rijksuniversiteit
groningen

faculteit Wiskunde en
Natuurwetenschappen

Hasse's Theorem on Elliptic Curves

with an extension to hyperelliptic curves of genus 2

Mirjam Soeten

Master Thesis Mathematics

University of Groningen

June 24, 2013

First Supervisor: Prof. Dr. J. Top

Second Supervisor: Drs. A.R.F. Everts

Abstract

Hasse's theorem on elliptic curves states an estimate for the number of points on an elliptic curve $E : y^2 + h(x)y = f(x)$ over $\mathbb{F}_q$ in terms of q. Yu I. Manin proved this theorem in 1956 in a completely elementary way. In this thesis, the proof of Manin will be studied. This proof will be extended to all characteristics. This extending needs the theory of twisting curves, reduction theory and valuations. Furthermore, with use of the computer program Magma we will illustrate Manin's argument.

After that, we will consider hyperelliptic curves of genus 2. In this case the polynomial $f(x)$ has degree 5 in stead of degree 3, while $h(x)$ has at most degree 2 in stead of degree 1. We try to do some steps of Manin's argument in this case, using Magma to do the computations.

Contents

1 Introduction

1.1 Summary

In 1924, Emil Artin made the following estimate. For p a prime number and $E/\mathbb{F}_p$ an elliptic curve, the number of points $\#E(\mathbb{F}_p)$ on E can be estimated by

$$|\#E(\mathbb{F}_p) - (p+1)| \leq 2\sqrt{p}. \tag{1.1}$$

Unfortunately, Artin was not able to prove his estimate. Then, in 1933, Helmut Hasse proved the estimate of Artin. But then André Weil generalized the statement of Artin. During his time in prison, Weil generalized the statement of Artin to one valid for all $q = p^r$ and for general genus. In 1948, this new theorem and the proof of it were published in a book written by Weil. In 1956, Yu I. Manin gave a completely elementary proof of Hasse's theorem for elliptic curve. Unfortunately, in most literature, this elementary proof is only given under the additional assumption that $ch(\mathbb{F}_q) \geq 5$.

In this thesis, Manin's proof of Hasse's theorem will be studied. First, the case $\text{char}(\mathbb{F}_q) \geq 5$ is extended to the case $\text{char}(\mathbb{F}_q) \geq 3$. The case $\text{char}(\mathbb{F}_q) = 2$ is treated seperately since in this case we use a different form of an elliptic curve. Also the case $\text{char}(\mathbb{F}_q) = 2$ is split in two subcases. The first subcase deals with the supersingular curves. The second subcase is the case of non-supersingular curves, i.e. the ones for which $j(E) \neq 0$.
After Manin's proof is written down in every case, we will try to show that this elementary proof is basically the same as the other proofs of Hasse's theorem, for example the proof as given in the book of Silverman. Furthermore, we give a shorter proof of some of the lemmas, valid for all characteristics.
The last thing done in this thesis is investigating whether the proof of Manin can be extended to the statement of Weil. With this we mean that we want to check whether Manin's proof can be extended to hyperelliptic curves of genus 2. Therefore, we first need some theory about these hyperelliptic curves.
Troughout the thesis, the computer program Magma is used a lot. With this computer program, we will show the steps taken in the proof for elliptic curves. In this way, hopefully we can see that all formulas are correct. For the hyperelliptic curves of genus 2, we don't know whether we can extend the proof, so we will use Magma to compute some of the steps.

1.2 Notation

In this thesis the following notation is used. The notation $K[x]$ means the polynomial ring of K in the variable x. So an element $f \in K[x]$ can be written as

$$f(x) = k_n x^n + ... + k_1 x + k_0$$

where $k_i \in K$. In the same way, $K(x)$ is the rational function field of K in the variable x. In this case, an element $f \in K(x)$ is a rational expression in x with all coefficients from K. Using this, we can obtain the field $\mathbb{F}_q$ with $q = p^r$, which is the finite field of q elements. $\mathbb{F}_q$ is defined as

$$\mathbb{F}_q = \mathbb{F}_{p^r} = \frac{\mathbb{F}_p[x]}{< \text{irr. polynomial} >}$$

with the irreducible polynomial a polynomial of degree r in x.
The characteristic of the field $\mathbb{F}_q$ is denoted by $\mathrm{char}(\mathbb{F}_q)$ and defined as the smallest number n such that $n \cdot 1 = 0$. The valuation of x at a point P is denoted by $v_P(x)$. A valuation is a value belonging to x satisfying the following three properties.

1. $v_P(x) = \infty \Leftrightarrow x = 0$
2. $v_P(xy) = v_P(x) + v_P(y)$
3. $v_P(x + y) \geq \min(v_P(x), v_P(y))$.

At last, the j-invariant and discriminant of an elliptic curve E are defined by

$$\begin{aligned} j(E) &= \frac{c_4^3}{\Delta} \\ \Delta &= -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6 \end{aligned}$$

where

$$\begin{aligned} b_2 &= a_1^2 + 4a_4 \\ b_4 &= 2a_4 + a_1 a_3 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2 \\ c_4 &= b_2^2 - 24b_4. \end{aligned}$$

2 Mathematical Background

Before we can state and prove the Hasse inequality on elliptic curves, we need some basic theory. In this chapter on mathematical background, we will discuss the mathematics of elliptic curves, such as their group law. Furthermore, we will discuss the Frobenius map.

2.1 Elliptic Curves

In this short section the definition of an elliptic curve will be given. An elliptic curve over a field K is a curve of genus 1 of the form

$$E/K: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 = f(x) \tag{2.1}$$

where the coefficients $a_i \in K$. Furthermore, the curve (2.1) must have a single point at infinity called $\mathcal{O}$ (so the curve has at least one point lying on it), and the curve must be nonsingular, which means both partial derivatives cannot equal zero at the same time. So for a point $(\alpha, \beta) \in E$ it must hold that

$$(a_1y - f'(x), 2y + a_1x + a_3)|_{(\alpha,\beta)} = (a_1\beta - f'(\alpha), 2\beta + a_1\alpha + a_3) \neq (0,0).$$

The general form of an elliptic curve (2.1) is called a long Weierstrass form. For different situations the long Weierstrass form can be reduced to a shorter form as will be seen in the chapters 3, 4 and 5. For example, when $\mathrm{char}(K) \geq 5$ the elliptic curve E can be written in short Weierstrass form given by

$$E/K: \quad y^2 = x^3 + a_4x + a_6.$$

As a result from E being nonsingular, $f(x)$ has three distinct roots. A point on the curve E/K is given by (x_0, y_0) with $x_0, y_0 \in K$ such that $y_0^2 + a_1x_0y_0 + a_3y_0 = x_0^3 + a_2x_0^2 + a_4x_0 + a_6$ An interesting property of elliptic curves is that the points on this curve form a group under addition of these points. How this group law is defined is done in the next section.

Example 2.1. Consider $K = \mathbb{R}$ and define the elliptic curve E by

$$E/\mathbb{R}: \quad y^2 = x^3 - x.$$

Then E is a curve consisting of two parts, see figure 1.

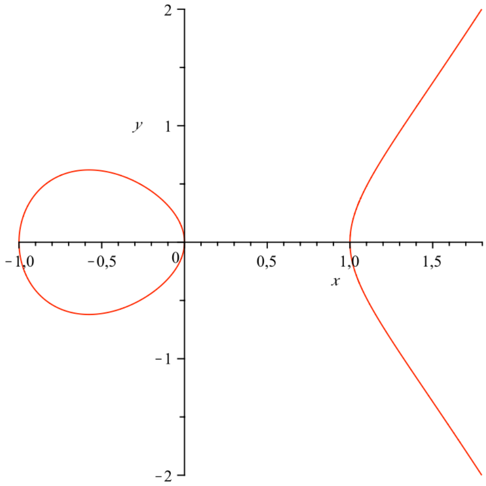

Figure 1: $E: \quad y^2 = x^3 - x$

2.2 Group law on elliptic curves

Let K be a field with $\mathrm{char}(K) = p \geq 3$. Suppose we have an elliptic curve defined by

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

where $a_2, a_4, a_6 \in K$. Take two points on this curve given by $\zeta_1 = (x_1, y_1)$ and $\zeta_2 = (x_2, y_2)$. Then the point $\zeta = \zeta_1 + \zeta_2$ is geometrically defined by drawing a line between ζ_1 and ζ_2, which intersects the curve in a third point $\zeta_3 = (x_3, y_3)$. The point ζ is now given by reflecting ζ_3 in the x-axis. When $\zeta_1 = \zeta_2$, drawing a line between ζ_1 and ζ_2 means drawing the tangent line to the elliptic curve at ζ_1, see also [19, III.2]. This process is shown in figure 2.

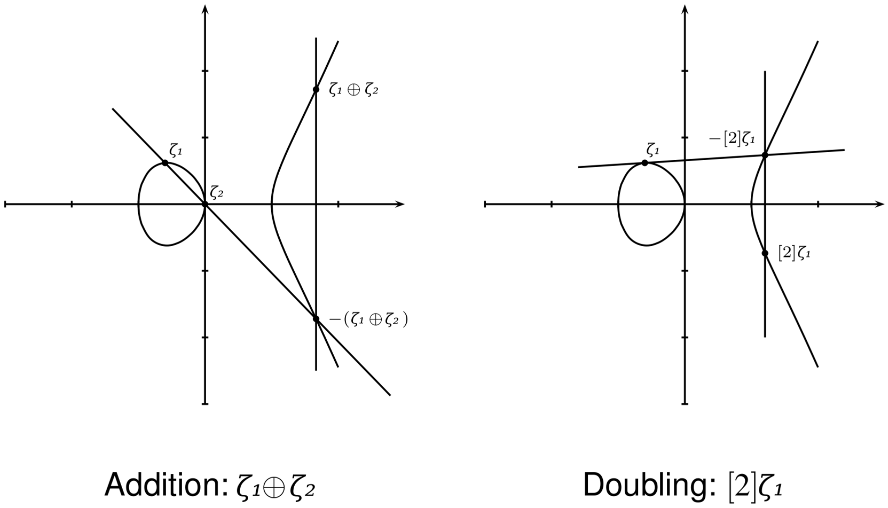

Figure 2: Addition and duplication formula

Doing this algebraically gives us that the line between ζ_1 and ζ_2 has a slope of

$$m = \begin{cases} \dfrac{y_1 - y_2}{x_1 - x_2} & \text{if } \zeta_1 \neq \zeta_2; \\ \dfrac{d/dx}{d/dy} = \dfrac{3x^2 + 2a_2x + a_4}{2y} & \text{if } \zeta_1 = \zeta_2; \\ \infty & \text{if } \zeta_1 = \zeta_2 = (\alpha, 0) \text{ with } \alpha \in K \end{cases}$$

The third case above is a special case. When $\zeta_1 = \zeta_2 = (\alpha, 0)$ for some $\alpha \in K$, we divide by zero in the second case, so we need to give a formula for this special case. When $y = 0$, the tangent line at ζ_1 will be a vertical line, and thus we will have $[2]\zeta_1 = \mathcal{O}$, yielding no problems. For the case $y \neq 0$, the line joining ζ_1 and ζ_2 is defined as $y = mx + B$ for $m, B \in K$. Substituting this equation into (2.2) gives us

$$\begin{aligned} &(mx + B)^2 = x^3 + a_2x^2 + a_4x + a_6 \\ \Rightarrow\ & x^3 - (m^2 - a_2)x^2 - (2mB - a_4)x - (B^2 - a_6) = 0. \end{aligned}$$

Now since this is the equation of a line intersecting an elliptic curve, there are three solutions given by ζ_1, ζ_2 and ζ_3. So by the property that we can write a polynomial in terms of its zeroes α_1, α_2 as $(x - \alpha_1)(x - \alpha_2) = x^2 - (\alpha_1 + \alpha_2)x + \alpha_1\alpha_2$, we know that $m^2 - a_2 = x_1 + x_2 + x_3$ and thus $x_3 = m^2 - a_2 - x_1 - x_2$. Furthermore we know that $x(\zeta_3) = x(\zeta) = x(\zeta_1 + \zeta_2)$ since reflecting in the x-axis doesn't change the x-coordinate. So, since we know $x(\zeta_3)$, we also know that $x(\zeta_1 + \zeta_2) = x(\zeta) = m^2 - a_2 - x_1 - x_2$. Writing this out yields

$$x(\zeta_1 + \zeta_2) = \left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2 - a_2 - (x_1 + x_2) \tag{2.3}$$

when $\zeta_1 \neq \zeta_2$ and

$$x([2]\zeta_1) = \left(\frac{3x_1^2 + 2a_2x_1 + a_4}{2y_1}\right)^2 - a_2 - 2x_1 \tag{2.4a}$$

$$= \frac{(f'(x_1))^2 - 4(2x_1 + a_2)f(x_1)}{4f(x_1)} \tag{2.4b}$$

when $\zeta_1 = \zeta_2$ and where $f(x) = x^3 + a_2x^2 + a_4x + a_6$. Here we found equation (2.4b) by writing the slope m in terms of $f(x)$ and $f'(x)$ and do the computation with these expressions. Furthermore, $[n]\zeta = \zeta + \zeta + ... + \zeta$ (n times) where $+$ denotes the addition on elliptic curves. There is one exception on formula (2.3). When we add two points $\zeta_1 = (0, \alpha) \in E$ and $\zeta_2 = (0, \beta) \in E$ with $\alpha \neq \beta$, we would divide by zero. But in this case, the line through ζ_1 and ζ_2 is a vertical line, so the third point of intersection with the curve is the point $\mathcal{O}$. Therefore, in this case, $\zeta_1 + \zeta_2 = \mathcal{O}$.
Summarizing we have the following cases:

- $\zeta_1 \neq \zeta_2$ and $(x(\zeta_1), x(\zeta_2)) \neq (0, 0)$. Then we can use formula (2.3), so

$$x(\zeta_1 + \zeta_2) = \left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2 - a_2 - (x_1 + x_2).$$

- $\zeta_1 \neq \zeta_2$ and $(x(\zeta_1), x(\zeta_2)) = (0,0)$. Then $\zeta_1 + \zeta_2 = \mathcal{O}$.
- $\zeta_1 = \zeta_2$ and $y(\zeta_1) = y(\zeta_2) \neq 0$. Then we can use formula (2.4a), so

$$x([2]\zeta_1) = \left(\frac{3x_1^2 + 2a_2x_1 + a_4}{2y_1}\right)^2 - a_2 - 2x_1.$$

- $\zeta_1 = \zeta_2$ and $y(\zeta_1) = y(\zeta_2) = 0$. Then $[2]\zeta_1 = \mathcal{O}$.

So these four formulas give us the addition law for elliptic curves. The addition law for elliptic curves written in other forms can be found in the same way, as we will see in later chapters.

2.3 Frobenius Map

We now consider the special case $K = \mathbb{F}_q$. Then according to [19, II.2], the Frobenius map is defined by

$$\phi : E \to E \tag{2.5}$$
$$(x, y) \mapsto (x^q, y^q). \tag{2.6}$$

Here E is an elliptic curve defined over $\mathbb{F}_q$. So ϕ raises the coordinates of a point $(x, y) \in E$ to the power q. In general, suppose L is a field with $\mathbb{F}_q$ as a subfield, and define

$$\begin{aligned} F : & L \to L \\ & \alpha \mapsto \alpha^q. \end{aligned}$$

Then the properties of the Frobenius map are given by the following lemma, see [7, pp.12]:

Lemma 2.1. *The map F satisfies the following properties:*

1. $(xy)^q = x^q y^q$*, so* $F(xy) = F(x)F(y)$
2. $(x + y)^q = x^q + y^q$*, so* $F(x + y) = F(x) + F(y)$
3. $\mathbb{F}_q = \{\alpha \in L | F(\alpha) = \alpha\}$.
4. *In the special case* $L = \mathbb{F}_q(t)$ *(the field of rational functions over* $\mathbb{F}_q$ *in a variable* t*), we have for* $\gamma(t) \in \mathbb{F}_q(t)$ *that* $\phi(\gamma(t)) = \gamma(t^q)$.

Since the proof is not necessary here, it is omitted. For the interested reader, see for example [7, pp.12]. Another property of the Frobenius map in $\mathbb{F}_q$ is that the map is bijective. To see this, check the injectivity and surjectivity in $\mathbb{F}_p$, and by the same reasons the bijectivity also holds in $\mathbb{F}_q$.

- **Injectivity**: By [18], a group homomorphism is injective if and only if the kernel is trivial, i.e. $\ker(\phi) = \{id\}$. By the properties 1 and 2 of lemma 2.1, we can conclude that $F : L \to L$ indeed is a group homomorphism. Furthermore, since there is a copy of $\mathbb{F}_q$ contained in L, i.e. $\mathbb{F}_q \subset L$, we know that $F(x) = 0$ implies $x = 0$ and thus the kernel is trivial. So indeed the map F is injective and thus also ϕ is injective.

- **Surjectivity**: We know ϕ is injective, and $\phi : \mathbb{F}_q \to \mathbb{F}_q$. By injectivity, 2 elements from $\mathbb{F}_q$ are mapped to different elements in $\mathbb{F}_q$. This yields that all elements in $\mathbb{F}_q$ should be reached because $\mathbb{F}_q$ and $\mathbb{F}_q$ have the same number of elements. So indeed ϕ is surjective.

So indeed we have that ϕ is a bijective map in $\mathbb{F}_q$.
Knowing these properties of the Frobenius map, we have all the required information about this map.

3 Hasse's Theorem: Case $\mathrm{char}(\mathbb{F}_q) \geq 3$

3.1 Stating the theorem

Start with taking an arbitrary prime number p and a random number $r \in \mathbb{N}$. Then define $q := p^r$. For this q, we consider the finite field $\mathbb{F}_q$. Also, take a general Weierstrass elliptic curve given by

$$E/\mathbb{F}_q : \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{3.1}$$

Then for this curve over the field $\mathbb{F}_q$ for general q we can define the Hasse theorem on elliptic curves.

Theorem 3.1 (Hasse's Theorem on Elliptic Curves)**.** *Take $a_1, \cdots, a_6 \in \mathbb{F}_q$ such that the discriminant $\Delta \neq 0$. Then the number $\#E(\mathbb{F}_q)$ of points over $\mathbb{F}_q$ on the elliptic curve E given by*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{3.2}$$

satisfies the inequality

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

The proof of theorem 3.1 in the way Manin did must be split in several cases. First we transform the curve (3.1) to an easier curve only valid in some characteristics. Then the proof of theorem 3.1 will be given in all these cases. In [5, 8.1, thm.3], the theorem is stated when $\mathrm{char}(\mathbb{F}_q) \geq 5$. In this case we have

Theorem 3.2 (Hasse's Theorem on Elliptic Curves, case $\mathrm{char}(\mathbb{F}_q) \geq 5$)**.** *Take $a_4, a_6 \in \mathbb{F}_q$ such that the discriminant $\Delta = -4a_4^3 - 27a_6^2 \neq 0$. Then the number $\#E(\mathbb{F}_q)$ of points over $\mathbb{F}_q$ on the elliptic curve E given by*

$$y^2 = x^3 + a_4x + a_6 \tag{3.3}$$

satisfies the inequality

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

For above elliptic curve we have that when considering $\mathrm{char}(\mathbb{F}_q) = 3$ the j-invariant of E is given by

$$\begin{aligned} j(E) &= 1728\frac{4a_2^3}{4a_2^3 + 27a_4^2} \\ &= 1728 \mod 3 \\ &= 0 \mod 3 \end{aligned}$$

and thus we only deal with a subset of the set of elliptic curves. This is because for every $j_0 \in \mathbb{F}_q$ there exists an elliptic curve E over $\mathbb{F}_q$ with $j(E) = j_0$. Since for the curve (3.3) we have $j(E) = 0$ always, we don't cover all elliptic curves in $\mathbb{F}_q$. So we want to modify the curve a bit to include the case $p = 3$. To do this, start again with the curve (3.2). Then by completing the squares on the left hand side we can rewrite the curve. So define $y' = y - a_1x - a_3$ and rewrite the coefficients to get as new curve

$$y^2 = x^3 + a_2x^2 + a_4x + a_6. \tag{3.4}$$

Then following [19, III.1] the discriminant and j-invariant of the elliptic curve (3.4) are given by

$$\begin{aligned}\Delta &= -256a_2^3a_6 + 64a_2^2a_4^2 + 8a_4^3,\\ j(E) &= \frac{16^3(a_2^2 - 3a_4)^3}{-256a_2^3a_6 + 64a_2^2a_4^2 + 8a_4^3}.\end{aligned}$$

Considering this last j-invariant in characteristic 3 gives us

$$j(E) = \frac{a_2^5}{a_2^3a_6 + a_2^2a_4^2 + 2a_4^3}$$

which indeed can take all values $j_0 \in \mathbb{F}_q$ for $q = 3^r$. This rewriting of elliptic curves changes the Hasse theorem 3.2 into

Theorem 3.3 (Hasse's Theorem on Elliptic Curves, case char($\mathbb{F}_q$) ≥ 3)**.** *Take $a_2, a_4, a_6 \in \mathbb{F}_q$ such that the discriminant $\Delta \neq 0$. Then the number $\#E(\mathbb{F}_q)$ of points over $\mathbb{F}_q$ on the elliptic curve E given by*

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

satisfies the inequality

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

In this form the theorem can be proven for char($\mathbb{F}_q$) ≥ 3. This will be done in the next section. The case char($\mathbb{F}_q$) $= 2$ changes the elliptic curve (3.1) to another form again, and thus also the theorem changes. This case will be treated in the chapters 4 and 5.

3.2 Proof of theorem 3.3

In this section we will give a proof of theorem 3.3 based on Manins paper [15] and Chahal's expositions [5],[6]. We will need three lemmas, in this section we will only state them. In the next section, all these lemmas will be proven.
During the whole proof, we will use the following notation:

- $q = p^r$ for some prime $p \neq 2$ and some $r \in \mathbb{N}$, $r \neq 0$,
- $K = \mathbb{F}_q(t)$, the function field in t over $\mathbb{F}_q$.

Given the elliptic curve $E/\mathbb{F}_q$ as in the statement of theorem 3.3, define the elliptic curve

$$E^{tw}/\mathbb{F}_q(t): \quad f(t)y^2 = x^3 + a_2x^2 + a_4x + a_6 \tag{3.5}$$

where

$$f(t) = t^3 + a_2t^2 + a_4t + a_6. \tag{3.6}$$

According to [19, App.A prop.1.2.b], these two curves are isomorphic over a finite field extension L of K, namely, over $L := K(s)$ where s satisfies the relation $s^2 = f(t)$, which on itself is an elliptic curve. With this extension, one has the isomorphism

$$\begin{aligned}\phi :& E \to E^{tw}\\ (x, y) \mapsto & (x, \frac{1}{\sqrt{f(t)}}y) = (x, \frac{1}{s}y)\end{aligned}$$

This means that E^{tw} forms a twist of E. The theory about finding a twisted curve for char($\mathbb{F}_q$) = 2 is treated in appendix B. For char($\mathbb{F}_q$) we only give the twisted curve (3.5).

Consider the group $E^{tw}(K) = \{(x, y) \in K | (x, y) \in E^{tw}\} \cup \{\mathcal{O}\}$. We have already found the duplication formulas (2.3) and (2.4a) for a curve $y^2 = x^3 + a_2x^2 + a_4x + a_6$. To find the duplication formulas for the curve (3.5), we have to modify these formulas a little bit by writing $f(t)y^2$ instead of y^2, yielding

$$x(\zeta_1 + \zeta_2) = f(t)\left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2 - a_2 - (x_1 + x_2) \tag{3.7}$$

when $\zeta_1 \neq \zeta_2$ and

$$\begin{aligned}x([2]\zeta_1) &= \left(\frac{3x_1^2 + 2a_2x_1 + a_4}{2\sqrt{f(t)}y_1}\right)^2 - a_2 - 2x_1\\ &= \frac{(f'(x_1))^2}{4f(t)y_1^2} - a_2 - 2x_1\\ &= \frac{(f'(x_1))^2 - 4(2x_1 + a_2)f(x_1)}{4f(x_1)} \end{aligned}\tag{3.8}$$

when $\zeta_1 = \zeta_2$ not of order 2. When $\zeta_1 = \zeta_2$ is of order 2, we have $[2]\zeta_1 = \mathcal{O}$. We need to know these equations because we want to formulate a recursion formula. To do this, we also need to know some starting points which are solutions of (3.5).

We know on the elliptic curve (3.4) we have two solutions over $L = \mathbb{F}_q(t, s)$ where s satisfies the relation $s^2 = f(t)$, namely $id = (t, s)$ and the image of the Frobenius map, (t^q, s^q). Under the isomorphism ϕ, on E^{tw} these points become

$$\begin{aligned}Q &= (t, 1)\\ P_0 &= (t^q, s^{q-1}) = (t^q, (t^3 + at + b))^{(q-1)/2} =: (x_0, y_0)\end{aligned}$$

as can be seen easily. Now we define a recursion formula by

$$P_n = P_0 + nQ$$

where $n \in \mathbb{Z}$. In the case $P_n \neq \mathcal{O}$, we can write $P_n = (x_n, y_n)$ yielding

$$(x_n, y_n) = (x_0, y_0) + n(t, 1). \tag{3.9}$$

Since both P_0 and Q form a solution of (3.5), also their sum P_n is a solution (since $E(\mathbb{F}_q)$ is a group). The next step is to derive an identity which helps us to prove theorem 3.3. Therefore, write $x_n = \frac{f_n}{g_n}$ in lowest form, where f_n is a monic polynomial in $\mathbb{F}_q[t]$. Define the function: $d : \mathbb{Z} \to \{0, 1, 2, 3, ...\}$ by

$$d(n) = d_n = \begin{cases} 0 & \text{if } P_n = \mathcal{O};\\ \deg(f_n) & \text{otherwise.}\end{cases}$$

As an example,

$$d(0) = \deg(t^q) = q.$$

We need this definition because of the following important lemma.

Lemma 3.1 (Basic Identity). $d_{n-1} + d_{n+1} = 2d_n + 2$.

The connection between theorem 3.3 and the function $d(n)$ defined above is given by the following lemma.

Lemma 3.2. $d_{-1} = \#E(\mathbb{F}_q)$.

Finally, we have

Lemma 3.3. *The function $d(n)$ is a quadratic polynomial in n. In fact,*

$$d(n) = d_n = n^2 - (\#E(\mathbb{F}_q) - (q+1))n + q$$

The proof of this last lemma can be given by combining the lemmas 3.1 and 3.2 and applying induction with respect to n. Here, the proof is omitted. For the interested reader, see for example [5, lemma 8.5]. By the last lemma, we can prove theorem 3.3. Consider the quadratic polynomial

$$d(x) = x^2 - (\#E(\mathbb{F}_q) - (q+1))x + q.$$

Then $d(x) \geq 0$ for all $x \in \mathbb{Z}$, which can be seen from the definition of $d(x)$: $d(x) = d(n)$ is defined as either 0 or the degree of the numerator of x_n, which is positive. Now consider the discriminant of $d(x)$, given by

$$D = (\#E(\mathbb{F}_q) - (q+1))^2 - 4q.$$

We will show that $D \leq 0$. Suppose this is false, so that $D > 0$. Then $d(x)$ has two real roots $\alpha < \beta$. Now use that $d(x)$ is a quadratic polynomial (and thus its graph is a parabola) and that $d(n) \geq 0$ for all integers n. See also figure 3, where the intersections with the x-axis are the roots α, β. On the open interval (α, β) the values of $d(x)$ are negative, so this interval contains no integers. Call k the largest integer such that $k \leq \alpha < k+1$. Also $k+1$ is an integer and thus $d(k+1) \geq 0$. This means that for $k+1$ it must hold that $k+1 \geq \beta$ since β is on the boundary between positive and negative values. Hence, $k \leq \alpha < \beta \leq k+1$, and thus $0 \leq \beta - \alpha \leq 1$. Then considering the discriminant D of $d(x)$ we have

$$1 \geq D = (\beta - \alpha)^2 = (\alpha + \beta)^2 - 4\alpha\beta = D \in \mathbb{Z}_{>0}$$

so it follows $D = 1$ and thus $\beta = \alpha + 1$. Since the interval $(\alpha, \beta) = (\alpha, \alpha + 1)$ contains no integers, it follows $\alpha = k \in \mathbb{Z}$. So the roots of $d(x)$ are two succesive integers. But this is impossible, since we can factorize $d(x)$ in terms of its roots, so $d(x) = (x-k)(x-(k+1)) = x^2 - (2k+1)x + k(k+1)$. This means that $q = k(k+1)$. Since $k(k+1)$ is always even (the product of two successive integers is even) but q itself is odd, we have a contradiction. So we can't have $D > 0$. So $D \leq 0$, which proves theorem 3.3. □

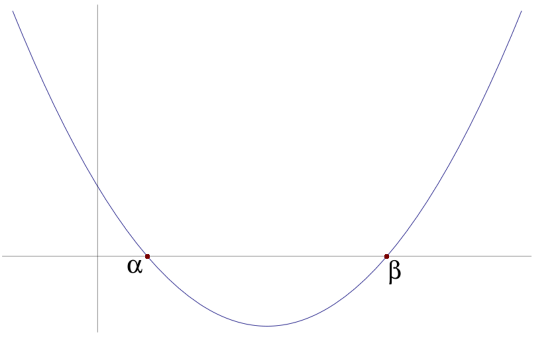

Figure 3: Illustration of the case $D > 0$.

3.2.1 Examples

In this subsection we will show that it is possible indeed to have $D = 0$ and $D < 0$.
We have $D = 0 \Leftrightarrow (\#E(\mathbb{F}_q) - (q+1))^2 = 4q$. This is possible only if q is a square and $\#E(\mathbb{F}_q) = q \pm 2\sqrt{q}$. Such elliptic curves exist: for example, take $q = 9$ and

$$E/\mathbb{F}_9 : \quad y^2 = x^3 + x^2 + x + 1.$$

Here $\mathbb{F}_9 = \mathbb{F}_3[\alpha]/ < \alpha^2 + 1 >$, so that α is a zero of the polynomial $x^2 + 1$. Then E contains the following points:

$$\begin{aligned} E(\mathbb{F}_q) = \{&(0, \pm 1), (1, \pm 1), (\alpha, \pm(\alpha + 2)), (2\alpha, \pm \alpha), \\ &(2\alpha + 1, \pm(\alpha + 1)), (2\alpha + 2, \pm(\alpha + 2)), (\alpha, 0), \mathcal{O}\} \end{aligned}$$

so 7 x-coordinates yielding two solutions, the point at infinity $\mathcal{O}$ and $(2, 0)$ of order 2 since also $(2, -0)$ should be a solution but this is the same point. So in total there are 16 points. This yields

$$\begin{aligned} d(x) &= x^2 - (\#E(\mathbb{F}_q) - (q+1))x + q \\ &= x^2 - (16 - (9+1))x + 9 \\ &= (x-3)^2 \end{aligned}$$

and thus there is a double zero, so we indeed have $D = 0$.
The other case, $D < 0$, is the case whenever q is not a square, as we saw above. But also for q a square $D < 0$ occurs. Take for example $q = 9$ and the curve

$$E/\mathbb{F}_q : \quad y^2 = x^3 + x^2 + 1.$$

Then we have the following points:

$$\begin{aligned} E(\mathbb{F}_q) = \{&(0, \pm 1), (2, \pm 1), (\alpha, \pm(\alpha + 1)), (2\alpha, \pm(\alpha + 2)), \\ &(1, 0), (\alpha + 2, 0), (2\alpha + 2, 0), \mathcal{O}\} \end{aligned}$$

where the points $(1, 0), (\alpha + 2, 0), (2\alpha + 2, 0)$ are all points of order 2. So in total there are 12 points, yielding

$$d(x) = x^2 - (12 - (9+1))x + 9 = x^2 - 2x + 9$$

and thus $D = 4 - 36 = -32 < 0$.

3.3 Proof of the lemmas

In this section the lemmas 3.2 and 3.1 will be proven. Because of the difficulty of the basic identity, this lemma will be the last one to prove.

3.3.1 Proof of lemma 3.2

In this subsection we want to prove $d_{-1} = \#E(\mathbb{F}_q)$.

Proof. Use the recursion formula $P_n = P_0 + nQ$ together with the addition formula (3.7) to get $(x_{-1}, y_{-1}) = (x_0, y_0) - (t, 1) = (x_0, y_0) + (t, -1)$ (assuming $P_n \neq \mathcal{O}$), see [19, III.2, alg. 2.3] and thus (using the Frobenius map)

$$\begin{aligned}
x_{-1} &= f(t)\left(\frac{y_0+1}{x_0-t}\right)^2 - a_2 - (x_0+t) \\
&= \frac{(t^3+a_2t^2+a_4t+a_6)\left[(t^3+a_2t^2+a_4t+a_6)^{(q-1)/2}+1\right]^2}{(t^q-t)^2} - a_2 - (t^q+t) \\
&= \frac{(f(t))^q + 2(f(t))^{(q-1)/2} + f(t)}{(t^q-t)^2} - a_2 - (t^q+t) \\
&= \frac{(t^{3q}+a_2t^{2q}+a_4t^q+a_6) + 2(t^3+a_2t^2+a_4t+a_6)^{(q-1)/2}}{(t^q-t)} \\
&\quad \frac{-a_2(t^{2q}-3t^{q+1}+t^2) - (t^{3q}-t^{2q+1}-t^{q+2}+t^3)}{(t^q-t)} \\
&= \frac{t^{2q+1}+R(t)}{(t^q-t)^2}
\end{aligned}$$

where $R(t)$ is a polynomial in t of order at most $2q$ (so that the degree of $R(t)$ is smaller than $2q+1$). But to find $d_{-1} = \deg(x_{-1})$, we first need to put x_{-1} in lowest terms, so we must check if there are common terms in numerator and denominator. Therefore consider the polynomial $(t^q - t)^2 = \prod_{\alpha \in \mathbb{F}_q} (t-\alpha)^2$. Then we can write

$$x_{-1} = \frac{(t^3+a_2t^2+a_4t+a_6)\left[(t^3+a_2t^2+a_4t+a_6)^{(q-1)/2}+1\right]^2}{\prod_{\alpha\in\mathbb{F}_q}(t-\alpha)^2} - a_2 - (t^q+t).$$

It suffices to compute which terms cancel from the first part of above formula. There are two terms that can cancel:

1. The $\alpha \in \mathbb{F}_q$ for which $(\alpha^3 + a_2\alpha^2 + a_4\alpha + a_6)^{(q-1)/2} = -1$, since then the square of the numerator equals zero, so α is a double zero (since α is also a double zero of the denominator), so $(t-\alpha)^2$ can be taken out from both numerator and denominator.

2. The $\alpha \in \mathbb{F}_q$ for which $f(\alpha) = \alpha^3 + a_2\alpha^2 + a_4\alpha + a_6 = 0$, since then the numerator equals zero, so α is a zero of $f(t)$ and not of the other factor of the numerator. Since by assumption $f(t)$ has only simple zeroes, $(t-\alpha)$ can be taken out from both numerator and denominator exactly once.

Denote by m the number of factors of type 1 and by n the number of factors of type 2. Then $d_{-1} = \deg(f_{-1}) = 2q + 1 - \text{(common factors)} = 2q + 1 - 2m - n$

because the common factors of type 1 count twice.
Now we have an expression for d_{-1}, so we need an expression for $\#E(\mathbb{F}_q)$. We know $\#E(\mathbb{F}_q) = (\#\text{points on } y^2 = x^3 + a_2x^2 + a_4x + a_6)$. This means we are looking for points (u, v) on the curve E. Take an $u \in \mathbb{F}_q$ arbitrary. Then there are three options.

1. $f(u) = 0$. Then we have $y^2 = f(u) = 0$ and thus there is exactly one solution, namely $(u, 0)$. If we recall the definition of n we can see that the total number of solutions of this type is n.

2. $f(u) \neq 0$ and $f(u)$ is no square. Then obviously there is no solution for the equation $y^2 = f(u)$.

3. $f(u) \neq 0$ and $f(u)$ is a square. This means $f(u) \in \mathbb{F}_q^{*2}$, which is equivalent with $f(u)^{(q-1)/2} = 1$. Then there are two solutions, namely $(u, \pm\sqrt{f(u)})$. Now we can use the following lemma:

   Lemma 3.4. *The map $\psi : \mathbb{F}_q* \to \mathbb{F}_q*$ mapping x to $x^{(q-1)/2}$ has the following properties:*

   - *ψ is a homomorphism of groups;*
   - *The image of ψ is given by $\{\pm 1\}$;*
   - *$\mathbb{F}_q * / \ker \simeq \{\pm 1\}$.*

   Using this lemma we have that the kernel of ψ is given by $\mathbb{F}_q^{*2}$ and thus the number of elements u giving two solutions is given by $q - m - n$. To see this, recall the definitions of m and n: n is the number of elements of type 2 and m is the number of elements u such that $f(u) = -1$. So the number of u with $f(u) = 1$ is

   $$\text{total}\#u - \#\{u|f(u) = 0\} - \#\{u|f(u) = -1\} = q - n - m.$$

   Since each u gives two solutions, we have that the number of solutions in this case is given by $2(q - n - m)$.

In total this gives that the number of solutions is $\#E(\mathbb{F}_q) = n+2(q-m-n)+1 = 2(q - m) - n + 1 = d_{-1}$ as the lemma stated. □

3.3.2 Proof of lemma 3.1

The second, and most difficult lemma is the basic identity: $d_{n-1} + d_{n+1} = 2d_n + 2$. The proof of the basic identity consists of two parts. The first part is proving the following lemma.

Lemma 3.5. *If $P_n \neq \mathcal{O}$, then writing $P_n = \left(\frac{f_n}{g_n}, y_n\right)$, it follows* $\deg(f_n) > \deg(g_n)$*. In particular, $x_n \neq 0$.*

Before proving this lemma, note: this lemma implies that the definition of the numbers d_n used in the basic identity changes to $d_n = 0 \Leftrightarrow P_n = \mathcal{O}$ (where first we had: $d_n = 0$ if $P_n = \mathcal{O}$). This result follows from considering the map $[n] + F$ where F denotes the Frobenius map. The actual proof of above note is omitted here.

Proof. We start by taking our elliptic curve (3.5) defined by

$$E^{tw}/\mathbb{F}_q(t) : (t^3 + a_2t^2 + a_4t + a_6)y^2 = x^3 + a_2x^2 + a_4x + a_6.$$

The next step is to consider $\mathbb{F}_q(t)$ as the function field of the projective line $\mathbb{P}^1$ over $\mathbb{F}_q$, and take the valuation v_∞ on $\mathbb{F}_q(t)$ corresponding to the point $\infty \in \mathbb{P}^1$, see [22, pp.2-10]. So $v_\infty(t) = -1$ and

$$v_\infty\left(\frac{f(t)}{g(t)}\right) = \deg(g(t)) - \deg(f(t)).$$

Then we can define a valuation ring at the point at infinity by

$$O_\infty = \left\{\frac{f}{g} \in \mathbb{F}_q(t) : v\left(\frac{f}{g}\right) \geq 0\right\}.$$

This valuation ring is even a local ring , which means that O_∞ has a unique maximal ideal $\mathcal{M}_\infty = O_\infty \backslash O_\infty^\times$ with $O_\infty^\times$ the group of units of O_∞, so here

$$O_\infty^\times = \left\{\frac{f}{g} \in \mathbb{F}_q(t) : v\left(\frac{f}{g}\right) = 0\right\}.$$

The maximal ideal of the local ring is given by

$$\mathcal{M} = \left\{\frac{f}{g} \in \mathbb{F}_q(t) : v\left(\frac{f}{g}\right) > 0\right\}$$

and $O_\infty/\mathcal{M} = \mathbb{F}_q$. Now a generator for $\mathcal{M}$ is an element x such that $v(x) = 1$. Then obviously a generator is given by $\frac{1}{t}$.

Now we have defined a valuation of $\mathbb{F}_q(t)$, we want to reduce our curve E^{tw} modulo $\mathcal{M}$ to an easier curve. To reduce E^{tw} modulo $\mathcal{M}$, we have to write E^{tw} in terms of the generator of $\mathcal{M}$, so in terms of $\frac{1}{t}$. Doing this with $\xi := \frac{x}{t}$, we get

$$\begin{aligned}
&(t^3 + a_2t^2 + a_4t + a_6)y^2 = x^3 + a_2x^2 + a_4x + a_6\\
\Rightarrow\ &(1 + a_2\frac{1}{t} + a_4\frac{1}{t^2} + a_6\frac{1}{t^3})y^2 = \left(\frac{x}{t}\right)^3 + a_2\frac{1}{t}\left(\frac{x}{t}\right)^2 + a_4\frac{1}{t^2}\left(\frac{x}{t}\right) + a_6\frac{1}{t^3}\\
\Rightarrow\ &(1 + a_2\frac{1}{t} + a_4\frac{1}{t^2} + a_6\frac{1}{t^3})y^2 = \xi^3 + a_2\frac{1}{t}\xi^2 + a_4\frac{1}{t^2}\xi + a_6\frac{1}{t^3}
\end{aligned}$$

Reducing $\mod \frac{1}{t}$ gives

$$\tilde{E}^{tw}/\mathbb{F}_q : y^2 = \xi^3$$

which is our new, reduced curve. Now if we make a plot of this new curve, we can easily see that there is a cusp at $\xi = 0$, so according to [19, VII.5], E^{tw} has bad, additive reduction and thus, according to [19, thm.VII.5.1], we have $\tilde{E}^{tw}_{ns}(\mathbb{F}_q) \simeq (\mathbb{F}_q, +)$, where for $F(x,y) = y^2 - f(x)$, $\tilde{E}^{tw}_{ns}$ is the reduced part of

$$E^{tw}_{ns} := \left\{(x_0, y_0) \in \mathbb{F}_q(t) \times \mathbb{F}_q(t) | (x_0, y_0) \in E^{tw}, \left(\frac{\partial F}{\partial x}, \frac{\partial F}{\partial y}\right)|_{(x_0,y_0)} \neq (0,0)\right\} \cup \{\mathcal{O}\}.$$

By [19, thm.VII.5.1], E^{tw}_{ns} is a group.

Now we look at the points on the curve.

- We know $Q = (t, 1) \in E^{tw}(\mathbb{F}_q(t))$, where the curve E^{tw} is given by

  $$(f(t)y^2 = f(x).$$

  Now writing the curve in terms of ξ means mapping the x-coordinate to $\frac{x}{t}$. So the point $(t, 1)$ will be mapped to $(\frac{t}{t}, 1) = (1, 1)$ and this point will stay the same under reduction modulo $\frac{1}{t}$. Then we can conclude Q reduces to a nonsingular point and thus $Q = (t, 1) \in E^{tw}_{ns}$.

- Another point on E^{tw} is given by $P_0 = (t^q, y)$ where $y = (f(t))^{(q-1)/2}$. Under the mapping $x \mapsto \frac{x}{t}$ this point reduces to $(t^{q-1}, \tilde{y})$. Now this point does change if we reduce modulo $\mathcal{M}$. Consider the valuation of this point, given by $v(t^{q-1}) = -(q-1) = 1-q$. Since $q \geq 3$ (because $p \geq 3$) we have that $v(t^{q-1}) \leq 0$, and thus the point will reduce to $\mathcal{O} = (0 : 1 : 0)$. So the point (t^{q-1}, y') has good reduction.

So a question arises. What points of $E^{tw}(\mathbb{F}_q(t))$ do lie in $E^{tw}_{ns}(\mathbb{F}_q(t))$? To answer this question, consider the following lemma.

Lemma 3.6. *For an arbitrary point $\zeta = (\frac{f}{g}, y) \in E^{tw}(\mathbb{F}_q(t))$, we have $\zeta \in E^{tw}_{ns}(\mathbb{F}_q(t))$ if $\deg(f) > \deg(g)$.*

Proof. Take $\zeta = (\frac{f}{g}, y) \in E^{tw}(\mathbb{F}_q(t))$. Then $\xi(\zeta) = (\frac{f}{gt}, \tilde{y})$ (since we are only interested in the x-coordinate, ignore the y-coordinate). Now we apply reduction modulo $\mathcal{M}$.

- Suppose $v(f) = v(tg)$. Then $v\left(\frac{f}{tg}\right) = 0$, so $\frac{f}{tg} \in O^\times$ which means $\frac{f}{tg} \notin \mathcal{M}$, so $\frac{f}{tg} \mod \mathcal{M} \neq 0$.

- Suppose $v(f) > v(tg)$. Then $v\left(\frac{f}{tg}\right) > 0$, so $\frac{f}{tg} \in \mathcal{M}$ which means $\frac{f}{tg} \mod \mathcal{M} = 0$.

- Suppose $v(f) < v(tg)$. Then $v\left(\frac{f}{tg}\right) < 0$, so $\frac{f}{tg} \mapsto (0 : 1 : 0)$.

From this we can conclude that a point is in $E^{tw}_{ns}(\mathbb{F}_q(t))$ if $v(f) \leq v(tg)$ since then the point ζ does not reduce to 0, so there is good reduction. So:

$$\begin{aligned}
&v(f) \leq v(tg) \\
&\Rightarrow -\deg(f) \leq -1 - \deg(g) \\
&\Rightarrow \deg(f) \geq 1 + \deg(g) \\
&\Rightarrow \deg(f) > \deg(g).
\end{aligned}$$

□

With proving this lemma, we have also proven the lemma that when $(x_n, y_n) \neq \mathcal{O}$ it must follow that $\deg(f_n) > \deg(g_n)$. That $x_n \neq 0$ follows from the reduction modulo $\mathcal{M}$. □

After proving this, we can prove the basic identity. First we consider three special cases before proving the general case.

- Assume $P_{n-1} = \mathcal{O}$. Then using $P_n = P_{n-1} + Q$ we have $P_n = Q$, hence $x_n = t$. Also, $P_{n+1} = P_n + Q = 2Q = 2(t, 1)$. By the duplication formula (3.8):

$$\begin{aligned} x(P_{n+1}) = x_{n+1} &= \frac{t^4 - 2a_4t^2 - 8a_6t + a_4^2 - 4a_2a_6}{4(t^3 + a_2t^2 + a_4t + a_6)} \\ &= \frac{(f'(t))^2 - 4(2t + a)f(t)}{4f(t)}. \end{aligned}$$

  Since $\gcd(4f(t), \text{numerator}) = \gcd(f(t), (f'(t))^2) = 1$ (which follows from the fact that $f(t)$ has no multiple zeroes since it is an elliptic curve) we have $d_{n+1} = 4$ since numerator and denominator have no common terms. Furthermore, $d_{n-1} = 0$ and $d_n = 1$ which yields the desired identity.

- Assume $P_n = \mathcal{O}$. Then $P_{n-1} = P_n - Q = -(t, 1) = (t, -1)$ and $P_{n+1} = P_n + Q = (t, 1)$. This gives $d_n = 0$ and $d_{n-1} = d_{n+1} = 1$, which yields the desired identity.

- Assume $P_{n+1} = \mathcal{O}$. Then $P_n = P_{n+1} - Q = -(t, 1) = (t, -1)$ and $P_{n-1} = P_n - Q = 2(t, -1)$. By the duplication formula (3.8):

$$x(P_{n-1}) = x_{n-1} = \frac{t^4 - 2a_4t^2 - 8a_6t + a_4^2 - 4a_2a_6}{4(t^3 + a_2t^2 + a_4t + a_6)}.$$

  So by the same argument used above, $d_{n-1} = 4$, $d_n = 1$ and $d_{n+1} = 0$, which yields the desired identity.

So we have seen that in these 3 special cases the basic identity holds. Now we want to prove the identity for the general case, where we may assume $P_{n-1}, P_n, P_{n+1} \neq \mathcal{O}$. First write

$$\begin{aligned} P_{n-1} &= P_n - Q \\ \Rightarrow (x_{n-1}, y_{n-1}) &= (x_n, y_n) + (t, -1). \end{aligned}$$

Then by the addition formula (3.7) we have

$$x_{n-1} = f(t)\left(\frac{y_n + 1}{x_n - t}\right)^2 - a_2 - (x_n + t).$$

Writing $x_n = \frac{f_n}{g_n}$ and writing everything with common denominators, we get

$$\begin{aligned} x_{n-1} &= \frac{f_{n-1}}{g_{n-1}} \\ &= \frac{-(tg_n - f_n)^2((t + a_2)g_n + f_n) + f(t)(1 + y_n)^2 g_n^3}{g_n(f_n - tg_n)^2} && (3.10a) \\ &= \frac{(tf_n + a_4g_n)(f_n + tg_n) + 2a_2tf_ng_n + 2a_6g_n^2 + 2f(t)g_n^2y_n}{(f_n - tg_n)^2} && (3.10b) \\ &= \frac{R}{(f_n - tg_n)^2}. && (3.10c) \end{aligned}$$

In exactly the same way we get

$$\begin{aligned} x_{n+1} &= \frac{f_{n+1}}{g_{n+1}} \\ &= \frac{-(tg_n - f_n)^2((t+a_2)g_n + f_n) + f(t)(1-y_n)^2 g_n^3}{g_n(f_n - tg_n)^2} && (3.11a) \\ &= \frac{(tf_n + a_4 g_n)(f_n + tg_n) + 2a_2 t f_n g_n + 2a_6 g_n^2 - 2f(t)g_n^2 y_n}{(f_n - tg_n)^2} && (3.11b) \\ &= \frac{S}{(f_n - tg_n)^2}. && (3.11c) \end{aligned}$$

Then we can multiply the above equations to get (after some manipulations of the formulas)

$$\begin{aligned} x_{n-1}x_{n+1} &= \frac{f_{n-1}f_{n+1}}{g_{n-1}g_{n+1}} && (3.12a) \\ &= \frac{RS}{(f_n - tg_n)^4} && (3.12b) \\ &= \frac{(tf_n - a_4 g_n)^2 - 4a_6 g_n(f_n + (t+a_2)g_n)}{(f_n - tg_n)^2}. && (3.12c) \end{aligned}$$

Note that the numerator in (3.12a) has degree $\deg(f_{n-1}f_{n+1}) = d_{n-1} + d_{n+1}$ and the numerator in (3.12c) has (using lemma 3.5) degree $\deg(t^2 f_n^2) = 2\deg(t) + 2\deg(f_n) = 2 + 2d_n$. So the basic identity will follow if we show that

$$g_{n-1}g_{n+1} \text{ and } (f_n - tg_n)^2 \text{ differ by a nonzero constant.}$$

We show this by proving that every irreducible polynomial $l(t) \in \mathbb{F}_q[t]$ divides $g_{n-1}g_{n+1}$ as many times as it divides $(f_n - tg_n)^2$. Therefore, consider the valuation map

$$v_l : \mathbb{F}_q(t) \to \mathbb{Z} \cup \{\infty\}$$

defined as the number of times l appears in the factorization of a polynomial, so if we can write $P = l^m Q$ for some polynomials P and Q, then $v_l(P) = m$. Then to prove the basic identity, we want to use what is said above, so we want to show that

$$v_l(g_{n-1}g_{n+1}) = v_l((f_n - tg_n)^2). \tag{3.13}$$

First consider equation (3.10c). We claim $R \in \mathbb{F}_q[t]$. Obviously $(tf_n + a_4 g_n)(f_n + tg_n) + 2a_2 t f_n g_n + 2a_6 g_n^2 \in \mathbb{F}_q[t]$, so consider $y_n f(t) g_n^2$. Since $P = \left(\frac{f_n}{g_n}, y_n\right) \in E^{tw}(\mathbb{F}_q(t))$, using the elliptic curve $f(t)y^2 = x^3 + a_2x^2 + a_4x + a_6$, we get

$$\begin{aligned} (f(t)g_n^2 y_n)^2 &= f(t) \cdot g_n^4 \cdot f(t) y_n^2 \\ &= f(t) \cdot g_n^4 \cdot \left(\frac{f_n^3}{g_n^3} + a_2\frac{f_n^2}{g_n^2} + a_4\frac{f_n}{g_n} + a_6\right) \\ &= f(t)\left(f_n^3 g_n + a_2 f_n^2 g_n^2 + a_4 f_n g_n^3 + a_6 g_n^4\right) \end{aligned}$$

and this last formula is a polynomial in $\mathbb{F}_q[t]$, so indeed $f(t)y_n g_n^2 \in \mathbb{F}_q[t]$ and thus also $R \in \mathbb{F}_q[t]$. In exactly the same way we have $S \in \mathbb{F}_q[t]$.
As $\frac{f_{n-1}}{g_{n-1}}$ and $\frac{f_{n+1}}{g_{n+1}}$ are written in lowest terms, from $x_{n-1} = \frac{R}{(f_n - tg_n)^2} = \frac{f_{n-1}}{g_{n-1}}$ and

$x_{n+1} = \frac{S}{(f_n - tg_n)^2} = \frac{f_{n+1}}{g_{n+1}}$ we can conclude that $f_{n-1} \mid R$ and $g_{n-1} \mid (f_n - tg_n)^2$ and in the same way, $f_{n+1} \mid S$, $g_{n+1} \mid (f_n - tg_n)^2$. This means that at least we have $v_l(g_{n\pm1}) \leq v_l((f_n - tg_n)^2)$. Furthermore, we can extend this statement to a stronger statement.

Lemma 3.7. $v_l(g_{n-1}g_{n+1}) \leq v_l((f_n - tg_n)^2)$.

Proof. Consider equation (3.12b). This fraction can be simplified to the one in equation (3.12c). It follows that $(f_n - tg_n)^2) \mid RS$. So there exist polynomials $R_1 \mid R$ and $S_1 \mid S$ such that $(f_n - tg_n)^2 = R_1S_1$. This means that

$$\frac{f_{n-1}}{g_{n-1}} = \frac{R}{(f_n - tg_n)^2}$$

can also be written as

$$\frac{f_{n-1}}{g_{n-1}} = \frac{R/R_1}{(f_n - tg_n)^2/R_1} = \frac{R/R_1}{S_1}.$$

Since $\frac{f_{n-1}}{g_{n-1}}$ is in lowest terms, it follows that $g_{n-1} \mid S_1$. In exactly the same way we get $g_{n+1} \mid R_1$ and thus $g_{n-1}g_{n+1} \mid R_1S_1 = (f_n - tg_n)^2$. So indeed we have $v_l(g_{n-1}g_{n+1}) \leq v_l((f_n - tg_n)^2)$. □

Now to finish the proof of our statement (3.13), we only need to show that the opposite of above lemma holds, so we need to show

$$v_l((f_n - tg_n)^2) \leq v_l(g_{n-1}g_{n+1}).$$

Therefore, consider two cases. In the first case we assume $v_l(f_n - tg_n) = 0$, in the second case we assume $v_l(f_n - tg_n) > 0$.

Case 1: Suppose $v_l(f_n - tg_n) = 0$. Since

$$0 \leq v_l(g_{n-1}g_{n+1}) \leq v_l((f_n - tg_n)^2) = 0$$

we have $v_l(g_{n-1}g_{n+1}) = v_l((f_n - tg_n)^2) = 0$, which proves statement (3.13).
Case 2: Suppose $v_l(f_n - tg_n) > 0$. Since we have

$$x_{n-1}x_{n+1} = \frac{RS}{(f_n - tg_n)^4} = \frac{(tf_n - a_4g_n)^2 - 4a_6g_n(f_n + (t + a_2)g_n)}{(f_n - tg_n)^2}$$

it follows that $v_l(RS) \geq 2$. Now we have two subcases, one where l divides exactly one of R and S, where we assume l divides R. The case where l divides S (but not R) is exactly the same and is therefore omitted. The other subcase considers l dividing both R and S.
Case 2a: Suppose $v_l(R) > 0$ but $v_l(S) = 0$. We also know $v_l(RS) > 0$. Using equation (3.12c), so using

$$\frac{f_{n-1}f_{n+1}}{g_{n-1}g_{n+1}} = \frac{RS}{(tg_n - f_n)^4} = \frac{(tf_n - a_4g_n)^2 - 4a_6g_n(f_n + (t + a_2)g_n)}{(f_n - tg_n)^2}$$

we can say $2v_l(f_n - tg_n) \leq v_l(RS)$, but since $v_l(RS) = v_l(R) + v_l(S) = v_l(R)$ we know $2v_l(f_n - tg_n) \leq v_l(R)$. If we now consider (3.10c), namely

$$\frac{R}{(f_n - tg_n)^2} = \frac{f_{n-1}}{g_{n-1}}$$

we can conclude $v_l(f_{n-1}) - v_l(g_{n-1}) \geq 0$, hence $v_l(g_{n-1}) = 0$ (which follows from $\gcd(f_{n-1}, g_{n-1}) = 1$). Summarizing we have $v_l(S) = v_l(g_{n-1}) = 0$ and $v_l(R) > 0$. From equation (3.11c) we get

$$v_l(S) - v_l((f_n - tg_n)^2) = v_l(f_{n+1}) - v_l(g_{n+1}) \tag{3.14}$$

and since $v_l(S) = 0$ and $v_l(f_n - tg_n) > 0$, the left hand side of above equation is smaller than zero. This means that it follows

$$v_l(f_{n+1}) - v_l(g_{n+1}) < 0$$

which is only possible if $v_l(g_{n+1}) > 0$, hence $v_l(f_{n+1}) = 0$ (which follows from lemma 3.5). So this gives us, using (3.14) that

$$v_l((f_n - tg_n)^2) = v_l(g_{n+1})$$

and since $v_l(g_{n-1}) = 0$, we get

$$v_l((f_n - tg_n)^2) = v_l(g_{n-1}g_{n+1})$$

proving statement (3.13).
Case 2b: Suppose $v_l(f_n - tg_n) > 0$, $v_l(R) > 0$ and $v_l(S) > 0$. Since $v_l(R) > 0$, using equation (3.10a), it follows

$$v_l\left(\frac{-(tg_n - f_n)^2((t + a_2)g_n + f_n) + f(t)(1 + y_n)^2 g_n^3}{g_n(f_n - tg_n)^2}\right) > 0.$$

This means that l must divide the numerator and thus, since $v_l(f_n - tg_n) > 0$ it follows that $v_l(f(t)(1 + y_n)^2 g_n^3) > 0$. In the same way we get from $v_l(S) > 0$ that $v_l(f(t)(1 - y_n)^2 g_n^3) > 0$. To proceed the proof of the basic identity in this case, we need the following claim.
Claim 1: $v_l(g_n) = 0$.

Proof. Assume $v_l(g_n) > 0$. Since $x_n = \frac{f_n}{g_n}$ is written in lowest terms, we have $\gcd(f_n, g_n) = 1$. On the other hand, the assumptions $v_l(f_n - tg_n) > 0$ and $v_l(g_n) > 0$ yield $v_l(f_n) > 0$ and thus $\gcd(f_n, g_n) \neq 1$. This is a contradiction, so $v_l(g_n) = 0$. □

This claim implies another claim.
Claim 2: $v_l(f(t)) = 1$.

Proof. Assume $v_l(f(t)) \neq 1$. Then, since $f(t)$ is an elliptic curve which cannot have multiple roots (not equal to $\mathcal{O}$), it must follow $v_l(f(t)) = 0$. Using $0 < v_l(f(t)(1 \pm y_n)^2) = v_l(f(t)) + 2v_l(1 \pm y_n) = 2v_l(1 \pm y_n)$ it follows $v_l(1 \pm y_n) > 0$. Hence also $v_l(2) = v_l((1 + y_n) + (1 - y_n)) > 0$, which is a contradiction. So indeed $v_l(f(t)) = 1$. □

Since we already know $v_l(g_{n-1}g_{n+1}) \leq v_l((f_n - tg_n)^2)$ the proof is finished when $v_l((f_n - tg_n)^2) \leq v_l(g_{n-1}g_{n+1})$. To prove this last statement, assume it is not true so that $v_l((f_n - tg_n)^2) > v_l(g_{n-1}g_{n+1})$. Recall (3.12c) and (3.12a), given by

$$\begin{aligned} x_{n+1}x_{n-1} &= \frac{f_{n-1}f_{n+1}}{g_{n-1}g_{n+1}} \\ &= \frac{(tf_n - a_4g_n)^2 - 4a_6g_n(f_n + (t+a_2)g_n)}{(f_n - tg_n)^2} \\ &=: \frac{T}{(f_n - tg_n)^2}. \end{aligned}$$

Combining this formula together with $v_l((f_n - tg_n)^2) > v_l(g_{n-1}g_{n+1})$ we must have $v_l(T) > 0$. Consider $T \mod l$. Since $v_l(T) > 0$ we have $T \mod l = 0$. Since $v_l(f_n - tg_n) > 0$ we have $\overline{f_n} = \overline{tg_n}$. Substituting this in the formula for T yields

$$\begin{aligned} \overline{0} = \overline{T} &= \overline{(t^2g_n - a_4g_n)^2} - \overline{4a_6g_n(tg_n + (t+a_2)g_n)} \\ &= \overline{g_n^2[(t^2 - a_4)^2 - 4a_6t - 4a_6(t+a_2)]} \\ &= \overline{g_n^2(t^4 - 2a_4t^2 - 8a_6t + a_4^2 - 4a_2a_6)}. \end{aligned}$$

Since $v_l(g_n) = 0$, so $\overline{g_n} \neq \overline{0}$, we must have $\overline{t^4 - 2a_4t^2 - 8a_6t + a_4^2 - 4a_2a_6} = \overline{0}$.Now this last formula is the same as the numerator of (3.8), so we also can write

$$\overline{(f'(t))^2 - 4(2t + a_2)f(t)} = \overline{0}.$$

And thus since $v_l(f(t)) = 1$ we have

$$\overline{(f'(t))^2} = \overline{0}.$$

But this implies that also $\overline{f'(t)} = \overline{0}$ and thus $v_l(f'(t)) > 0$. So we know l divides both $f(t)$ and $f'(t)$, and thus $f(t)$ has a double zero, which is a contradiciton. This yields $v_l((f_n - tg_n)^2) \leq v_l(g_{n-1}g_{n+1})$ as desired.
So we have proven that $v_l(g_{n-1}g_{n+1}) = v_l((f_n - tg_n)^2)$ holds in all cases, which proves the basic identity. □

4 Hasse's Theorem: Case char(K) = 2, $j(E) = 0$

In this chapter we will deal with the case $\mathrm{char}(\mathbb{F}_q) = 2$. Here we can consider two cases, namely the curves for which $j(E) = 0$ and the curves for which $j(E) \neq 0$. First we deal with the curves where $j(E) = 0$, which are the supersingular curves.

4.1 Proof of Hasse's theorem

To prove Hasse's theorem in $\mathrm{char}(\mathbb{F}_q) = 2$ we need to know how in this case an elliptic curve can be written. Therefore, we use the following theorem.

Theorem 4.1. *When* $\mathrm{char}(\mathbb{F}_q) = 2$*, every elliptic curve* $E/\mathbb{F}_q$ *with j-invariant* $j(E) = 0$ *can be given by the equation*

$$y^2 + a_3 y = x^3 + a_4 x + a_6$$

in which $a_3 \neq 0$*.*

Proof. Start with the general Weierstrass curve given by

$$E/\mathbb{F}_q : \quad y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

To transform this curve to the form stated in theorem 4.1, use that $j(E) = 0$. Computing $j(E)$ using [19, III.1], [19, App.A]) and $\mathrm{char}(\mathbb{F}_q) = 2$ yields

- $b_2 = a_1^2 + 4a_4 = a_1^2$,
- $b_4 = 2a_4 + a_1 a_3 = a_1 a_3$,
- $b_6 = a_3^2 + 4a_6 = a_3^2$,
- $b_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2 = a_1^2 a_6 + a_1 a_3 a_4 + a_2 a_3^2 + a_4^2$,
- $c_4 = b_2^2 - 24 b_4 = b_2^2 = a_1^4$.

Then we can define the j-invariant and the discriminant of E as

- $\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6 = b_2^2 b_8 + b_6^2 + b_2 b_4 b_6$,
- $j(E) = c_4^3/\Delta = a_1^{12}/\Delta$.

Now since $j(E) = 0$ we can conclude that $a_1 = 0$ and thus E already reduces to

$$E : \quad y^2 + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

Now make the substitution

$$y = y', \quad x = x' + a_2$$

to arrive at the reduced curve

$$E : \quad y^2 + a_3 y = x^3 + a_4 x + a_6 = f(x).$$

In this case, since $a_1 = 0 = a_2$ we have

- $b_2 = 0$,

- $b_4 = 0$,
- $b_6 = a_3^2$.

And thus the discriminant is given by

$$\Delta = -27b_6^2 = b_6^2 = a_3^4.$$

Since for an elliptic curve E it must hold $\Delta \neq 0$ it follows $a_3 \neq 0$. □

To prove Hasse's theorem, we proceed in the same way as in chapter 3. This means that first we have to find a twist of E, called E^{tw} such that $E \cong E^{tw}$ over L where L is the quadratic extension $L = \mathbb{F}_q(t, s)$ of $K = \mathbb{F}_q(t)$ where s, t satisfy $s^2 + a_3 s = t^3 + a_t + a_6 = f(t)$. To see the construction of the twist, see appendix B.1. After some computations we find that the twist of E is given by

$$\begin{aligned} E^{tw} : y^2 + a_3 y &= f(x) + f(t) \\ &= x^3 + a_4 x + a_6 + t^3 + a_4 t + a_6 \\ &= x^3 + a_4 x + t^3 + a_4 t. \end{aligned} \tag{4.1}$$

The next step is to find the group law for this curve E^{tw}. To find these formulas, use [19, III.2.2.3]. With $\zeta_i = (x_i, y_i) \in E^{tw}, i = 1, 2$ this results in the following group law:

$$x(\zeta_1 + \zeta_2) = \left(\frac{y_2 + y_1}{x_2 + x_1}\right)^2 + (x_1 + x_2), \tag{4.2a}$$

$$x([2]\zeta_1) = \frac{x^4 + a_4^2}{a_3^2} = \frac{(f'(x))^2}{a_3^2}. \tag{4.2b}$$

Here the (first) addition formula only holds when $x_1 \neq x_2$. We now need to find some points on the curve E and E^{tw} so that we can define the basic identity later on. Consider again the quadratic extension $L = \mathbb{F}_q(t, s)$ of $K = \mathbb{F}_q(t)$. This makes E and E^{tw} isomorphic over L via the isomorphism (see appendix B.1)

$$\begin{aligned} &\psi : E \to E^{tw} \\ &(x, y) \mapsto (x, y + s). \end{aligned}$$

Then over $\mathbb{F}_q(t, s)$ we have $(t, s) \in E(\mathbb{F}_q(t, s))$ and $(t^q, s^q) \in E(\mathbb{F}_q(t, s))$. The images of these points under the isomorphism ψ are the corresponding points on $E^{tw}(\mathbb{F}_q(t, s))$, yielding

$$Q = (t, s + s) = (t, 0) \in E^{tw}(\mathbb{F}_q(t, s))$$

and

$$P_0 = (t^q, s^q + s) \in E^{tw}(\mathbb{F}_q(t, s)).$$

For the point P_0 we have the following lemma.

Lemma 4.1. *The element $s^q + s \in \mathbb{F}_q(t, s)$ belongs to the subring $\mathbb{F}_q[t]$. Furthermore, as a polynomial in t, its degree equals $3q/2$.*

Proof. For the subring $\mathbb{F}_q[t]$ we have $\mathbb{F}_q[t] \subseteq \mathbb{F}_q(t) \subseteq \mathbb{F}_q(t,s)$. We know $s^q + s \in \mathbb{F}_q(t,s)$, so the first step is to show $s^q + s \in \mathbb{F}_q(t)$, the second step is to show $s^q + s \in \mathbb{F}_q[t]$.
The Galois group of the extension $\mathbb{F}_q(t) \subseteq \mathbb{F}_q(t,s)$ is given by $Gal(\mathbb{F}_q(t,s)/\mathbb{F}_q(t)) = \{id, \sigma\}$ where σ is defined by $\sigma : s \mapsto s + a_3$, see also appendix B.1. Then $\mathbb{F}_q(t) = \mathbb{F}_q(t,s)^{<\sigma>} = \{\xi \in \mathbb{F}_q(t,s) : \sigma(\xi) = \xi\}$. Then it is quite easy to see that $s^q + s \in \mathbb{F}_q(t)$:

$$\begin{aligned}\sigma(s^q + s) &= (s + a_3)^q + (s + a_3)\\ &= s^q + a_3 + s + a_3\\ &= s^q + s.\end{aligned}$$

The second step is to verify that $s^q + s \in \mathbb{F}_q[t]$. For this, we will use that $\mathbb{F}_q(t,s)$ is the field of rational functions defined over $\mathbb{F}_q$ on the elliptic curve E. The subring of all functions in $\mathbb{F}_q(t,s)$ which are defined in every point of E except possibly $\mathcal{O}$ equals $\mathbb{F}_q[t][s]$. Since $s^q + s$ is in this subring and $s^q + s \in \mathbb{F}_q(t)$ we have

$$s^q + s \in \mathbb{F}_q[t][s] \cap \mathbb{F}_q(t) = \mathbb{F}_q[t].$$

To find the degree of $s^q + s$, we use the twisted curve E^{tw} given by

$$E^{tw} : \quad y^2 + a_3 y = x^3 + a_4 x + t^3 + a_4 t.$$

On this curve obviously we have the point at infinity: $\mathcal{O} \in E^{tw}$. For this point at infinity, we can consider the valuation of x, given by $v_\infty(x) = -2$. This means that $v_\infty(x^3) = 3v_\infty(x) = -6$ and since the valuations of the left hand side and right hand side should be equal we know that $v_\infty(y^2) = v_\infty(x^3)$ and thus $v_\infty(y) = -3$. Now we can use that $v_\infty(x^d) = -2d$ to get that $v_\infty(\text{polynomial in } x) = -2\deg(\text{polynomial in } x)$. Taking as our polynomial $y^q + y$ (which is a polynomial in x by the part just proven) we get

$$\begin{aligned}v_\infty(y^q + y) &= -2\deg(y^q + y)\\ \Rightarrow -3q &= -2\deg(y^q + y)\end{aligned}$$

yielding $\deg(y^q + y) = 3q/2$ which is always an integer since q is a power of 2. So also $\deg(s^q + s) = 3q/2$. □

Knowing this, we can define points $P_n \in E^{tw}(\mathbb{F}_q(t))$ as before by

$$P_n = P_0 + nQ.$$

If $P_n \neq \mathcal{O}$, write $P_n = (x_n, y_n)$ and $x_n = \frac{f_n}{g_n}$ for coprime polynomials $f_n, g_n \in \mathbb{F}_q[t]$. Define the function $d : \mathbb{Z} \to \{0, 1, 2, 3, \cdots\}$ as

$$d(n) = d_n = \begin{cases} 0 & \text{if } P_n = \mathcal{O};\\ \deg(f_n) & \text{otherwise.}\end{cases}$$

From this definition we arrive at the following lemma.

Lemma 4.2 (Basic Identity). $d_{n-1} + d_{n+1} = 2d_n + 2.$

The connection between theorem 3.1 and the function $d(n)$ defined above is again given by the following lemma.

Lemma 4.3. *$d_{-1} = \#E(\mathbb{F}_q)$.*

Finally, we have

Lemma 4.4. *The function $d(n)$ is a quadratic polynomial in n. In fact,*

$$d(n) = d_n = n^2 - (\#E(\mathbb{F}_q) - (q+1))n + q.$$

Consider the quadratic polynomial

$$d(x) = x^2 - (\#E(\mathbb{F}_q) - (q+1))x + q.$$

Then $d(x) \geq 0$ for all $x \in \mathbb{Z}$, which can be seen from the definition of $d(x)$: $d(x) = d(n)$ is defined as either 0 or the degree of the numerator of x_n, which is positive. Now consider the discriminant of $d(x)$, given by

$$D = (\#E(\mathbb{F}_q) - (q+1))^2 - 4q.$$

Again we will show that $D \leq 0$. Suppose this is false, so that $D > 0$. Then there are two real roots α and β of the polynomial $d(x)$. By the same argument as in the case of $\mathrm{char}(\mathbb{F}_q) \geq 3$, we have that it must follow that α and β are two successive integers m and $m+1$. Furthermore, for these points we have $d(m) = d(m+1) = 0$, and by the definition of $d(x) = d(n) = d_n$ we have that

$$\begin{aligned} d(m) &= d_m = \deg(P_0 + mQ) = 0 \\ d(m+1) &= d_{m+1} = \deg(P_0 + (m+1)Q) = 0. \end{aligned}$$

Yielding (again by the definition of d_n) that

$$\begin{aligned} P_0 + mQ &= \mathcal{O} \\ P_0 + (m+1)Q &= \mathcal{O}. \end{aligned}$$

Substracting above two equations gives $Q = \mathcal{O}$, which is not possible since we defined Q to be the point $Q = (t^q, s^q)$. So indeed $D > 0$ is not possible, yielding $D \leq 0$, which proves the initial theorem. □

4.2 Examples

In this subsection we will show that it is possible indeed to have $D = 0$ and $D < 0$.

We have $D = 0 \Leftrightarrow (\#E(\mathbb{F}_q) - (q+1))^2 = 4q$. This is possible only if q is a square and $\#E(\mathbb{F}_q) = q \pm 2\sqrt{q}$. Such elliptic curves exist: for example, take $q = 4$ and

$$E: \quad y^2 + y = x^3.$$

Here $\mathbb{F}_q = \mathbb{F}_4 = \mathbb{F}_2[\alpha]/ < \alpha^2 + \alpha + 1 >$ so that α is a zero of the polynomial $x^2 + x + 1$. Then E contains the following points:

$$E(\mathbb{F}_q) = \{(0,0), (0,1), (1,\alpha), (1,\alpha+1), (\alpha,\alpha), (\alpha,\alpha+1), (\alpha+1,\alpha), (\alpha+1,\alpha+1), \mathcal{O}\}.$$

So there are 8 x-coordinates giving 2 solutions and the point at infinity, so 9 points in total. This yields

$$\begin{aligned} d(x) &= x^2 - (\#E(\mathbb{F}_q) - (q+1))x + q \\ &= x^2 - (9 - (4+1))x + 4 \\ &= (x-2)^2 \end{aligned}$$

and thus there is a double zero, yielding $D = 0$ is indeed possible.
The other case, $D < 0$ is possible whenever q is not a square. But also for q a square $D < 0$ occurs. Take for example $q = 4$ and

$$E: \quad y^2 + y = x^3 + x.$$

Then we have the following points:

$$E(\mathbb{F}_q) = \{(0,0), (0,1), (1,0), (1,0), \mathcal{O}\}$$

So in total there are 5 points, yielding

$$d(x) = x^2 - (5 - (4+1))x + 4 = x^2 + 4$$

and thus $D = -16 < 0$.

4.3 Proof of lemma 4.3

In this section we will prove that $d_{-1} = \#E(\mathbb{F}_q)$ for $\text{char}(\mathbb{F}_q) = 2$ and $j(E) = 0$. The first step is to find d_{-1}. For $P_n \neq \mathcal{O}$ we use the recursion formula $P_n = P_0 + nQ = (t^q, s^q + s) + n(t, 0)$ together with the addition formula

$$x(\zeta_1 + \zeta_2) = \left(\frac{y_2 + y_1}{x_2 + x_1}\right)^2 + (x_1 + x_2).$$

To compute d_{-1} we need to compute the x-coordinate of P_{-1}, i.e. x_{-1}. So use

$$\begin{aligned} P_{-1} = (x_{-1}, y_{-1}) &= (t^q, s^q + s) - 1(t, 0) \\ &= (t^q, s^q + s) + (t, a_3) (\text{see [19, III.2.2.3]}) \end{aligned}$$

to get

$$\begin{aligned} x_{-1} &= \left(\frac{a_3 + (s^q + s)}{t + t^q}\right)^2 + (t^q + t) \\ &= \left(\frac{s^q + s + a_3}{t^q + t}\right)^2 + (t^q + t). \end{aligned}$$

Note that $s^q + s$ is in fact a polynomial in t, as we have seen in lemma 4.1. Now to proceed the proof of the lemma, we need to solve the following problem:

Is the x_{-1} above in lowest terms?

To solve this problem, we will check if there are common terms in numerator and denominator. Writing x_{-1} as one fraction we get

$$\begin{aligned} x_{-1} &= \left(\frac{s^q + s + a_3}{t^q + t}\right)^2 + (t^q + t) \\ &= \frac{s^{2q} + s^2 + a_3^2 + t^{3q} + t^{2q+1} + t^{q+2} + t^3}{(t^q + t)^2} \\ &= \frac{t^{2q+1} + t^{q+2} + t^3 + s^2 + a_3^2 + a_3 s^q + a_4 t^q + a_6}{(t^q + t)^2} \\ &= \frac{t^{2q+1} + t^{q+2} + a_4 t + a_3^2 + a_4 t^q + a_3(s^q + s)}{(t^q + t)^2} \end{aligned}$$

where we used the relation of the elliptic curve $s^2+a_3s = t^3+a_4t+a_6$ combined with the following relation which is obtained from applying the Frobenius map:

$$s^{2q} + t^{3q} = a_3s^q + a_4t^q + a_6.$$

Note that in lemma 4.1 we already concluded that for $s^q + s \in \mathbb{F}_q[t]$ we have $\deg(s^q + s) = \frac{3q}{2}$. Knowing this we can easily see that

$$\deg(t^{2q+1} + t^{q+2} + a_4t + a_3^2 + a_4t^q + a_3(s^q + s)) = 2q + 1.$$

To find the common terms in numerator and denominator, take an arbitrary point $\alpha \in \mathbb{F}_q$. Then we have that $\alpha^q = \alpha$ and thus the denominator of x_{-1} has a factor $(t - \alpha)^2$. So there is a common term if also the numerator equals zero at this α. To evaluate the numerator of x_{-1} at $t = \alpha$, note that $\mathbb{F}_q[t] \subset \mathbb{F}_q[t][s]$ where the latter ring consists of functions on E. So evaluating a polynomial at $t = \alpha$ is the same as evaluating the polynomial regarded as a function on E at a point $(\alpha, \beta) \in E$. The result is independent of β. Therefore, for the chosen $\alpha \in \mathbb{F}_q$, find a corresponding β such that the point $(\alpha, \beta) \in E$, i.e. $\beta^2 + a_3\beta = \alpha^3 + a_4\alpha + a_6 = f(\alpha)$. Then we have two possibilities:

1. $\beta \in \mathbb{F}_q$: this means that $\beta^q = \beta$. Substituting the point (α, β) in the numerator of x_{-1} and using that $\alpha^q = \alpha$, $\beta^q = \beta$ we get

$$\begin{aligned} t^{2q+1} + t^{q+2} + t^3{+}s^2 + a_3^2 + a_3s^q + a_4t^q + a_6|_{(\alpha,\beta)} \\ &= \alpha^{2q+1} + \alpha^{q+2} + \alpha^3 + a_4\alpha + a_6 + \beta^2 + a_3\beta^q + a_3^2 \\ &= (\alpha^2)^q \cdot \alpha + \alpha^2 \cdot \alpha^q + f(\alpha) + \beta^2 + a_3\beta + a_3^2 \\ &= 2\alpha^3 + \beta^2 + a_3\beta + a_3^2 + f(\alpha) \\ &= (\beta^2 + a_3\beta + f(\alpha)) + a_3^2 \\ &= a_3^2 \neq 0 \end{aligned}$$

where $\beta^2 + a_3\beta + f(\alpha) = 0$ since (α, β) is a point on the elliptic curve. So when $\beta \in \mathbb{F}_q$, the numerator does not equal zero, and thus there is no common term $(t - \alpha)$ in numerator and denominator.

2. $\beta \notin \mathbb{F}_q$: this means that $\beta^q = \beta + a_3$, since by the Frobenius map β^q is also a zero of the polynomial $y^2 + a_3y = 0$. Since this polynomial has only two zeroes, β^q is mapped to the other zero of the polynomial, i.e. to β. Then the numerator of x_{-1} evaluated in the point (α, β) becomes

$$\begin{aligned} t^{2q+1} + t^{q+2} + t^3{+}s^2 + a_3^2 + a_3s^q + a_4t^q + a_6|_{(\alpha,\beta)} \\ &= \alpha^{2q+1} + \alpha^{q+2} + \alpha^3 + a_4\alpha + a_6 + \beta^2 + a_3\beta^q + a_3^2 \\ &= 2\alpha^3 + f(\alpha) + \beta^2 + a_3(\beta + a_3) + a_3^2 \\ &= \beta^2 + a_3\beta + f(\alpha) \\ &= 0. \end{aligned}$$

So when $\beta \notin \mathbb{F}_q$ we have that there is a common term in numerator and denominator, which cancels and thus lowers the degree of the numerator. Now for each α in this case the common term cancels twice. To see this, consider again x_{-1} given by

$$\begin{aligned} x_{-1} &= \left(\frac{a_3 - (s^q + s)}{t - t^q}\right)^2 - (t^q + t) \\ &= \frac{P(t)^2 + (t^q + t)^3}{(t^q + t)^2}. \end{aligned}$$

We already know that at $t = \alpha$ the term $(t^q + t)$ equals zero, and furthermore the numerator of x_{-1} equals zero because there is a common term. This means that also $P(t)$ evaluated at α equals zero, and thus at $t = \alpha$ the common term cancels twice. So

$$\begin{aligned} d_{-1} &= \deg(\text{numerator}(x_{-1})) \\ &= 2q + 1 - \text{common terms} \\ &= 2q + 1 - 2\#\{\alpha \in \mathbb{F}_q | \nexists \beta \in \mathbb{F}_q \text{ such that } (\alpha, \beta) \in E\}. \end{aligned}$$

Since the total number of possible choices for α is given by q, we can also write

$$\begin{aligned} d_{-1} &= 2q + 1 - 2\#\{\alpha \in \mathbb{F}_q | \nexists \beta \in \mathbb{F}_q \text{ such that } (\alpha, \beta) \in E\} \\ &= 2q + 1 - 2\left(q - \#\{\alpha \in \mathbb{F}_q | \exists \beta \in \mathbb{F}_q \text{ such that } (\alpha, \beta) \in E\}\right) \\ &= 1 + 2\#\{\alpha \in \mathbb{F}_q | \exists \beta \in \mathbb{F}_q \text{ such that } (\alpha, \beta) \in E\}. \end{aligned}$$

The last step is to find $\#E(\mathbb{F}_q)$. Assume we have $\alpha \in \mathbb{F}_q$ which is the x-coordinate of a point in $E(\mathbb{F}_q)$. Then α is the x-coordinate of exactly two points, namely (α, β) and $(\alpha, \beta + a_3)$. Since $a_3 \neq 0$, these points are never equal. This yields, including the point at infinity that

$$\#E(\mathbb{F}_q) = 1 + 2\#\{\alpha \in \mathbb{F}_q | \exists \beta \in \mathbb{F}_q \text{ such that } (\alpha, \beta) \in E\}$$

So indeed $\#E(\mathbb{F}_q) = d_{-1}$ as we wanted to prove. □

4.4 Proof of lemma 4.2

The other important lemma used is the basic identity, stating $d_{n-1} + d_{n+1} = 2d_n + 2$. Before proving this, we need to prove the following lemma.

Lemma 4.5. *If $P_n \neq \mathcal{O}$, then writing $P_n = \left(\frac{f_n}{g_n}, y_n\right)$, one has $\deg(f_n) > \deg(g_n)$, and $x_n \neq 0$.*

Proof. Consider our twisted elliptic curve (4.1) given by

$$E^{tw}/\mathbb{F}_q(t): \quad y^2 + a_3 y = x^3 + a_4 x + t^3 + a_4 t.$$

Just like in the proof of lemma 3.5, we construct a valuation at the point at infinity, and we define the valuation ring O_∞, its group of units $O_\infty^\times$ and the unique maximal ideal $\mathcal{M}$. Again a generator for $\mathcal{M}$ is given by $\frac{1}{t}$. The next step is to reduce the curve E^{tw} modulo $\mathcal{M}$. Therefore, multiply E^{tw} with $1/t^6$ to obtain

$$\begin{aligned} & y^2 + a_3 y = x^3 + a_4 x + a_6 + t^3 + a_4 t + a_6 \\ \Rightarrow & \left(\frac{y}{t^3}\right)^2 + a_3 \frac{1}{t^3}\left(\frac{y}{t^3}\right) = \left(\frac{x}{t^2}\right)^3 + a_4 \frac{1}{t^4}\left(\frac{x}{t^2}\right) + a_6 \frac{1}{t^6} + \frac{1}{t^3} + a_4 \frac{1}{t^5} + a_6 \frac{1}{t^6}. \end{aligned}$$

Make the substitution $\eta = \frac{y}{t^3}$, $\xi = \frac{x}{t^2}$ to get

$$E^{tw}: \quad \eta^2 + a_3 \frac{1}{t^3}\eta = \xi^3 + a_4 \frac{1}{t^4}\xi + \frac{1}{t^3} + a_4 \frac{1}{t^5}.$$

Now we expressed E^{tw} in terms of the generator of $\mathcal{M}$, which means that we can reduce this curve modulo $\frac{1}{t}$ to get

$$\tilde{E}^{tw}/\mathbb{F}_q: \quad \eta^2 = \xi^3.$$

This curve is singular with singular point $(\xi, \eta) = (0, 0)$, so according to [19, VII.5] E^{tw} has bad, additive reduction and thus, according to [19, thm.VII.5.1], we have $\tilde{E}^{tw}_{ns}(\mathbb{F}_q) \simeq (\mathbb{F}_q, +)$. Now we look at the points $P_0, Q \in E^{tw}(\mathbb{F}_q(t))$ and consider their reduction in $\tilde{E}^{tw}(\mathbb{F}_q)$.

- We know $Q = (t, 0) \in E^{tw}(\mathbb{F}_q(t))$. Now writing the curve in terms of ξ means mapping the x-coordinate to $\frac{x}{t^2}$. So the point $Q = (t, 0)$ will be mapped to $(\frac{1}{t}, 0)$ and under reduction modulo $\frac{1}{t}$ this point will map to $\tilde{Q} = (0, 0)$. This means Q maps to a singular point on the reduced curve.
- Another point on E^{tw} is given by $P_0 = (t^q, s^q + s)$ where $s^q + s \in \mathbb{F}_q[t]$. Under the mapping $x \mapsto \frac{x}{t^2}$ this point is given by $(t^{q-2}, \tilde{y})$ where $\tilde{y}$ is the y-coordinate of the mapping $x \mapsto \frac{x}{t^2}$ applied on s^q+s. Now when reducing modulo $\mathcal{M}$ also the point P_0 changes. The only question is whether P_0 maps to a nonsingular point. Since $v_\infty(t^{q-2}) = q - 2 \leq 0$, we have $t^{q-2} \notin \mathcal{M}$, hence P_0 does not reduce to the singular point $(0, 0)$.

So again a question arises. What points of $E^{tw}(\mathbb{F}_q(t))$ do lie in $E^{tw}_{ns}(\mathbb{F}_q(t))$, i.e. map to a nonsingular point? To answer this question, we use the following lemma.

Lemma 4.6. *For an arbitrary point $\zeta = (\frac{f}{g}, y) \in E^{tw}(\mathbb{F}_q(t))$, one has*

$$\zeta \in E^{tw}_{ns}(\mathbb{F}_q(t)) \Leftrightarrow \deg(f) > \deg(g) + 1.$$

Proof. Take $\zeta = (\frac{f}{g}, y) \in E^{tw}(\mathbb{F}_q(t))$. Then $\xi(\zeta) = (\frac{f}{gt^2}, \frac{y}{t^3})$. Now we apply reduction modulo $\mathcal{M}$.

- Suppose $v(f) = v(t^2 g)$. Then $v\left(\frac{f}{t^2 g}\right) = 0$, so $\frac{f}{t^2 g} \in O^\times$ which means $\frac{f}{t^2 g} \notin \mathcal{M}$, so $\frac{f}{t^2 g} \mod \mathcal{M} \neq 0$, hence ζ does not reduce to the singular point.
- Suppose $v(f) > v(t^2 g)$. Then $v\left(\frac{f}{t^2 g}\right) > 0$, so $\frac{f}{t^2 g} \in \mathcal{M}$ which means $\frac{f}{t^2 g} \mod \mathcal{M} = 0$, so ζ reduces to the singular point.
- Suppose $v(f) < v(t^2 g)$. Then $v\left(\frac{f}{t^2 g}\right) < 0$, so $\frac{f}{t^2 g} \mapsto (0 : 1 : 0)$ which is a nonsingular point.

This shows that

$$\begin{aligned} \zeta \in E^{tw}_{ns}(\mathbb{F}_q(t)) &\Leftrightarrow v_\infty(f) \leq v_\infty(t^2 g) \\ &\Leftrightarrow -\deg(f) \leq -2 - \deg(g) \\ &\Leftrightarrow \deg(f) > \deg(g) + 1 \end{aligned}$$

□

Note that $E^{tw}_{ns}(\mathbb{F}_q(t))$ is a group, which means that for two points in this group also their sum must be in the group. Earlier we've seen that Q maps to the singular point $(0,0)$. Now consider $2Q$ given by

$$2Q = 2(t,0) = \frac{t^4 + a_4^2}{a_3^2}.$$

Then $\xi(2Q) = \frac{t^4+a_4^2}{t^2a_3^2}$ and thus $v_\infty(\xi(2Q)) = -2$ yielding $2Q$ does not map to the singular point. This means, since $P_0 \in E^{tw}_{ns}(\mathbb{F}_q(t))$, also $P_0 + nQ \in E^{tw}_{ns}(\mathbb{F}_q(t))$ for even numbers n. Now for the odd n, use the following lemma.

Lemma 4.7. *If $\zeta \in E^{tw}_{ns}(\mathbb{F}_q(t))$, then writing $\zeta = \left(\frac{f}{g}, y\right)$ one has* $\deg(num(x(\zeta+Q))) > \deg(den(x(\zeta + Q)))$.

Proof. Taking $Q = (t,0)$ we have

$$\begin{aligned} x(\zeta + Q) &= x\left(\left(\frac{f}{g}, y\right) + (t,0)\right) \\ &= \left(\frac{0+y}{t+\frac{f}{g}}\right)^2 + \left(t + \frac{f}{g}\right) \\ &= \frac{y^2g^2 + t^3g^2 + tf^2 + t^2gf + \frac{f^3}{g}}{t^2g^2 + f^2} \\ &= \frac{f^2t + fgt^2 + g^2t^3 + a_3g^2y + a_4fg}{f^2 + g^2t^2} \end{aligned}$$

yielding (using $\zeta \in E^{tw}_{ns}$ and thus $\deg(f) > \deg(g) + 1$)

$$\deg(\text{num}(x(\zeta+Q))) = \deg(f^2t+fgt^2+g^2t^3+a_3g^2y+a_4fg) = \deg(f^2t) = 1+2\deg(f)$$

and

$$\deg(\text{den}(x(\zeta + Q))) = \deg(f^2 + g^2t^2) = \deg(f^2) = 2\deg(f)$$

so indeed $\deg(\text{num}(x(P + Q))) > \deg(\text{den}(x(P + Q)))$. □

This means that also $P_0 + Q \in E^{tw}_{ns}(\mathbb{F}_q(t))$ and thus $P_0 + nQ \in E^{tw}_{ns}(\mathbb{F}_q(t))$ for all numbers n, and thus also for this sum we have that the degree of the numerator is greater than the degree of the denominator. That $x_n \neq 0$ follows from the reduction modulo $\mathcal{M}$. □

After proving this, we can prove the basic identity. First we consider three special cases before proving the general case. For these special cases, we need the duplication formula (4.2b) given by

$$x([2]\zeta) = \frac{x^4 + a_4^2}{a_3^2}.$$

- Assume $P_{n-1} = \mathcal{O}$. Then using $P_n = P_{n-1} + Q$ we have $P_n = Q$, hence $x_n = t$. Also, $P_{n+1} = P_n + Q = 2Q = 2(t,0)$. By the above duplication formula:

$$x(P_{n+1}) = \frac{t^4 + a_4^2}{a_3^2}.$$

Since $\gcd(t^4 + a_4^2, a_3^2) = 1$ (a_3 is just a constant), it follows $d_{n+1} = 4$. Furthermore, $d_{n-1} = 0$ and $d_n = 1$ which yields the desired identity.

- Assume $P_n = \mathcal{O}$. Then $P_{n-1} = P_n - Q = -(t, 0) = (t, a_3)$ and $P_{n+1} = P_n + Q = (t, 0)$. This gives $d_n = 0$ and $d_{n-1} = d_{n+1} = 1$, which yields the desired identity.
- Assume $P_{n+1} = \mathcal{O}$. Then $P_n = P_{n+1} - Q = (t, a_3)$ and $P_{n-1} = P_n - Q = 2(t, a_3)$. By the duplication formula (3.8):
$$x_{n-1} = \frac{t^4 + a_4^2}{a_3^2}.$$
So by the same argument used above, $d_{n-1} = 4$, $d_n = 1$ and $d_{n+1} = 0$, which yields the desired identity.

So when one of P_{n-1}, P_n or P_{n+1} is the point at infinity $\mathcal{O}$, the basic identity holds. So for the general case we may assume that neither of those three points equals the point at infinity. We know

$$P_{n-1} = P_n - Q = P_n + (t, a_3)$$

where $P_{n-1} = (x_{n-1}, y_{n-1})$. By the addition formula (4.2a) we can compute $x_{n-1} = x(P_{n-1})$:

$$\begin{aligned}
x_{n-1} &= \left(\frac{a_3 + y_n}{t + x_n}\right)^2 + (x_n + t) \\
&= \frac{a_3^2 + y_n^2 + (t + x_n)^3}{(t + x_n)^2} \\
&= \frac{a_3^2 + (x_n^3 + a_4 x_n + t^3 + a_4 t + a_3 y_n) + t^3 + t^2 x_n + t x_n^2 + x_n^3}{(t + x_n)^2} \\
&= \frac{a_3^2 + a_4 x_n + a_4 t + a_3 y_n + t^2 x_n + t x_n^2}{(t + x_n)^2}.
\end{aligned}$$

Writing $x_n = \frac{f_n}{g_n}$ in lowest terms, multiplying by $\frac{g_n^2}{g_n^2}$, using $\operatorname{char}(\mathbb{F}_q) = 2$ and simplifying yields

$$\begin{aligned}
x_{n-1} &= \frac{f_{n-1}}{g_{n-1}} && \text{(4.3a)} \\
&= \frac{a_3^2 g_n^2 + a_4 f_n g_n + a_4 t g_n^2 + a_3 y_n g_n^2 + t^2 f_n g_n + t f_n^2}{(t g_n + f_n)^2} \\
&= \frac{a_3^2 g_n^2 + a_3 y_n g_n^2 + (f_n + t g_n)(t f_n + a_4 g_n)}{(f_n + t g_n)^2} && \text{(4.3b)} \\
&= \frac{R}{(f_n + t g_n)^2}. && \text{(4.3c)}
\end{aligned}$$

Note that we have $R \in \mathbb{F}_q[t]$. To see this, consider R given by

$$R = (a_4 g_n + t f_n)(f_n + t g_n) + a_3 g_n^2 y_n + a_3^2 g_n^2.$$

Obviously, $(a_4 g_n + t f_n)(f_n + t g_n) \in \mathbb{F}_q[t]$ since both $f_n, g_n \in \mathbb{F}_q[t]$. By the same reason we also have $a_3^2 g_n^2 \in \mathbb{F}_q[t]$. So consider $a_3 g_n^2 y_n$. If we take a point $\zeta \in E^{tw}$ we know $\zeta = \left(\frac{f_n}{g_n}, y_n\right)$ and thus

$$\begin{aligned} y_n^2 + a_3 y_n &= \left(\frac{f_n}{g_n}\right)^3 + a_4\left(\frac{f_n}{g_n}\right) + t^3 + a_4 t \\ \Rightarrow (y_n g_n^2)^2 + a_3 g_n^2 (g_n^2 y_n) &= f_n^3 g_n + a_4 f_n g_n^3 + t^3 g_n^4 + a_4 t g_n^4. \end{aligned}$$

In the last line we can see that $(y_n g_n^2)^2 + a_3 g_n^2 (g_n^2 y_n)$ is a polynomial in t. This implies that $g_n^2 y_n \in \mathbb{F}_q(t)$ cannot have a denominator of degree ≥ 1 since $g_n^2 y_n$ is a zero of the polynomial $x^2 + ax + b \in \mathbb{F}_q[t][x]$. This means that we must have $g_n^2 y_n \in \mathbb{F}_q[t]$ and since $a_3 \in \mathbb{F}_q$ we also have $a_3 g_n^2 y_n \in \mathbb{F}_q[t]$. Putting everything together indeed yields $R \in \mathbb{F}_q[t]$. In exactly the same way we get

$$\begin{aligned} x_{n+1} &= \frac{f_{n+1}}{g_{n+1}} && (4.4a) \\ &= \left(\frac{y_n}{t + x_n}\right)^2 + (x_n + t) \\ &= \frac{(x_n^3 + a_4 x_n + t^3 + a_4 t + a_3 y_n) + (t + x_n)^3}{(t + x_n)^2} \\ &= \frac{a_4 x_n + a_4 t + a_3 y_n + t^2 x_n + t x_n^2}{(t + x_n)^2} \\ &= \frac{a_4 f_n g_n + a_4 t g_n^2 + a_3 y_n g_n^2 + t^2 f_n g_n + t f_n^2}{(t g_n + f_n)^2} \\ &= \frac{a_3 y_n g_n^2 + (f_n + t g_n)(t f_n + a_4 g_n)}{(f_n + t g_n)^2} && (4.4b) \\ &= \frac{S}{(f_n + t g_n)^2} && (4.4c) \end{aligned}$$

with $S \in \mathbb{F}_q[t]$. Multipliying (4.3c) and (4.4c) using the computer program Mathematica gives the following result:

$$\begin{aligned} x_{n+1} x_{n-1} &= \frac{f_{n-1} f_{n+1}}{g_{n-1} g_{n+1}} && (4.5a) \\ &= \frac{RS}{(f_n + t g_n)^4} && (4.5b) \\ &= \frac{(f_n + t g_n)^2 (a_4^2 g_n^2 + f_n^2 t^2 + a_3^2 g_n (f_n + t g_n))}{(f_n + t g_n)^4} && (4.5c) \\ &= \frac{a_4^2 g_n^2 + f_n^2 t^2 + a_3^2 g_n (f_n + t g_n)}{(f_n + t g_n)^2}. && (4.5d) \end{aligned}$$

Note that the numerator in (4.5a) has degree $\deg(f_{n-1} f_{n+1}) = d_{n-1} + d_{n+1}$ and the numerator in (4.5d) has (using lemma 4.5) degree $\deg(t^2 f_n^2) = 2\deg(t) + 2\deg(f_n) = 2 + 2d_n$. So the basic identity will follow if we show that

$$g_{n-1} g_{n+1} \text{ and } (f_n + t g_n)^2 \text{ differ by a nonzero constant.}$$

We show this by proving that every irreducible polynomial $l(t) \in \mathbb{F}_q[t]$ divides $g_{n-1} g_{n+1}$ as many times as it divides $(f_n + t g_n)^2$. Therefore, consider the valuation map

$$v_l : \mathbb{F}_q(t) \to \mathbb{Z} \cup \{\infty\}$$

defined as the number of times l appears in the factorization of a quotient of polynomials. Then to prove the basic identity, we want to use what is said above, so we want to show that

$$v_l(g_{n-1}g_{n+1}) = v_l((f_n + tg_n)^2). \tag{4.6}$$

To prove this, consider again (4.3c) and (4.4c):

$$x_{n-1} = \frac{f_{n-1}}{g_{n-1}} = \frac{R}{(f_n + tg_n)^2},$$
$$x_{n+1} = \frac{f_{n+1}}{g_{n+1}} = \frac{S}{(f_n + tg_n)^2}.$$

As $\frac{f_{n-1}}{g_{n-1}}$ and $\frac{f_{n+1}}{g_{n+1}}$ are written in lowest terms, from $x_{n-1} = \frac{R}{(f_n - tg_n)^2} = \frac{f_{n-1}}{g_{n-1}}$ and $x_{n+1} = \frac{S}{(f_n - tg_n)^2} = \frac{f_{n+1}}{g_{n+1}}$ we can conclude that $f_{n-1} \mid R$ and $g_{n-1} \mid (f_n + tg_n)^2$ and in the same way, $f_{n+1} \mid S$, $g_{n+1} \mid (f_n + tg_n)^2$. This means that at least we have

$$v_l(g_{n\pm1}) \leq v_l((f_n + tg_n)^2).$$

Furthermore, we have

Lemma 4.8. $v_l(g_{n-1}g_{n+1}) \leq v_l((f_n + tg_n)^2)$.

Since the proof of this lemma is exactly the same as the proof of lemma 3.7, it is omitted here. To show equality in lemma 4.8, consider the following two cases (where we split case 2 in two subcases).

Case 1: Suppose $v_l(f_n + tg_n) = 0$. This yields

$$0 \leq v_l(g_{n-1}g_{n+1}) \leq v_l((f_n + tg_n)^2) = 0$$

and thus

$$v_l(g_{n-1}g_{n+1}) = 0 = v_l((f_n + tg_n)^2)$$

which is what we wanted to prove.

Case 2: Suppose $v_l(f_n - tg_n) > 0$. Use formula (4.5d) given by

$$x_{n-1}x_{n+1} = \frac{a_4^2g_n^2 + f_n^2t^2 + a_3^2g_n(f_n + tg_n)}{(f_n + tg_n)^2} = \frac{RS}{(f_n + tg_n)^4}$$

to conclude that $(f_n + tg_n)^2 \mid RS$ and thus, since $v_l(f_n + tg_n) > 0$, also $v_l(RS) > 0$. Now we have two subcases, one where l divides exactly one of R and S, where we assume l divides R. The case where l divides S (but not R) is exactly the same and is therefore omitted. The other subcase considers l dividing both R and S.

Case 2a: Assume $v_l(R) > 0$ but $v_l(S) = 0$. Then

$$2v_l(f_n + tg_n) \leq v_l(RS) = v_l(R) + v_l(S) = v_l(R).$$

Since

$$x_{n-1} = \frac{f_{n-1}}{g_{n-1}} = \frac{R}{(f_n + tg_n)^2},$$

it follows that $v_l(f_{n-1}) - v_l(g_{n-1}) = v_l(x_{n-1}) \geq 0$. So it follows that $v_l(g_{n-1}) = 0$ since otherwise $v_l(\gcd(f_{n-1}, g_{n-1})) \geq 0$. Now we can use exactly the same argument as in case 2a from section 3.3.2 to conclude that

$$v_l(g_{n+1}) = v_l((f_n + tg_n)^2)$$

and thus

$$v_l(g_{n-1}g_{n+1}) = v_l(g_{n-1}) + v_l(g_{n+1}) = v_l((f_n + tg_n)^2)$$

which is what we wanted to prove.
Case 2b: Assume $v_l(R), v_l(S), v_l(f_n + tg_n) > 0$. Since $v_l(R) > 0$ and $v_l(S) > 0$ and $R + S = a_3^2 g_n^2$, it follows that

$$v_l(a_3^2 g_n^2) > 0$$

hence $v_l(g_n) > 0$. Since in claim 1 in section 3.3.2 we have proven that it is impossible to have $v_l(g_n) > 0$, this case cannot happen. So we are in one of the other two cases, in which we have proven statement (4.6).

5 Hasse's Theorem: Case $j(E) \neq 0$

In this chapter we will deal with the case $\text{char}(\mathbb{F}_q) = 2$ but $j(E) \neq 0$.

5.1 Proof of Hasse's theorem

To prove Hasse's theorem in $\text{char}(\mathbb{F}_q) = 2$ for $j(E) \neq 0$ we need to know how in this case an elliptic curve E can be written.

Theorem 5.1. *When* $\text{char}(\mathbb{F}_q) = 2$*, every elliptic curve* $E/\mathbb{F}_q$ *with j-invariant* $j(E) \neq 0$ *can be given by the equation*

$$y^2 + xy = x^3 + a_2x^2 + a_6$$

in which $a_6 \neq 0$.

Proof. The first part of the proof is the same as the proof of theorem 4.1. We again get as j-invariant and discriminant

- $\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 = b_2^2b_8 + b_6^2 + b_2b_4b_6$,
- $j(E) = c_4^3/\Delta = a_1^{12}/\Delta$.

Since $j(E) \neq 0$ we have $a_1 \neq 0$. Now apply the transformation (see [19, III.1, appendix A])

$$y = a_1^3y' + \frac{a_1^2a_4 + a_3^2}{a_1^3}, \quad x = a_1^2x' + \frac{a_3}{a_1}$$

to arrive at the curve

$$E: \quad y^2 + xy = x^3 + a_2x^2 + a_6 = f(x). \tag{5.1}$$

In this case we have

- $b_2 = a_1^2 = 1$,
- $b_4 = 0$,
- $b_6 = 0$,
- $b_8 = a_1^2a_6$.

And thus the discriminant is given by

$$\Delta = -b_2^2b_8 = -a_1^4(a_1^2a_6) = a_6.$$

Since for an elliptic curve E it must hold $\Delta \neq 0$ it follows $a_6 \neq 0$. □

Remark: Given $E/\mathbb{F}_q$ with equation $y^2 + xy = f(x)$, note that the map

$$\begin{aligned}\gamma :&\mathbb{F}_q \to \mathbb{F}_q\\ &a \mapsto a^2\end{aligned}$$

is an automorphism. Hence, $\beta \in \mathbb{F}_q$ exists such that $\beta^2 = a_6$. This means that always $(0, \beta) \in E(\mathbb{F}_q)$ and this point is a point of order 2. In particular, this implies that $\#E(\mathbb{F}_q)$ is even for any $E/\mathbb{F}_q$ with $j(E) \neq 0$. To prove the Hasse inequality, we proceed in the same way as in the chapters 3.2 and 4.1. So first we want to find a twist of E. How this twist is constructed can be found in appendix B.2. The result of this computation is the following curve E^{tw} with $E \cong E^{tw}$ over the quadratic extension $L = \mathbb{F}_q(t,s)$ of $K = \mathbb{F}_q(t)$ where s, t satisfy $s^2 + ts = f(t)$:

$$E^{tw}: \quad y^2 + xy = x^3 + \left(a_2 + \frac{f(t)}{t^2}\right) x + a_6. \tag{5.2}$$

This twist is isomorphic to E via the isomorphism

$$\psi : (x,y) \mapsto \left(x, y + \frac{sx}{t}\right).$$

The next step is to find the addition formulas for the elliptic curve E^{tw}. According to [19, p.54, alg.2.3] the duplication formulas for the points $\zeta_1 = (x_1, y_1)$ and $\zeta_2 = (x_2, y_2)$ are given by (the first formula only holds for $x_1 \neq x_2$)

$$x(\zeta_1 + \zeta_2) = \left(\frac{y_2 + y_1}{x_2 + x_1}\right)^2 + \left(\frac{y_2 + y_1}{x_2 + x_1}\right) + \left(a_2 + \frac{f(t)}{t^2}\right) + x_1 + x_2, \tag{5.3a}$$

$$x([2]\zeta_1) = \frac{x^4 + a_6}{4x^3 + x^2}. \tag{5.3b}$$

Following the method used in earlier situations, we need to find two points on the curve E^{tw} so that we can define the numbers d_n used in the basic identity later on. From equations (5.1) and (5.2) it can be seen that over $\mathbb{F}_q(t,s)$ we have $(t,s) \in E(\mathbb{F}_q(t,s))$ and $(t^q, s^q) \in E(\mathbb{F}_q(t,s))$. The corresponding points on $E^{tw}(\mathbb{F}_q(t,s))$ are given by the images of above points under the isomorphism ψ, yielding

$$Q = \left(t, s + \frac{st}{t}\right) = (t, 0) \in E^{tw}(\mathbb{F}_q(t,s))$$

and

$$P_0 = \left(t^q, s^q + \frac{st^q}{t}\right) = (t^q, s^q + st^{q-1}) \in E^{tw}(\mathbb{F}_q(t,s)).$$

In the point P_0 we have the term $s^q + st^{q-1}$. For this term, we have the following lemma.

Lemma 5.1. *The element $s^q + st^{q-1} \in \mathbb{F}_q(t,s)$ belongs to the subring $\mathbb{F}_q[t]$. Furthermore, as a polynomial in t, its degree equals $3q/2$.*

Proof. The proof of lemma 5.1 is exactly the same as the proof of lemma 4.1 with replacing $s^q + s$ by $s^q + st^{q-1}$ and $\sigma : s \mapsto s + a_3$ by $\sigma : s \mapsto s + t$. Therefore the proof is omitted here. □

The next step is to define points $P_n \in E^{tw}(\mathbb{F}_q(t))$ by

$$P_n = P_0 + nQ.$$

If $P_n \neq \mathcal{O}$, write $P_n = (x_n, y_n)$ and $x_n = \frac{f_n}{g_n}$ for $f_n, g_n \in \mathbb{F}_q[t]$ with $\gcd(f_n, g_n) = 1$. We can define the function

$$d(n) = d_n = \begin{cases} 0 & \text{if } P_n = \mathcal{O}; \\ \deg(f_n) & \text{otherwise.} \end{cases}$$

From this definition we arrive at the following lemma, analogous to the previous cases.

Lemma 5.2. $d_{n-1} + d_{n+1} = 2d_n + 2$.

The connection between theorem 3.1 and the function $d(n)$ defined above is given by the following lemma.

Lemma 5.3. $d_{-1} = \#E(\mathbb{F}_q)$.

Finally, we arrive at

Lemma 5.4. *The function $d(n)$ is a quadratic polynomial in n. In fact,*

$$d(n) = d_n = n^2 - (\#E(\mathbb{F}_q) - (q+1))n + q. \tag{5.4}$$

Consider the quadratic polynomial

$$d(x) = x^2 - (\#E(\mathbb{F}_q) - (q+1))x + q.$$

Then $d(x) \geq 0$ for all $x \in \mathbb{Z}$, which can be seen from the definition of this polynomial, $d(x)$ is defined as either zero of the degree of the numerator of x_n, which is positive. Now consider the discriminant of $d(x)$, given by

$$D = (\#E(\mathbb{F}_q) - (q+1))^2 - 4q.$$

We will show that must hold $D \leq 0$. Assume not, so that $D > 0$. Then there are two real roots $\alpha < \beta$ for the polynomial $d(x)$. Now we can proceed just as in the case $\mathrm{char}(\mathbb{F}_q) = 2$ with $j(E) = 0$. So we must have that α and β are two successive integers m and $m+1$. For these points we have $d(m) = d(m+1) = 0$ and by the definition of $d(n)$ we have

$$\begin{aligned} d(m) &= d_m = \deg(P_0 + mQ) = 0 \\ d(m+1) &= d_{m+1} = \deg(P_0 + (m+1)Q) = 0. \end{aligned}$$

As is done below lemma 3.5, this means that

$$\begin{aligned} P_0 + mQ &= \mathcal{O} \\ P_0 + (m+1)Q &= \mathcal{O}. \end{aligned}$$

Substracting above two equations gives $Q = \mathcal{O}$, which is not possible since we defined Q to be the point $Q = (t^q, s^q + st^{q-1})$. So indeed $D > 0$ is not possible, yielding $D \leq 0$, which proves the Hasse inequality. □

5.2 Examples

In this subsection we will show that it is possible indeed to have $D = 0$ and $D < 0$.
We have $D = 0 \Leftrightarrow (\#E(\mathbb{F}_q) - (q+1))^2 = 4q$. This is possible only if q is a square and $\#E(\mathbb{F}_q) = q \pm 2\sqrt{q}$.

Lemma 5.5. *When $\mathrm{char}(\mathbb{F}_q) = 2$ it is not possible to find an elliptic curve E with $j(E) \neq 0$ such that $D = 0$.*

Proof. Take the elliptic curve E defined by

$$E/\mathbb{F}_q : \quad y^2 + xy = x^3 + a_2x^2 + a_6.$$

In the remark below theorem 5.1, we have already seen that for such a curve E it must hold that $\#E(\mathbb{F}_q)$ is even. So $\#E(\mathbb{F}_q) - q - 1$ is odd since q is even. This means that also $(\#E(\mathbb{F}_q) - q - 1)^2$ is odd, and since $4q$ is even it is impossible to have equality. So $D = 0$ is not possible. □

The other case, $D < 0$ is possible whenever q is not a square. But also for q a square $D < 0$ occurs. Take for example $q = 4$ and

$$E/\mathbb{F}_4 : \quad y^2 + xy = x^3 + 1.$$

Here $\mathbb{F}_q = \mathbb{F}_4 = \mathbb{F}_2[\alpha]/ < \alpha^2 + \alpha + 1 >$ so that α is a zero of the polynomial x^2+x+1 which is irreducible over $\mathbb{F}_2[x]$. Then E contains the following points:

$$E(\mathbb{F}_q) = \{(0,1), (1,0), (1,1), (\alpha, 0), (\alpha, \alpha), (\alpha+1, 0), (\alpha+1, \alpha+1), \mathcal{O}\}\,.$$

Here $(0,1)$ is a point of order 2, which means that $[2](0,1) = \mathcal{O}$. So in total $E(\mathbb{F}_q)$ consists of 8 points. This gives

$$\begin{aligned} d(x) &= x^2 - (\#E(\mathbb{F}_q) - (q+1))x + q \\ &= x^2 - (8 - (4+1))x + 4 \\ &= x^2 - 3x + 4 \end{aligned}$$

with $D = 9 - 4 \cdot 4 = -7 < 0$.

5.3 Proof of lemma 5.3

In this section we want to prove that for the elliptic curve $E/\mathbb{F}_q$ we have $d_{-1} = \#E(\mathbb{F}_q)$. We will prove this lemma by first finding d_{-1}, and then by finding $\#E(\mathbb{F}_q)$.

We know $d_{-1} = \deg(\text{num}(x_{-1}))$, so first we need to find x_{-1}. By the recursion formula defined earlier, for $P_0, Q \in E^{tw}$, x_{-1} is given by

$$x_{-1} = x(P_{-1}) = x(P_0 - Q).$$

Use the addition formula (5.3b) to get

$$\begin{aligned} x_{-1} &= (x_0, y_0) - (t, 0) \\ &= (t^q, s^q + st^{q-1}) + (t, t) \\ &= \left(\frac{t + s^q + st^{q-1}}{t + t^q}\right)^2 + \left(\frac{t + s^q + st^{q-1}}{t + t^q}\right) + \left(a_2 + \frac{f(t)}{t^2}\right) + (t + t^q) \end{aligned}$$

Now use the following relations to simplify the above expression:

- By the relation of the elliptic curve $E/\mathbb{F}_q(t, s)$ we have $s^2 = st + f(t)$.
- We have $f(t) + t^3 + a_2t^2 + a_6 = 2f(t) = 0$ since $\text{char}(\mathbb{F}_q) = 2$.
- By the same relation as the first point, using the Frobenius morphism, we get $s^{2q} + t^q s^q = t^{3q} + a_2t^{2q} + a_6$.

Then simplifying the above expression of x_{-1} we get

$$\begin{aligned} x_{-1} &= \frac{s^2t^{2q-2} + t^{q+1} + ts^q + st^q + st^{2q-1} + f(t)t^{2q-2} + t^{2q+1} + t^{2+q}}{(t + t^q)^2} \\ &= \frac{s^2t^{2q-2} + t^{q+1} + ts^q + st^q + st^{2q-1} + a_2t^{2q} + a_6t^{2q-2} + t^{2+q}}{(t + t^q)^2} \\ &= \frac{(st + f(t))t^{2q-2} + t^{q+1} + ts^q + st^q + st^{2q-1} + a_2t^{2q} + a_6t^{2q-2} + t^{2+q}}{t + t^q)^2} \\ &= \frac{t^{2q+1} + t^{q+1} + t^{q+2} + ts^q + st^q}{(t + t^q)^2}. \end{aligned}$$

To proceed the proof of the lemma, we need to solve the following problem:

Is the x_{-1} above in lowest terms?

We proceed in the same way as in the other cases. So to solve this problem, we need to verify whether there are common terms in numerator and denominator. Before we are able to do this, we need to know the degree of the numerator of x_{-1} written in the form above. From lemma 5.1 we already know $\deg(s^q + st^{q-1}) = 3q/2$. Multiplying with t yields

$$\deg(ts^q + st^q) = \left(\frac{3q}{2} + 1\right) = \frac{3q+2}{2}.$$

This means that for $q \geq 2$ it follows

$$\deg(t^{2q+1} + t^{q+1} + t^{q+2} + ts^q + st^q) = 2q + 1.$$

Knowing this, find the common terms by taking an $\alpha \in \mathbb{F}_q$ and finding a corresponding β such that $\beta^2 + \alpha\beta = f(\alpha)$, i.e. $(\alpha, \beta) \in E$. Since $\alpha \in \mathbb{F}_q$, we know $\alpha^q = \alpha$ and the denominator of x_{-1} equals zero. Then we have three possibilities: $(\alpha, \beta) \in E(\mathbb{F}_q)$ with $\alpha \neq 0$, (α, β) is the unique point of order 2 given by $(\alpha, \beta) = (0, \beta) \in E(\mathbb{F}_q)$ and $(\alpha, \beta) \notin E(\mathbb{F}_q)$.

1. Assume (α, β) is the point of order 2. As we have seen in the remark below lemma 5.1, it must follow that $\alpha = 0$ and $\beta^2 = f(0) = a_6 \neq 0$. So $\beta \in \mathbb{F}_q$. For this point $(0, \beta)$ it follows that

   $$t^{2q+1} + t^{q+1} + t^{q+2} + ts^q + st^q|_{(0,\beta)} = 0$$

   which means that there is a common term in numerator and denominator, since both equal zero at the point $(0, \beta)$. The question is how many times it cancels from numerator and denominator. Therefore, consider the derivative of $t^{2q+1} + t^{q+1} + t^{q+2} + ts^q + st^q$. To find this derivative, we first need to find the derivative of $s^q + st^{q-1}$. We know $s^q + st^{q-1} \in \mathbb{F}_q[t]$, so for the derivative this must also hold. Furthermore, we have the relation of the elliptic curve given by $s^2 + st = t^3 + a_2t^2 + a_6$, and for this relation the derivatives must remain the same, so they must satisfy $(s^2 + ts)' = (t^3 + a_2t^2 + a_6)'$ (where ' stands for the derivative with respect to t). Writing this out yields

   $$2ss' + ts' + s = 3t^2 + 2a_2t = t^2$$

   hence

   $$s' = \frac{t^2 + s}{t}. \tag{5.5}$$

   Knowing this we can find the derivative of $s^q + st^{q-1}$, yielding

   $$\begin{aligned}(s^q + st^{q-1})' &= qs^{q-1}s' + s't^{q-1} + s(q-1)t^{q-2} \\ &= \frac{t^2 + s}{t}t^{q-1} + (q-1)st^{q-2} \\ &= t^{q-2}(t^2 + qs + s - s) \\ &= t^q. \end{aligned} \tag{5.6}$$

Using this last relation (5.6), we can find the derivative of the numerator of x_{-1} written in the form $t^{2q+1}+t^{q+1}+t^{q+2}+ts^q+st^q$. This yields (still using ' as the derivative with respect to t and using $2=q=0 \mod q$)

$$\begin{aligned}&\left(t^{2q+1}+t^{q+1}+t^{q+2}+ts^q+st^q\right)'\\&=(2q+1)t^{2q}+(q+1)t^q+(q+2)t^{q+1}+(s^q+qts^{q-1}s'+s't^q+qt^{q-1}s)\\&=t^{2q}+t^q+\left(s^q+\left(\frac{t^2+s}{t}\right)t^q\right)\\&=t^{2q}+t^q+s^q+st^{q-1}+t^{q+1}.\end{aligned}\tag{5.7}$$

And thus, evaluating at the point of order 2, $(\alpha,\beta)=(0,\beta)$, we get

$$\begin{aligned}\left(t^{2q+1}+t^{q+1}+t^{q+2}+ts^q+st^q\right)'|_{(0,\beta)}&=s^q|_{(0,\beta)}\\&=\beta^q=a_6^{q/2}\\&\neq 0.\end{aligned}$$

So the derivative of the numerator does not equal zero, while the numerator itself equals zero. This means we have a common term that cancels exactly once.

2. Assume $\beta \in \mathbb{F}_q$ and $\alpha \neq 0$. Then $\beta^q=\beta$, and if we substitute this in the numerator of x_{-1} we get

$$\begin{aligned}t^{2q+1}+t^{q+1}+t^{q+2}+ts^q+st^q&=\alpha^{2q+1}+\alpha^{q+1}+\alpha^{q+2}+\alpha\beta^q+\beta\alpha^q\\&=(\alpha^2)^q\alpha+\alpha^q\alpha+\alpha^q\alpha^2+\alpha\beta+\beta\alpha\\&=\alpha^3+\alpha^2+\alpha^3\\&=\alpha^2.\end{aligned}$$

   This means, since the numerator does not equal zero, that there are no common terms in numerator and denominator and thus there are no terms that cancel and can lower the degree. So consider the other possibility.

3. Assume $\beta \notin \mathbb{F}_q$. Then $\beta^q=\beta+\alpha$ since by the Frobenius map, β^q is mapped to the other zero of $y^2+\alpha y$, i.e. to $\beta+\alpha$. Then substituting the point (α,β) in the numerator of x_{-1} we get

$$\begin{aligned}t^{2q+1}+t^{q+1}+t^{q+2}+ts^q+st^q&=\alpha^{2q+1}+\alpha^{q+1}+\alpha^{q+2}+\alpha\beta^q+\beta\alpha^q\\&=(\alpha^2)^q\alpha+\alpha^q\alpha+\alpha^q\alpha^2+\alpha(\beta+\alpha)+\beta\alpha\\&=\alpha^3+\alpha^2+\alpha^3+\alpha\beta+\alpha^2+\alpha\beta\\&=0\end{aligned}$$

   and thus there are terms in the numerator and denominator that cancel. The only question is how many times it cancels. By the same reason as in the case $j(E)=0$, we know each term cancels twice.

Combining above three points yields that the total number of common terms in numerator and denominator is given by the point of order 2 plus each α such that $\beta \notin \mathbb{F}_q$ counting twice, so (counting the point (α,β) with $\alpha=0$ seperately)

$$\begin{aligned}\text{common terms}&=1+2\#\left\{\alpha\in\mathbb{F}_q|\nexists\beta\in\mathbb{F}_q\text{ such that }(\alpha,\beta)\in E,\alpha\neq 0\right\}\\&=1+2(q-\#\left\{\alpha\in\mathbb{F}_q|\exists\beta\in\mathbb{F}_q\text{ such that }(\alpha,\beta)\in E,\alpha\neq 0\right\}-1).\end{aligned}$$

And thus

$$\begin{aligned} d_{-1} &= \deg(\text{numerator}(x_{-1})) \\ &= 2q + 1 - (\text{common terms}) \\ &= 2q + 1 - (1 + 2(q - \#\{\alpha \in \mathbb{F}_q | \exists \beta \in \mathbb{F}_q \text{ such that } (\alpha, \beta) \in E, \alpha \neq 0\} - 1)) \\ &= 2 + 2\#\{\alpha \in \mathbb{F}_q | \exists \beta \in \mathbb{F}_q \text{ such that } (\alpha, \beta) \in E, \alpha \neq 0\}. \end{aligned}$$

Now the last step to finish the proof is finding $\#E(\mathbb{F}_q)$. Assume we have $\alpha \in \mathbb{F}_q$ which is the x-coordinate of a point in $E(\mathbb{F}_q)$. If $\alpha = 0$, then we have 1 point, namely the point of order 2. If $\alpha \neq 0$, then α is the x-coordinate of exactly two points, namely (α, β) and $(\alpha, \beta + \alpha)$. This yields, including the point at infinity that

$$\begin{aligned} \#E(\mathbb{F}_q) &= 1 + 1 + 2\#\{\alpha \in \mathbb{F}_q | \exists \beta \in \mathbb{F}_q \text{ such that } (\alpha, \beta) \in E, \alpha \neq 0\} \\ &= 2 + 2\#\{\alpha \in \mathbb{F}_q | \exists \beta \in \mathbb{F}_q \text{ such that } (\alpha, \beta) \in E, \alpha \neq 0\} \\ &= d_{-1}. \end{aligned}$$

This proves the lemma. □

5.4 Proof of lemma 5.2

The other important lemma is the basic identity, stating that $d_{n-1} + d_{n+1} = 2d_n + 2$.

Before proving the basic identity, we need to prove the following lemma.

Lemma 5.6. *If $P_n \neq \mathcal{O}$, then writing $P_n = \left(\frac{f_n}{g_n}, y_n\right)$, it follows* $\deg(f_n) > \deg(g_n)$. *Furthermore, $x_n \neq 0$.*

Proof. Consider the twisted elliptic curve (5.2) given by

$$E^{tw}/\mathbb{F}_q(t): \quad y^2 + xy = x^3 + \left(a_2 + \frac{f(t)}{t^2}\right)x^2 + a_6.$$

Just as in the previous cases, construct the valuation v_∞, the rings O and $O^\times$ and the maximal ideal $\mathcal{M}$. Then a generator for $\mathcal{M}$ is given by $\frac{1}{t}$ and to reduce E^{tw} modulo $\mathcal{M}$ we need to write E^{tw} in terms of the generator $\frac{1}{t}$. Therefore, multiply E by $\frac{1}{t^6}$ to get

$$\left(\frac{y}{t^3}\right)^2 + \frac{1}{t}\left(\frac{x}{t^2}\right)\left(\frac{y}{t^3}\right) = \left(\frac{x}{t^2}\right)^3 + \left(\frac{a_2}{t^2} + \frac{f(t)}{t^4}\right)\left(\frac{x}{t^2}\right)^2 + \frac{a_6}{t^6}.$$

Make the substitution $\eta = \frac{y}{t^3}$, $\xi = \frac{x}{t^2}$ to obtain

$$E^{tw}: \quad \eta^2 + \frac{1}{t}\xi\eta = \xi^3 + \left(\frac{a_2}{t^2} + \frac{f(t)}{t^4}\right)\xi^2 + \frac{a_6}{t^6}.$$

Now we expressed E^{tw} in terms of the generator of $\mathcal{M}$, which means that we can reduce this curve modulo $\frac{1}{t}$ to get

$$\tilde{E}^{tw}/\mathbb{F}_q: \quad \eta^2 = \xi^3.$$

Also this curve is singular with singular point $(\eta, \xi) = (0, 0)$, so according to [19, VII.5] E^{tw} has bad, additive reduction and thus, according to [19, thm VII.5.1], we have $\tilde{E}^{tw}_{ns}(\mathbb{F}_q) \simeq (\mathbb{F}_q, +)$. Now we look at the points on the curve.

- We know $Q = (t, 0) \in E^{tw}(\mathbb{F}_q(t))$. Now writing the curve in terms of ξ means mapping the x-coordinate to $\frac{x}{t^2}$. So the point $Q = (t, 0)$ will be written as $(\frac{1}{t}, 0)$ and under reduction modulo $\frac{1}{t}$ this point will map to $\tilde{Q} = (0, 0)$. This means Q maps to a singular point on the reduced curve.
- Another point on E^{tw} is given by $P_0 = (t^q, s^q + st^{q-1})$ where $s^q + st^{q-1} \in \mathbb{F}_q[t]$. Under the mapping $x \mapsto \frac{x}{t^2}$ this point is given by $(t^{q-2}, \tilde{y})$ where $\tilde{y}$ is the y-coordinate of the mapping $x \mapsto \frac{x}{t^2}$ applied on $s^q + st^{q-1}$. Now when reducing modulo $\mathcal{M}$ also the point P_0 changes. The only question is whether P_0 maps to a nonsingular point. Since $v_\infty(t^{q-2}) = 2 - q \leq 0$, we have $t^{q-2} \notin \mathcal{M}$, hence P_0 does not reduce to the singular point $(0, 0)$.

So a question arises. What points of $E^{tw}(\mathbb{F}_q(t))$ do lie in $E^{tw}_{ns}(\mathbb{F}_q(t))$, i.e. reduce to a nonsingular point modulo $\frac{1}{t}$? To answer this question, use the following lemma.

Lemma 5.7. *For an arbitrary point* $\zeta = \left(\frac{f}{g}, y\right) \in E^{tw}(\mathbb{F}_q(t))$*, one has*

$$\zeta \in E^{tw}_{ns}(\mathbb{F}_q(t)) \Leftrightarrow \deg(f) > \deg(g) + 1.$$

Proof. Take $\zeta = \left(\frac{f}{g}, y\right) \in E^{tw}(\mathbb{F}_q(t))$ arbitrary. Then $\xi(\zeta) = \left(\frac{f}{gt^2}, \frac{y}{t^3}\right)$. Now apply reduction modulo $\mathcal{M}$.

- Suppose $v(f) = v(t^2 g)$. Then $v\left(\frac{f}{t^2 g}\right) = 0$, so $\frac{f}{t^2 g} \in O^\times$ which means $\frac{f}{t^2 g} \notin \mathcal{M}$, so $\frac{f}{t^2 g} \mod \mathcal{M} \neq 0$, hence ζ does not reduce to the singular point.
- Suppose $v(f) > v(t^2 g)$. Then $v\left(\frac{f}{t^2 g}\right) > 0$, so $\frac{f}{t^2 g} \in \mathcal{M}$ which means $\frac{f}{t^2 g} \mod \mathcal{M} = 0$ so ζ reduces to the singular point.
- Suppose $v(f) < v(t^2 g)$. Then $v\left(\frac{f}{t^2 g}\right) < 0$, so ζ reduces to $(0 : 1 : 0)$ which is nonsingular.

This shows

$$\begin{aligned} \zeta \in E^{tw}_{ns}(\mathbb{F}_q(t)) &\Leftrightarrow v_\infty(f) \leq v_\infty(t^2 g) \\ &\Leftrightarrow -\deg(f) \leq -2 - \deg(g) \\ &\Leftrightarrow \deg(f) > \deg(g) + 1 \end{aligned}$$

which proves the lemma. □

Note that $E^{tw}_{ns}(\mathbb{F}_q(t))$ is a group, which means that for two points in this group also their sum must be in the group. Earlier we've seen that Q maps to the singular point $(0, 0)$. Now consider $2Q$ given by

$$2Q = 2(t, 0) = \frac{t^4 + a_6}{t^2}.$$

Then $\xi(2Q) = \frac{t^4 + a_6}{t^4}$ and thus $v_\infty = 0$, yielding $2Q$ does not map to the singular point. This means, since $P_0 \in E^{tw}_{ns}(\mathbb{F}_q(t))$, also $P_0 + nQ \in E^{tw}_{ns}(\mathbb{F}_q(t))$ for even numbers n. Now for the odd n, use the following lemma.

Lemma 5.8. *If $P \in E_{ns}^{tw}(\mathbb{F}_q(t))$, then writing $P = \left(\frac{f}{g}, y\right)$ one has* $\deg(num(x(P+Q))) > \deg(den(x(P+Q)))$.

Proof. The proof is the same as the proof of lemma 4.7 when using addition formula (5.3a). Because of the length of the formulas, the proof is omitted here. □

This means that also $P_0 + Q \in E_{ns}^{tw}(\mathbb{F}_q(t))$ and thus $P_0 + nQ \in E_{ns}^{tw}(\mathbb{F}_q(t))$ for all numbers n, and thus also for this sum we have that the degree of the numerator is greater than the degree of the denominator. That $x_n \neq 0$ follows from the reduction modulo $\mathcal{M}$. □

Knowing this, we are ready to prove the basic identity. Just as in the previous cases, first we prove three special cases before proving the general case. For the special cases we need the duplication formula (5.3b) given by

$$x([2]\zeta_1) = \frac{x^4 - a_6}{4x^3 + x^2}.$$

- Assume $P_{n-1} = \mathcal{O}$. Then $P_n = \mathcal{O} + Q = (t, 0)$ and $P_{n+1} = P_n + Q - 2(t, 0)$. By the duplication formula we have

  $$x(P_{n+1}) = \frac{t^4 + a_6}{t^2}.$$

  Since $\gcd(t^4 + a_6, t^2) = 1$, it follows that $d_{n+1} = 4$. Furthermore, $d_{n-1} = 0$ and $d_n = 1$, so indeed the basic identity holds.

- Assume $P_n = \mathcal{O}$. Then $P_{n-1} = P_n - (t, 0) = (t, t)$ and $P_{n+1} = P_n + (t, 0) = (t, 0)$. This automatically gives $d_{n-1} = d_{n+1} = 1$ and $d_n = 0$ which yields the basic identity.

- Assume $P_{n+1} = \mathcal{O}$. Then $P_n = P_{n+1} - (t, 0) = (t, t)$ and $P_{n-1} = P_n - Q = 2(t, t)$. This gives

  $$x(P_{n-1}) = \frac{t^4 + a_6}{t^2}.$$

  By exactly the same argument as above, we have $d_{n+1} = 0$, $d_n = 1$ and $d_{n-1} = 4$ which yields the basic identity.

After these three special cases we consider the general case where we can assume that neither P_{n-1}, P_n or P_{n+1} is the point at infinity $\mathcal{O}$. Since we want to prove that

$$d_{n-1} + d_{n+1} = 2d_n + 2$$

we are interested in x_{n-1} and x_{n+1}. Since $P_n \neq \mathcal{O}$ we can write $P_n = (x_n, y_n)$ and it follows that

$$\begin{aligned} P_{n-1} &= P_n - Q \\ &= (x_n, y_n) + (t, t). \end{aligned}$$

Then using addition formula (5.3a), using $y^2 + xy = x^3 + a_2x^2 + a_6 + \frac{f(t)}{t^2}x^2$, writing $x_n = \frac{f_n}{g_n}$ and simplifying we get

$$\begin{aligned}
x_{n-1} &= \left(\frac{t+y_n}{t+x_n}\right)^2 + \left(\frac{t+y_n}{t+x_n}\right) + \left(a_2 + \frac{f(t)}{t^2}\right) + (t+x_n) \\
&= \frac{tx_n + ty_n + tx_n^2 + t^2x_n + (f(t) + t^3 + a_2t^2 + a_6)}{(t+x_n)^2} \\
&= \frac{tx_n + ty_n + tx_n^2 + t^2x_n}{(t+x_n)^2} \\
&= \frac{ty_ng_n^2 + tf_ng_n + tf_n(f_n + tg_n)}{(f_n + tg_n)^2} \qquad (5.8a) \\
&= \frac{R}{(f_n + tg_n)^2}. \qquad (5.8b)
\end{aligned}$$

Note that $R \in \mathbb{F}_q[t]$. To see this, again write down the equation of the elliptic curve:

$$y_n^2 + x_ny_n = x_n^3 + a_2x_n^2 + a_6$$

and thus it follows by writing $x_n = \frac{f_n}{g_n}$ that

$$(y_ng_n^2)^2 + (y_ng_n^2)f_ng_n = f_n^3g_n + a_2f_n^2g_n^2 + a_6g_n^4.$$

This gives that $(y_ng_n^2)^2 + (y_ng_n^2)f_ng_n$ is a polynomial in t and by the same argument used in the case $j(E) = 0$ we have $y_ng_n^2 \in \mathbb{F}_q[t]$, hence $R \in \mathbb{F}_q[t]$.
In the same way we have

$$\begin{aligned}
P_{n+1} &= P_n + Q \\
&= (x_n, y_n) + (t, 0)
\end{aligned}$$

which yields

$$\begin{aligned}
x_{n+1} &= \left(\frac{y_n}{t-x_n}\right)^2 - \left(\frac{y_n}{t-x_n}\right) - \left(a_2 + \frac{f(t)}{t^2}\right) - (t+x_n) \\
&= \frac{ty_n + tx_n^2 + t^2x_n + (f(t) + t^3 + a_2t^2 + a_6)}{(t+x_n)^2} \\
&= \frac{ty_n + tx_n^2 + t^2x_n}{(t+x_n)^2} \\
&= \frac{ty_ng_n^2 + tf_n(f_n + tg_n)}{(f_n + tg_n)^2} \qquad (5.9a) \\
&= \frac{S}{(f_n + tg_n)^2} \qquad (5.9b)
\end{aligned}$$

with $S \in \mathbb{F}_q[t]$.
So writing $x_{n\pm1} = \frac{f_{n\pm1}}{g_{n\pm1}}$ in lowest terms we have

$$x_{n-1} = \frac{f_{n-1}}{g_{n-1}} = \frac{R}{(f_n + tg_n)^2} = \frac{ty_ng_n^2 + tf_ng_n + tf_n(f_n + tg_n)}{(f_n + tg_n)^2}, \qquad (5.10)$$

$$x_{n+1} = \frac{f_{n+1}}{g_{n+1}} = \frac{S}{(f_n + tg_n)^2} = \frac{ty_ng_n^2 + tf_n(f_n + tg_n)}{(f_n + tg_n)^2}. \qquad (5.11)$$

Using these two formulas and substituting $y_n^2 = x_n y_n + f(x_n) + \frac{f(t)}{t^2}$, we obtain $x_{n-1}x_{n+1}$:

$$\begin{aligned}
x_{n-1}x_{n+1} &= \frac{f_{n-1}f_{n+1}}{g_{n-1}g_{n+1}} && (5.12a)\\
&= \frac{RS}{(f_n+tg_n)^4} && (5.12b)\\
&= \frac{t^2y_n^2g_n^4 + t^2f_ng_n^3y_n + t^2f_n^3g_n + t^3f_n^2g_n^2 + t^2f_n^4 + t^4f_n^2g_n^2}{(f_n+tg_n)^4}\\
&= \frac{(a_6g_n^2 + f_n^2t^2)(f_n+tg_n)^2}{(f_n+tg_n)^4}\\
&= \frac{a_6g_n^2 + f_n^2t^2}{(f_n+tg_n)^2}. && (5.12c)
\end{aligned}$$

Note that the numerator in (5.12a) has degree $d_{n+1} + d_{n-1}$ and the numerator in (5.12c) has degree $2d_n + 2$. So the basic identity holds if

$$g_{n-1}g_{n+1} \text{ and } (f_n + tg_n)^2 \text{ differ by a nonzero constant.}$$

To show this, take an irreducible polynomial $l \in \mathbb{F}_q[t]$ and show it divides both terms the same number of times. Therefore, consider the valuation map

$$v_l : \quad \mathbb{F}_q(t) \to \mathbb{Z} \cup \{\infty\}$$

defined as the number of times the irreducible polynomial l appears in the factorization of a quotient of polynomials in $\mathbb{F}_q[t]$. Then we want to show that

$$v_l(g_{n-1}g_{n+1}) = v_l((f_n + tg_n)^2). \tag{5.13}$$

Consider again (5.8b) and (5.9b):

$$\begin{aligned}
x_{n-1} &= \frac{f_{n-1}}{g_{n-1}} = \frac{R}{(f_n+tg_n)^2},\\
x_{n+1} &= \frac{f_{n+1}}{g_{n+1}} = \frac{S}{(f_n+tg_n)^2}.
\end{aligned}$$

As $\frac{f_{n-1}}{g_{n-1}}$ and $\frac{f_{n+1}}{g_{n+1}}$ are written in lowest terms, from above two formulas we can conclude that $f_{n-1} \mid R$, $g_{n-1} \mid (f_n + tg_n)^2$ and $f_{n+1} \mid S$, $g_{n+1} \mid (f_n + tg_n)^2$. This means that at least we have

$$v_l(g_{n\pm1}) \leq v_l((f_n + tg_n)^2).$$

Furthermore, we have

Lemma 5.9. $v_l(g_{n-1}g_{n+1}) \leq v_l((f_n + tg_n)^2)$.

Again the proof is omitted since it is exactly the same as the proof of lemma 3.7. To show equality in the lemma, consider the following cases.

Case 1: Suppose $v_l(f_n + tg_n) = 0$. Then we have

$$0 \leq v_l(g_{n+1}g_{n-1}) \leq v_l((f_n + tg_n)^2) = 0$$

which yields

$$v_l((f_n + tg_n)^2) = 0 = v_l(g_{n-1}g_{n+1})$$

which is what we wanted to prove.
Case 2: Suppose $v_l(f_n + tg_n) > 0$. Then using formulas (5.12b) and (5.12c) given by

$$x_{n-1}x_{n+1} = \frac{f_{n-1}f_{n+1}}{g_{n-1}g_{n+1}} = \frac{RS}{(f_n + tg_n)^4} = \frac{a_6^2 g_n^2 + f_n^2 t^2}{(f_n + tg_n)^2}$$

yields $(f_n + tg_n)^2 \mid RS$. So since $v_l(f_n + tg_n) > 0$, also $v_l(RS) > 0$. Now this case splits in two subcases, one where l divides exactly one of R and S, where we assume l divides R. The case where l divides S (but not R) is exactly the same and is therefore omitted. The other subcase considers l dividing both R and S.
Case 2a: Assume $v_l(R) > 0$ and $v_l(S) = 0$. Then

$$2v_l(f_n + tg_n) \leq v_l(RS) = v_l(R) + v_l(S) = v_l(R).$$

Applying (5.10) gives $v_l(g_{n-1}) = 0$ since we can divide out the denominator from R. Now by exactly the same reasoning as case 2a in section 3.3.2, we can conclude that $v_l(g_{n+1}) = v_l((f_n + tg_n)^2)$. This yields

$$v_l(g_{n-1}g_{n+1}) = v_l(g_{n-1}) + v_l(g_{n+1}) = v_l((f_n + tg_n)^2)$$

which we wanted to prove.
Case 2b: Assume $v_l(R) > 0$ and $v_l(S) > 0$. This implies, using $R + S = tf_ng_n$, that $v_l(tf_ng_n) > 0$. In the same way as in claim 1 from section 3.3.2 we have $v_l(g_n) = 0$, hence $v_l(tf_n) > 0$. We also have $v_l(RS) > 0$, so $v_l(a_6g_n^2 + f_n^2t^2) > 0$. Since $v_l(tf_n) > 0$ it follows $v_l(a_6g_n^2) > 0$, hence $v_l(g_n) > 0$. Since we just said this is impossible, this case will not occur. So we are in one of the other cases, in which we are done.

So in all possible cases, we have proven

$$v_l(g_{n-1}g_{n+1}) = v_l((f_n + tg_n)^2)$$

which proves the basic identity. □

6 Link to other proofs

In this chapter we consider the connection between the proof of Manin and the proof of Silverman, and we will give a much shorter proof of the lemmas 3.5, 4.5 and 5.6.

6.1 Connection to Silverman

In this section we will show how the proof of Manin basically is the same as other proofs, for example the proof in [19, V.1.1.1]. Start with a random elliptic curve E over $\mathbb{F}_q$ for $q = p^r$, and p a random prime. Following the proof of Silverman (which will be skipped) we arrive at the following relation:

$$\#E(\mathbb{F}_q) = \deg(\phi - 1).$$

Here ϕ is the Frobenius map given by

$$\begin{aligned} \phi : &E \to E \\ &(x, y) \mapsto (x^q, y^q). \end{aligned}$$

This gives a formula to find the number of points on E.
But we also followed the proof of Manin, see the chapters 3, 4 and 5. In these proofs we also found a formula to compute the number of points on the elliptic curve, namely

$$\#E(\mathbb{F}_q) = d_{-1}.$$

To show the relation between the proofs of Manin and Silverman, we therefore want to show that

$$d_{-1} = \deg(\phi - 1).$$

To show this relation, we want to prove a more general statement from which this relation above follows. Define the following map:

$$\begin{aligned} [n] : &E \to E \\ &P \mapsto n \cdot P. \end{aligned}$$

The relation we want to show is that

$$\deg(\phi + [n]) = \max\{\deg(f_n), \deg(g_n)\} \tag{6.1}$$

since if this relation holds for all $n \in \mathbb{Z}$, it also holds for $n = -1$ and thus

$$\deg(\phi - 1) = \max\{\deg(f_{-1}), \deg(g_{-1})\}$$

and in the proof of Manin it holds that this expression equals d_{-1}. To prove above relation, first consider the mapping $\phi + [n]$. We have

$$\begin{aligned} \phi + [n] : &E \to E \\ &(x, y) \mapsto (r(x, y), y_n(x, y)). \end{aligned}$$

Here r, y_n are rational expressions in x, y in $\mathbb{F}_q(E)$ since the sum of two points on the elliptic curve gives again a point on the curve, which can be expressed in terms of x and y again by the addition formula. Now we want to know how $r(x, y)$ looks like.

Lemma 6.1. *After mapping (x, y) to $(\phi+[n])(x, y)$, we have $r(x, y)$ is a rational expression in x, i.e. $r(x, y) = \frac{f_n(x)}{g_n(x)}$ for some functions $f_n, g_n \in \mathbb{F}_q[x]$*

Proof. Proof this lemma by induction, so first take $n = 0$. Then we have

$$(\phi + [n])(x, y) = \phi(x, y) = (x^q, y^q)$$

and thus indeed $r(x, y) = x^q$ is a rational expression in x. To make the rest of the proof more clear, also consider $n = 1$. Then we have

$$\begin{aligned}(\phi + [1])(x, y) &= \phi(x, y) + (x, y)\\ &= (x^q, y^q) + (x, y)\\ &= \left(\frac{f_1(x)}{g_1(x)}, y_1(x, y)\right)\end{aligned}$$

where the last line follows because of the addition formula (see (2.3)), which makes sure that the x-coordinate of the third point is a rational expression in x. Now assume this lemma holds for n. Then try to show it for $n + 1$:

$$\begin{aligned}(\phi + [n + 1])(x, y) &= \phi(x, y) + [n + 1](x, y)\\ &= (\phi(x, y) + [n](x, y)) + (x, y)\\ &= \left(\frac{f_n(x)}{g_n(x)}, y_n(x, y)\right) + (x, y)\\ &= \left(\frac{f_{n+1}(x)}{g_{n+1}(x)}, y_{n+1}(x, y)\right)\end{aligned}$$

where the last line again follows from (2.3). So indeed we have

$$\begin{aligned}\phi + [n] :&E \to E\\ (x, y) \mapsto (r(x, y), y_n(x, y)) &= \left(\frac{f_n(x)}{g_n(x)}, y_n(x, y)\right).\end{aligned}$$

□

Knowing this, we have the following field extension:

$$\mathbb{F}_q(r, y_n) \subset \mathbb{F}_q(x, y).$$

Using this, we arrive at the following.

Definition 6.1. $\deg(\phi + [n])$ *is defined as the degree of above extension.*

This gives us the following diagram:

$$\begin{array}{ccc} \mathbb{F}_q(r, y_n) & \subset & \mathbb{F}_q(x, y)\\ \bigcup_2 & & \bigcup_2\\ \mathbb{F}_q(r) & \subset & \mathbb{F}_q(x). \end{array}$$

Here both extensions from the lower to the upper fields are of degree 2 since y and y_n both satisfy the elliptic curve and are thus quadratic in y. Furthermore, since $-(x, y)$ gives a completely different point, the degree is exactly 2. Another way to see this is using [21, def 6.2], stating that the degree of an extension is the dimension of $\mathbb{F}_q(r, y_n)$ considered as a $\mathbb{F}_q(r)$-vectorspace. A basis for $\mathbb{F}_q(r, y_n)$ as a $\mathbb{F}_q(r)$-vectorspace is given by $\{1, y_n\}$ and obviously this dimension is 2, i.e.

$$\dim_{\mathbb{F}_q(r)} \mathbb{F}_q(r, y_n) = 2.$$

Following the above diagram from $\mathbb{F}_q(r)$ to $\mathbb{F}_q(x, y)$ via both ways gives us that

$$2 \cdot \deg[\mathbb{F}_q(x, y) : \mathbb{F}_q(r, y_n)] = 2 \cdot \deg[\mathbb{F}_q(x) : \mathbb{F}_q(r)]$$

and using the definition that $\deg[\mathbb{F}_q(x, y) : \mathbb{F}_q(r, y_n)] = \deg(\phi + [n])$ gives us that

$$\deg(\phi + [n]) = \deg[\mathbb{F}_q(x) : \mathbb{F}_q(r)].$$

Lemma 6.2. *For a field k with rational function field $k(t)$ and polynomials $f, g \in k[t]$ with $\gcd(f, g) = 1$ one has that $k\left(\frac{f}{g}\right) \subset k(t)$ is an extension of degree $\max\{\deg(f), \deg(g)\}$. So when taking $k = \mathbb{F}_q$, by writing $f = f_n$, $g = g_n$, one has $[\mathbb{F}_q(t) : \mathbb{F}_q\left(\frac{f}{g}\right)] = \max\{\deg(f), \deg(g)\}$.*

Proof. We will give the proof only for the special case $k = \mathbb{F}_q(t)$ since this is the case we are interested in.
According to [21, thm 6.6] for an algebraic extension $[k(t) : k\left(\frac{f}{g}\right)]$ we have $\deg[k(t) : k\left(\frac{f}{g}\right)] = \deg(m(X))$ where m is the minimal polynomial of t over $k\left(\frac{f}{g}\right)$, i.e. the unique monic polynomial such that $m(t) = 0$ and $m(X)$ is irreducible in the polynomial ring $k\left(\frac{f}{g}\right)[X]$. So we want to find the minimal polynomial $m(X)$ of the extension

$$[\mathbb{F}_q(t) : \mathbb{F}_q(r)] = \left[\mathbb{F}_q(t) : \mathbb{F}_q\left(\frac{f(t)}{g(t)}\right)\right].$$

Therefore, define the polynomial $m(X) \in \mathbb{F}_q\left(\frac{f}{g}\right)[X]$ by

$$m(X) = g(X) \cdot \frac{f(t)}{g(t)} - f(X).$$

Then indeed $m(t) = 0$ as required. Furthermore, write

$$b = \frac{f(t)}{g(t)}$$

to get

$$m(X) = g(X) \cdot b - f(X) \in \mathbb{F}_q(b)[X].$$

Now we have to check whether this polynomial is irreducible in $\mathbb{F}_q(b)[X]$. To do this, use the lemma of Gauss, which states that if a polynomial f is irreducible in $K[X]$, then it is also irreducible in $K(X)$. So here consider $\mathbb{F}_q[b][X]$. Note that

$$\mathbb{F}_q[b][X] = \mathbb{F}_q[b, X] = \mathbb{F}_q[X][b].$$

And thus, considering m as a polynomial in b we have

$$m(b) = g(X)b - f(X)$$

which is irreducible in $\mathbb{F}_q[X][b]$ since $m(b)$ is a linear polynomial. So m is irreducible in $\mathbb{F}_q[b][X]$ and thus also in $\mathbb{F}_q[b,X]$ and in $\mathbb{F}_q[X][b]$. So indeed $m(X)$ is an irreducible polynomial in $\mathbb{F}_q(b)[X]$. This implies that $m(X)$ is the minimal polynomial, so

$$[\mathbb{F}_q(t) : \mathbb{F}_q(r)] = \left[\mathbb{F}_q(t) : \mathbb{F}_q\left(\frac{f(t)}{g(t)}\right)\right] = \deg(m(X))$$

and from

$$m(X) = g(X) \cdot b - f(X) \in \mathbb{F}_q(b)[X]$$

it is quite easy to see that $\deg(m(X)) = \max\{\deg(f(t)), \deg(g(t))\}$. □

Combining everything (since we are working over $\mathbb{F}_q(t)$ we can write all fields and polynomials in terms of t) gives

$$\deg(\phi + [n]) = \deg[\mathbb{F}_q(t) : \mathbb{F}_q(r)] = \deg(m(X)) = \max\{\deg(f_n(t)), \deg(g_n(t))\}$$

which we wanted to prove. So indeed the proofs of Manin and Silverman are basically the same via the relation

$$\deg(\phi + [n]) = \max\{\deg(f_n), \deg(g_n)\}$$

which yields (in the case of the proof of Manin)

$$\deg(\phi - 1) = \max\{\deg(f_{-1}), \deg(g_{-1})\} = \deg(f_{-1}) = d_{-1}.$$

6.2 Proof of the three lemmas

In this subsection we will give a proof of the lemmas 3.5, 4.5 and 5.6 without using reduction theory. The new proof will make use of the order of poles at the point $\mathcal{O}$, and the proof is valid for all three cases. The lemma we want to prove is the following:

Lemma 6.3. *If $P \in E(\mathbb{F}_q)$ satisfies $P \neq \mathcal{O}$, then writing $P = \left(\frac{f}{g}, y\right)$, it follows $\deg(f) > \deg(g)$.*

Proof. The map $\phi \in End_{\mathbb{F}_q}(E,E)$ is a homomorphism. A requirement on this is that the point at infinity $\mathcal{O}$ is mapped into $\mathcal{O}$. Furthermore, $End_{\mathbb{F}_q}(E,E)$ can be identified with $E(\mathbb{F}_q(t,s))$ and therefore it is enough to consider points $P \in E(\mathbb{F}_q(t,s))$.

We know for a point $P \in E(\mathbb{F}_q(t,s))$ we can write $P = \left(\frac{f(t)}{g(t)}, y(s,t)\right)$. Now for this point P, consider the order of the pole at $\mathcal{O}$ of both $f(t)$ and $g(t)$. As we have seen in the proof of lemma 4.1, for t it holds that $v_\infty(t) = -2$ and thus for a polynomial $f(t)$ of degree m one has

$$v_\infty(f(t)) = -2m.$$

In the same way, for $g(t)$ of degree n one has

$$v_\infty(g(t)) = -2n.$$

This means that

$$v_\infty\left(\frac{f(t)}{g(t)}\right) = -2m + 2n.$$

Claim: $v_\infty\left(\frac{f(t)}{g(t)}\right) < 0$.

To prove this claim, assume the statement is not true. This means that $v_\infty\left(\frac{f(t)}{g(t)}\right) = -2m + 2n \geq 0$ and thus $n \geq m$. Applying ϕ on this point P then means that $v_\infty(\phi(P)) > 0$, and thus $\mathcal{O}$ is not mapped to $\mathcal{O}$. This means the claim must be true.

Then using this claim one has $P = \left(\frac{f(t)}{g(t)}, y(s,t)\right)$ maps $\mathcal{O}$ to $\mathcal{O} \Leftrightarrow v_\infty\left(\frac{f(t)}{g(t)}\right) < 0$ and from this it follows

$$-2m + 2n < 0 \Leftrightarrow m > n.$$

Since m and n were defined as the degrees of the polynomials $f(t)$ and $g(t)$ it follows $\deg(f(t)) > \deg(g(t))$.

□

This much shorter argument proves the same as the reduction theory, and is valid for all characteristics. Note: J.W.S. Cassels notes in his review of the proof of Manin that he is not sure that $\deg(f_n) > \deg(g_n)$ for the f_n defined in Manins way. But here we have shown in two different ways that indeed this statement holds. For the review of Cassels, see [3].

7 Curves of genus 2

In all previous chapters we considered elliptic curves of the general form

$$E/\mathbb{F}_q : \quad y^2 + (a_1x + a_3)y = x^3 + a_2x^2 + a_4x + a_6 = f(x). \tag{7.1}$$

Recall that an elliptic curve is a curve of genus 1. In this chapter we will consider curves of genus 2, yielding the following definition, see [14].

Definition 7.1. *A hyperelliptic curve of genus 2 is a curve C of the form*

$$C/\mathbb{F}_q : \quad y^2 + h(x)y = f(x) \tag{7.2}$$

satifying the following properties:

1. *$f(x) \in \mathbb{F}_q[x]$ is a monic polynomial of degree 5 given by $f(x) = x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0$,*

2. *$h(x) \in \mathbb{F}_q[x]$ is a polynomial of at most degree 2,*

3. *There are no points (α, β) on the curve C such that both partial derivatives of C equal zero at the same time, so for $(\alpha, \beta) \in C$ we must have*

$$(h'(\alpha)\beta - f'(\alpha), 2\beta + h(\alpha)) \neq (0, 0).$$

Remark: A more general definition of a hyperelliptic curve over a field K is a curve C admitting a seperable $2:1$ morphism to a rational curve D over K. In case $K = \mathbb{F}_q$ it is known that any rational curve D is isomorphic to $\mathbb{P}^1$ over K, so here the definition may be given as a curve admitting a seperable $2:1$ morphism to $\mathbb{P}^1$. Our definition adds the requirements that C has genus 2, the morphism is given by $(x, y) \mapsto x$ and that the point at infinity on $\mathbb{P}^1$ has only one pre-image in C.

Example 7.1. To compare the picture of an hyperelliptic curve of genus 2 to the one of an elliptic curve as given in figure 1, consider the following hyperelliptic curve of genus 2 over $\mathbb{R}$.

$$C/\mathbb{R} : \quad y^2 = x^5 - 2x^4 - 7x^3 + 8x^2 + 12x.$$

Then this curve has a graph that looks like the one in figure 1, only with one closed loop extra. See also figure 4.

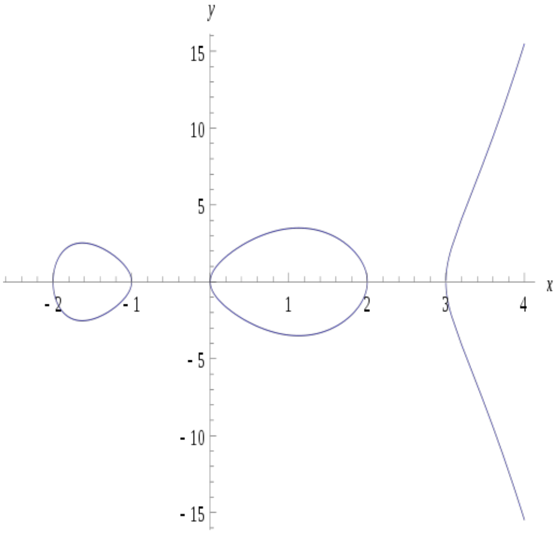

Figure 4: A hyperelliptic curve of genus 2 over $\mathbb{R}$

Andrew Weil proved (1942/1948) a Hasse inequality for arbitrary curves over $\mathbb{F}_q$. For the specific curve defined above, this inequality is given by the following theorem.

Theorem 7.1 (Hasse's Theorem on Hyperelliptic Curves of genus 2)**.** *For the hyperelliptic curve C defined above in* (7.2)*, the number $\#C(\mathbb{F}_q)$ of points over $\mathbb{F}_q$ satisfies the inequality*

$$|\#C(\mathbb{F}_q) - (q+1)| \leq 4\sqrt{q}.$$

We want to prove the Hasse inequality for hyperelliptic curves in the same way as is done in the previous chapters. We do not know if this is possible. Therefore, in this chapter we try to do some of the steps taken in the proof as done in chapter 3, using the computer program Magma to do most of the calculations. Furthermore, we only consider the case char($\mathbb{F}_q$) ≥ 3, in which we can rewrite the hyperelliptic curve (7.2) in the form

$$C/\mathbb{F}_q : \quad y^2 = f(x) \tag{7.3}$$

where $f(x) = x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0$.
The first step is to find the group law on the Jacobian of hyperelliptic curves. Before defining this Jacobian, we need the following two definitions, see also [19, II.3]

Definition 7.2. *A divisor is a formal sum $\sum_{P \in C} n_P P$ where P are points on the curve C and the n_P are numbers nonzero for only finitely many P. A divisor of degree 0 is a divisor such that $\sum n_P = 0$.*

Definition 7.3. *A divisor of a function f is defined as $div(f) = (\sum zeroes - \sum poles)$ including multiplicity. These divisors are also called principal divisors.*

Combining above two definitions we arrive at the definition of the Jacobian of a curve.

Definition 7.4. *The Jacobian of a hyperelliptic curve $C/\mathbb{F}_q$ is defined as the group of divisorclasses, i.e. the group of divisors of degree 0 modulo principal divisors. The Jacobian is denoted by $Jac(C)$.*

Next we want to find a function that can give us the numbers d_n to define some basic identity. To do this, Magma defines $C/\mathbb{F}_q(t,s)$ where t,s satisfy

$$s^2 = f(t).$$

Furthermore, we need to know in which way points on the Jacobian of a curve are defined. According to [4] an arbitrary divisor class can be written in the form

$$D = [P_1 + P_2 - 2P_\infty]$$

where P_1 and P_2 are points on the curve C and P_∞ is the unique point at infinity. When one of P_1 or P_2 equals P_∞, say $P_2 = P_\infty$, we can write the divisor class as

$$D = [P_1 - P_\infty].$$

In Magma, a point $P \in Jac(C)$ is written as

$$(g(x), y(x), z)$$

where $g(x), y(x), z$ have the following meaning:

- z equals 2 if the divisor class can be written as $P_1 + P_2 - 2P_\infty$, and z equals 1 if it can be written as $P_1 - P_\infty$.
- $g(x)$ is a monic polynomial of degree 1 or degree 2, depending on the value of z. When z equals 2, $g(x)$ is a quadratic polynomial, when z equals 1, $g(x)$ is a linear polynomial. Solving $g(x) = 0$ gives the x-coordinates of the points P_i ($i \neq \infty$) in the divisor class.
- To find the corresponding y-coordinate of the point, compute $y(x)$ with the x-coordintate found from $g(x)$. When two points are needed in the divisor class, but only one x-coordinate is obtained from $g(x)$, also take the point $(x, -y)$.

To make this more clear, consider the following example.

Example 7.2. Take as the hyperelliptic curve C the curve defined by

$$C/\mathbb{F}_7 : \quad y^2 = x^5 + 4x^4 + 6x^3 + 3x^2 + x + 4$$

Asking Magma for two random points on the Jacobian of C gives as result

$$\begin{aligned} P &= (x, 5, 1) \\ Q &= (x^2 + 5x, 5x + 5, 2) \\ P + Q &= (x^2 + 6x + 4, 2x + 2, 2) \end{aligned}$$

This means that the divisor classes of these points are the following.

$$\begin{aligned} P &= [(0,5) - P_\infty] \\ Q &= [(0,5) + (2,1) - 2P_\infty] = [(0,2) + (0,5) - 2P_\infty] \\ P + Q &= [(-3 + \sqrt{5}, 3 + 2\sqrt{5}) + (-3 - \sqrt{5}, 3 - 2\sqrt{5}) - 2P_\infty]. \end{aligned}$$

Now try to proceed with the proof for hyperelliptic curves in the same way as the proof for elliptic curves. This means we need to find two points P_0, Q on $Jac(C)$ so that we can define some basic identity later on. Again, we can choose

$$\begin{aligned} P_0 &= [(t^q, s^q) - P_\infty] \\ Q &= [(t, s) - P_\infty]. \end{aligned} \tag{7.4}$$

To find the numbers d_n, we can use the following two functions defined in [9].

$$\begin{aligned} F_0(x_1, x_2) &= 2f_0 + f_1(x_1 + x_2) + 2f_2(x_1x_2) + f_3(x_1x_2)(x_1 + x_2) \\ &\quad + 2f_4(x_1x_2)^2 + (x_1x_2)^2(x_1 + x_2) \end{aligned} \tag{7.5a}$$

$$k_4([\zeta_1 + \zeta_2 - 2P_\infty]) = k_4(\zeta_1 + \zeta_2) = \frac{F_0(x_1, x_2) - 2y_1y_2}{(x_1 - x_2)^2}. \tag{7.5b}$$

where $\zeta_1 = (x_1, y_1) \in C$, $\zeta_2 = (x_2, y_2) \in C$ and f_i are the coefficients of the polynomial $f(x)$.

The reason for choosing this function k_4 is the following. Just as for the elliptic curves, we are looking for a symmetric function (in x or y) for defining the numbers d_n. This means that we are looking for some function σ such that $\sigma(P) = \sigma(-P)$ for a point $P \in C$. In the case of elliptic curves, this symmetric function is given by adding the x-coordinates of two points, so there we take $x_1 + x_2$. Indeed this function is symmetric in x_1 and x_2. For the hyperelliptic curves, since a divisor class is written as

$$[P_1 + P_2 - 2P_\infty]$$

we can choose one of the following functions.

- x_1x_2: $(x_1x_2)(-P) = (x_1x_2)(P)$;
- $x_1 + x_2$: $(x_1 + x_2)(P) = (x_1 + x_2)(-P)$;
- y_1y_2: $(y_1y_2)(P) = ((-y_1)(-y_2))(-P) = (y_1y_2)(-P)$;
- k_4.

The function $y_1 + y_2$ doesn't satisfy the symmetry, since $y(-P) = -y(P)$ and thus $(y_1 + y_2)(-P) = -(y_1 + y_2)(P)$. After some computations, it turns out the first three functions above don't give us a relation. Therefore take k_4 as the desired function.

With this function k_4 we arrive at the following lemma.

Lemma 7.1. *For the points $P_0 = (t^q, s^q)$ and $Q = (t, s)$ the relation between k_4 and $\#C(\mathbb{F}_q)$ is given by*

$$\deg(\textit{numerator}(k_4(P_0 - Q))) - q - 1 = \#C(\mathbb{F}_q)$$

For elliptic curves we had the situation that $\deg(d_{-1}) = \#E(\mathbb{F}_q)$ where $d_{-1} = \deg(\text{numerator}(P_0 - Q))$, so for hyperelliptic curves we almost have the same lemma, only using k_4. So we could say

$$d_{-1} = \deg(\text{numerator}(k_4)(P_0 - Q)).$$

Therefore, it seems a logical choice to define the numbers d_n by

$$d_n = \deg(\mathrm{num}(k_4(P_0 + nQ))).$$

We can prove lemma 7.1 in the same way as we have proven lemma 3.2.

Proof. For $P_0 = (t^q, s^q)$ and $Q = (t, s)$, the function k_4 is given by

$$\begin{aligned} k_4 &= \frac{2f_0 + f_1(t^q + t) + 2f_2(t^{q+1}) + f_3(t^{q+1})(t^q + t) + 2f_4(t^{q+1})^2 + (t^{q+1})^2(t^q + t) + 2s^{q+1}}{(t^q - t)^2} \\ &= \frac{t^{3q+2} + t^{2q+3} + 2f_4t^{2q+2} + f_3(t^{q+2} + t^{2q+1}) + 2f_2t^{q+1} + f_1(t + t^q) + 2f_0 + 2s^{q+1}}{(t^q - t)^2}. \end{aligned}$$

Note that

$$\deg(s^{q+1}) = \deg(f(t)^{(q+1)/2}) = \frac{5(q+1)}{2}$$

and thus

$$\deg(\mathrm{num}(k_4)) = 3q + 2.$$

The next step is to find whether there are common terms in numerator and denominator which can lower the degree of the numerator of k_4. This is also done in the same way as in the proof of lemma 3.2. So we take an $\alpha \in \mathbb{F}_q$ and a corresponding β such that $(\alpha, \beta) \in C$. Since $\alpha \in \mathbb{F}_q$, $(t^q - t)^2|_{(\alpha,\beta)}$ has a double zero, so there is a common term in numerator and denominator if also the numerator evaluated at (α, β) equals zero. For the chosen point (α, β) we have the following possibilities.

- $\beta \in \mathbb{F}_q$. Evaluating the numerator of k_4 at (α, β) and using $\beta^q = \beta$ gives

$$\begin{aligned} \mathrm{num}(k_4)|_{(\alpha,\beta)} &= \alpha^{3q+2} + \alpha^{2q+3} + 2f_4\alpha^{2q+2} + f_3(\alpha^{q+2} + \alpha^{2q+1}) + 2f_2\alpha^{q+1} \\ &\quad + f_1(\alpha + \alpha^q) + 2f_0 + 2\beta^{q+1} \\ &= \alpha^5 + \alpha^5 + 2f_4\alpha^4 + f_3(\alpha^3 + \alpha^3) + 2f_2\alpha^2 \\ &\quad + f_1(\alpha + \alpha) + 2f_0 + 2\beta^2 \\ &= 2(\alpha^5 + f_4\alpha^4 + f_3\alpha^3 + f_2\alpha^2 + f_1\alpha + f_0) + 2(f(\alpha)) \\ &= 4f(\alpha) \\ &= 4\beta^2. \end{aligned}$$

  So there is cancellation only for $\beta = 0$, so when $(\alpha, 0) \in C(\mathbb{F}_q)$. In this case, α is a simple zero of the equation $f(x) = 0$.

- $\beta \notin \mathbb{F}_q$. This means that β^q is the other possible zero of $y^2 = f(\alpha)$, which means that $\beta^q = -\beta$. Then evaluating the numerator of k_4 at (α, β) gives

$$\begin{aligned} \mathrm{num}(k_4)|_{(\alpha,\beta)} &= \alpha^{3q+2} + \alpha^{2q+3} + 2f_4\alpha^{2q+2} + f_3(\alpha^{q+2} + \alpha^{2q+1}) + 2f_2\alpha^{q+1} \\ &\quad + f_1(\alpha + \alpha^q) + 2f_0 + 2\beta^{q+1} \\ &= 2(\alpha^5 + f_4\alpha^4 + f_3\alpha^3 + f_2\alpha^2 + f_1\alpha + f_0) - 2\beta^2 \\ &= 2f(\alpha) - 2f(\alpha) \\ &= 0 \end{aligned}$$

  which means there is a common term in numerator and denominator.

So we have seen there is a common term in the numerator and denominator of k_4 when $\beta \notin \mathbb{F}_q$. The next question is how many times this term drops out. Therefore, consider the derivative of the numerator of k_4, because if this derivative does not equal zero when evaluating at (α, β), the common term drops out only once.
To compute the derivative of the numerator, consider the equation of the hyperelliptic curve C. Since the equation must stay true when taking partial derivatives, we arrive at the following equation.

$$s^2 = f(t) \Rightarrow 2s \cdot s' = f'(t)$$

and thus

$$s' = \frac{f'(t)}{2s}.$$

Knowing this, we can compute the derivative of the numerator of k_4. Using $q = 0 \mod q$ this yields

$$\begin{aligned}\frac{d}{dt}(\text{num}(k_4)) &= (3q+2)t^{3q+1} + (2q+3)t^{2q+2} + 2f_4(2q+2)t^{2q+1} + f_3(q+2)t^{2q+1} \\ &\quad + f_3(2q+1)t^{2q} + 2f_2(q+1)t^q + f_1(qt^{q-1}+1) + 2(q+1)s^q s' \\ &= 2t^{3q+1} + 3t^{2q+2} + 4f_4t^{2q+1} + 2f_3t^{q+1} + f_3t^{2q} + 2f_2t^q + f_1 + s^{q-1}f'(t).\end{aligned}$$

Since we considered the point (α, β) with $\beta \notin \mathbb{F}_q$ (and thus $\beta^q = -\beta$), also evaluate the derivative at this point, yielding

$$\begin{aligned}\left(\frac{d}{dt}(\text{num}(k_4))\right)|_{(\alpha,\beta)} &= 2\alpha^{3q+1} + 3\alpha^{2q+2} + 4f_4\alpha^{2q+1} + 2f_3\alpha^{q+1} + 2f_2\alpha^q \\ &\quad + f_1 + \beta^{q-1}f'(\alpha) \\ &= 5\alpha^4 + 4f_4\alpha^3 + 3f_3\alpha^2 + 2f_2\alpha + f_1 + \beta^q\beta^{-1}f'(\alpha) \\ &= f'(\alpha) - \beta\beta^{-1}f'(\alpha) \\ &= 0.\end{aligned}$$

Since also the derivative cancels at (α, β), we can conclude that the common term cancels more than once. This means that the common term in the numerator and denominator of k_4 cancels twice (since the denominator only cancels twice). So for the divisor class $[P_0 - Q]$ (which can be written as $[\zeta_1 + \zeta_2 - 2P_\infty]$ for points $\zeta_1, \zeta_2 \in C$) we have

$$\begin{aligned}\deg(\text{num}(k_4)) &= 3q + 2 - \text{common terms} \\ &= 3q + 2 - 2\#\{\alpha \in \mathbb{F}_q | \nexists \beta \in \mathbb{F}_q \text{ such that } (\alpha,\beta) \in C\} - \#\{\alpha \in \mathbb{F}_q | f(\alpha) = 0\} \\ &= 3q + 2 - 2\left(q - \#\{\alpha \in \mathbb{F}_q | \exists \beta \in \mathbb{F}_q \text{ such that } (\alpha,\beta) \in C\}\right) - \#\{\alpha \in \mathbb{F}_q | f(\alpha) = 0\} \\ &= q + 2 + 2\#\{\alpha \in \mathbb{F}_q | \exists \beta \in \mathbb{F}_q \text{ such that } (\alpha,\beta) \in C\} - \#\{\alpha \in \mathbb{F}_q | f(\alpha) = 0\}.\end{aligned}$$

Furthermore, the number of points on C (including the point at infinity $\mathcal{O}$) is given by

$$\begin{aligned}\#C(\mathbb{F}_q) &= 1 + \#\{\alpha \in \mathbb{F}_q | (\alpha, 0) \in C\} + 2\#\{\alpha \in \mathbb{F}_q | (\alpha,\beta) \in C, \beta \neq 0\} \\ &= 1 + \#\{\alpha \in \mathbb{F}_q | f(\alpha) = 0\} + 2\#\{\alpha \in \mathbb{F}_q | f(\alpha) \neq 0, f(\alpha) \text{ a square}\} \\ &= 1 + 2\#\{\alpha \in \mathbb{F}_q | f(\alpha) \text{ a square}\} - \#\{\alpha \in \mathbb{F}_q | f(\alpha) = 0\}\end{aligned}$$

where the last term in the last line follows from double counting.
From this it follows that

$$\deg(\text{num}(k_4)) - q - 1 = \#C(\mathbb{F}_q)$$

which we wanted to prove. □

So again, since above lemma holds, we take k_4 to be the function to construct the numbers d_n, yielding

$$d_n = \deg(\text{num}(k_4(P_0 + nQ))).$$

Using this defintion, we try to find some basic identity. For the elliptic curves (where $f(x)$ is of degree 3) the basic identity is a second order recursion formula, which means we need two previous numbers d_{n-1} and d_n to compute d_{n+1}. This is due to the fact that the degree map

$$End(E) \to \mathbb{Z}$$

is quadratic (i.e. $\deg(n\phi) = n^2 \deg(\phi)$). Therefore, the corresponding polynomial is given by

$$d(n) = n^2 + (\#E(\mathbb{F}_q) - q - 1)n + q.$$

For a curve C of genus g, the Jacobian $Jac(C)$ is an abelian variety of dimension g. It follows from [17, IV, par. 19, thm. 2] that in this case the degree map

$$End(Jac(C)) \to \mathbb{Z}$$

is a polynomial map of degree $2g$. This means that for genus 2, the corresponding polynomial is quartic, i.e. given by

$$d(n) = n^4 - \alpha n^3 + \beta n^2 - \alpha q n + q^2 \qquad (7.6)$$

where $\alpha = \#C(\mathbb{F}_q) - q - 1$ and $|\beta| \leq 6q$, see [10, par.2.1]. Therefore, the recursion formula will be a fourth order recursion formula of the form

$$a_1 d_{n+2} + a_2 d_{n+1} + a_3 d_n + a_4 d_{n-1} + a_5 d_{n-2} = c.$$

Using the quartic polynomial (7.6) the coefficients a_i can be found, yielding the basic identity for hyperelliptic curves of genus 2, given by

$$d_{n+2} - 4d_{n+1} + 6d_n - 4d_{n-1} + d_{n-2} = 24. \qquad (7.7)$$

All above information can be put in a Magma program. This yields the following result.

```
Punten2:=function(p,r,i); //Case char=>3
  //p:= prime number
        //r:= power of the prime
  //i:= compute (2i+1) numbers d_n
  q:=p^r;
  Fq<v>:=GF(q); //Define Fq
  Fqt<t>:=FunctionField(Fq); //Define Fq(t)
  P<x>:=PolynomialRing(Fq); //Define Fq[x] to be able to
     use x
```

```
R<Y>:=PolynomialRing(Fqt); //Define Fq(t)[Y] to use Y

a0:=Random(Fq);
a1:=Random(Fq);
a2:=Random(Fq);
a3:=Random(Fq);
a4:=Random(Fq);

Fqts<s>:=ext<Fqt|Y^2-(t^5+a4*t^4+a3*t^3+a2*t^2+a1*t+a0)>;
    //Define Fq(t,s)

C1:=HyperellipticCurve(x^5+a4*x^4+a3*x^3+a2*x^2+a1*x+a0);
    //Hyperelliptic curve over Fq
C2:=BaseExtend(C1,Fqts); //Same hyperelliptic curve
    over Fq(t,s)
J1:=Jacobian(C1);
J2:=Jacobian(C2);

Pol<M>:=PolynomialRing(Fqts);    //Construct the points
    P0,Q on the Jacobian of C2 via constructing a new
    variable
Q:=J2![Pol!(M-t),s];
P0:=J2![Pol!(M-t^q),s^q];

Basic:= [];
for n:=-i to i do     //Here compute the numbers dn
    which are defined as the degree of k4
  Pn:=P0+n*Q;
  Pn1:=Pn[1];
  Pn2:=Pn[2];
  a:=Coefficient(Pn1,1);
  b:=Coefficient(Pn1,0);
  c:=Coefficient(Pn2,1);
  d:=Coefficient(Pn2,0);
  k4:=(2*a0-a*a1+2*b*a2-a*b*a3+2*b^2*a4-a*b^2+2*a*c*d
      -2*b*c^2-2*d^2)/(a^2-4*b);
  Basic:=Append(Basic,(Degree(k4)/2)); //Compute the
      numbers dn via the degree of k4
end for;
X:=Basic[i]-q-1; //Find the number d_{-1} for the
    relation to #C1

k:=1; //Define k:=n-2 and rewrite Basic identity
Identity:=[];
while (k ge 1) and (k lt (2*i-2)) do
  G:=Basic[k]+Basic[k+4]+6*Basic[k+2]-4*Basic[k+1]-4*Basic[k+3]-24;
  Identity:=Append(Identity,G);
  k:=k+1;
end while;
```

```
  printf "Number of points on C1: %o\n",#C1;
  printf "Degree(num(k_4(P_0,-Q))): %o\n",X;
  printf "\n\n";
  printf "Numbers d_n given by: %o\n",Basic;
  printf "Basic Identity given by: %o\n ",Identity;

  return "";
end function;
```

In this program we have done the following.
We started with defining the necessary fields and rings, so the field $\mathbb{F}_q = \texttt{GF(q)}$, the field extension $\mathbb{F}_q(t,s) = \texttt{Fqts}$ and the polynomial rings $\mathbb{F}_q[x]$ and $\mathbb{F}_q(t)[Y]$. After this is done, the two hyperelliptic curves C_1 and C_2 together with their Jacobians are defined, where C_2 is the extension of C_1 over $\mathbb{F}_q(t,s)$. Finally, the points P_0 and Q as in (7.4) are defined. After this is done, we can start computing the numbers k_4 for the points P_0 and nQ. Here k_4 is written in another form than in equation (7.5b), namely in the following way. Recall a point on the Jacobian in Magma is denoted by $(g(x), y(x), z)$. When $g(x)$ is quadratic, we can write it as

$$x^2 + ax + b = (x - x_1)(x - x_2) = x^2 - (x_1 + x_2)x + x_1x_2$$

for zeroes x_1 and x_2. This means that the points x_1 and x_2 needed in the formula for k_4 given by (7.5b) can also be expressed in terms of a and b. The same holds for $y(x)$, which is given by

$$y(x) = cx + d$$

and thus also y_1y_2 can be expressed in terms of a, b, c, d. Rewriting k_4 in these terms, using $(x_1 + x_2) = a$, $x_1x_2 = b$, yields

$$k_4 = \frac{2f_0 - af_1 + 2bf_2 - abf_3 + 2b^2f_4 - ab^2 + 2acd - 2bc^2 - 2d^2}{a^2 - 4b}$$

which is the form used in the computer program above.
In the last loop the recursion formula $d_{n-2} + d_{n+2} + 6d_n - 4d_{n-1} - 4d_{n+1} - 24$ is computed. If this new basic identity is correct, all these outputs should equal zero.
If we run this program a few times, we get the following output.

> Punten2(5,1,5);
Number of points on C1: 4
Degree(num($k_4(P_0, -Q)$)): 4

Numbers d_n given by: [40, 30, 22, 12, 10, 20, 14, 20, 32, 48, 70]
Basic Identity given by: [-10, -30, -56, 32, -58, -20, -20]

> Punten2(5,1,10);
Number of points on C1: 7
Degree(num($k_4(P_0, -Q)$)): 7

Numbers d_n given by: [205, 181, 145, 115, 88, 65, 46, 31, 20, 13, 25, 11, 14, 25, 36, 55, 76, 101, 130, 163, 195]

Basic Identity given by: [-45, -20, -25, -24, -24, -24, -9, -84, 64, -76, -23, -8, -38, -16, -26, -24, -29]

> Punten2(3,1,10);
Number of points on C1: 2
Degree(num($k_4(P_0, -Q)$)): 2

Numbers d_n given by: [186, 138, 118, 89, 66, 46, 30, 18, 10, 6, 15, 10, 14, 30, 46, 64, 90, 118, 150, 183, 223]
Basic Identity given by: [28, -42, -20, -25, -24, -24, -15, -60, 26, -44, -39, -10, -20, -36, -16, -29, -15]

> Punten2(11,1,5);
Number of points on C1: 15
Degree(num($k_4(P_0, -Q)$)): 15

Numbers d_n given by: [87, 66, 49, 36, 27, 55, 21, 22, 31, 42, 57]
Basic Identity given by: [-24, 9, -156, 172, -148, -3, -16]

> Punten2(43,1,5);
Number of points on C1: 40
Degree(num($k_4(P_0, -Q)$)): 40

Numbers d_n given by: [116, 102, 92, 86, 84, 215, 92, 100, 116, 134, 156]
Basic Identity given by: [-24, 105, -540, 748, -532, 93, -16]

As we can see in the results, indeed the number of points on the hyperelliptic curve C_1 and the degree of the numerator of k_4 evaluated at P_0 and Q are equal. But the results in the numbers of the Basic Identity are very strange. They are not zero as we hoped. Also when taking quite large numbers n in computing $P_0 + nQ$ we do not get the value zero. The conclusion we can make is that somewhere must be a mistake, but we do not know where the mistake is yet.

8 Conclusions

8.1 Conclusions

In this thesis we considered the Hasse inequality, stating that for an elliptic curve $E/\mathbb{F}_q$ the number of points $\#E(\mathbb{F}_q)$ is estimated by

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

We followed the proof of Manin, where we've split the proof of the theorem in three cases. The first case is the case of $\text{char}(\mathbb{F}_q) \geq 3$. Since originally Manin only considered $\text{char}(\mathbb{F}_q) \geq 5$, we extended his proof in this first case. The other two cases deal with $\text{char}(\mathbb{F}_q) = 2$, where we, just like for $\text{char}(\mathbb{F}_q) \geq 3$, first needed to find a quadratic twist of the elliptic curve E. Further, we could follow the proof of Manin, where only the proofs of the lemmas and the formulas had to be changed. It turned out that we succeeded in extending Manin's argument to all characteristics. To show this argument and make it more visible, we used the computer program Magma to check the results of the formulas. It turned out that all formulas are correct. The Magma program computes the number of points on the curve E and shows all steps taken in the proof of Manin.
After extending Manin's argument, we have shown that basically this argument is the same as the proof given in for example Silverman. This section gives a nice connection to other known proofs of Hasse's theorem. We also gave another proof of the lemma's 3.5, 4.5 and 5.6 without using reduction theory. The new proof is valid for all characteristics and is shorter than the proof using reduction theory.
The last chapter considered hyperelliptic curves of genus 2. First we didn't know whether it would be possible to extend Manin's proof to hyperelliptic curves of genus 2. Therefore, we tried to do some of the steps. It turned out that it was possible to find a formula for the number of points on the curve, given by

$$\deg(\text{num}(k_4(P_0 - Q))) - q - 1 = \#C(\mathbb{F}_q).$$

The proof of above lemma is also given. Furthermore, this gave us a clue how to define the numbers d_n, namely as

$$d_n = \deg(\text{num}(k_4(P_0 + nQ))).$$

For these numbers d_n, we constructed a recursion formula using the corresponding quartic polynomial. After that we've put everything in Magma to see what happens and to see if the numbers d_n found above are correct. According to Magma, the formula for the number of points on a curve is correct. This we've expected, since we were able to prove the lemma. But when checking the numbers d_n using the recursion formula, Magma returned strange numbers. We didn't found a pattern in these numbers, and we weren't able to see what we did wrong. Therefore, we stopped at this point. The conclusion for hyperelliptic curves of genus 2 is that there is a mistake somewhere. This can be in the definition of the numbers d_n, although it seems this definition is allright. The mistake can also be somewhere else, for example that we should take another field in stead of $\mathbb{F}_q(t, s)$. By the mistake we made, we are not able to continue Manin's argument. So we've found a formula for the number of points on a hyperelliptic curve of genus 2, but were not able to finish the proof of Hasse's theorem on hyperelliptic curves of genus 2.

8.2 Further Research

In further research it seems a logical choice to proceed extending Manin's argument to hyperelliptic curves of genus 2. Further research can find the mistake made in this thesis. When this succeeds, maybe it is possible to extend Manin's argument to hyperelliptic curves of genus 2.

8.3 Acknowledgements

First of all, I would like to thank my first supervisor prof. dr. Jaap Top in special for all his support during last year. Without his help and support I would not have been able to finish this thesis. Furthermore, I would like to thank drs. Anneroos Everts for being my second supervisor. I would also like to thank my family and boyfriend Sander Bus, they always supported me last year. At last, I would like to thank my friends for helping me writing the thesis. In this, I would like to mention Jaap Hollander, who has helped me a lot with the ICT like the programming.

A References

References

[1] J.W.S. Cassels, *Diophantine Equations with Special References to Elliptic Curves*, Journal of London Mathematical Society 41 (1966), pp 193-291

[2] J.W.S. Cassels, *Lectures on Elliptic Curves*, London Mathematical Society Student Texts 24, 1991

[3] J.W.S. Cassels, *Review of 'On cubic congruences to a prime modulus' by Yu. I. Manin*, Jour. Izv. Akad. Nauk SSSR Ser. Mat., volume 20, 1956, pp. 673-678, http://www.ams.org/mathscinet-getitem?mr=81308

[4] J.W.S. Cassels and E.V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*, London Mathematical Society Lecture Note Series 230

[5] J.S. Chahal, *Topics in Number Theory*, Plenum Press, 1988

[6] J.S. Chahal, *Manin's Proof of the Hasse Inequality Revisited*, Nieuw Archief voor Wiskunde, no. 2, july 1995, pp 219–232

[7] J.S. Chahal and B. Osserman, *The Riemann Hypothesis for Elliptic Curves*, ICPCA/SWS, 2008, pp. 431-442, math.ucdavis.edu/ osserman/math/riemann-elliptic.ps

[8] C. Costello and K. Lauter, *Group Law Computations on Jacobians of Hyperelliptic Curves*, SAC'11 Proceedings of the 18th international conference on Selected Areas in Cryptography, Springer-Verlag Berlin, Heidelberg 2012, pp. 92-117

[9] E.V. Flynn, *The Arithmetic of Hyperelliptic Curves*, Algorithms in Algebraic Geometry and Applications, Progress in Mathematics Volume 143, 1995, pp. 165-175

[10] P. Gaudry and R. Harley, *Counting Points on Hyperelliptic Curves over Finite Fields*, J. Ramanujan Math. Soc. 16, 2001, pp. 323-338

[11] P.A. Grillet, *Abstract Algebra*, Springer-Verlag, 2007 (Graduate Text in Mathematics no. 242)

[12] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, 1977 (Graduate Text in Mathematics no. 52)

[13] A.W. Knapp, *Elliptic Curves*, Princeton University Press, 1992

[14] T. Lange, *Formulae for arithmetic on genus 2 hyperelliptic curves*, Applicable Algebra in Engineering, Communication and Computing, vol.15, 2003, pp.295–328

[15] Y.I. Manin, *On cubic congruences to a prime modulus*, Jour. Izv. Akad. Nauk SSSR Ser. Mat., volume 20, 1956, pp. 673-678

[16] J. Milne, *Fields and Galois Theory*, Notes for Math 596, University of Michigan, Winter 1994

[17] D. Mumford, *Abelian Varieties*, Oxford University Press, 1974

[18] Oort, Lenstra, van Geemen, *Algebra: Ringen, Lichamen*, Rijksuniversiteit Groningen, vakgroep Wiskunde, 1997

[19] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, 2009, 2nd edition (Graduate Text in Mathematics no. 106)

[20] J.H. Silverman and J.Tate, *Rational Points on Elliptic Curves*, Springer, 1992

[21] I. Stewart, *Galois Theory*, Chapman&Hall/CRC, 2004, 3rd edition

[22] H. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag, 2009, 2nd edition

[23] http://mathworld.wolfram.com/LegendreSymbol.html

[24] http://commalg.wiki-site.com/index.php/Birational_map_of_varieties

[25] http://en.wikipedia.org/wiki/Frobenius_endomorphism

B Twists

In this appendix we will describe the way to find a twist of an elliptic curve. We will deal with the case $\text{char}(\mathbb{F}_q) = 2$, since the other case $(\text{char}(Fq) \geq 3)$ works exactly the same.
To start, notice that a twist of an elliptic curve E is an elliptic curve E^{tw} such that $E \cong E^{tw}$ over a finite extension L of K for two fields $K \subset L$. So basically, we want to find a curve that is isomorphic to E over some field L. But since this is quite hard to do directly, we use some Galois theory and the next proposition.

Proposition B.1.

$$\begin{aligned}
&\exists \phi : E_1 \tilde{\to} E_2, \textit{ with } \phi \textit{ defined over } L\\
\Leftrightarrow &\exists \psi : E_1 \cdots \to E_2, \textit{ with } \psi \textit{ a birational map defined over } L, \textit{ sending } \mathcal{O} \textit{ to } \mathcal{O}\\
\Leftrightarrow &\exists \psi^* : K(E_2) \to K(E_1) \textit{ with } \psi^* \textit{ the identity on } L \textit{ and } \psi^* \textit{ fixes the valuation}\\
&\textit{at } \mathcal{O}, \textit{ i.e. } v_{\mathcal{O}}(f) = v_{\mathcal{O}}(\psi^* f)\ \forall f.
\end{aligned}$$

This proposition needs a little bit more explanation and also the sketch of the proof. Therefore, we assume that $E_1/K \cong E_2/K$ and we explain the three lines that follow.

- The first line is quite obvious. We assume E_1 and E_2 are isomorphic. Then of course there exists an isomorphism $\phi : E_1 \to E_2$. By definition, ϕ should satisfy $\phi(\mathcal{O}_1) = \mathcal{O}_2$, which means that the point at infinity of E_1 is mapped to the point at infinity of E_2.

- The second line means there exists a birational map ψ which also satisfies $\psi(\mathcal{O}_1) = \mathcal{O}_2$. Before we explain why this line is true, we need to know the definition of a birational map, see also [24].

  Definition B.1. *$\psi : E_1 \to E_2$ is birational if for two subsets $U_1, U_2 \subset E_1$ and two morphisms of varieties $f_{U_i} : U_i \to E_2$, ψ satisfies the equivalence relation $(f_{U_1}, U_1) \sim (f_{U_2}, U_2)$ iff $f_{U_1} = f_{U_2}$ on $U_1 \cap U_2$. Furthermore, there exists an inverse mapping $\psi_2 : E_2 \to E_1$ with $\psi \circ \psi_2 = id_{E_2}$ and $\psi_2 \circ \psi = id_{E_1}$.*

  Now since ϕ is an isomorphism, by definition ϕ is bijective. So if we define a map ψ in the same way as ϕ then also ψ is bijective and thus there exists an inverse mapping ψ^{-1} with the desired properties. Since the two varieties E_1 and E_2 are isomorphic, also the equivalence relation holds.

- This last part requires that there should exist a map ψ^* such that

  $$\begin{aligned} x &\mapsto f_1(\tilde{x}, \tilde{y})\\ y &\mapsto f_2(\tilde{x}, \tilde{y}) \end{aligned}$$

  and ψ^* injective. Here $K(E_i)$ is the function field of the curve E_i over K. To see why this statement holds, see [1, p.221].

So if we want two isomorphic curves, we need to find an injective map ψ^* between the function fields of the curves. To do this, we proceed as follow.
Since we need the elliptic curves to be isomorphic over L, we first need to find

this extension L, which we want to be a quadratic extension. Because the curves E and E^{tw} will turn out to be isomorphic over L, they will have the same function field $L(E^{tw}) = L(E)$. So we need to find $L(E)$. Finally we want to find a subfield D of $L(E)$ satisfying

$$\{\beta \in D | \beta \text{ is algebraic over } K\} = K. \tag{B.1}$$

This subfield D will give the isomorphic we are looking for.

B.1 char$(K) = 2$, $j(E) = 0$

To make things easier, we start with a curve $E/\mathbb{F}_q$ in stead of $E/\mathbb{F}_q(t)$. Then E is given by

$$E/\mathbb{F}_q: \quad y^2 + a_3y = x^3 + a_4x + a_6$$

where char$(K) =$ char$(\mathbb{F}_q) = 2$ and $j(E) = 0$. To find a quadratic extension L of K, take for L the splitting field of K. According to [21, p.108], this is the field L such that an irreducible polynomial g in $K[x]$ splits in L, so it can be written as $g(x) = k(x-s_1)...(x-s_n)$ for zeroes $s_i \in L$. In this case, we take $L = K(s)$ where s satisfies the irreducible polynomial $g(x) = x^2+x+a \in K[x]$, i.e. $s^2+s+a = 0$ for some $a \in \mathbb{F}_q$. Knowing this, we can give an expression for $L(E)$. We know $L = K(s)$ and $K(E) = K(x, y)$. Using from $y(y + a_3) = x^3 + a_4x + a_6$ that

$$y \cdot y^{-1} = y \cdot \frac{y + a_3}{x^3 + a_4x + a_6} = 1$$

we can see that also y^{-1} is a polynomial in y over $K(x)$ and thus $K(E) = K(x, y) = K(x)[y]$. Combining this with the definition of L gives us

$$L(E) = K(s)(E) = K(x, y, s) = K(x)[y][s]$$

which also can be written as

$$L(E) = K(x) + K(x) \cdot y + K(x) \cdot s + K(x) \cdot sy. \tag{B.2}$$

Now we want to find a subfield D of this $L(E)$. It turns out that for a twist of an elliptic curve E we need $D = L(E)^{<\sigma>} = \{\beta \in L(E) | \sigma(\beta) = \beta\}$. Here $\sigma : L \to L$ is a K-automorphism, which means it is a homomorphism satisfying $\sigma(k) = k \ \forall k \in K$. The automorphism σ needed must satisfy

- $\sigma|_L \neq$ id,
- $\sigma|_{K(E)} = [-1]$, which means it sends a point $P \in E$ to $-P$.

So first we need to find all possible automorphisms before we can pick the correct one. Finding all automorphisms is equivalent with finding the Galois group of L/K which is defined as Gal$(L : K) = \{\sigma : L \to L | \ \sigma \text{ is a } K-\text{automorphism}\}$. So in our situation, consider Gal$(L(E)/K(x))$. This group consists of four elements, which can be found using the definitions of E and $g(x)$. Since E is defined as $E : y(y + a_3) = x^3 + a_4x + a_6$ we can map y to the other zero $y + a_3$. That we indeed keep the same curve follows immediately:

$$\begin{aligned} y^2 + a_3y \mapsto &(y + a_3)^2 + a_3(y + a_3) \\ &= y^2 + a_3^2 + a_3y + a_3 \\ &= y^2 + a_3y. \end{aligned}$$

Now in our irreducible polynomial $g(x)|_s = s^2+s+a = 0$ we can map $s \mapsto s+1$, which also doesn't change the polynomial:

$$\begin{aligned} s^2 + s + a \mapsto & (s+1)^2 + (s+1) + a \\ &= s^2 + 1 + s + 1 + a \\ &= s^2 + s + a. \end{aligned}$$

And so, combining above two mappings, we arrive at the following four K-automorphisms.

$$\begin{aligned} \sigma_1 : \quad & \text{id}, \\ \sigma_2 : \quad & y \mapsto y + a_3 \\ & s \mapsto s, \\ \sigma_3 : \quad & y \mapsto y \\ & s \mapsto s + 1, \\ \sigma_4 : \quad & y \mapsto y + a_3 \\ & s \mapsto s + 1. \end{aligned}$$

Now we need to find the automorphism that gives us the isomorphism we need to get two isomorphic elliptic curves. As said earlier, this automorphism must satify the following two properties:

- $\sigma|_L \neq$ id,
- $\sigma|_{K(E)} = [-1]$, which means it sends a point $P \in E$ to $-P$.

Because of the first property we can already exclude σ_1. Furthermore, according to [19, p.53] for a point $P \neq \mathcal{O}$ written as $P = (x, y) \in E$ the map $[-1] : E \to E$ is given by

$$[-1]P = [-1](x, y) = (x, -y - a_3) = (x, y + a_3).$$

So by the second property also σ_3 can be excluded since y has to be mapped to $y + a_3$. So we have to choose between σ_2 and σ_4. Now first consider σ_2. To see what this map does, we put σ_2 into matrix form:

$$\sigma_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ a_3 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & a_3 & 1 \end{pmatrix}$$

where in every row is shown what happens to respectively $K(x), yK(x), sK(x)$ and $syK(x)$ under the mapping σ_2. So consider for example the fourth row. Under σ_2, $syK(x)$ is mapped to

$$\begin{aligned} syK(x) \mapsto & s(y + a_3)K(x) \\ &= syK(x) + a_3 sK(x). \end{aligned}$$

Computing $\sigma_2 - I$ yields

$$\sigma_2 - I = \begin{pmatrix} 0 & 0 & 0 & 0 \\ a_3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & a_3 & 0 \end{pmatrix}$$

and this matrix has two independent components, namely $K(x)$ and $K(x)s$. This gives us that

$$L(E)^{<\sigma_2>} = K(x,s) = L(x)$$

which violates property (B.1) and thus also σ_2 is not the automorphism we are looking for. So we are left with σ_4. In matrix form this is given by

$$\sigma_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ a_3 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & a_3 & 1 \end{pmatrix}.$$

To check how many independent components this matrix has, we take $\sigma_4 - I$ and reduce this matrix as far as possible, yielding

$$\sigma_4 - I = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & a_3 & 0 \end{pmatrix}.$$

And thus we can see that there are two independent components, namely $yK(x) + a_3sK(x)$ and $K(x)$. This gives us that

$$L(E)^{<\sigma_4>} = K(x)[a_3s + y].$$

This is the field we are looking for because it satisfies the two properties and gives a new curve. To find this new curve which turns out to be the twisted curve, use again the relations

$$\begin{aligned} &s^3 + s = a, \\ &y^2 + a_3y = x^3 + a_4x + a_6. \end{aligned}$$

Calling $\eta = a_3s + y$ yields

$$\begin{aligned} \eta^2 + a_3\eta &= (a_3s + y)^2 + a_3(a_3s + y) \\ &= a_3^2(s^2 + s) + (y^2 + a_3y) \\ &= a_3^2a + x^3 + a_4x + a_6. \end{aligned}$$

And thus the twisted curve is given by (renaming $\eta = y$)

$$E' : \quad y^2 + a_3y = x^3 + a_4x + (a_6 + a_3^2a).$$

Indeed this curve is isomorphic with our original E over $L = K(s)$ via the isomorphism

$$\psi : (x,y) \mapsto (x, y + a_3s)$$

because substituting $y = y + a_3s$ in the equation for E gives the equation for E', and furthermore, the mapping $y \mapsto y + a_3s$ is invariant under σ_4. Now we are not done completely yet. Above story only holds for $K = \mathbb{F}_q$ with irreducible polynomial $g(x) = x^2 + x + 1 \in K[x]$. When taking $K = \mathbb{F}_q(t)$ our irreducible polynomial $g(x)$ changes to

$$g(x) = x^2 + a_3x + f(t)$$

where $f(t) = t^3 + a_4 t + a_6$. The idea of finding the twisted curve over $L = K(s)$ where s satisfies $g(s) = 0$ is almost the same as above, only the automorphism changes to

$$\begin{aligned} \sigma_4: \quad & y \mapsto y + a_3 \\ & s \mapsto s + a_3. \end{aligned}$$

Furthermore, the isomorphism changes. To see this, assume the previous isomorphism ψ still holds. Then this isomorphism must be invariant under σ_4, which means we must have $\sigma_4(y + a_3 s) = y + a_3 s$. But it turns out we have

$$\begin{aligned} \sigma_4(y + a_3 s) &= (y + a_3) + a_3(s + a_3) \\ &= y + a_3 s + a_3 + a_3^2. \end{aligned}$$

So to get an invariant mapping we take as new isomorphism

$$\psi : (x, y) \mapsto (x, y + s)\,. \tag{B.3}$$

This mapping of y is indeed invariant under σ_4. Using this isomorphism, again by defining $\eta = y + s$ as twisted curve we obtain

$$E^{tw}: \quad y^2 + a_3 y = x^3 + a_4 x + a_6 + f(t).$$

So summarizing we have the following two curves that are isomorphic over $L = K(s) = \mathbb{F}_q(t)(s)$:

$$\begin{aligned} E/\mathbb{F}_q(t): \quad & y^2 + a_3 y = x^3 + a_4 x + a_6 \\ E^{tw}/\mathbb{F}_q(t, s): \quad & y^2 + a_3 y = x^3 + a_4 x + a_6 + f(t) \end{aligned}$$

where the isomorphism between the curves is given by

$$\begin{aligned} \psi :& E \to E^{tw} \\ & (x, y) \mapsto (x, y + s)\,. \end{aligned}$$

B.2 char$(K) = 2$, $j(E) \neq 0$

In this section we will find the twist of the curve in the case $j(E) \neq 0$. The elliptic curve E is given by

$$E/\mathbb{F}_q(t): \quad y^2 + xy = x^3 + a_2 x^2 + a_6.$$

The way the twisted curve is constructed is exactly the same as in the previous section. Therefore, most details will be omitted. Again as the quadratic extension of $K = \mathbb{F}_q$ we take the splitting field $L = K(s)$ where s satisfies the polynomial $g(x) = x^2 + x + a \in K[x]$. Then finding the automorphism satisfying the required properties yields

$$\begin{aligned} \sigma_4: \quad & y \mapsto y + x, \\ & s \mapsto s + 1. \end{aligned}$$

If we put this σ_4 into matrix form and find the independent components, we end up with

$$\sigma_4 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ x & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ x & 1 & x & 1 \end{pmatrix}.$$

Hence, the reduced form of $\sigma_4 - I$ is given by

$$\sigma_4 - I = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & x & 0 \end{pmatrix}$$

which has the two independent components $K(x)$ and $xs + y$. This gives us

$$L(E)^{<\sigma_4>} = K(x)[xs + y].$$

Then taking $\eta = s + y$ yields

$$\eta^2 + x\eta = y^2 + xy + x^2 a$$

hence the twisted curve over $L = K(s)$ is given by

$$E' : \quad y^2 + xy = x^3 + (a_2 + a)x^2 + a_6.$$

Since the curve E is defined over $\mathbb{F}_q(t)$, we need to twist E over $K = \mathbb{F}_q(t)$ instead of over $\mathbb{F}_q$. Therefore, take as irreducible polynomial over $K[x]$ the polynomial $g(x) = x^2 + tx + f(t)$, and take s as a root of this polynomial. Then the automorphism σ_4 changes to

$$\begin{aligned} \sigma_4 : \quad & y \mapsto y + x, \\ & s \mapsto s + t, \end{aligned}$$

and in the same way as the previous section also the isomorphism ψ changes, in this case it changes to

$$\begin{aligned} \psi : & E \to E^{tw} \\ & (x, y) \mapsto \left(x, y + \frac{sx}{t}\right). \end{aligned} \tag{B.4}$$

Defining $\eta = y + \frac{xs}{t}$ and renaming $\eta = y$ yields the final twisted curve

$$E^{tw}/\mathbb{F}_q(t,s) : \quad y^2 + xy = x^3 + \left(a_2 + \frac{f(t)}{t^2}\right) x^2 + a_6$$

which is isomorphic to $E/\mathbb{F}_q(t)$ over $L = \mathbb{F}_q(t,s)$ via the isomorphism given by (B.4).

C Implementing genus 1 in Magma

In this section we will discuss the programs written in Magma that are used to check Manin's proof. Below is the program for the case $\mathrm{char}(\mathbb{F}_q) = 2$ with $j(E) \neq 0$. In this case the elliptic curve and its twist are given by

$$\begin{aligned} E/\mathbb{F}_q: &\quad y^2 + xy = x^3 + a_2x^2 + a_6, \\ E^{tw}/\mathbb{F}_q(t): &\quad y^2 + xy = x^3 + \left(a_2 + \frac{f(t)}{t^2}\right)x^2 + a_6. \end{aligned}$$

In this case the program creates above two curves, and counts the points on the curve E via the normal way. The points on E^{tw} are counted via computing d_{-1} just as we did in the proof. These two numbers should be equal. Furthermore, the quadratic polynomial $d(n)$ is computed to see that it really is a parabola. Also d_n is computed so that we can check if indeed $d_n = d(n)$. This results in the following program.

```
Punten3:=function(p,r,i); //Case char=2, j neq 0. Input:
    p a prime, i the length of the interval for computing
    d(n)
  q:=p^r;
  Fq<v>:=GF(q); //Construct Fq
  Fqt<t>:=FunctionField(Fq); //Construct the function
      field Fq(t) over Fq
  a1:=1;
  a2:=Random(Fq);
  a6:=Random(Fq);

  while (a6 eq 0) do     //To exclude the case a6=0
      (which is not allowed since then the discriminant
      =0) be sure that we pick a_6 random but not equal
      to zero
    a6:=Random(Fq);
  end while;
  R<Y>:=PolynomialRing(Fqt);
  Fqts<s>:=ext<Fqt|Y^2+t*Y-(t^3+a2*t^2+a6)>; //Create
      the extension over Fq(t,s)
  E1:=EllipticCurve([Fq|a1,a2,0,0,a6]); //Construct E
      over Fq
  E2:=EllipticCurve([Fqts|a1,a2,0,0,a6]); //Construct
      the twisted curve over Fq(t,s)
  Q:=E2![t,s]; //Here we make the two points Q and P0
  P0:=E2![t^q,s^q];
  N:=Numerator(Fqt!(P0-Q)[1]);
  A:=#E1;
  D:=Degree(N); //This step computes d_{-1}

  printf "d_n given by ";
  for n:= -i to i do
    dn:=Fqt!(P0+n*Q)[1];
    B:=Numerator(dn);
    X:=Degree(B); //Here d_n is computed via the degree
        of the numerator of x_n
    printf "%o ",X;
  end for;

  printf "\n";

  printf "d(n) given by ";
  d1:=Degree(Numerator(Fqt!(P0-Q)[1]));
  d0:=Degree(Numerator(Fqt!(P0)[1]));
  for n:= -i to i do
    dn1:=n^2-(d1-d0-1)*n+d0; //This step computes d(n)
        via de quadratic expression
    printf "%o ",dn1;
  end for;

  printf "\n\n";

  printf "Number of points on E1: %o\n", A; //Here the
      number of points on the curve is printed. They
      should be equal.
  printf "Degree of num(x_{-1}): %o\n", D;
  return "";
end function;
```

If we run this program to see what happens we get the following result:

> Punten3(2,8,5);
d_n given by 396 364 334 306 280 256 234 214 196 180 166
$d(n)$ given by 396 364 334 306 280 256 234 214 196 180 166

Number of points on E1: 280
Degree of num(x_{-1}): 280

> Punten3(3,2,5);
d_n given by 44 33 24 17 12 9 8 9 12 17 24
$d(n)$ given by 44 33 24 17 12 9 8 9 12 17 24

Number of points on E1: 12
Degree of num(x_{-1}): 12

From this we can see that indeed the method of Manin works, we get exactly the same number of points via both methods. A strange thing is that this program also seems to work for primes $p \neq 2$. Indeed the program runs, but the result is not true. This is because lemma 4.3 does not hold when we use this specific curve E and E^{tw} for char($\mathbb{F}_q$) ≥ 3. The reason for this is that a lot of terms in the computation of x_{-1} do not cancel. Following the proof of lemma 4.3 we get that there are no common terms in numerator and denominator and thus we should get $d_{-1} = 2q + 1$. But then we do not have $d_{-1} = \#E(\mathbb{F}_q)$ and thus the lemma fails.

So the program works for primes $p \geq 3$ but the result is meaningless.
The programs for the cases $\mathrm{char}(\mathbb{F}_q) = 2$ with $j(E) = 0$ and $\mathrm{char}(\mathbb{F}_q) \geq 3$ are the same, only the extension to $\mathbb{F}_q(t,s)$ has an other curve and E, E^{tw} are different. Because the programs are quite the same the program for $\mathrm{char}(\mathbb{F}_q) \geq 3$ will not be shown here.
Interesting to see is what happens when we use the program for $\mathrm{char}(\mathbb{F}_q) \geq 3$ and we use $p = 2$. Running this program a few times yields
> Punten(3,2,5);
d_n given by 44 33 24 17 12 9 8 9 12 17 24
$d(n)$ given by 44 33 24 17 12 9 8 9 12 17 24

Number of points on E1: 12
Degree of num(x_{-1}): 12

> Punten(11,3,5);
d_n given by 1051 1103 1157 1213 1271 1331 1393 1457 1523 1591 1661
$d(n)$ given by 1051 1103 1157 1213 1271 1331 1393 1457 1523 1591 1661

Number of points on E1: 1271
Degree of num(x_{-1}): 1271

> Punten(2,4,5);

Punten(
p: 2,
r: 4,
i: 5
)
$>> Fqts < s >:= ext < Fqt|Y^2 - (t^3 + a2 * t^2 + a4 * t + a6) >;$

Runtime error in $ext < ... >$: Polynomial must be separable

From this we can see that the program works correct for primes $p \geq 3$ but for $p = 2$ we get an error, namely that the polynomial is not separable. This means that the two zeroes of the polynomial are equal. Indeed the two zeroes are given by y and $-y$ which are equal in $\mathrm{char}(\mathbb{F}_q) = 2$ so we have a problem. Therefore, this program gives an error when taking the incorrect prime p. Overall, both programs work fine for the corresponding correct prime numbers, and the programs show that the argument of Manin is indeed correct.