university of groningen

faculty of mathematics and natural sciences

Hesse pencil in characteristic two

Bachelor Project Mathematics

July 2015

Student: A. Tuijp

First supervisor: Prof.dr. J. Top

Second supervisor: Dr. A.E. Sterk

Abstract

In this paper we look at flex points on elliptic curves and to what extend they characterize the curve itself. In characteristic different from two and three, there exists a certain theorem about this by A. Anema. We will show that this theorem is also true in characteristic two. First, we give a short introduction to elliptic curves, the three-torsion group and the Weil-pairing. Then, given an elliptic curve in characteristic two, we define a curve that is in some way analogous to the Hessian in other characteristics: it intersects the elliptic curve only at its flex points. We use this alternative Hessian curve to define a Hesse pencil in characteristic two. Finally, we prove the only remaining proposition in Anema's proof for which an alternative proof is needed in characteristic two.

Contents

Introduction

Elliptic curves have been an object of interest in mathematics for a long time. They occurred for the first time in the work of Diophantus, even though he did not mention them by their name as we know it. Diophantus lived about 2000 years ago and is often called the 'father of algebra' [5]. More recently, about 20 years ago, Andrew Wiles used elliptic curves in his proof of Fermat's last theorem [6]. Nowadays, elliptic curves are still being studied a lot and they find many applications, for example in cryptography.

Exactly one hundred years ago, Dickson wrote an article about the inflexion points of cubic curves modulo two [2]. Here 'modulo two' can be read as 'characteristic two' and this is almost exactly what we will be looking at in this thesis: the flex points of curves in characteristic two. The only difference is that we will restrict ourselves to those cubic curves that define elliptic curves.

Our main goal in this thesis is to show that a certain theorem of A. Anema [1], which he proves for all characteristics except for two and three, is in fact also true in characteristic two. In chapter one we will state the theorem and explore some new concepts such as elliptic curves, Weil-pairings and 3-torsion groups.

In order to complete the proof in characteristic two, we will have to define a curve that plays a role analogous to the Hessian in other characteristics. We will define this curve in chapter two, where we will have to distinguish between the elliptic curves that have j-invariant nonzero and those that have j-invariant zero. We will show that the alternative Hessian does indeed satisfy the needed properties of the classic Hessian.

A large part of the proof of Anema does not depend on the characteristic of the field, so it is also valid in characteristic two. In chapter three, we will examine a proposition in Anema's proof for which it is not directly clear that it holds in characteristic two.

We were not the first ones to define a Hessian curve in characteristic two. In fact, Glynn [4] did so in 1998, using a very different notation than we do. In the appendix, we will show that our results match his. In the appendix we also include the MAGMA code used for some of the calculations.

1 Unraveling the theorem

The theorem by Anema which we will examine in characteristic two is the following:

Theorem 1.1. *If E and E' are elliptic curves given by some Weierstrass equation defined over k, then $E_{t_0} \cong_k E'$ for some $t_0 \in \mathbb{P}^1(k)$ if and only if there exists a symplectic isomorphism $E[3] \to E'[3]$.*

This theorem contains many concepts which may be new to the reader (as they were to the author at the start of this project). In this chapter we will try to explain the concepts which are needed in order to understand chapters two and three of this thesis and we will try to get a grasp of the meaning of the theorem.

1.1 A field of characteristic 2

Throughout this entire thesis, k will be a field. This means that it is a set which is closed under addition $(+)$ and multiplication $(\cdot)$ and which satisfies the 6 properties below [3]:

(R1) $(k, +, 0)$ is an abelian group, so

- $a + (b + c) = (a + b) + c$ for all $a, b, c \in k$
- $0 + a = a + 0 = a$ for all $a \in k$
- for every $a \in R$ there exists an additive inverse $-a \in R$ for which $a + (-a) = (-a) + a = 0$
- $a + b = b + a$ for all $a, b \in k$

(R2) associativity of $\cdot$: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in k$
(R3) distributve: $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$ for all $a, b, c \in k$
(R4) $1 \cdot a = a \cdot 1 = a$ for all $a \in k$
(R5) commutative: $a \cdot b = b \cdot a$ for all $a, b \in k$
(R6) $1 \neq 0$, and for all $a \in k$, $a \neq 0$, there is a multiplicative inverse $a^{-1} \in k$ for which $a \cdot \ a^{-1} = a^{-1} \cdot a = 1$.

As was announced before, we will consider the case where our field k has 'characteristic 2'.

Definition 1.2. *Let 1 be the unit element of a field K. If there is an element n of $\mathbb{Z}$ such that $1 + 1 + ... + 1$ (n terms) $= 0$, then the smallest positive element of $\mathbb{Z}$ with that property is called the characteristic of K. If there is no such number, the characteristic of K is 0.*

This definition implies that a field with characteristic 2 has the property that $1 + 1 = 0$. This means that for any element $a \in K$, $a + a = 0$, because it follows

from the properties of a field that $a+a = 1a+1a = (1+1)a = 0a = 0$. This may make calculations in characteristic two easy, because $2 = 0$ and we can replace a $-$ by a $+$ whenever we want. For example, in characteristic 2, the following equation

$$(x + y)^2 = 2z$$

becomes

$$x^2 = y^2.$$

1.2 An elliptic curve

We will define an elliptic curve as follows: an elliptic curve E is the set of points $(X : Y : Z) \in \mathbb{P}^2$ given by an equation $F = 0$. Here F should be homogeneous, have degree 3 and be smooth, which means that there are no points where all three partial derivatives are zero. Also, the point $(0 : 1 : 0)$ should lie on the curve and be a flex point, which means that the tangent line at this point must intersect the curve only in this point, with multiplicity 3.

Using a suitable change of coordinates, the equation defining an elliptic curve can always be written in a special form called the Weierstrass form:

$$Y^2Z + a_1XYZ + a_3Y = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

We say that E is defined over a field k if the coefficients a_i are elements of k. As we saw above, the points on the curve are elements of $\mathbb{P}^2$. This means that two points are considered to be the same if one is a multiple of the other. This makes sense, because if some point $(x : y : z)$ would satisfy the homogeneous Weierstrass equation, then so would the point $(cx : cy : cz)$. Let us consider a point on the curve on the curve with $Z = 0$. It follows from the Weierstrass equation that X must be zero as well, so in fact the only point on the curve with $Z = 0$ is the point $(0 : 1 : 0)$, which is our inflexion point. For all other points on the curve, we might as well set $Z = 1$, because only the ratio between X, Y and Z matters. So for $Z \neq 0$, we can set $x = X/Z$ and $y = Y/Z$ and find the following (affine) Weierstrass equation:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1}$$

This equation defines the same elliptic curve as the previous homogeneous equation, as long as we do not forget about the point $(0 : 1 : 0)$, which we will call O. We will encounter both notations in the rest of this thesis.

An elliptic curve E can be equipped with a group law, which means that we can add two points on the curve and find a third point on the curve. If we look at E as a group, the point O is the zero element, which explains its name.

The way in which points on an elliptic curve are added can best be explained using a picture over the real numbers: figure 1. To add two distinct points P

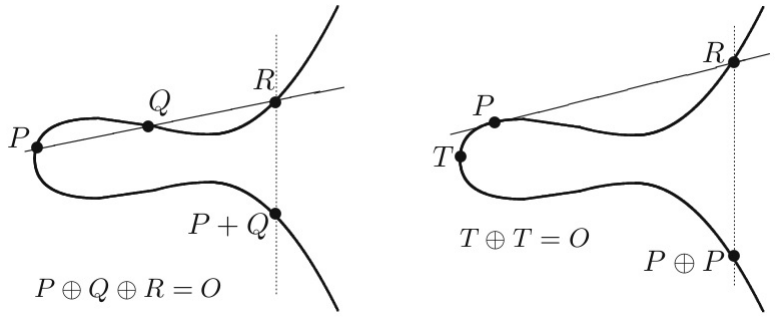

Figure 1: Adding points on an elliptic curve

and Q, one computes the line that goes through these two points and determines the third point of intersection with the curve. In the picture on the left, this is point R. If one then computes the line through R and O, which is in the picture a vertical line through R, then the remaining point of intersection of this line with the curve is the sum $P + Q$. If $P = Q$, then the line through both points should be replaced by the tangent line to the curve at P. It follows from this procedure that O is the zero element of the group: suppose we would add Q and O. Then we draw the line through Q and O, and find a third intersection point S. Then we draw the line through S and O and we find of course our point Q again, so $Q + O = Q$. We can also see that R and $P + Q$ (in the picture on the left) are additive inverses of each other: the line through both points intersects the curve again in the point O. Now we should compute the line through O and O: the tangent line at O. But O is a flex point, so this tangent line intersects the curve with multiplicity 3, so the sum of R and $P+Q$ is O.

This way of adding points can be extended to an arbitrary field k, because the notions of (tangent) lines and points of intersection can be, too. It is obvious that the addition of points in this way is commutative: the line through P and Q is the same line as the one through Q and P. It is also associative but that will not be shown here.

If E is given by the Weierstrass equation (1), the procedure can be expressed as explicit formulas in terms of the coordinates of the points as follows [7, p.53]:

- Let $P_0 = (x_0, y_0)$, then $-P_0 = (x_0, -y_0 - a_1x_0 - a_3)$.
- Let $P_1 + P_2 = (x_1, y_1) + (x_2, y_2) = (x_3, y_3) = P_3$.
  If $x_1 = x_2$ and $y_1 + y_2 + a_1x_2 + a_3 = 0$, then

  $$P_1 + P_2 = O.$$

  Otherwise:

  $$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2,$$

$$y_3 = -(\lambda + a_1)x_3 - \nu - a_3$$

with

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, \quad \nu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}.$$

In this notation, $y = \lambda x + \nu$ is the tangent line through P_1 and P_2, or the tangent line if the two points are the same.

In the next chapters, we will do some calculations with elliptic points in characteristic two. For example, we will calculate $-P$ and $2P$ for a point $P = (x, y)$ on E. In characteristic 2 (so $2 = 0$) and with $P_1 = P_2$, the formulas for adding points and taking the inverse simplify to

$$-P = (x, y + a_1x + a_3)$$

and $2P = (x_3, y_3)$, with

$$x_3 = \lambda^2 + a_1\lambda + a_2,$$

$$y_3 = (\lambda + a_1)x_3 + \nu + a_3$$

and

$$\lambda = \frac{x^2 + a_4 + a_1y}{a_1x + a_3}, \quad \nu = \frac{x^3 + a_4x + a_3y}{a_1x + a_3}.$$

Each elliptic curve E has a certain value associated to it, called the j-invariant $j(E)$. This j-invariant is invariant under isomorphisms, which means that two elliptic curves are isomorphic (with the isomorphism possibly defined over some extension field) if and only if they have the same j-invariant.

1.3 Elliptic curves in characteristic two

In a field with characteristic 2, elliptic curves can be transformed into a simpler form, using a suitable change of coordinates. There are two different types of elliptic curves in characteristic two: those with j-invariant nonzero and those with j-invariant zero. Each type has its own special Weierstrass form [7, p.409]:

- Type A: $j(E) \neq 0$:

$$y^2 + xy = x^3 + a_2x^2 + a_6, \quad \Delta = a_6, \quad j(E) = 1/a_6$$

- Type B: $j(E) = 0$:

$$y^2 + a_3y = x^3 + a_4x + a_6, \quad \Delta = a_3^4, \quad j(E) = 0.$$

The discriminant Δ is a value that should be nonzero, in order for the curve to be smooth.

1.4 The three-torsion group $E[3]$

The 3-torsion group $E[3]$ is defined as follows:

$$E[3] = \{P \in E : 3P = O\}.$$

It is easy to see that this is a subgroup of E. Clearly, O is an element of $E[3]$: $O + O + O = O$. If $3P = O$ and $3Q = O$, then

$$3(P + Q) = P + Q + P + Q + P + Q = 3P + 3Q = O + O = O,$$

because the addition of points is commutative.

The elements of $E[3]$ are exactly the flex points of E. This follows from the way in which points are added on an elliptic curve. If P is a flex point, then its tangent line intersects the curve again at P. The line through P and O intersects the curve again at $-P$, which must therefore equal $P + P$, so $2P = -P$, which is is equivalent to $3P = 0$. In fact, the only way in which you can add a point P to itself and find $-P$ is when the tangent line through the point intersects the curve three times at that point, so if $3P = O$, then P must be a flex point.

An important property which we will use in chapter 3 of this thesis is the following[7]:

$$E[3] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

In chapter 2 will show that there are nine flex points of E in characteristic two. Because they all have order 1 or 3, the group must indeed have the structure above.

1.5 The Hesse pencil

In the theorem we encounter E_{t_0}. This is an elliptic curve in the so-called Hesse pencil of E: a family of curves which are a combination of E and the Hessian of E. We will here explain what the Hessian and Hesse pencil are in characteristic different from two and why the Hesse pencil fails in characteristic two. In chapter two we will then define an alternative Hessian.

The Hessian of a polynomial F is defined as follows: let $F \in k[X, Y, Z]$ be a homogeneous polynomial of degree n. Then

$$\mathrm{Hess}(F) = \det \begin{pmatrix} \frac{\partial^2 F}{\partial X^2} & \frac{\partial^2 F}{\partial X \partial Y} & \frac{\partial^2 F}{\partial X \partial Z} \\ \frac{\partial^2 F}{\partial X \partial Y} & \frac{\partial^2 F}{\partial Y^2} & \frac{\partial^2 F}{\partial Y \partial Z} \\ \frac{\partial^2 F}{\partial X \partial Z} & \frac{\partial^2 F}{\partial Y \partial Z} & \frac{\partial^2 F}{\partial Z^2} \end{pmatrix}.$$

If F has degree three, the Hesse pencil of the curve $C = \mathcal{Z}(F)$ is defined as

$$\mathcal{C} = \mathcal{Z}\big(tF + \mathrm{Hess}(F)\big)$$

over $k(t)$. Note that the Hessian is either zero or a homogeneous polynomial of degree $3n-6$, so F and $\mathrm{Hess}(F)$ have the same degree only when $n=3$.

If we use a slightly different notation, then the Hesse pencil is defined by

$$\mathcal{C} = \mathcal{Z}\big(tF + s\mathrm{Hess}(F)\big)$$

where $(t:s) \in \mathbb{P}^1(\bar{k})$. Two points in $\mathbb{P}^1(\bar{k})$ are considered to be equal if they are multiples of each other, because they are the lines in the plane through the origin. So if s is nonzero, we can write $(t:s)$ as $(t/s:1) = (t_0:1)$ for some t_0, which we will just write as t_0. The point $(1:0)$ will be written as ∞. This allows us to use the following notation for a curve in the Hesse pencil of C:

$$C_{t_0} = \mathcal{Z}\big(t_0F + \mathrm{Hess}(F)\big)$$
$$C_\infty = C.$$

If k is a field of characteristic 2, then the Hessian of F, a homogeneous polynomial of degree 3, will always equal zero. This can be seen as follows: F has the following form:

$$a_1X^3+a_2XY^2+a_3XZ^2+a_4X^2Y+a_5Y^3+a_6YZ^2+a_7X^2Z+a_8Y^2Z+a_9Z^3+aXYZ$$

with a_i and a elements of k. For the first nine terms of F, it can easily be seen that the second (mixed) derivative will always equal zero: it will have one of the following forms:

- 0
- $2 \cdot 3 \cdot a_iX_j$
- $2 \cdot a_iX_j$

where X_j may be X, Y or Z. In characteristic 2, all of these forms equal 0. Therefore, we see that in our Hessian matrix, we only need to deal with the tenth term, for which the second mixed derivative is not necessarily zero. The Hessian matrix thus reduces to $\begin{pmatrix} \frac{\partial^2 F}{\partial X^2} & \frac{\partial^2 F}{\partial X \partial Y} & \frac{\partial^2 F}{\partial X \partial Z} \\ \frac{\partial^2 F}{\partial X \partial Y} & \frac{\partial^2 F}{\partial Y^2} & \frac{\partial^2 F}{\partial Y \partial Z} \\ \frac{\partial^2 F}{\partial X \partial Z} & \frac{\partial^2 F}{\partial Y \partial Z} & \frac{\partial^2 F}{\partial Z^2} \end{pmatrix} = \begin{pmatrix} 0 & aZ & aY \\ aZ & 0 & aX \\ aY & aX & 0 \end{pmatrix}$.

Expanding along the first row, we see that the determinant of this matrix is equal to $0 - aZ(0 - aXaY) + aY(aZaX - 0) = a^3XYZ + a^3XYZ = 0$.

If the Hessian of the curve C is zero, then the Hesse pencil will equal the curve C itself, which is not very interesting. Therefore, we will define an alternative Hessian and Hesse pencil and we will show that it satisfies the following very interesting property: a point P is a flex point of C (a curve in $\mathbb{P}^2$ given by a homogeneous polynomial F) if and only if it is a flex point of every curve in the Hesse pencil of C. Anema proves this for the classic Hessian in characteristic not two and in the next chapter we will prove it in characteristic two for our alternative Hesse pencil.

1.6 The Weil-pairing

The word 'symplectic' in the theorem means 'respecting the Weil-pairing'. The Weil-pairing e_3 is a surjective mapping:

$$e_3 : E[3] \times E[3] \longrightarrow \mu_3,$$

(where μ_3 is the group of the third roots of unity,) which has the following properties:

- It is bilinear:

$$e_3(S_1 + S_2, T) = e_3(S_1, T)e_3(S_2, T)$$
$$e_e(S, T_1 + T_2) = e_3(S, T_1)e_3(S, T_2).$$

- It is alternating:

$$e_3(T, T) = 1,$$

  so in particular,

$$e_3(S, T) = e_3(T, S)^{-1}.$$

These are the properties we will be needing in chapter 3 of this thesis. For a definition, a proof of these properties, more properties and more information on the Weil-pairing, we refer to [7].

1.7 The essence of the theorem

We are now a bit closer to being able to understand theorem 1.1. It is a statement about two elliptic curves: E and E'. For one of them, E, the Hesse Pencil has been constructed: a family of curves which depend on a parameter $t \in \mathbb{P}^1(\bar{k})$. Now there are two statements about these two curves which are equivalent:

1. There is a curve E_{t_0} in the Hesse pencil of E, which is isomorphic to E' as elliptic curves over k. Note that here t_0 is an element of $\mathbb{P}^1(k)$, so t is in k instead of its closure!

2. The three-torsion groups (which contain the flex points) of E and E' have the same group structure and there exists an isomorphism between them which respects the Weil-pairing.

In other words, we can say that this theorem is about how elliptic curves are characterized by their flex points.

2 Alternative Hesse pencil in characteristic two

As we have announced before, we will now define an alternative Hessian and Hesse pencil for characteristic two. Then we will prove that this pencil satisfies the properties needed for Anema's proof of the theorem: the flex points of the elliptic curve E are exactly the flex points of every curve in the Hesse pencil of E.

Let E be an elliptic curve given by a Weierstrass equation over k. Because there are two different Weierstrass forms in characteristic two, this chapter splits into two parts: one for each Weierstrass form. The proofs are essentially the same for both forms, but the calculations are a little different.

In the appendix, you can see that the Hessians we give are the same as the ones Glynn gives in his article [4]. Note however that Glynn defines a Hessian for any curve $C = \mathcal{Z}(F)$ with $F \in k[X, Y, Z]$ homogeneous of degree 3, and that Anema defines it even for degree n, whereas we define it only for those functions F that define an elliptic curve. Since theorem 1.1 is only about elliptic curves, it is no problem if we do not define the Hesse pencil for those curves that are not elliptic curves.

2.1 The case $j(E) \neq 0$

We have seen that in this case, E is given by:

$$y^2 + xy = x^3 + a_2x^2 + a_6, \quad \Delta = a_6, \quad j = 1/a_6.$$

Let us define $\mathrm{Hess}(E)$ as the curve defined by the following equation:

$$y^2 + xy^2 + x^2y + xy + a_2x^3 + a_2x^2 + a_6x = 0.$$

This means that our Hesse pencil $\mathcal{E}$ is given by:

$$t(y^2 + xy + x^3 + a_2x^2 + a_6) + y^2 + xy^2 + x^2y + xy + a_2x^3 + a_2x^2 + a_6x = 0.$$

From now on, we will denote individual curves in the Hesse pencil by E_t. We should remember that $E_\infty = E$ is also a curve in the Hesse pencil. In the next paragraphs, we will show that the Hessian and Hesse pencil have the desired properties.

2.1.1 Flex points of E

We will first show that E and the Hessian curve only intersect at the flex points of E:

Proposition 2.1. *If P is a point on E, an elliptic curve with $j(E) \neq 0$, then P is a flex point of E if and only if $P \in E \cap \mathrm{Hess}(E)$.*

Proof. First of all, let us look at the point O. This point is a flex point on E, which can be seen as follows. The homogeneous equation describing E is:

$$Y^2Z + XYZ = X^3 + a_2X^2Z + a_6Z^3.$$

We will dehomogenize this equation by setting $Y = 1$, so $x = X/Y$ and $z = Z/Y$:

$$F = z + xz + x^3 + a_2x^2z + a_6z^3 = 0.$$

This gives $F_x = z + x^2$ and $F_z = 1 + x + a_2x^2 + a_6z^2$, so the tangent line in the point O is the following:

$$\begin{aligned} 0 &= F_x(0,0)(x-0) + F_z(0,0)(z-0) \\ &= 0(x-0) + 1(z-0) \\ &= z \end{aligned}$$

So the tangent line is $z = 0$, the line at infinity. Substituting $z = 0$ in the equation $F = 0$ yields $x^3 = 0$, which has $x = 0$ as its solution with multiplicity 3. So the tangent line in the point $(0 : 1 : 0)$ intersects the elliptic curve with multiplicity 3, which means that O is a flex point of E. By looking at the homogeneous equation of $\mathrm{Hess}(E)$, we see that $(0 : 1 : 0)$ is also a point on $\mathrm{Hess}(E)$. Therefore, the proposition is true for the flex point O, which is the only point in $E \cap \mathrm{Hess}(E)$ with $z = 0$.

We will now look at the other flex points. We have already seen in 1.4 that P is a flex point of E if and only if $3P = 0$. This is equivalent to $-P = 2P$. We will now figure out what this means for the coordinates of a flex point $P = (x, y)$.

If we compare the equation $y^2 + xy = x^3 + a_2x^2 + a_6$ to the more general equation of an elliptic curve

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

we find that $a_1 = 1, a_3 = 0$, and $a_4 = 0$. Using the equations from section 1.2, we find the following formulas for $-P$ and $2P = P + P$:

$$-P = (x, y + x)$$

and

$$2P = (\lambda^2 + \lambda + a_2\ ,\ (\lambda + 1)(\lambda^2 + \lambda + a_2) + \nu)$$

with

$$\lambda = x + \frac{y}{x}, \quad \nu = x^2.$$

Note that we are only interested in points P with x nonzero, because for $P = (0, y)$ we find $P = -P$, so $2P = O$, which means that $3P \neq O$, since $P \neq O$.

Comparing the x- and y-coordinates, we see that $-P = 2P$ (or equivalently, P is a flex point) if and only if the following two equations hold:

$$\begin{aligned}
&(E1) \quad x = x^2 + (\frac{y}{x})^2 + x + \frac{y}{x} + a_2 \\
&(E2) \quad y + x = (x + \frac{y}{x} + 1)(x^2 + (\frac{y}{x})^2 + x + \frac{y}{x} + a_2) + x^2
\end{aligned}$$

Using the fact that P lies on E, so that $x^3 = y^2 + xy + a_2x^2 + a_6$, we can rewrite equation $(E1)$:

$$\begin{aligned}
& x = x^2 + (\frac{y}{x})^2 + x + \frac{y}{x} + a_2 \\
\Leftrightarrow\ & 0 = x^2 + (\frac{y}{x})^2 + \frac{y}{x} + a_2 \\
\Leftrightarrow\ & 0 = x^4 + y^2 + xy + a_2x^2 \qquad (2) \\
& \quad = x(y^2 + xy + a_2x^2 + a_6) + y^2 + xy + a_2x^2 \\
& \quad = y^2 + xy^2 + x^2y + xy + a_2x^3 + a_2x^2 + a_6x
\end{aligned}$$

We are now ready to prove the proposition in both directions:

$(\Longrightarrow)$ Let us assume that $P = (x, y)$ is a flex point on E. We have just seen that comparing the x-coordinates of $-P$ and $2P$ gives us equation $(E1)$ and that from this equation it follows that

$$y^2 + xy^2 + x^2y + xy + a_2x^3 + a_2x^2 + a_6x = 0,$$

which means that $P = (x, y) \in \mathrm{Hess}(E)$. We assumed that P is a flex point of E, so clearly $P \in E$, and therefore $P \in E \cap \mathrm{Hess}(E)$.

$(\Longleftarrow)$ Now assume that $P \in E \cap \mathrm{Hess}(E)$. This means that

$$y^2 + xy + x^3 + a_2x^2 + a_6 = 0$$

and

$$y^2 + xy^2 + x^2y + xy + a_2x^3 + a_2x^2 + a_6x = 0.$$

We have already seen that $(E1)$ follows from these two equations. If we can show that $(E2)$ holds as well, the proof is complete:

$$\begin{aligned}
& (x + \frac{y}{x} + 1)(x^2 + (\frac{y}{x})^2 + x + \frac{y}{x} + a_2) + x^2 \\
&= (x + \frac{y}{x} + 1)x + x^2 \quad \text{(from } (E1)\text{)} \\
&= x^2 + y + x + x^2 \\
&= y + x.
\end{aligned}$$

We see that both $(E1)$ and $(E2)$ are satisfied, so we may conclude that $P = (x, y)$ is a flex point on E. $\square$

Note that we could also say the following: $P = (x, y)$ is a flex point on E if and only if P is on E and satisfies equation (2). Equivalently, using the equation describing E, we could say that $P = (x, y)$ is a flex point on E if and only if P is on E and satisfies

$$x^4 + x^3 + a_6 = 0.$$

This equation has four distinct solutions for x and because for every (nonzero) x there are 2 y-coordinates such that (x, y) is on E, we may conclude that there are 8 points (x, y) on E satisfying this equation. Together with O, these are the nine elements of $E[3]$.

2.1.2 Flex points of the Hesse pencil

We have seen that P is a flex point of E if and only if P lies on E and on $\mathrm{Hess}(E)$. Now we will show that the flex point P also lies on every curve in the Hesse pencil $\mathcal{E}$, which is a linear combination of E and $\mathrm{Hess}(E)$. More interestingly, we will also show that P is a flex point of every curve in the Hesse pencil. Recall that the Hesse pencil is given by

$$t(y^2 + xy + x^3 + a_2x^2 + a_6) + y^2 + xy^2 + x^2y + xy + a_2x^3 + a_2x^2 + a_6x = 0.$$

Proposition 2.2. *If P is a flex point on E, an elliptic curve with $j(E) \neq 0$, then it is also a point on the Hesse pencil $\mathcal{E}$ and it is again a flex point.*

Proof. The first part of the proof is easy: it follows directly from the construction of $\mathcal{E}$. Let $P = (\xi, \eta)$ be a flex point on E. It follows that

$$\eta^2 + \xi\eta^2 + \xi^2\eta + \xi\eta + a_2\xi^3 + a_2\xi^2 + a_6\xi = 0$$

because P is a flex point of E. Also, if P lies on E, then

$$\eta^2 + \xi\eta + \xi^3 + a_2\xi^2 + a_6 = 0,$$

so clearly

$$t(\eta^2 + \xi\eta + \xi^3 + a_2\xi^2 + a_6) + \eta^2 + \xi\eta^2 + \xi^2\eta + \xi\eta + a_2\xi^3 + a_2\xi^2 + a_6\xi = 0$$

for every t, which means that P lies on every curve in the Hesse pencil.

To prove that P is also a flex point $\mathcal{E}$, we will determine the tangent line to $\mathcal{E}$ at the point P and show that it intersects $\mathcal{E}$ at P with multiplicity 3. If we set

$$F := t(y^2 + xy + x^3 + a_2x^2 + a_6) + y^2 + xy^2 + x^2y + xy + a_2x^3 + a_2x^2 + a_6x,$$

then the Hesse pencil is given by $F = 0$ and the tangent line at (ξ, η) by

$$\begin{aligned} 0 &= F_x(\xi, \eta)(x + \xi) + F_y(\xi, \eta)(y + \eta) \\ &= \big(t\eta + t\xi^2 + \eta^2 + \eta + a_2\xi^2 + a_6\big)(x + \xi) + \big(t\xi + \xi^2 + \xi\big)(y + \eta) \end{aligned}$$

If we substitute

$$y = \eta + \frac{t\eta + t\xi^2 + \eta^2 + \eta + a_2\xi^2 + a_6}{t\xi + \xi^2 + \xi}(x + \xi)$$

in $F = 0$, we can find the following equation:

$$(**)(x + \xi)^3 = 0 \tag{3}$$

with

$$\begin{aligned}(**) = &\frac{a_6t + a_6 + t^5 + t^4 + t + 1}{a_6^2 + t^8 + t^6 + t^4 + t^2}\xi^3 + \frac{a_6t + a_6}{a_6^2 + t^8 + t^6 + t^4 + t^2}\xi^2 \\ &+ \frac{a_6^2 + a_6t^3 + a_6t^2 + a_6t + a_6 + t^8 + t^7 + t^4 + t^3}{a_6^2 + t^8 + t^6 + t^4 + t^2}\xi \\ &+ \frac{a_6^2t + a_6t^3 + a_6t^2 + a_6t + a_6 + t^9 + t^7 + t^5 + t^3}{a_6^2 + t^8 + t^6 + t^4 + t^2}.\end{aligned}$$

Here we have used MAGMA (the code can be found in the appendix) and the facts that $\eta^2 + \xi\eta + \xi^3 + a_2\xi^2 + a_6 = 0$ (because P lies on E) and $\eta^2 + \xi\eta^2 + \xi^2\eta + \xi\eta + a_2\xi^3 + a_2\xi^2 + a_6\xi = 0$ (because P is a flex point).

The solutions for x of equation (3) give the intersection points of $\mathcal{E}$ and the tangent line at P. We see immediately that $x = \xi$ is the only zero, which has order 3. If we fill in $x = \xi$ in the formula for the tangent line, we see that the corresponding y-coordinate must be η. This means that the tangent line intersects the Hesse pencil with multiplicity 3 at the point $P = (\xi, \eta)$, so P is a flex point of the Hesse pencil.

Clearly the point O is also a point on the Hesse pencil and it is also a flex point, which can be shown in the same way. The tangent line to the Hesse pencil at O will be computed in the next chapter. □

2.2 The case $j(E) = 0$

Recall that in this case E is of the form:

$$y^2 + a_3y = x^3 + a_4x + a_6, \quad \Delta = a_3^4, \quad j = 0.$$

Let us define Hess(E) by:

$$xy^2 + a_3xy + a_4x^2 + (a_3^2 + a_6)x + a_4^2 = 0,$$

so the Hesse pencil $\mathcal{E}$ becomes:

$$t(y^2 + a_3y + x^3 + a_4x + a_6) + xy^2 + a_3xy + a_4x^2 + (a_3^2 + a_6)x + a_4^2 = 0.$$

2.2.1 Flex points of E

Proposition 2.3. *If P is a point on E, an elliptic curve with $j(E) = 0$, then P is a flex point if and only if $P \in E \cap \mathrm{Hess}(E)$.*

Proof. For O the exact same argument holds as when $j(E) \neq 0$. We will now again determine a condition that must hold for the points P for which $-P = 2P$.

Using the same formulas for $2P$ and $-P$ as in the previous paragraph, we find this time that if $P = (x, y)$, then

$$-P = (x, y + a_3)$$

and

$$2P = (\lambda^2, \lambda^3 + \nu + a_3)$$

with

$$\lambda = \frac{x^2 + a_4}{a_3}, \quad \nu = \frac{x^3}{a_3} + \frac{a_4 x}{a_3} + y.$$

Comparing the x-coordinates gives us the following equation: $x = \frac{x^4}{a_3^2} + \frac{a_4^2}{a_3^2}$, or:

$$a_3^2 x = x^4 + a_4^2 \tag{4}$$

Using the fact that P lies on the elliptic curve, so $x^3 = y^2 + a_3 y + a_4 x + a_6$, we see that

$$\begin{aligned} 0 &= a_3^2 x + x(y^2 + a_3 y + a_4 x + a_6) + a_4^2 \\ &= xy^2 + (a_3^2 + a_6)x + a_4 x^2 + a_3 xy + a_4^2 \end{aligned}$$

We see that comparing the y-coordinates again does not give us any new conditions, because $\nu = \lambda x + y$, which gives

$$\begin{aligned} y + a_3 &= \lambda^3 + \nu + a_3 \\ \Rightarrow y &= \lambda^3 + \lambda x + y \\ \Rightarrow 0 &= \lambda^3 + \lambda x \end{aligned}$$

which we know is true if $x = \lambda^2$, that is, if the x-coordinates of $-P$ and $2P$ are equal. □

From equation (4) we can deduce that there are indeed 9 flex points of E, just like in the case where $j(E) \neq 0$.

2.2.2 Flex points of the Hesse pencil

Proposition 2.4. *If P is a flex point on E, an elliptic curve with $j(E) = 0$, then it is also a point on the Hesse pencil $\mathcal{E}$ and it is again a flex point.*

Proof. This proof is the same as for the case $j(E) \neq 0$. Here we find the following equation for the tangent line

$$y = \eta + \frac{t\xi^2 + a_4 t + \xi^3 + a_4\xi + a_3^2}{a_3 t + a_3 \xi}(x + \xi)$$

and substituting this again into the equation of the Hesse pencil gives

$$(**)(x + \xi)^3 = 0$$

with

$$(**) = \frac{a_3^4}{a_3^4 t^2 + a_4^4 + t^8}\xi^3 + \frac{a_3^2 a_4^2 + a_3^2 t^4}{a_3^4 t^2 + a_4^4 + t^8}\xi^2 + \frac{a_4^4 + t^8}{a_3^4 t^2 + a_4^4 + t^8}\xi + \frac{a_3^6 + a_3^4 t^3 + a_3^2 a_4^2 t^2 + a_3^2 t^6 + a_4^4 t + t^9}{a_3^4 t^2 + a_4^4 + t^8}.$$

We see that there is again a triple intersection between the tangent line and the Hesse pencil at $P = (\xi, \eta)$. Again, the statement is also true for O. □

2.3 Another property

Another property of the Hesse pencil, which is independent of the type of elliptic curve, is the following:

Corollary 2.5. *Let $P \in E_{t_0} \cap E_{t_1}$. If $t_0 \neq t_1$, then P is a flex point on E.*

Proof. Let E be given by $F = 0$ and let Hess(E) be given by $H = 0$. Suppose that P is an element of E_{t_0} and of E_{t_1}, then

$$t_0 F(P) + H(P) = 0$$

and

$$t_1 F(P) + H(P) = 0.$$

If t_0 or t_1 equals ∞, then it follows directly that $F(P) = 0$. If not, then subtracting these two equations gives

$$(t_0 - t_1)F(P) = 0.$$

Because $t_0 \neq t_1$ (and because a field contains no zero divisors), we find that $F(P) = 0$, so $P \in E$. If we substitute $F(P) = 0$ in one of the two equations above, we see that $H(P) = 0$ as well, which means that $P \in$ Hess(E). It follows from proposition 2.1 that P is a flex point on E. □

3 Completing the proof in characteristic two

In the previous chapter, we have defined an alternative Hesse pencil and shown that this pencil has the desired properties. We can now follow Anema's proof almost completely, since most arguments do not involve the characteristic of k. There is only one proposition for which the proof needs to be adjusted for characteristic two, because here actual calculations are done with the Hesse pencil. In this chapter I will prove this proposition (it is currently prop. 4.10 in Anema's thesis):

Proposition 3.1. *Let E and E' be elliptic curves given by a Weierstrass equation defined over k. If $\phi : E[3] \to E'[3]$ is an isomorphism which respects the Weil-pairings, then there exists a linear change of coordinates $\Phi : E_{t_0} \to E'$ for some $t_0 \in \mathbb{P}^1(\bar{k})$ such that $\Phi\,|_{E[3]} = \phi$.*

3.1 Isomorphisms respecting the Weil-pairing

The following lemma will be used in the proof of the proposition:

Lemma 3.2. *Let E and E' be elliptic curves. Then 24 out of 48 isomorphisms $E[3] \to E'[3]$ respect the Weil-pairings.*

Proof. We have already seen that $E[3]$ and $E'[3]$ are isomorphic to $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$. Therefore we can look at the isomorphisms between the two groups as 2-by-2 matrices $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. This matrix maps $(1,0)$ to (a,c) and $(0,1)$ to (b,d), (with $a,b,c,d \in \mathbb{Z}/3\mathbb{Z}$,) which completely defines the isomorphism. Because an isomorphism has an inverse, A needs to be an invertible matrix. This means that a and b cannot both be zero. This leaves 8 possibilities for (a,b). If a choice has been made for (a,b), then (c,d) cannot be a multiple of (a,b), which rules out 3 possibilities. The other 6 possibilities for (c,d) however do give us an invertible matrix A. So we may conclude that there are $8 \times 6 = 48$ isomorphisms from $E[3]$ to $E'[3]$.

Now we want to determine how many of these isomorphisms respect the Weil-pairings. Let $\{\mathbf{e_1}, \mathbf{e_2}\}$ be a basis for $E[3]$. Then

$$\begin{aligned} e_3(A\mathbf{e_1}, A\mathbf{e_2}) &= e_3(a\mathbf{e_1} + c\mathbf{e_2}, b\mathbf{e_1} + d\mathbf{e_2}) \\ &= e_3(a\mathbf{e_1}, b\mathbf{e_1})e_3(a\mathbf{e_1}, d\mathbf{e_2})e_3(c\mathbf{e_2}, b\mathbf{e_1})e_3(c\mathbf{e_2}, d\mathbf{e_2}) \\ &= e_3(\mathbf{e_1}, \mathbf{e_1})^{ab} e_3(\mathbf{e_1}, \mathbf{e_2})^{ad} e_3\mathbf{e_2}, \mathbf{e_1})^{bc} e_3(\mathbf{e_2}, \mathbf{e_2})^{cd} \\ &= 1 \cdot e_3(\mathbf{e_1}, \mathbf{e_2})^{ad} e_3(\mathbf{e_1}, \mathbf{e_2})^{-bc} \cdot 1 \\ &= e_3(\mathbf{e_1}, \mathbf{e_2})^{ad-bc} \end{aligned}$$

We see that the Weil-pairing is respected if $ad - bc = \det(A) = 1$. The question is: are there 24 such matrices A? We saw that there are 48 matrices with determinant nonzero, so determinant equal to 1 or 2. I will now show that

there are just as many matrices with determinant 1 as there are matrices with determinant 2. Let B be a matrix with $\det(B) = 2$. Then B defines a bijection between the matrices with determinant 1 and 2: $A \mapsto BA$. Clearly, if $\det(A) = 1$, then $\det(BA) = 2$. The mapping is injective, because $BA = BC$ implies $A = C$ (because B is invertible) and it is surjective because for every C with $\det(C) = 2$, we can find an A with $C = BA$, namely: $A = B^{-1}C$, which has determinant 1. So B is indeed a bijection, which means that the number of matrices with determinant 1, which is the number of isomorphisms respecting the Weil-pairing, must be 24. □

3.2 The case $j(E) \neq 0$

3.2.1 The Weierstrass form of $\mathcal{E}$

In order to prove proposition 3.1, we want to determine the Weierstrass form of our Hesse pencil, because that allows us to calculate its j-invariant.

Recall that the Hesse pencil is the following:

$$\begin{aligned} & t(y^2z + xyz + x^3 + a_2x^2z + a_6z^3) \\ & \quad + xy^2 + x^2y + a_2x^3 + a_6xz^2 + y^2z + xyz + a_2x^2z = 0 \\ \Rightarrow\ & (t+1)y^2z + (t+1)xyz + xy^2 + x^2y \\ & \quad + (t+a_2)x^3 + a_2(t+1)x^2z + a_6xz^2 + ta_6z^3 = 0. \end{aligned}$$

Suppose $t \neq 1$. We want to find a suitable change of coordinates that gives us an equation in Weierstrass form:

$$\eta^2\zeta + \xi\eta\zeta = \xi^3 + b_2\xi^2\zeta + b_6\zeta^3.$$

The first step in doing this is finding the tangent line at the point O. By setting $y = 1$ and computing the derivatives with respect to x and z, we find that the tangent line is given by

$$x + (t+1)z = 0.$$

Our transformation should map this line to the line $\zeta = 0$. Let us define the coordinate transformation as follows:

$$\zeta := x + (t+1)z.$$

We can now rewrite the equation, using $z = \frac{x+\zeta}{t+1}$:

$$\begin{aligned}
&(t+1)y^2\Big(\frac{x+\zeta}{t+1}\Big) + (t+1)xy\Big(\frac{x+\zeta}{t+1}\Big) + xy^2 + x^2y + (t+a_2)x^3 \\
&\quad + a_2(t+1)x^2\Big(\frac{x+\zeta}{t+1}\Big) + a_6x\Big(\frac{x+\zeta}{t+1}\Big)^2 + ta_6\Big(\frac{x+\zeta}{t+1}\Big)^3 \\
&= y^2\zeta + y^2x + xy\zeta + x^2y + xy^2 + x^2y + (t+a_2)x^3 + a_2x^2\zeta + a_2x^3 \\
&\quad + \frac{a_6}{(t+1)^2}x\zeta^2 + \frac{a_6}{(t+1)^2}x^3 + \frac{a_6t}{(t+1)^3}(\zeta^3 + x\zeta^2 + x^2\zeta + x^3) \\
&= y^2\zeta + xy\zeta + \Big(t + \frac{a_6}{(t+1)^3}\Big)x^3 + \Big(a_2 + \frac{a_6t}{(t+1)^3}\Big)x^2\zeta + \frac{a_6}{(t+1)^3}x\zeta^2 \\
&\quad + \frac{a_6t}{(t+1)^3}\zeta^3 \\
&= 0.
\end{aligned}$$

If we multiply this equation by $(t+\frac{a_6}{(t+1)^3})^2$, which is the square of the coefficient of x^3, and then apply the following rescaling

$$\begin{aligned}
\xi &= \Big(t + \frac{a_6}{(t+1)^3}\Big)x \\
\dot{y} &= \Big(t + \frac{a_6}{(t+1)^3}\Big)y,
\end{aligned}$$

we get a term ξ^3 with coefficient 1:

$$\begin{aligned}
&\dot{y}^2\zeta + \xi\dot{y}\zeta + \xi^3 + \Big(a_2 + \frac{a_6t}{(t+1)^3}\Big)\xi^2\zeta + \frac{a_6}{(t+1)^3}\Big(t + \frac{a_6}{(t+1)^3}\Big)\xi\zeta^2 \\
&\quad + \Big(t + \frac{a_6}{(t+1)^3}\Big)^2\frac{a_6t}{(t+1)^3}\zeta^3 = 0.
\end{aligned}$$

To get rid of the $\xi\zeta^2$-term, we introduce the new variable η by:

$$\dot{y} = \eta + \frac{a_6}{(t+1)^3}\Big(t + \frac{a_6}{(t+1)^3}\Big)\zeta.$$

This will finally give us an equation of the right form:

$$\begin{aligned}
&\Big(\eta + \frac{a_6}{(t+1)^3}\Big(t + \frac{a_6}{(t+1)^3}\Big)\zeta\Big)^2\zeta + \xi\Big(\eta + \frac{a_6}{(t+1)^3}\Big(t + \frac{a_6}{(t+1)^3}\Big)\zeta\Big)\zeta + \xi^3 \\
&\quad + \Big(a_2 + \frac{a_6 t}{(t+1)^3}\Big)\xi^2\zeta + \frac{a_6}{(t+1)^3}\Big(t + \frac{a_6}{(t+1)^3}\Big)\xi\zeta^2 \\
&\quad + \Big(t + \frac{a_6}{(t+1)^3}\Big)^2 \frac{a_6 t}{(t+1)^3}\zeta^3 \\
&= \eta^2\zeta + \frac{a_6^2}{(t+1)^6}\Big(t^2 + \frac{a_6^2}{(t+1)^6}\Big)\zeta^3 + \xi\eta\zeta + \frac{a_6}{(t+1)^3}\Big(t + \frac{a_6}{(t+1)^3}\Big)\xi\zeta^2 + \xi^3 \\
&\quad + \Big(a_2 + \frac{a_6 t}{(t+1)^3}\Big)\xi^2\zeta + \frac{a_6}{(t+1)^3}\Big(t + \frac{a_6}{(t+1)^3}\Big)\xi\zeta^2 \\
&\quad + \Big(t + \frac{a_6}{(t+1)^3}\Big)^2 \frac{a_6 t}{(t+1)^3}\zeta^3 \\
&= \eta^2\zeta + \xi\eta\zeta + \xi^3 + \Big(a_2 + \frac{a_6 t}{(t+1)^3}\Big)\xi^2\zeta \\
&\quad + \Big(\Big(t + \frac{a_6}{(t+1)^3}\Big)^2 \frac{a_6 t}{(t+1)^3} + \frac{a_6^2}{(t+1)^6}\Big(t^2 + \frac{a_6^2}{(t+1)^6}\Big)\Big)\zeta^3 \\
&= \eta^2\zeta + \xi\eta\zeta + \xi^3 + b_2\xi^2\zeta + b_6\zeta^3 \\
&= 0.
\end{aligned}$$

with

$$\begin{aligned}
b_2 &= a_2 + \frac{a_6 t}{(t+1)^3}, \\
b_6 &= \frac{a_6}{(t+1)^3}\Big(t^3 + \frac{a_6 t^2}{(t+1)^3} + \frac{a_6^2 t}{(t+1)^6} + \frac{a_6^3}{(t+1)^9}\Big).
\end{aligned}$$

Let this family of curves be denoted by $\mathcal{E}^W$ and let an individual curve in the pencil be denoted by E_t^W.

The j-invariant of a curve in the Hesse pencil, which depends on t, is

$$\begin{aligned}
j(E_t^W) = 1/b_6 &= \frac{(t+1)^3}{a_6\Big(t^3 + \frac{a_6 t^2}{(t+1)^3} + \frac{a_6^2 t}{(t+1)^6} + \frac{a_6^3}{(t+1)^9}\Big)} \\
&= \frac{(t+1)^{12}}{a_6\Big(t^3(t+1)^9 + a_6 t^2(t+1)^6 + a_6^2 t(t+1)^3 + a_6^3\Big)} \\
&= \frac{(t+1)^{12}}{a_6\big(t^4 + t^3 + t^2 + t + a_6\big)^3}
\end{aligned}$$

If $t = 1$, the transformations we used above are not valid. In fact, it is not possible to transform E_1 into a Weierstrass equation of this form, because the j-invariant of E_1 is zero. So we will try to transform it into the other Weierstrass form in characteristic 2:

$$\eta^2\zeta + b_3\eta\zeta^2 = \xi^3 + b_4\xi\zeta^2 + b_6\zeta^3.$$

By filling in $t = 1$ in our Hesse pencil, we see that E_1 is given by

$$xy^2 + x^2y + (1 + a_2)x^3 + a_6xz^2 + a_6z^3 = 0.$$

We can again find the tangent line by setting $y = 1$ and find that the tangent line is given by $x = 0$. We want to map this line to $\zeta = 0$, so we can 'swap' x and z as follows:

$$\zeta := x, \quad \dot{x} := z.$$

Substituting this for x and z gives us:

$$y^2\zeta + y\zeta^2 + a_6\dot{x}^3 + a_6\dot{x}^2\zeta + (1 + a_2)\zeta^3 = 0.$$

By multiplying the equation by a_6^2 and setting

$$\eta := \frac{1}{a_6}y, \quad \ddot{x} := \frac{1}{a_6}\dot{x},$$

we get

$$\eta^2\zeta + a_6\eta\zeta^2 + \ddot{x}^3 + a_6\ddot{x}^2\zeta + a_6^2(1 + a_2)\zeta^3 = 0.$$

Finally, by setting

$$\xi := \ddot{x} + a_6\zeta,$$

our equation becomes

$$\begin{aligned}
&\eta^2\zeta + a_6\eta\zeta^2 + \xi^3 + a_6\xi^2\zeta + a_6^2\xi\zeta^2 + a_6^3\zeta^3 + a_6\xi^2\zeta + a_6^3\zeta^3 + a_6^2(1 + a_2)\zeta^3 \\
&= \eta^2\zeta + a_6\eta\zeta^2 + \xi^3 + a_6^2\xi\zeta^2 + a_6^2(1 + a_2)\zeta^3 \\
&= \eta^2\zeta + b_3\eta\zeta^2 + \xi^3 + b_4\xi\zeta^2 + b_6\zeta^3 = 0.
\end{aligned}$$

Which is indeed the Weierstrass form for a curve with j-invariant 0. We have seen that for every t, there exists a linear transformation $E_t \to E_t^W$. Let us denote this transformation by A_t.

3.2.2 Proof of the proposition

Proof of proposition 3.1 if $j(E) \neq 0$.
Now given another elliptic curve E' with j-invariant j_0', we want to determine t for which our Hesse pencil has the same j-invariant. First, let us assume that j_0' is nonzero and not equal to j_0.

$$\begin{aligned}
&j_0' = j(E_t^W) \\
\Leftrightarrow\ &(t+1)^{12} = j_0'a_6\big(t^4 + t^3 + t^2 + t + a_6\big)^3
\end{aligned}$$

Define the polynomial

$$G = (t+1)^{12} + j_0' a_6 \big(t^4 + t^3 + t^2 + t + a_6\big)^3.$$

The roots of this polynomial give $E_{t_0}^W$'s with j-invariant equal to j_0'. The discriminant of this polynomial can be computed using MAGMA or Mathematica (MAGMA code can be found in the appendix) and equals $a_6^{44} j_0'^{14}$, which is nonzero, because j_0' and a_6 are nonzero. Because G has degree twelve and a nonzero discriminant, it has twelve different roots t_i in $\bar{k}$.

For every t_i, there is an isomorphism A_{t_i} between E_{t_i} and $E_{t_i}^W$, induced by the change of coordinates we have seen above. For every t_i which is a root of G, there is an isomorphism Ψ_i between $E_{t_i}^W$ and E', because they have equal j-invariants. Lastly, there exist 2 automorphisms σ of E' [7, p.410]. If we would take the composition of these three isomorphisms and restrict it to the 3-torsion group of E_{t_i}, which equals the 3-torsion group of E, we get $12 \times 2 = 24$ isomorphisms $\phi_{i,\sigma}$:

$$\phi_{i,\sigma} = \sigma \ \circ \ \Psi_i \ \circ \ A_{t_i} \ |_{E_{t_i}[3]} : \ E[3] \to E'[3].$$

These 24 isomorphisms are all different and respect the Weil-pairing (see [1] for the details, this argument is independent of the characteristic of k).

Now assume that $j_0' = j_0 \neq 0$. Then $j_0' a_6 = 1$, because $j_0 = 1/a_6$. Now our polynomial G becomes a polynomial of degree 11 with discriminant $a_6^{30} \neq 0$. So this gives us 11 different t's in $\bar{k}$ that give an E_t^W with j-invariant equal to j_0. But another curve that has this j-invariant is $E_\infty = E$. So again we find 12 different t's and in the same way as above, we find 24 isomorphisms respecting the Weil-pairing.

If $j_0' = 0$, G doesn't give us any roots, because t could not equal one in that case. However, we have seen that E_1 has j-invariant zero, so $t = 1$ is the only value we find. Bcause E' has j-invariant zero and k has characteristic 2, its automorphism group has 24 elements [7, p.410]. So again we find 24 isomorphisms respecting the Weil-pairing.

We can now complete the proof of proposition 3.1. We see that for every value of j_0', we find 24 isomorphisms $\phi_{i,\sigma} : E[3] \to E'[3]$. It follows from lemma 3.2 that these are all the possible isomorphisms $E[3] \to E'[3]$ that respect the Weil-pairings. So if we assume that ϕ is an isomorphism which respects the Weil-pairings, then it must equal $\phi_{i,\sigma}$ for some i and σ. For these i and σ, the map $\Phi := \sigma \ \circ \ \Psi_i \ \circ \ A_{t_i}$ is the map we were looking for, which completes the proof. □

3.3 The case $j(E) = 0$

In this case the calculations are a little bigger, because there are 3 a_i's now. Therefore, and because the derivation of the Weierstrass form has already been

treated elaborately in the case where $j(E) \neq 0$, the detailed calculations for this case will not be fully given here. The steps however will be explained.

3.3.1 The Weierstrass form of $\mathcal{E}$

The Hesse pencil is given by:

$$\begin{aligned} &t(y^2z + a_3yz^2 + x^3 + a_4xz^2 + a_6z^3) \\ &\quad + xy^2 + a_3xyz + a_4x^2z + (a_3^2 + a_6)xz^2 + a_4^2z^3. \end{aligned}$$

The tangent line can again be computed by setting $y = 1$ and computing the partial derivatives with respect to x and z. This gives the following equation for the tangent line:

$$x + tz = 0.$$

Because this line should be mapped to the line $\zeta = 0$, we will define the new variable ζ by

$$z = \frac{x + \zeta}{t}.$$

This gives an equation of the form

$$y^2\zeta + c_1y\zeta^2 + c_2xy\zeta + c_3x^3 + c_4x^2\zeta + c_5x\zeta^2 + c_6\zeta^3 = 0.$$

Here the c_i's are combinations of t and the a_i's. If we multiply the equation by c_3^2 and introduce the new variables

$$\dot{x} := c_3x, \qquad \dot{y} := c_3y,$$

our equation transforms to

$$\dot{y}^2\zeta + d_1\dot{x}\dot{y}\zeta + d_3\dot{y}\zeta^2 + \dot{x}^3 + d_2\dot{x}^2\zeta + d_4\dot{x}\zeta^2 + d_6\zeta^3 = 0.$$

This is already in Weierstrass form, but by introducing ξ and η by

$$x = d_1^2\xi + \frac{d_3}{d_1}\zeta, \qquad y = d_1^3\eta + \frac{d_1^2d_4 + d_3^2}{d_1^3}\zeta,$$

and by dividing the equation by the nonzero term $\frac{a_3^6}{t^6}$ we find $\mathcal{E}^W$, the simpler Weierstrass form of $\mathcal{E}$ in characteristic two:

$$\begin{aligned} &\eta^2\zeta + \xi\eta\zeta + \xi^3 + \frac{\left({a_3}^8 + {a_3}^6a_4t + {a_3}^6a_6 + {a_3}^6t^3\right)}{{a_3}^8}\xi^2\zeta \\ &\quad + \frac{\left({a_3}^6t^3 + {a_3}^4{a_4}^2t^2 + {a_3}^4t^6 + {a_3}^2{a_4}^4t + {a_3}^2t^9 + {a_4}^6 + {a_4}^4t^4 + {a_4}^2t^8 + t^{12}\right)}{{a_3}^8}\zeta^3 \\ &= \eta^2\zeta + \xi\eta\zeta + \xi^3 + b_2\xi^2\zeta + b_6\zeta^3 \\ &= 0. \end{aligned}$$

The j-invariant of E_t^W for $t \neq 0$ is given by

$$j(E_t^W) = \frac{{a_3}^8}{{a_3}^6 t^3 + {a_3}^4 {a_4}^2 t^2 + {a_3}^4 t^6 + {a_3}^2 {a_4}^4 t + {a_3}^2 t^9 + {a_4}^6 + {a_4}^4 t^4 + {a_4}^2 t^8 + t^{12}}.$$

If $t = 0$, so if E_t is the Hessian curve, the transformations above are not valid. Therefore, we will treat this case separately. The Hessian was defined by the following equation

$$xy^2 + a_3 xyz + a_4 x^2 z + (a_3^2 + a_6) xz^2 + a_4^2 z^3 = 0.$$

Just like in the case where $j(E) \neq 0$ and $t = 1$, the tangent line at O is given by $x = 0$, so we will again swap x and z, using $\dot{x}$ and ζ as our new variables, giving:

$$y^2\zeta + a_3 \dot{x} y \zeta + a_4^2 \dot{x}^3 + (a_3^2 + a_6)\dot{x}^2 \zeta + a_4 \dot{x} \zeta^2 = 0.$$

In order to set the coefficients of the xyz- and the x^3-terms equal to 1, and to get rid of the xz^2-term, we multiply the equation by $\frac{a_4^4}{a_3^6}$ and introduce the new variables

$$\xi := \frac{a_4^2}{a_3^2}., \quad \eta := \frac{a_4^2}{a_3^3} y + \frac{a_4^3}{a_3^4} \zeta.$$

We find the following Weierstrass equation:

$$\eta^2 \zeta + \xi \eta \zeta + \xi^3 + \frac{a_3^2 + a_6}{a_3^2} \xi^2 \zeta + \frac{a_4^6}{a_3^8} \zeta^3 = 0.$$

The j-invariant of this curve is $\frac{a_3^8}{a_4^6}$, so we may conclude that for every t, so even for $t = 0$, the j-invariant of E_t^W is given by:

$$j(E_t^W) = \frac{{a_3}^8}{{a_3}^6 t^3 + {a_3}^4 {a_4}^2 t^2 + {a_3}^4 t^6 + {a_3}^2 {a_4}^4 t + {a_3}^2 t^9 + {a_4}^6 + {a_4}^4 t^4 + {a_4}^2 t^8 + t^{12}}.$$

3.3.2 Proof of the proposition

Proof of proposition 3.1 if $j(E) = 0$. Again, we want to show that for every j_0', there exist 24 different isomorphisms. First, assume that $j_0' \neq 0$. Then we can define

$$G := a_3^4 \big(a_3^8 + \big({a_3}^6 t^3 + {a_3}^4 {a_4}^2 t^2 + {a_3}^4 t^6 + {a_3}^2 {a_4}^4 t + {a_3}^2 t^9 + {a_4}^6 + {a_4}^4 t^4 + {a_4}^2 t^8 + t^{12} \big) \big),$$

a polynomial of degree 12 with discriminant $a_3^{176} j_0'^{14} = \Delta(E)^{44} j_0'^{14}$. G has therefore 12 different roots, which are all solutions t_i for which $j(E_{t_i}^W) = j_0'$. Again, together with the 2 automorphisms σ, we find 24 isomorphisms.

Now assume that $j_0' = 0$. In this case, the curve in the Hesse pencil we are looking for, is E itself: this curve has j-invariant zero. And again the automorphism group has order 24 so also in this case, we find 24 isomorphisms, which completes the proof. □

Conclusion

The conclusion of this thesis is the following: if we define an alternative Hesse pencil, then theorem 1.1 by Anema is also true in characteristic two.

In the first chapter we explored new concepts that occurred in theorem 1.1. We examined elliptic curves, which are at the same time a curve and a group. We looked at the 3-torsion group, which is essentially the same as the group of flex points of an elliptic curve. The classic Hessian was studied and we gave a short introduction to the Weil-paring.

In the second chapter we defined the alternative Hessian and corresponding Hesse pencil and proved that it satisfies the properties we need: the flex points of an elliptic curve E are also the flex points of the Hesse pencil of E, and if a point lies on two different curves in the Hesse pencil, then it must be a flex point.

The biggest part of Anema's proof of theorem 1.1 is also valid in characteristic two. In chapter 3, we examined the only proposition in his proof for which this was not the case and we provided a proof for this proposition in characteristic 2 using our alternative Hesse pencil. By doing this, we have in fact proved theorem 1.1. Actually, our proof of the theorem in characteristic two is very similar to Anema's proof for the other characteristics.

Acknowledgements

First and most important of all, I would like to thank my supervisor Jaap Top for trusting me with this subject, for the numerous sessions in his office in which I have learned so much, for being understanding in case of 'personal circumstances' and for pointing out that 'O' that was not yet written between dollar signs. Secondly, I would like to thank Alef Sterk for being my second supervisor. Lastly, I would like to thank Remko for his support and encouragements and for never refusing to have another discussion about fields of characteristic two, even on holiday, on the bike or at 11 o'clock in the evening.

Bibliography

[1] A. Anema. *PhD thesis in preparation.* University of Groningen.

[2] L.E. Dickson. Invariantive theory of plane cubic curves modulo 2. *American Journal of Mathematics*, 37:107–116, 1915.

[3] B. van Geemen, H.W. Lenstra, F. Oort, and J. Top. *Algebraische structuren.* February 2014.

[4] D.G. Glynn. On cubic curves in projective planes of characteristic two. *Australasian Journal of Combinatorics*, 17:1–20, 1998.

[5] J.J. O'Connor and E.F. Robertson. Diophantus. `http://www-history.mcs.st-and.ac.uk/Biographies/Diophantus.html`, July 2015.

[6] J.J. O'Connor and E.F. Robertson. Fermat's last theorem. `http://www-history.mcs.st-andrews.ac.uk/HistTopics/Fermat's_last_theorem.html`, July 2015.

[7] J.H. Silverman. *The Arithmetic of Elliptic Curves.* Springer, 1985.

A The Hesse pencil as defined by Glynn

A.1 $j(E) \neq 0$

Glynn also defines a Hesse pencil in his article. Here we will show that this is the same pencil as we have defined in our thesis.

Glynn defines a cubic curve as follows, using his special notation:

$$C(A, a) = \{x \in \pi | xAx^2 + ax\hat{x} = 0\}$$

where A is a 3×3 matrix over K and $a \in K$, such that A and a are not both zero.

We can translate this as follows: C consists of those points $(x_0 : x_1 : x_2) \in \mathbb{P}^2$ for which

$$\begin{aligned} xAx^2 + ax\hat{x} &:= \begin{pmatrix} x_0 & x_1 & x_2 \end{pmatrix} \begin{pmatrix} a_{00} & a_{01} & a_{02} \\ a_{10} & a_{11} & a_{12} \\ a_{20} & a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} x_0^2 \\ x_1^2 \\ x_2^2 \end{pmatrix} + a \begin{pmatrix} x_0 & x_1 & x_2 \end{pmatrix} \begin{pmatrix} x_1x_2 \\ x_0x_2 \\ x_0x_1 \end{pmatrix} \\ &= x_0(a_{00}x_0^2 + a_{01}x_1^2 + a_{02}x_2^2) + x_1(a_{10}x_0^2 + a_{11}x_1^2 + a_{12}x_2^2) \\ &\quad + x_2(a_{20}x_0^2 + a_{21}x_1^2 + a_{22}x_2^2) + a(3x_0x_1x_2) \\ &= a_{00}x_0^3 + a_{01}x_0x_1^2 + a_{02}x_0x_2^2 + a_{10}x_0^2x_1 + a_{11}x_1^3 + a_{12}x_1x_2^2 \\ &\quad + a_{20}x_0^2x_2 + a_{21}x_1^2x_2 + a_{22}x_2^3 + ax_0x_1x_2 \\ &= 0 \end{aligned}$$

We are working with elliptic curves defined by

$$C = Z(y^2z + a_1xyz + a_3yz^2 + x^3 + a_2x^2z + a_4xz^2 + a_6z^3).$$

We will now try to find A and a in the notation of Glynn corresponding to this elliptic curve. Setting $(x_0, x_1, x_2) = (x, y, z)$, we see that for $a = a_1$ and the following A, our elliptic curve is equal to $C(A, a)$ in Glynn's notation:

$$A = \begin{pmatrix} a_{00} & a_{01} & a_{02} \\ a_{10} & a_{11} & a_{12} \\ a_{20} & a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} 1 & 0 & a_4 \\ 0 & 0 & a_3 \\ a_2 & 1 & a_6 \end{pmatrix}$$

Theorem A.1. *The set C' of tangent lines to $C = C(A, a)$, classically the dual of a sextic curve, is in the case of even characteristic a dual cubic curve (or cubic envelope) $C' := C(A', a^2)^t$. Let $A := (a_{ij}), (i, j = 0, 1, 2)$. Then A' is the 3×3 matrix over K given by*

$$A' := adj(A)^t + a \begin{pmatrix} 0 & a_{02} & a_{01} \\ a_{12} & 0 & a_{10} \\ a_{21} & a_{20} & 0 \end{pmatrix}, \text{ where}$$

$$adj(A)^t := \begin{pmatrix} a_{11}a_{22} + a_{12}a_{21} & a_{10}a_{22} + a_{12}a_{20} & a_{10}a_{21} + a_{11}a_{20} \\ a_{01}a_{22} + a_{02}a_{21} & a_{00}a_{22} + a_{02}a_{20} & a_{00}a_{21} + a_{01}a_{20} \\ a_{01}a_{12} + a_{02}a_{11} & a_{00}a_{12} + a_{02}a_{10} & a_{00}a_{11} + a_{01}a_{10} \end{pmatrix}$$

We will first compute $adj(A)^t$ (which is just the cofactor matrix with a plus instead of every minus, because of characteristic 2) for the matrix A corresponding to our elliptic curve:

$$adj(A)^t = \begin{pmatrix} a_3 & a_2a_3 & 0 \\ a_4 & a_6 + a_2a_4 & 1 \\ 0 & a_3 & 0 \end{pmatrix}$$

so

$$\begin{aligned} A' &= adj(A)^t + a \begin{pmatrix} 0 & a_{02} & a_{01} \\ a_{12} & 0 & a_{10} \\ a_{21} & a_{20} & 0 \end{pmatrix} \\ &= \begin{pmatrix} a_3 & a_2a_3 & 0 \\ a_4 & a_6 + a_2a_4 & 1 \\ 0 & a_3 & 0 \end{pmatrix} + a_1 \begin{pmatrix} 0 & a_4 & 0 \\ a_3 & 0 & 0 \\ 1 & a_2 & 0 \end{pmatrix} \\ &= \begin{pmatrix} a_3 & a_1a_4 + a_2a_3 & 0 \\ a_4 + a_1a_3 & a_6 + a_2a_4 & 1 \\ a_1 & a_3 + a_1a_2 & 0 \end{pmatrix} \end{aligned}$$

So $C' = C(A', a_1^2)$. To find A'', the matrix of the cubic curve $C'' := (C')'$, we will do the same for A' as we just did for A. I will write the coefficients of the matrix A' as a'_{ij}.

$$\begin{aligned} adj(A')^t &= \begin{pmatrix} a_3 + a_1a_2 & a_1 & (a_4 + a_1a_3)(a_3 + a_1a_2) + a_1(a_6 + a_2a_4) \\ 0 & 0 & a_3(a_3 + a_1a_2) + a_1(a_1a_4 + a_2a_3) \\ a_1a_4 + a_2a_3 & a_3 & a_3(a_6 + a_2a_4) + (a_4 + a_1a_3)(a_1a_4 + a_2a_3) \end{pmatrix} \\ &= \begin{pmatrix} a_3 + a_1a_2 & a_1 & a_3a_4 + a_1a_3^2 + a_1^2a_2a_3 + a_1a_6 \\ 0 & 0 & a_3^2 + a_1^2a_4 \\ a_1a_4 + a_2a_3 & a_3 & a_3a_6 + a_1a_4^2 + a_1^2a_3a_4 + a_1a_2a_3^2 \end{pmatrix}. \end{aligned}$$

On the other hand we have:

$$\begin{aligned} a_1^2 \begin{pmatrix} 0 & a'_{02} & a'_{01} \\ a'_{12} & 0 & a'_{10} \\ a'_{21} & a'_{20} & 0 \end{pmatrix} &= a_1^2 \begin{pmatrix} 0 & 0 & a_1a_4 + a_2a_3 \\ 1 & 0 & a_4 + a_1a_3 \\ a_3 + a_1a_2 & a_1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 & a_1^2(a_1a_4 + a_2a_3) \\ a_1^2 & 0 & a_1^2(a_4 + a_1a_3) \\ a_1^2(a_3 + a_1a_2) & a_1^3 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0 & 0 & a_1^3a_4 + a_1^2a_2a_3 \\ a_1^2 & 0 & a_1^2a_4 + a_1^3a_3 \\ a_1^2a_3 + a_1^3a_2 & a_1^3 & 0 \end{pmatrix} \end{aligned}$$

Adding the two matrices we computed above, we find A'':

$$\begin{aligned}
A'' &= adj(A')^t + a_1^2 \begin{pmatrix} 0 & a'_{02} & a'_{01} \\ a'_{12} & 0 & a'_{10} \\ a'_{21} & a'_{20} & 0 \end{pmatrix} \\
&= \begin{pmatrix} a_3 + a_1a_2 & a_1 & a_3a_4 + a_1a_3^2 + a_1^2a_2a_3 + a_1a_6 \\ 0 & 0 & a_3^2 + a_1^2a_4 \\ a_1a_4 + a_2a_3 & a_3 & a_3a_6 + a_1a_4^2 + a_1^2a_3a_4 + a_1a_2a_3^2 \end{pmatrix} \\
&\qquad + \begin{pmatrix} 0 & 0 & a_1^3a_4 + a_1^2a_2a_3 \\ a_1^2 & 0 & a_1^2a_4 + a_1^3a_3 \\ a_1^2a_3 + a_1^3a_2 & a_1^3 & 0 \end{pmatrix} \\
&= \begin{pmatrix} a_3 + a_1a_2 & a_1 & a_3a_4 + a_1a_3^2 + a_1a_6 + a_1^3a_4 \\ a_1^2 & 0 & a_3^2 + a_1^3a_3 \\ a_1a_4 + a_2a_3 + a_1^2a_3 + a_1^3a_2 & a_3 + a_1^3 & a_3a_6 + a_1a_4^2 + a_1^2a_3a_4 + a_1a_2a_3^2 \end{pmatrix}
\end{aligned}$$

The Hessian of C is now $C'' = (C')' = C(A'', a^4 = C(A'', a_1^4)$, which we can write as all points (x_0, x_1, x_2) for which

$$\begin{aligned}
&a''_{00}x_0^3 + a''_{01}x_0x_1^2 + a''_{02}x_0x_2^2 + a''_{10}x_0^2x_1 + a''_{11}x_1^3 + a''_{12}x_1x_2^2 \\
&\quad + a''_{20}x_0^2x_2 + a''_{21}x_1^2x_2 + a''_{22}x_2^3 + a^4x_0x_1x_2 \\
&= (a_3 + a_1a_2)x_0^3 + a_1x_0x_1^2 + (a_3a_4 + a_1a_3^2 + a_1a_6 + a_1^3a_4)x_0x_2^2 \\
&\quad + a_1^2x_0^2x_1 + (a_3^2 + a_1^3a_3)x_1x_2^2 + (a_1a_4 + a_2a_3 + a_1^2a_3 + a_1^3a_2)x_0^2x_2 \\
&\quad + (a_3 + a_1^3)x_1^2x_2 + (a_3a_6 + a_1a_4^2 + a_1^2a_3a_4 + a_1a_2a_3^2)x_2^3 + a_1^4x_0x_1x_2 \\
&= 0.
\end{aligned}$$

If $a_1 = 1, a_3 = 0$ and $a_4 = 0$, and with $(x_0, x_1, x_2) = (x, y, z)$, this does indeed equal the Hessian we defined for the case $j(E) \neq 0$:

$$xy^2 + x^2y + a_2x^3 + a_6xz^2 + y^2z + xyz + a_2x^2z = 0.$$

A.2 $j(E) = 0$

In the case $j(E) = 0$, we are dealing with an elliptic curve of the form

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

In the alternative notation, this corresponds to the curve $C(A, 0)$, with

$$A = \begin{pmatrix} a_{00} & a_{01} & a_{02} \\ a_{10} & a_{11} & a_{12} \\ a_{20} & a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} 1 & 0 & a_4 \\ 0 & 0 & a_3 \\ 0 & 1 & a_6 \end{pmatrix}.$$

We see that $|A| = a_3$. We use theorem 3.14 to compute the 'Hessian' of this curve:

$$B = \begin{pmatrix} 0 & a_{12} & a_{21} \\ a_{02} & 0 & a_{20} \\ a_{01} & a_{10} & 0 \end{pmatrix} = \begin{pmatrix} 0 & a_3 & 1 \\ a_4 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

$$ABA = \begin{pmatrix} 1 & 0 & a_4 \\ 0 & 0 & a_3 \\ 0 & 1 & a_6 \end{pmatrix} \begin{pmatrix} 0 & a_3 & 1 \\ a_4 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & a_4 \\ 0 & 0 & a_3 \\ 0 & 1 & a_6 \end{pmatrix}$$
$$= \begin{pmatrix} 0 & 1 & a_3^2 + a_6 \\ 0 & 0 & 0 \\ a_4 & 0 & a_4^2 \end{pmatrix}$$

So the Hessian curve, $C(ABA, |A|)$, is given by

$$Z(xy^2 + (a_3^2 + a_6)xz^2 + a_4x^2z + a_4^2z^3 + a_3xyz)$$

or, equivalently,

$$xy^2 + (a_3^2 + a_6)x + a_4x^2 + a_4^2 + a_3xy = 0,$$

which matches our own Hessian.

B MAGMA code

B.1 Verifying a formula in 2.1.2

```
F:=GF(2);
K<a2,a6,t>:=FunctionField(F,3);
P2<X,Y,Z>:=ProjectiveSpace(K,2);
C:=Curve(P2,t*(Y^2*Z+X*Y*Z+X^3+a2*X^2*Z+a6*Z^3)+
    Y^2*Z+X*Y^2+X^2*Y+X*Y*Z+a2*X^3+a2*X^2*Z+a6*X*Z^2);
P:=C![0,1,0];
E,phi:=EllipticCurve(C,P);

PK<x>:=PolynomialRing(K);
I:=ideal<PK | x^4+x^3+a6>;
L<xi>:=PK/I;
PL<y>:=PolynomialRing(L);
J:=ideal<PL | y^2+xi*y+xi^3+a2*xi^2+a6>;
M<eta>:=PL/J;

PM<T>:=PolynomialRing(M);

st:=(t*(eta+xi^2)+eta^2 + eta+a2*xi^2+a6)/(t*xi+xi^2+xi);
Y:=eta+st*(T+xi);
pol:=t*(Y^2+T*Y+T^3+a2*T^2+a6)+
    Y^2+T*Y^2+T^2*Y+T*Y+a2*T^3+a2*T^2+a6*T;
sst:=Coefficient(pol,3);
ppol:=sst*(T+xi)^3;
pol-ppol;
---------

0
```

B.2 Discriminant of G

```
F:=GF(2);
K<a6,j>:=FunctionField(F,2);
PK<t>:=PolynomialRing(K);
pol:= (t+1)^12 + j*a6*(t^3*(t+1)^9 +
    a6*t^2*(t+1)^6 + a6^2*t*(t+1)^3 + a6^3);
Discriminant(pol);
---------

a6^44*j^14
```