}]4y^2 f_k \\ &= [(x^3 + Ax + B)(f_k)^2(x - x^{p^2}) - f_{k-1}f_{k+1}]4(x^3 + Ax + B)f_k.\end{aligned}$$

Now Equation (2.3.40) turns into

$$\begin{aligned}&4^q y^q (yf_r)^{3q}\left[\alpha_{\text{even}}\left((yf_k)^2\beta_{\text{even}}^2(2x^{q^2} + x) - \beta_{\text{even}}^2 f_{k+1}f_{k-1} - \alpha_{\text{even}}^2(yf_k)^2\right)\right. \\ &\left. -y^{q^2}\beta_{\text{even}}^3(yf_k)^2\right] - \beta_{\text{even}}^3(yf_k)^2\left[yf_{r+2}(f_{r-1})^2 - yf_{r-2}(f_{r+1})^2\right] = 0.\end{aligned}$$

Factoring out powers of y gives

$$\begin{aligned}&4^q y^{4q}(f_r)^{3q}\Big[\alpha_{\text{even}}\big[y^2(f_k)^2\beta_{\text{even}}^2(2x^{q^2} + x) - \beta_{\text{even}}^2 f_{k+1}f_{k-1} \\ &- y^2\alpha_{\text{even}}^2(f_k)^2\big] - y^{q^2+2}\beta_{\text{even}}^3(f_k)^2\Big] \\ &- y^3\beta_{\text{even}}^3(f_k)^2\big[f_{r+2}(f_{r-1})^2 - f_{r-2}(f_{r+1})^2\big] = 0.\end{aligned}$$

Using that $y^2 = x^3 + Ax + B$, we have

$$\begin{aligned}&4^q(x^3 + Ax + B)^{2q}(f_r)^{3q}\Big[\alpha_{\text{even}}\big[(x^3 + Ax + B)(f_k)^2\beta_{\text{even}}^2(2x^{q^2} + x) \\ &- \beta_{\text{even}}^2 f_{k+1}f_{k-1} - y^2\alpha_{\text{even}}^2(f_k)^2\big] - y^{q^2}(x^3 + Ax + B)\beta_{\text{even}}^3(f_k)^2\Big] \\ &- y(x^3 + Ax + B)\beta_{\text{even}}^3(f_k)^2\big[f_{r+2}(f_{r-1})^2 - f_{r-2}(f_{r+1})^2\big] = 0.\end{aligned}$$

Let us call the left-hand side of the previous equation $Q(x)$.

Proposition 2.15

- If $\gcd(Q(x), f_l(x)) = 1$, then $t \equiv \tau \pmod{\ell}$.
- If $\gcd(Q(x), f_l(x)) \neq 1$, then $t \equiv -\tau \pmod{\ell}$.

Proof.

- If $\gcd(Q(x), f_l(x)) = 1$, then by Reasoning C.2, there is no $P \in E[\ell]$ satisfying $\phi_\ell^2(P) + [k]P = [\tau]\phi_\ell(P)$. Then, by Remark 2.5, $\phi_\ell^2(P) + [k]P = -[\tau]\phi_\ell(P)$ is verified. Hence, $t \equiv -\tau \pmod{\ell}$.
- If $\gcd(Q(x), f_l(x)) \neq 1$, then by Reasoning C.2, there is $P \in E[\ell]$ satisfying $\phi_\ell^2(P) + [k]P = [\tau]\phi_\ell(P)$. So, $t \equiv \tau \pmod{\ell}$.

□

This concludes the algorithm to compute $t \pmod{\ell}$ presented in Schoof's paper [Sch85, p. 487-489].

2.4 Chinese Remainder theorem

This is the third step of Schoof's algorithm described in Summary 2.1 [Sch85, p. 490]. The Chinese Remainder theorem is used to determine $t \pmod{\prod_{\substack{\ell \leq L \\ \ell \neq 2,p}} \ell}$.

Proposition 2.16: Chinese remainder theorem

Let $m_1, m_2, \ldots, m_k \in \mathbb{N}^*$ be pairwise coprime. Then the following system

$$\begin{cases} x & \equiv a_1 \pmod{n_1} \\ x & \equiv a_2 \pmod{n_2} \\ & \vdots \\ x & \equiv a_k \pmod{n_k} \end{cases}$$

has a unique solution $\bar{x}$ modulo $M = m_1 m_2 \ldots m_k$. Reformulating: if we have $\gcd(m_i, m_j) = 1$ for $i \neq j$, then the system of congruences is verified by one unique $\bar{x} \in [0, M-1]$.

A Projective Spaces

In this section, we introduce projective spaces and briefly compare them to affine spaces to show some differences. After that, we describe what curves look like in projective spaces. In preparation for the next section, we also introduce the concepts of singular curves and points at infinity.

A.1 Homogeneous coordinates

Let us define an equivalence relation which will be useful later to define the projective space. Let K be a field. For each integer $n \in \mathbb{N}^*$, we define the n-dimensional affine space $\mathbb{A}^n$ as the n-fold product K^n, that is

$$\mathbb{A}^n(K) = \{(x_0, x_1, \ldots, x_{n-1}) \mid x_0, x_1, \ldots, x_{n-1} \in K\}. \tag{A.1.1}$$

We say that $(x_0, x_1, \ldots, x_{n-1}) \in \mathbb{A}^n$ and $(y_0, y_1, \ldots, y_{n-1}) \in \mathbb{A}^n$ and denote it by $(x_0, x_1, \ldots, x_{n-1}) \sim (y_0, y_1, \ldots, y_{n-1})$ if and only of there is a $\lambda \in K^*$ such that $(x_0, \ldots, x_2) = \lambda(y_0, \ldots, y_2)$.

Proposition A.1

The relation $\sim$ is an equivalence relation. The equivalence class of $(x_0, x_1, \ldots, x_{n-1}, x_n) \in \mathbb{A}^{n+1}$ is denoted by $[x_0 : x_1 : \ldots : x_n]$ and called *homogeneous coordinates*.

Proof. Let $x, y, z \in \mathbb{A}^n(K)$ with $x = (x_0, \ldots, x_n), y = (y_0, \ldots, y_n)$ and $z = (z_0, \ldots, z_n)$.

1. **Symmetry**: If $x \sim y$, then there is a $\lambda \in K^*$ such that $(x_0, \ldots, x_n) = \lambda(y_0, \ldots, y_n)$. Multiplying on both sides by λ^{-1} gives us finally $(y_0, \ldots, y_n) = \frac{1}{\lambda}(x_0, \ldots, x_n)$ and so $y \sim x$.

2. **Reflexivity**: Wee see that $x \sim x$ by taking λ to be the neutral multiplicative element of K.

3. **Transitivity**: If $x \sim y$ and $y \sim z$, then there exist $\lambda, \mu \in K^*$ such that $(x_0, \ldots, x_n) = \lambda(y_0, \ldots, y_n)$ and $(y_0, \ldots, y_n) = \mu(z_0, \ldots, z_n)$. Then $(x_0, \ldots, x_n) = (\lambda\mu)(z_0, \ldots, z_n)$, hence $x \sim z$.

□

Using the equivalence relation from Proposition A.1, we now have all the tools to define projective spaces.

Definition A.1: Projective Space

Let K be a field. The *projective n-space* over K is defined as

$$\mathbb{P}^n(K) \coloneqq \left(K^{n+1} \setminus \{0\}\right) / \sim,$$

where $\sim$ is the equivalence relation defined in Proposition A.1.

Remark A.1. You will also find references that defined the projective n-space over K in the following way:

$$\mathbb{P}^n(K) \coloneqq \{[x_0 : x_1 : \cdots : x_n] \mid (x_0, \ldots, x_n) \in \mathbb{A}^{n+1}(K), (x_0, \ldots, x_n) \neq 0\}.$$

Remark A.2. The *homogenization* of the affine coordinates $(x_0, x_1, \ldots, x_{n-1}) \in \mathbb{A}^n(K)$ is the class $[x_0x_n : x_1x_n : \ldots : x_{n-1}x_n : x_n]$ for any non-zero $x_n \in K^*$. The homogenization does not depend on the choice of x_n because any two non-zero choices $x_n, x_n' \in K^*$ produce the same class.

Example A.1. If $(2, 3) \in \mathbb{A}^2(\mathbb{R})$, its homogenization is $[2 : 3 : 1] \in \mathbb{P}^2(\mathbb{R})$. Conversely, the homogeneous coordinates $[5 : 1 : 3] \in \mathbb{P}^2(\mathbb{R})$ can be transformed into $\left(\frac{5}{3}, \frac{1}{3}\right) \in \mathbb{A}^2(\mathbb{R})$.

Definition A.2: Points at infinity

The points at infinity of $\mathbb{P}^n(K)$ are homogeneous coordinates of the form $[x_0 : x_1 : \ldots : x_{n-1} : 0]$.

Remark A.3. The points at infinity are not in $\mathbb{A}^n(K)$

Remark A.4. Specifically, all the points of the form $[x_0 : x_1 : 0] \in \mathbb{P}^2(K)$ form a line at infinity. Hence the projective 2-space over as field K can be seen as extension of the affine 2-space over the same field K.

A.2 Curves in $\mathbb{P}^2(K)$

Definition A.3: Homogeneous Polynomial

A polynomial $f \in K[x_0, ..., x_n]$ is homogeneous of degree $d \geq 1$ if $f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n)$ for all $\lambda \in K \setminus \{0\}$. We write $\deg(f) = d$.

Example A.2. $f(x, y, z) = x^2y^2 + 2xyz^2 + 17z^4$ is a homogeneous polynomial of degree 4.

Definition A.4: Curves in $\mathbb{P}^2(K)$

Let K be a field and let $f \in K[X, Y, Z]$ be a non-constant homogeneous polynomial of degree $d \geq 1$. Then, a *curve* C *in* $\mathbb{P}^2(K)$ is the set of all homogeneous points $[\alpha : \beta : \gamma] \in \mathbb{P}^2(K)$ such that $f(\alpha, \beta, \gamma) = 0$.

Let $F(x, y, z)$ be a **homogeneous polynomial** of degree $d \geq 1$ (i.e., every monomial in F has total degree d). The **homogeneous curve** in the projective plane $\mathbb{P}^2$ (over a field K, e.g., $\mathbb{R}$ or $\mathbb{C}$) is the set of points:

$$C = \big\{[x : y : z] \in \mathbb{P}^2 \mid F(x, y, z) = 0\big\},$$

where $[x : y : z]$ denotes homogeneous coordinates (defined up to a non-zero scalar multiple).

Remark A.5 (Homogenization of equations). The homogenized version of a (2-variable) polynomial $g(x, y) \in K[x, y]$ is $G(x, y, z) = g\left(\frac{x}{z}, \frac{y}{z}\right) \cdot z^{\deg(g)}$, where $\deg(g)$ is the highest sum of exponents in any term of $g(x, y)$. The dehomogenization of a homogeneous polynomial $G(x, y, z)$ is $G(x, y, 1)$.

Example A.3. For example,

- $f(x, y) = x^2y^4 + x + 2 + y^3 \in \mathbb{R}[x, y]$ becomes $x^2y^4 + xz^5 + 2z^6 + y^3z^3$.
- $x^2y^3z + x^2z^4 + z^6$ becomes $x^2y^3 + x^2 + 1 \in \mathbb{R}[x, y]$.

Example A.4 (Line in $\mathbb{P}^2(K)$). Take the polynomial:

$$F(x, y, z) = ax + by + cz, \quad \text{where } a, b, c \in K,$$

where at least one coefficient is non-zero. Then the set

$$H = \{[\alpha : \beta : \gamma] \in \mathbb{P}^2(K) \mid F(\alpha, \beta, \gamma) = 0\}$$

is a projective line.

Not all the curves in $\mathbb{P}^2(K)$ behave the same way. Indeed, one could categorize them into so-called "singular curves" or "non-singular curves".

Definition A.5: Singular Curve

A curve of degree d is called *singular* at a point $A = [X : Y : Z] \in \mathbb{P}^2(K)$ if

$$\frac{\partial f}{\partial X} = \frac{\partial f}{\partial Y} = \frac{\partial f}{\partial Z} = 0.$$

Definition A.6: Non-Singular Curve

A curve is called *non-singular* if it is not singular at any point of $\mathbb{P}^2(K)$.

We now illustrate Definitions A.5 and A.6 with explicit examples.

Example A.5. Let C be the projective curve over a field K defined by $f(X,Y,Z) = 3XZ + Y^2$. We calculate the partial derivatives and try to find a singular point:

$$\begin{cases} \frac{\partial f}{\partial X} = 3Z = 0 \\ \frac{\partial f}{\partial Y} = 2Y = 0 \\ \frac{\partial f}{\partial Z} = 3X = 0 \end{cases}$$

The only solution to this system is when $x = y = 0$. However, we know that $[0:0:0]$ is not in $\mathbb{P}^2(K)$. Hence C is non-singular.

Example A.6. Now let C be the projective curve in K defined by $f(X,Y,Z) = 7X^3 + 2Y^3$. We can instantly see that $\frac{\partial f}{\partial Z} = 0$. So, every point of the form $P_i = [0:0:z_i]$ (with $z_i \neq 0$) are singular points and therefore C is a singular curve.

Let us now look at a definition of maps between curves and what it means for this map to be separable.

Definition A.7: Map between Curves

Let C_1 and C_2 be algebraic curves. A *map* between them is a map

$$\phi : C_1 \to C_2$$

that assigns to each point $P \in C_1$ a point $\phi(P) \in C_2$.

Definition A.8: Morphism

A map $\phi : C_1 \to C_2$ is called a *morphism* if it is given locally by rational functions that are non-singular at every point.

Definition A.9: Separable Map

Let $\phi : C_1 \to C_2$ be a nonconstant morphism of algebraic curves over a field K. The map ϕ is **separable** if the induced field extension $K(C_1)/\phi^* K(C_2)$ of function fields is separable.

B Proofs of Previous Propositions

This appendix contains

- relatively basic proofs and
- proofs that need a lot of algebraic computations..

This decision was made to avoid disrupting the flow of the main text.

Proposition B.1: (Proposition 1.1)

If $\text{char}(K) \neq 2$, then Equation (1.1.1) can be written as $(y')^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$, where $y' = 2(y + a_1x + a_3)$. In other words, the terms in xy disappear.

Proof. Set $y \coloneqq \frac{1}{2}(y' - a_1x - a_3)$. Squaring both sides yields

$$\begin{aligned} y^2 &= \left(\frac{1}{2}(y' - a_1x - a_3)\right)^2 \\ &= \frac{1}{4}(y')^2 + \frac{1}{4}a_1^2x^2 + \frac{1}{4}a_3^2 - \frac{1}{2}a_1xy' + \frac{1}{2}a_1a_3x - \frac{1}{2}a_3y'. \end{aligned}$$

By replacing the explicit expressions of y and y^2 into (1.1.1), we get

$$\begin{aligned} &\frac{1}{4}(y')^2 + \frac{1}{4}a_1^2x^2 + \frac{1}{4}a_3^2 - \frac{1}{2}a_1xy' + \frac{1}{2}a_1a_3x - \frac{1}{2}a_3^2 + \frac{1}{2}a_1xy' \\ =&\frac{1}{2}a_1^2x^2 + \frac{1}{2}a_1a_3x - \frac{1}{2}a_3y' + \frac{1}{2}a_1a_3x + \frac{1}{2}a_3^2 + x^3 + a_2x^2 + a_4x + a_6. \end{aligned}$$

By simplifying the common terms in the previous equation and then rearranging the resulting equation, we obtain

$$\frac{1}{4}(y')^2 = x^3 + x^2\left(a_2 + \frac{1}{4}a_1^2\right) + x\left(a_4 + \frac{1}{2}a_1a_3\right) + \left(a_6 + \frac{1}{4}a_3^2\right).$$

Multiplying the previous equation by 4 gives us:

$$(y')^2 = 4x^3 + x^2(4a_2 + a_1^2) + x(4a_4 + 2a_1a_3) + (4a_6 + a_3^2).$$

Replacing $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$, and $b_6 = a_3^2 + 4a_6$ into the previous equation, we get that:

$$(y')^2 = 4x^3 + b_2x^2 + 2b_4x + b_6. \tag{B.0.1}$$

□

Proposition B.2: (Proposition 1.2)

If $\text{char}(K) \notin \{2, 3\}$, we can even rewrite Equation (1.1.1) as $y^2 = x^3 + Ax + B$ with $A, B \in \overline{K}$.

Proof. Substituting $x = \frac{x'-3b_2}{36}$ and $y = \frac{y'}{108}$ into (B.0.1), we get

$$\begin{aligned}\left(\frac{y'}{108}\right)^2 &= 4\left(\frac{x'-3b_2}{36}\right)^3 + b_2\left(\frac{x'-3b_2}{36}\right)^2 + 2b_4\left(\frac{x'-3b_2}{36}\right) + b_6 \\ &= 4\frac{(x')^3 - 9b_2(x')^2 + 27b_2^2x' - 27b_2^3}{36^3} \\ &\quad + b_2\left(\frac{(x')^2 - 6b_2x' + 9b_2^2}{36^2}\right) + 2b_4\left(\frac{x'-3b_2}{36}\right) + b_6.\end{aligned}$$

Multiplying this expression by 36^3 gives

$$\begin{aligned}4(y')^2 = 4\left[(x')^3 - 9b_2(x')^2 + 27b_2^2x' - 27b_2^3\right] \\ + 36b_2\big((x')^2 - 6b_2x' + 9b_2^2\big) \\ + 2\cdot 36^2b_4(x'-3b_2) + 36^3b_6.\end{aligned}$$

Expanding the previous equation yields

$$\begin{aligned}4(y')^2 = 4(x')^3 - 36b_2(x')^2 + 108b_2^2x' - 108b_2^3 + 36b_2(x')^2 \\ - 216b_2^2x' + 324b_2^3 - 6\cdot 36^2b_4x' - 2\cdot 36^2b_4\cdot 3b_2 + 36^3b_6.\end{aligned}$$

Now assembling the common terms in the previous equation and simplifying, we obtain

$$\begin{aligned}4(y')^2 &= 4(x')^3 + (36b_2 - 36b_2)(x')^2 \\ &\quad + (108b_2^2 - 216b_2^2 + 2\cdot 36^2b_4)x' \\ &\quad + (-108b_2^3 + 324b_2^3 - 6\cdot 36^2b_2b_4 + 36^3b_6) \\ &= 4(x')^3 + \left(-108b_2^2 + 2\cdot 36^2b_4\right)x' \\ &\quad + (216b_2^3 - 6\cdot 36^2b_2b_4 + 36^3b_6).\end{aligned}$$

Now, if we substitute $c_4 = b_2^2 - 24b_4$ and $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$ in the latter equation, and divide by 4, we obtain

$$(y')^2 = (x')^3 - 27c_4x' - 54c_6,$$

which concludes the proof. □

Proposition B.3: (Proposition 1.3)

The discriminant of the polynomial $f(x) = x^3 + Ax + B$ becomes $\Delta_f = -(4A^3 + 27B^2)$.

Proof. The derivative $f'(x) = 3x^2 + A$. We have that

$$\Delta_f = \frac{(-1)^{3\cdot(3-1)/2}}{1}\mathrm{Res}(f, f') = (-1)^3\mathrm{Res}(f, f') = -\mathrm{Res}(f, f'),$$

where

$$\mathrm{Res}(f, f') = \begin{vmatrix} B & 0 & A & 0 & 0 \\ A & B & 0 & A & 0 \\ 0 & A & 3 & 0 & A \\ 1 & 0 & 0 & 3 & 0 \\ 0 & 1 & 0 & 0 & 3 \end{vmatrix} = 4A^3 + 27B^2.$$

The result follows. □

Proposition B.4: (Proposition 2.2)

The division polynomials $\Psi_m(x, y)$, where $m \in \mathbb{N}_{\geq 3}$ can be written in the form

$$\Psi_m = \begin{cases} mx^{\frac{m^2-1}{2}} + \mathcal{O}\left(x^{\frac{m^2-1}{2}-2}\right) & \text{if } m \text{ is odd,} \\ myx^{\frac{m^2-4}{2}} + \mathcal{O}\left(yx^{\frac{m^2-4}{2}-2}\right) & \text{if } m \text{ is even.} \end{cases}$$

Proof. We do a proof by induction.

Base cases:

$n = 3$: $\Psi_3 = 3x^4 + 6x^2 + 128x - A^2 = 3x^{\frac{3^2-1}{2}} + \mathcal{O}\left(x^{\frac{3^2-1}{2}-2}\right)$

$n = 4$: $\Psi_4 = y(4x^6 - 20Ax^4 + 80Bx^3 - 20A^2x^2 - 16ABy - 32B^2 - 4A^2)$

$= 4yx^{\frac{4^2-4}{2}} + \mathcal{O}\left(yx^{\frac{4^2-4}{2}-2}\right)$

Computing Ψ_5 and Ψ_6 with the recursion formulas (2.1.1) and (2.1.2), we see

$n = 5$: $\Psi_5 = 5x^{\frac{5^2-1}{2}} + \mathcal{O}\left(x^{\frac{5^2-1}{2}-2}\right)$,

$n = 6$: $\Psi_6 = 6yx^{\frac{6^2-4}{2}} + \mathcal{O}\left(yx^{\frac{6^2-4}{2}-2}\right)$.

This finishes the base cases.

Induction steps

We now admit Proposition B.4 for a certain fixed $m + 2$, where $m \geq 3$. Then we show that it is true for $2m$ and $2m + 1$. This way, we prove Proposition B.4 for all m in $\mathbb{N}_{\geq 3}$. To do this we need to compute Ψ_{2m} and Ψ_{2m+1} which are given by (2.1.1), respectively (2.1.2).

Case 1: In this case, we consider the following recursion formula

$$\Psi_{2m+1} = \Psi_{m+2}(\Psi_m)^3 - \Psi_{m-1}(\Psi_{m+1})^3. \tag{B.0.2}$$

We start by computing $\Psi_{m+2}(\Psi_m)^3$. Next, we calculate $\Psi_{m-1}(\Psi_{m+1})^3$. Now we only need to subtract $\Psi_{m-1}(\Psi_{m+1})^3$ from $\Psi_{m+2}(\Psi_m)^3$ and get the expression

for Ψ_{2m+1} in Equation (B.0.2).

Subcase (a): Let m be even.
Using the induction hypothesis on the first term of Equation (B.0.2) gives us

$$\begin{aligned}
&\Psi_{m+2}(\Psi_m)^3 \qquad\qquad (B.0.3)\\
&= \left[(m+2)yx^{\frac{(m+2)^2-4}{2}} + \mathcal{O}\left(yx^{\frac{(m+2)^2-8}{2}}\right)\right]\left[myx^{\frac{m^2-4}{2}} + \mathcal{O}\left(yx^{\frac{m^2-8}{2}}\right)\right]^3\\
&= \left[(m+2)yx^{\frac{m^2+4m}{2}} + \mathcal{O}\left(yx^{\frac{m^2+4m-4}{2}}\right)\right]\left[myx^{\frac{m^2-4}{2}} + \mathcal{O}\left(yx^{\frac{m^2-8}{2}}\right)\right]^3\\
&= (m+2)m^3y^4x^{\frac{m^2+4m}{2}+3\frac{m^2-4}{2}} + \mathcal{O}\left(y^4x^{\frac{m^2+4m-4}{2}}x^{\frac{3(m^2-4)}{2}}\right). \qquad (B.0.4)
\end{aligned}$$

We know that $y^2 = x^3 + Ax + B = x^3 + \mathcal{O}(x)$. Replacing this into (B.0.4) yields

$$\begin{aligned}
&(m^4+2m^3)x^6x^{\frac{m^2+4m+3m^2-12}{2}} + \mathcal{O}\left(x^6x^{\frac{m^2+4m-4+3(m^2-4)}{2}}\right)\\
&= (m^4+2m^3)x^{\frac{4m^2+4m}{2}} + \mathcal{O}\left(x^{\frac{4m^2+4m-4}{2}}\right). \qquad (B.0.5)
\end{aligned}$$

Now we apply the induction hypothesis to the second term in (B.0.2) and do all the necessary computations. We get

$$\begin{aligned}
&\Psi_{m-1}(\Psi_{m+1})^3\\
&= \left[(m-1)x^{\frac{(m-1)^2-1}{2}} + \mathcal{O}\left(x^{\frac{(m-1)^2-5}{2}}\right)\right]\left[(m+1)x^{\frac{(m+1)^2-1}{2}} + \mathcal{O}\left(x^{\frac{(m+1)^2-5}{2}}\right)\right]^3\\
&= \left[(m-1)x^{\frac{m^2-2m}{2}} + \mathcal{O}\left(x^{\frac{m^2-2m-4}{2}}\right)\right]\left[(m+1)x^{\frac{m^2+2m}{2}} + \mathcal{O}\left(x^{\frac{m^2+2m-4}{2}}\right)\right]^3\\
&= (m-1)(m+1)^3x^{\frac{m^2-2m}{2}+\frac{3(m^2+2m)}{2}} + \mathcal{O}\left(x^{\frac{m^2-2m-4}{2}}x^{\frac{3(m^2+2m)}{2}}\right)\\
&= (m^4+2m^3-2m-1)x^{\frac{4m^2+4m}{2}} + \mathcal{O}\left(x^{\frac{4m^2+4m-4}{2}}\right). \qquad (B.0.6)
\end{aligned}$$

Substituting (B.0.5) and (B.0.6) into (B.0.2) yields

$$\begin{aligned}
\Psi_{2m+1} &= (m^4+2m^3)x^{\frac{4m^2+4m}{2}} + \mathcal{O}\left(x^{\frac{(4m^2+4m-4)}{2}}\right)\\
&\quad - (m^4+2m^3-2m-1)x^{\frac{4m^2+4m}{2}} + \mathcal{O}\left(x^{\frac{(4m^2+4m-4)}{2}}\right)\\
&= (2m+1)x^{\frac{(2m+1)^2-1}{2}} + \mathcal{O}\left(x^{\frac{(2m^2+1)^2-5}{2}}\right).
\end{aligned}$$

This finishes the subcase where m is even.

Subcase (b): Suppose m is odd.
Applying the induction hypothesis to the first term of (B.0.2) and doing all the computations, we get

$$\begin{aligned}\Psi_{m+2}(\Psi_m)^3 &= \left[(m+2)x^{\frac{(m+2)^2-1}{2}} + \mathcal{O}\left(x^{\frac{(m+2)^2-5}{2}}\right)\right]\left[mx^{\frac{m^2-1}{2}} + \mathcal{O}\left(x^{\frac{m^2-5}{2}}\right)\right]^3 \\ &= \left[(m+2)x^{\frac{m^2+4m+3}{2}} + \mathcal{O}\left(x^{\frac{m^2+4m-1}{2}}\right)\right]\left[mx^{\frac{m^2-1}{2}} + \mathcal{O}\left(x^{\frac{m^2-5}{2}}\right)\right]^3 \\ &= (m+2)m^3x^{\frac{m^2+4m+3}{2}+\frac{3(m^2-1)}{2}} + \mathcal{O}\left(x^{\frac{m^2+4m-1}{2}}x^{\frac{3(m^2-1)}{2}}\right) \\ &= (m^4+2m^3)x^{\frac{4m^2+4m}{2}} + \mathcal{O}\left(x^{\frac{4m^2+4m-4}{2}}\right). \end{aligned} \tag{B.0.7}$$

Now we use the induction hypothesis on the second term in (B.0.2). This gives us

$$\begin{aligned}&\Psi_{m-1}(\Psi_{m+1})^3 \\ &= \left[(m-1)yx^{\frac{(m-1)^2-4}{2}} + \mathcal{O}\left(yx^{\frac{(m-1)^2-8}{2}}\right)\right]\left[(m+1)yx^{\frac{(m+1)^2-4}{2}} + \mathcal{O}\left(yx^{\frac{(m+1)^2-8}{2}}\right)\right]^3 \\ &= \left[(m-1)yx^{\frac{m^2-2m-3}{2}} + \mathcal{O}\left(yx^{\frac{m^2-2m-7}{2}}\right)\right]\left[(m+1)yx^{\frac{m^2+2m-3}{2}} + \mathcal{O}\left(yx^{\frac{m^2+2m-7}{2}}\right)\right]^3 \\ &= (m-1)(m+1)^3y^4x^{\frac{m^2-2m-3}{2}+3\frac{m^2+2m-3}{2}} + \mathcal{O}\left(y^4x^{\frac{m^2-2m-7}{2}}x^{\frac{3(m^2+2m-3)}{2}}\right).\end{aligned}$$

Substituting $y^2 = x^3 + \mathcal{O}(x)$ into the previous expression and manipulating the exponents yields

$$\begin{aligned}&\left[(m-1)(m^3+3m^2+3m+1)x^6x^{\frac{4m^2+4m-12}{2}} + \mathcal{O}\left(x^6x^{\frac{4m^2+4m-16}{2}}\right)\right] \\ &= (m^4+2m^3-2m-1)x^{\frac{4m^2+4m}{2}} + \mathcal{O}\left(x^{\frac{4m^2+4m-4}{2}}\right).\end{aligned} \tag{B.0.8}$$

Now putting (B.0.7) and (B.0.8) into (B.0.2), we get

$$\begin{aligned}\Psi_{2m+1} &= (m^4+2m^3)x^{\frac{4m^2+4m}{2}} + \mathcal{O}\left(x^{\frac{4m^2+4m-4}{2}}\right) \\ &\quad - \left[(m^4+2m^3-2m-1)x^{\frac{4m^2+4m}{2}} + \mathcal{O}\left(x^{\frac{4m^2+4m-4}{2}}\right)\right] \\ &= (2m+1)x^{\frac{(2m+1)^2-1}{2}} + \mathcal{O}\left(x^{\frac{(2m+1)^2-5}{2}}\right).\end{aligned}$$

This finishes the subcase where m is odd. This is also the end of case 1.

Case 2: In this case, we consider the following recursion formula:

$$\Psi_{2m} = \Psi_m(\Psi_{m-2}(\Psi_{m-1})^2 - \Psi_{m-2}(\Psi_{m+1})^2)(2y)^{-1}. \tag{B.0.9}$$

To avoid getting long computations, we split (B.0.9) into smaller computations. We are going to start by computing $\Psi_{m-2}(\Psi_{m-1})^2$ and $\Psi_{m-2}(\Psi_{m+1})^2$. Then by

a simple subtraction, we get $\Psi_{m-2}(\Psi_{m-1})^2 - \Psi_{m-2}(\Psi_{m+1})^2$. Now we only need multiply the previous expression by $\Psi_m/(2y)$ to end up at Equation (B.0.9).

Subcase (a): Let m be even.
Applying the induction hypothesis to $\Psi_{m+2}(\Psi_{m-1})^2$ and simplifying the exponents yields

$$\begin{aligned}
&\Psi_{m+2}(\Psi_{m-1})^2 \\
&= \left[y(m+2)x^{\frac{(m+2)^2-4}{2}} + \mathcal{O}\left(yx^{\frac{(m+2)^2-8}{2}}\right)\right]\left[(m-1)x^{\frac{(m-1)^2-1}{2}} + \mathcal{O}\left(x^{\frac{(m-1)^2-5}{2}}\right)\right]^2 \\
&= \left[(m+2)yx^{\frac{m^2+4m}{2}} + \mathcal{O}\left(yx^{\frac{m^2+4m-4}{2}}\right)\right]\left[(m-1)x^{\frac{m^2-2m}{2}} + \mathcal{O}\left(x^{\frac{m^2-2m-4}{2}}\right)\right]^2.
\end{aligned}$$

Performing the multiplication in the previous expression gives us

$$\begin{aligned}
&= (m+2)(m^2-2m+1)yx^{\frac{m^2+4m}{2}+\frac{2(m^2-2m)}{2}} + \mathcal{O}\left(yx^{\frac{m^2+4m-4}{2}+\frac{2(m^2-2m)}{2}}\right) \\
&= (m^3-3m+2)^2yx^{\frac{3m^2}{2}} + \mathcal{O}\left(yx^{\frac{3m^2-4}{2}}\right). \qquad \text{(B.0.10)}
\end{aligned}$$

Using the induction hypothesis on $\Psi_{m-2}(\Psi_{m+1})^2$ and performing the multiplication, we get

$$\begin{aligned}
&\Psi_{m-2}(\Psi_{m+1})^2 \\
&= \left[(m-2)yx^{\frac{(m-2)^2-4}{2}} + \mathcal{O}\left(yx^{\frac{(m-2)^2-8}{2}}\right)\right]\left[(m+1)x^{\frac{(m+1)^2-1}{2}} + \mathcal{O}\left(x^{\frac{(m+1)^2-5}{2}}\right)\right]^2 \\
&= \left[(m-2)yx^{\frac{m^2-4m}{2}} + \mathcal{O}\left(yx^{\frac{m^2-4m-4}{2}}\right)\right]\left[(m+1)x^{\frac{m^2+2m}{2}} + \mathcal{O}\left(yx^{\frac{m^2+2m-4}{2}}\right)\right]^2 \\
&= (m+2)(m^2+2m+1)yx^{\frac{m^2-4m}{2}+2\frac{m^2+2m}{2}} + \mathcal{O}\left(yx^{\frac{m^2-4m-4+2(m^2+2m)}{2}}\right) \\
&= (m^3-3m-2)yx^{\frac{3m^2}{2}} + \mathcal{O}\left(yx^{\frac{3m^2-4}{2}}\right). \qquad \text{(B.0.11)}
\end{aligned}$$

When we subtract (B.0.11) from (B.0.10), we obtain

$$\begin{aligned}
&\Psi_{m-2}(\Psi_{m-1})^2 - \Psi_{m-2}(\Psi_{m+1})^2 \\
&= (m^3-3m+2)^2yx^{\frac{3m^2}{2}} + \mathcal{O}\left(yx^{\frac{3m^2-4}{2}}\right) \\
&\quad - \left[(m^3-3m-2)yx^{\frac{3m^2}{2}} + \mathcal{O}\left(yx^{\frac{3m^2-4}{2}}\right)\right] \\
&= 4yx^{\frac{3m^2}{2}} + \mathcal{O}\left(yx^{\frac{3m^2-4}{2}}\right). \qquad \text{(B.0.12)}
\end{aligned}$$

Applying the induction hypothesis to Ψ_m and multiplying Ψ_m by (B.0.12) gives

us

$$\begin{aligned}2y\Psi_{2m} &= \left[myx^{\frac{m^2-4}{2}} + \mathcal{O}\left(yx^{\frac{m^2-8}{2}}\right)\right] \cdot \left[4yx^{\frac{3m^2}{2}} + \mathcal{O}\left(yx^{\frac{3m^2-4}{2}}\right)\right] \\ &= 4my^2x^{\frac{m^2-4+3m^2}{2}} + \mathcal{O}\left(y^2x^{\frac{m^2-8+3m^2}{2}}\right) \\ &= 4y^2mx^{\frac{(2m)^2-4}{2}} + \mathcal{O}\left(y^2x^{\frac{(2m)^2-8}{2}}\right).\end{aligned}$$

Multiplying by $(2y)^{-1}$, we get the final expression of (B.0.9), that is

$$\begin{aligned}\Psi_{2m} &= \left[4my^2x^{\frac{4m^2-4}{2}} + \mathcal{O}\left(y^2x^{\frac{(2m)^2-8}{2}}\right)\right](2y)^{-1} \\ &= 2myx^{\frac{(2m)^2-4}{2}} + \mathcal{O}\left(yx^{\frac{(2m)^2-8}{2}}\right).\end{aligned}$$

This finishes the subcase where m is even.

Subcase (b): Let m be odd.
Applying the induction hypothesis to $\Psi_{m+2}(\Psi_{m-1})^2$ and simplifying the exponents yields

$$\begin{aligned}&\Psi_{m+2}(\Psi_{m-1})^2 \\ &= \left[(m+2)x^{\frac{(m+2)^2-1}{2}} + \mathcal{O}\left(x^{\frac{(m+2)^2-5}{2}}\right)\right]\left[(m-1)yx^{\frac{(m-1)^2-4}{2}} + \mathcal{O}\left(yx^{\frac{(m-1)^2-8}{2}}\right)\right]^2 \\ &= \left[(m+2)x^{\frac{m^2+4m+3}{2}} + \mathcal{O}\left(x^{\frac{m^2+4m-1}{2}}\right)\right]\left[(m-1)yx^{\frac{m^2-2m-3}{2}} + \mathcal{O}\left(yx^{\frac{m^2-2m-7}{2}}\right)\right]^2\end{aligned}$$

We leave y^2 the way it is in regards of the last step where we need to divide by $(2y)^{-1}$. Performing the multiplication in the previous expression yields

$$\begin{aligned}&(m+2)(m^2-2m+1)y^2x^{\frac{m^2+4m+3}{2}+2\frac{m^2-2m-3}{2}} + \mathcal{O}\left(y^2x^{\frac{m^2+4m-1+2(m^2-2m-3)}{2}}\right) \\ &= (m^3-3m+2)y^2x^{\frac{3m^2-3}{2}} + \mathcal{O}\left(y^2x^{\frac{3m^2-7}{2}}\right).\end{aligned}$$

Using the induction hypothesis on $\Psi_{m-2}(\Psi_{m+1})^2$ and performing the multiplication, we get

$$\begin{aligned}&\Psi_{m-2}(\Psi_{m+1})^2 \\ &= \left[(m-2)x^{\frac{(m-2)^2-1}{2}} + \mathcal{O}\left(x^{\frac{(m-2)^2-5}{2}}\right)\right]\ \left[(m+1)yx^{\frac{(m+1)^2-4}{2}} + \mathcal{O}\left(yx^{\frac{(m+1)^2-8}{2}}\right)\right]^2 \\ &= \left[(m-2)x^{\frac{m^2-4m+3}{2}} + \mathcal{O}\left(x^{\frac{m^2-4m-1}{2}}\right)\right]\left[(m+1)yx^{\frac{m^2+2m-3}{2}} + \mathcal{O}\left(yx^{\frac{m^2+2m-7}{2}}\right)\right]^2.\end{aligned} \tag{B.0.13}$$

Doing the multiplication in the previous expression gives us

$$(m+2)(m^2+2m+1)y^2x^{\frac{m^2-4m+3}{2}+2\frac{m^2+2m-3}{2}}+\mathcal{O}\Big(y^2x^{\frac{m^2-4m-1+2(m^2+2m-3)}{2}}\Big)$$
$$=(m^3-3m-2)y^2x^{\frac{3m^2-3}{2}}+\mathcal{O}\Big(y^2x^{\frac{3m^2-7}{2}}\Big). \tag{B.0.14}$$

Subtracting (B.0.14) from (B.0.13), we get

$$\begin{aligned}&\Psi_{m-2}(\Psi_{m-1})^2-\Psi_{m-2}(\Psi_{m+1})^2\\ =&\Big[(m^3-3m+2)y^2x^{\frac{3m^2-3}{2}}+\mathcal{O}\Big(y^2x^{\frac{3m^2-7}{2}}\Big)\Big]\\ &+\Big[(m^3-3m-2)y^2x^{\frac{3m^2-3}{2}}+\mathcal{O}\Big(y^2x^{\frac{3m^2-7}{2}}\Big)\Big]\\ =&4y^2x^{\frac{3m^2-3}{2}}+\mathcal{O}\Big(y^2x^{\frac{3m^2-7}{2}}\Big).\end{aligned}$$

Applying the induction hypothesis to Ψ_m and multiplying Ψ_m by (B.0.12) gives us

$$\begin{aligned}&=(mx^{\frac{m^2-1}{2}}+\mathcal{O}\Big(x^{\frac{m^2-5}{2}}\Big))\cdot(4y^2x^{\frac{3m^2-3}{2}}+\mathcal{O}\Big(y^2x^{\frac{3m^2-7}{2}}\Big))\\ &=4my^2x\frac{m^2-1+3m^2-3}{2}+\mathcal{O}\Big(y^2x^{\frac{m^2-5+3m^2-3}{2}}\Big)\\ &=4my^2x^{\frac{4m^2-4}{2}}+\mathcal{O}\Big(y^2x^{\frac{(2m)^2-8}{2}}\Big).\end{aligned}$$

Multiplying by $(2y)^{-1}$, we get the final expression

$$\begin{aligned}\Psi_{2m}&=\Big[4my^2x^{\frac{(2m)^2-4}{2}}+\mathcal{O}\Big(y^2x^{\frac{(2m)^2-8}{2}}\Big)\Big](2y)^{-1}\\ &=2myx^{\frac{(2m)^2-4}{2}}+\mathcal{O}\Big(yx^{\frac{(2m)^2-8}{2}}\Big).\end{aligned}$$

This finishes the subcase where m is odd. □

C Reasonings

Remark C.1. The greatest common divisor for two univariate polynomials is usually defined as a monic polynomial. This means that the gcd can either be 1 or a monic polynomial $D(X)$ of degreee $d \geq 1$.

Reasoning C.1. We know that the roots of the division polynomial $\Psi_\ell(x)$ are exactly the x-coordinates of the ℓ-torsion points (e.g. $[\ell]P = \mathcal{O}$, see Definition 1.12). This means that, if $f_\ell(x_0) = 0$, then there is a point $P = (x_0, y) \in E[\ell]$.

Reasoning C.2. Let us take two polynomials $P(x) \in K[x]$ and $f_\ell(x) \in K[x]$ defined in Proposition 2.2. Then, we want to determine the greatest common divisor of these two polynomials. We will denote it by $\gcd(P(x), f_\ell(x))$. Then, we have two possibilities:

- If $\gcd(P(x), f_\ell(x)) = 1$:
  Then the two polynomials $P(x)$ and $f_\ell(x)$ have no common factor (except maybe a constant which is not taken into account in the gcd, as explained in Remark C.1). So, clearly, they do not share a common root. This means that there is no x_0 such that $P(x_0) = 0$ and $f_\ell(x_0) = 0$ simultaneously.
- If $\gcd(P_1(x), P_2(x)) \neq 1$:
  By Remark C.1, the greatest common divisor must be a monic polynomial $D(X)$ of degreee $d \geq 1$. Let us call x_0 (one of the) roots of $D(x)$, which means $D(x_0) = 0$. Then $P(x_0) = 0$ and $f_\ell(x_0) = 0$ simultaneously. By Reasoning C.1, the second equation gives us that there is $P \in E[\ell]$. Furthermore, the first equation tells us that this P satisfies the polynomial $P(x)$.

Reasoning C.3. Let $P \in E[\ell]$, then, by Definition 1.12 $[\ell]P = \mathcal{O}$. Suppose there exists $q \in \mathbb{R}$, then $[q]P = [k]P + [n\ell]P$ for $n \in \mathbb{N}$ and $k \equiv q \pmod{\ell}$. By assumption, $[\ell]P = \mathcal{O}$, and so $[n\ell]P = \mathcal{O}$. By by Remark 1.5, this implies that $[q]P = [k]P$ where $k \equiv q \pmod{\ell}$

Reasoning C.4. Let us consider the equation

$$\phi_l(P) = \pm[\alpha]P, \tag{C.0.1}$$

where $\phi_l(P)$ and $[\alpha]P$ are given by Remark 1.7, respectively Proposition 2.1. Then Equation (C.0.1) can be split into $\phi_l(P) = [\alpha]P$, and $\phi_l(P) = -[\alpha]P$. Let us denote $[\alpha]P$ by $(X([\alpha]P), Y([\alpha]P))$. Similarly, we write $(X(-[\alpha]P), Y(-[\alpha]P))$ for $-[\alpha]P$. We realize that $X([\alpha]P) = X(-[\alpha]P)$ by Remark 1.6.

Proposition C.1

Let $P = (x, y) \in E[\ell]$. The following expressions do not vanish on $E[\ell]$ for ℓ a prime number not equal to 2:

(1) y^2,

(2) the polynomials $f_k(x)$ when $0 < k < \ell$ (see Definition 2.2).

Proof. (1) Suppose $y = 0$. Then we can write $P = (x, 0)$. Now by the group law in Remark 1.5, $-P = (x, -0) = (x, 0)$. We can see that $P = -P$ and rearranging everything to one side yields $[2]P = \mathcal{O}$. So $P \in E[2]$. We supposed at the beginning of the algorithm that $\ell \neq 2$. So by Proposition 1.11, we have that $P \notin E[\ell]$.

(2) Let us now show that $f_k(x)$ does not vanish on $E[\ell]$. From Proposition 2.3 we have $f_k(x) = 0$ if and only if $[k]P = 0$. But we assumed $0 < k < \ell$, so it only vanishes on $E[k]$ and in particular not on $E[\ell]$.

□

Remark C.2. Since K has non-zero divisors, for $a, b \in K$: if $a \neq 0$ and $b \neq 0$, then $ab \neq 0$. Then, Proposition C.1(2) can be extended by induction: $f_k^n(x) \neq 0$ for any integer $n \geq 1$. Since Ψ_k is just a rewriting of f_k, $\Psi_k^n \neq 0$. Also x^3+Ax+B does not vanish on $E[\ell]$ because $y^2 = x^3+Ax+B$ and Proposition C.1(1) applies.

References

[Bar03] Edward J. Barbeau. *Polynomials*. Problem Books in Mathematics. Springer, 2nd edition, 2003.

[CLO07] David A. Cox, John B. Little, and Donal. O'Shea. *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*. Undergraduate texts in mathematics. Springer, New York, 3rd ed. edition, 2007.

[Dev24] The Sage Developers. *SageMath*, 2024. Version 10.3.

[Fri17] Stefan Friedl. An elementary proof of the group law for elliptic curves. pages 3–8, 2017.

[Has36] Helmut Hasse. Zur theorie der abstrakten elliptischen funktionenkörper. III. *Journal für die reine und angewandte Mathematik (Crelle's Journal)*, 175:193–208, 1936.

[HJ13] Roger A. Horn and Charles R. Johnson. *Matrix Analysis*. Cambridge University Press, Cambridge, 2 edition, 2013.

[Sch85] René Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of Computation*, 44(170):483–494, 1985. Accessed: 27.05.2025.

[Sch17] Martin Schlichenmaier. Algebraic curves. pages 84–70, 2017.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*. Graduate texts in mathematics ; 106. Springer-Verlag, New York, 2nd ed. edition, 2009.

[Was08] Lawrence C. Washington. *Elliptic curves : number theory and cryptography*. Discrete mathematics and its applications. Chapman & Hall/CRC, Boca Raton, FL, 2nd ed. edition, 2008.

[Wel25] Ben Welter. My geogebra figures. `https://www.geogebra.org/m/ctmjrjyq`, 2025.

Acknowledgements

I am deeply grateful to my supervisor, Dr. Baril Boudreau, for proposing this research topic and providing invaluable guidance throughout this work. Thank you very much for sharing your passion and knowledge with me, whether in mathematics, LaTeX-formatting, or broader academic mentorship. Our near-weekly meetings were a constant opportunity to clarify doubts. Whenever we couldn't meet, you responded to my emails with remarkable speed—even late at night or on weekends, ensuring progress at any time. I sincerely appreciate your mentorship and support which contributed to the completion of this work. You taught me skills that I consider invaluable for my future studies. You were a great supervisor!

A heartful thank you to some of my classmates for shattering my stereotype of "math people" being boring. Indeed, they can be incredibly fun and interesting. You made my studies not just bearable, but truly enjoyable. If it weren't for your camaraderie, I might have given up on my studies after the first semester. You are the reason I stayed, and I'm grateful for that.

最後になりますが、日本で出会ったすべての方々に感謝の気持ちを伝えたいです。私はここで人生で最高の時間を過ごし、皆さんには「本当の」学生生活を教えていただきました。特に早稲田奉仕園の寮生の皆さんとWKGKクラブのメンバーには心から感謝しています。この経験は、私の心に永遠に刻まれることでしょう。Tititi!