university of groningen / faculty of science and engineering / mathematics and applied mathematics

Points of order 3 on elliptic curves in characteristic 3

Bachelor's Project Mathematics

July 2022

Student: W.B.J. Klijn

First supervisor: Prof. dr. J. Top

Second assessor: Dr. P. Kiliçer

Abstract

In this paper we will study points of order 3 on elliptic curves defined over perfect fields of characteristic 3. First, there is a short introduction on elliptic curves and related concepts. After this, we distinguish the two forms elliptic curves over characteristic 3 can have. We then do specific computations for points of order 3 in these forms. Finally, we classify elliptic curves that contain points of order 3 in characteristic 3 by showing that any elliptic curve with a point of order 3 is isomorphic to some curve in a certain family of elliptic curves. These points of order 3 can be K-rational, for which the work has already been done, but they can also be $K(\sqrt{d})$-rational for some quadratic extension $K(\sqrt{d})$ of K.

Contents

1 Introduction

Elliptic curves are objects of great mathematical interest. They have come up in equations that were already being studied a very long time ago, known as Diophantine equations. Only in the 20th century have mathematicians started to develop most of the theory surrounding them. They turns out to be a lot more than just some equation: for example, the set of points on an elliptic curve forms an abelian group. Nowadays, there is very deep theory around elliptic curves that was famously used by Andrew Wiles to prove Fermat's Last Theorem [6]. One of the well-known Millenium Prize Problems also deals with elliptic curves: the Birch and Swinnerton-Dyer conjecture. Besides this, elliptic curves have found plenty of more direct applications as well, mainly within cryptography.

One thing that has been studied extensively with regards to the group law on elliptic curves are points of finite order. Some well-known results, such as the Nagell-Lutz theorem, are about points of finite order. In particular, for points of order 3, lots of work has already been done to make clear which curves have these points in specific characteristics.

For perfect fields with characteristics not equal to 2 and 3, the so-called Hesse pencil of an elliptic curve was used. This produced a family of curves. After this, some Galois theory was used to show that other curves with points of order 3 are part of this family. There are two cases that were ignored during this work, namely characteristics 2 and 3. These two characteristics tend to make computations a lot more complicated. For example, the most well-known form of an elliptic curve, $y^2 = x^3 + ax + b$, assumes the characteristic not being 2 or 3.

The work for characteristic 2 was done a few years ago in another bachelor's thesis. It did not use the Hesse pencil, since the Hessian of a curve in characteristic 2 is 0. Instead, it constructed an alternative pencil that produced a family of curves. Besides this, similar techniques were used. A full summary of other characteristics is given in [1].

One part that remained was the case of characteristic 3. One crucial thing that was used in the other cases was the Weil pairing of the subgroup of points of order 3. This Weil pairing only exists if the characteristic does not divide the order. For points of order 3, this holds for characteristics not equal to 3, but not for characteristic 3 itself. The aim of this paper is to fill in this final gap that exists with characteristic 3.

This was done in part by N. P. Smart and E. J. Westwood in [4]. They assumed one of the coefficients of the elliptic curve to be a square. Because of this, they only found points of order 3 that are inside of $E(K)$. We will be considering the case

where this coefficient can also be non-square. In this case, our point of order 3 does not exist in $E(K)$, but rather in $E(K(\sqrt{d}))$ for some quadratic field extension of K. This will lead us to a general family of elliptic curves that are precisely the ones containing points of order 3, whether they lie in $E(K)$ or in $E(K(\sqrt{d}))$.

2 Elliptic Curves

2.1 Preliminaries on fields

Before we start, we will briefly introduce some properties of fields that will be very useful to understand in the rest of this paper. Thus, we explicitly discuss them here. The reader might be familiar with these already.

Definition 2.1. The **characteristic** of a field K is the smallest $n \in \mathbb{Z}_{>0}$ such that

$$\underbrace{1 + \ldots + 1}_{\text{n terms}} = 0$$

If no such n exists, we say that $\text{char}(K) = 0$.

For fields, it can be proven that this characteristic is always either 0 or a prime p. This definition means that for any $a \in K$ with $\text{char}(K) = p$ with p prime, we have

$$\underbrace{a + \ldots + a}_{\text{p terms}} = a \underbrace{(1 + \ldots + 1)}_{\text{p terms}} = a \cdot 0 = 0$$

Another useful property is that in characteristic p, it holds that for $a, b \in K$, $(a + b)^p = a^p + b^p$. This is because all other terms in the expansion have a multiple of p as their coefficient.

Initially, we will not be working in any particular characteristic as the theory introduced here works for any characteristic. From chapter 4 we will start working in fields of characteristic 3.

We will also be working over perfect fields. This has many equivalent definitions, but the one that will directly apply to us is the following:

Definition 2.2. A field K is perfect if it has characteristic 0, or if it has characteristic $p > 0$ and every element is a pth power. In other words, we can take the pth root of any element in the field, and it will exist within the field.

In practice, many fields are perfect: every characteristic 0 field is, by definition, perfect, and so are all finite fields. In this paper, the general theory of elliptic curves holds for any field, but from section 4.2 we will be working over perfect fields.

Besides these notions, some familiarity will be assumed on what field extensions and Galois groups are.

2.2 Elliptic curves

Elliptic curves are defined over the projective plane. We can think of the projective plane as the Euclidean plane, with an additional "line at infinity", with parallel lines intersecting at some point at infinity, and parallel planes intersecting at this line. In practice, this means that we need to denote coordinates in the projective plane as $[X : Y : Z]$, as opposed to the usual affine, non-projective coordinates (x, y). By setting $Z = 1$, we can find our affine coordinates. Taking $Z = 0$ gives us the points on the line at infinity.

If we multiply every coordinate by the same nonzero constant α, we get $[\alpha X : \alpha Y : \alpha Z]$. In the projective plane, these points are the same.

Definition 2.3. An elliptic curve E is a smooth cubic curve in the projective plane defined over a field K, along with a chosen point $\mathcal{O} \in E$.

Cubic curves are functions in the projective plane over three variables $x, y, z \in K$ that are a linear combination of third degree monomials, such as x^3, x^2z and xyz. Imposing the extra requirement that they be smooth is what makes these cubic curves elliptic curves.

The set $E(K)$ denotes all the K-rational points on the elliptic curve. That is, all the points that satisfy the given equation $E = 0$ with all coordinates in K.

While this is the official definition, it's not very useful to work with. Fortunately, we can write any elliptic curve in the Weierstrass normal form. This allows us to see them in a normalized way. The (affine) Weierstrass form of an elliptic curve E is

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

With x, y variables in K, and a_1, a_2, a_3, a_4, a_6 constant coefficients in K.

We can also view the Weierstrass form in homogeneous coordinates. To do this, we can perform the substitutions $x = X/Z$ and $y = Y/Z$, and multiply the equation by Z^3, to get

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

Any affine points on the curve can be found by setting $Z = 1$. This yields the affine Weierstrass form as seen above. If we set $Z = 0$, we get points on the line at infinity. If you fill this in, it follows that to satisfy the equation, we will need $X = 0$ as well. Hence, the only point at infinity that satisfies the equation is $[0 : 1 : 0]$, with $Y = 1$ chosen for convenience. In the Weierstrass form, we always have our point $\mathcal{O}$ such that $\mathcal{O} = [0 : 1 : 0]$.

With the coefficients of the Weierstrass form, we can define some quantities as-

sociated with them, as also given by Silverman in [2]. These will be useful for computational work that we will be doing later on.

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\ c_4 &= b_2^2 - 24b_4 \\ \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\ j(E) &= \frac{c_4^3}{\Delta} \end{aligned}$$

A notable thing about Δ is that if it is 0, our curve is no longer smooth and hence we no longer have an elliptic curve. Hence, we have that E in Weierstrass form is an elliptic curve if and only if $\Delta \neq 0$. For this reason, we will always need that $\Delta \neq 0$.

An important fact about $j(E)$ is that it is an invariant, commonly named the j-invariant. This means that two isomorphic elliptic curves have the same j-invariant. We will return to the j-invariant later, after we understand what is meant by an isomorphism of elliptic curves.

The important thing to keep in mind is that in affine coordinates, we are ignoring the point $\mathcal{O}$. This is generally not an issue, but if the need comes, we can switch to homogeneous coordinates at any time. However, working in affine coordinates makes computations a lot easier.

3 Group law, elements of order three

3.1 The group law on elliptic curves in Weierstrass form

Rational points on elliptic curves form an additive abelian group. How does this group law work? To start, note that any line through an elliptic curve crosses the elliptic curve in exactly 3 places. This is because our curves are smooth and cubic. There might be a point with higher multiplicity, and it could also be the point at infinity $\mathcal{O}$.

A logical place to start for the group law would thus be that for two points P and Q on the curve E, we take the line through these two points. Then, we take the third point of intersection to be $P + Q$. This third point will always exist, since we have a cubic curve. Unfortunately, this doesn't quite work. It simply will not satisfy the group axioms. Instead, we will call this operation $*$, so this operation on the points P and Q results in $P * Q$. If $P = Q$, we take the tangent line at P, since this line intersects P with a multiplicity of at least 2.

To find the actual group law, we repeat the process, but we now use $P * Q$ and $\mathcal{O}$. Then, by looking at the line through these two points, and taking its third point of intersection, we find the actual point $P + Q$. So, $P + Q = (P * Q) * \mathcal{O}$. Note that in the Weierstrass form, we always have $\mathcal{O} = [0 : 1 : 0]$. Hence, taking the line through a point and $\mathcal{O}$ means that we mirror the point in the x-axis.

The image below gives a graphical intuition of the group law for an elliptic curve over $\mathbb{R}$. While this image would not work so well with, for example, finite fields, the theory still applies.

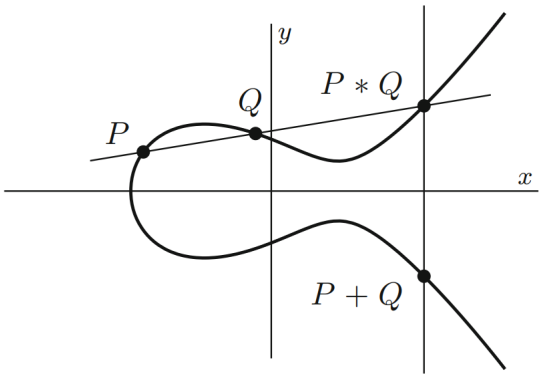

Figure 1: The group law in Weierstrass form [3]

Theorem 3.1. The rule described above is a group law that turns the set of K-rational points on an elliptic curve into an abelian group, with identity element

$\mathcal{O}$.

Proof. We will check the group axioms one by one.

First, it is quite clear that the $*$ operation is commutative. If we take the third point of intersection of a line going through two other points, the order in which we look at these two points is irrelevant. Thus, the $+$ operation is also commutative.

We can indeed show that $\mathcal{O}$ is the identity element. Consider $P + \mathcal{O}$. Whatever point $P * \mathcal{O}$ is, we know that intersecting it again with $\mathcal{O}$ yields P, since the line that we take through $P * \mathcal{O}$ and $\mathcal{O}$ is the same one as the line through P and $\mathcal{O}$. So, we have that $P + \mathcal{O} = (P * \mathcal{O}) * \mathcal{O} = P$.

We can, for any point P, construct its inverse $-P$. To do this, we can consider a point $S = \mathcal{O} * \mathcal{O}$. Then, $-P = P * S$. Indeed: we then find that $P + -P = (P * -P) * \mathcal{O} = S * \mathcal{O} = \mathcal{O}$.

For associativity, it suffices to show that for $P, Q, R \in E(K)$, we have $(P+Q)*R = P*(Q+R)$, because associativity ultimately requires that both of these points have the same result when taking the line through it and $\mathcal{O}$.

From here, it works best to graphically show that this indeed holds. Below is an image that shows how it works. Note that in this picture, Tate and Silverman chose their $\mathcal{O}$ as a point on the affine plane. This is because they explain this group law for general cubics, as opposed to only equations in the Weierstrass form. In our case, the point $\mathcal{O}$ will always be the point at infinity.

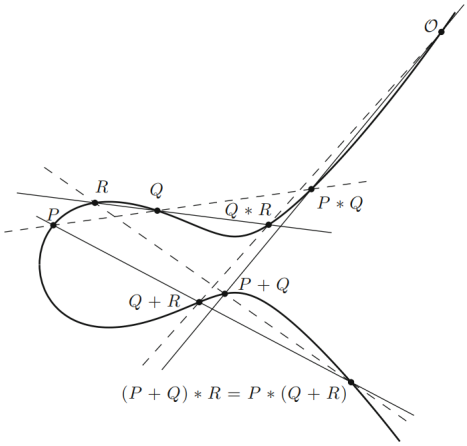

Figure 2: Associativity of the group law [3]

One can work out the details of associativity fully, by, for example, using the formulas for point addition for curves in Weierstrass form, which will be given later. We will not include this in this paper. □

We can make certain changes to the variables x and y to create isomorphisms over K from one curve in Weierstrass form to another. For x, we can set $x = u^2x' + r$ and for y we can set $y = u^3y' + u^2sx + t$ for $u, r, s, t \in K, u \neq 0$. With these changes, we can compute the change of the coefficients in the Weierstrass equation.

One can also compute the value of j for these transformed coordinates as well as the original equation, and turns out that they are always the same. Thus, two isomorphic curves will have the same j-invariant, explaining its name as an invariant.

The converse is not always true, however. Only for algebraically closed fields does this always hold. This is because for any two curves with the same j-invariant, isomorphisms between them can always be found over $\bar{K}$. However, if we have two specific elliptic curves with the same j-invariant, it is always possible to find an isomorphism that is defined over a certain finite and separable extension of K. In general, this extension will be of degree dividing 24.

We have a way to add points in our group. However, it would help to have explicit formulas to do these computations, especially since the visual interpretation does not work that well anymore if we consider elliptic curves of finite fields. Section III.2 of [2] contains explicit formulas for addition, inversion and doubling of points. We will only be interested in the inversion and doubling formulas. Hence, the other formulas are omitted. For an arbitrary point on an elliptic curve $P = (x, y)$, we have

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

$$x([2]P) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6}$$

Here, $x([2]P)$ is the x-coordinate of the point $P + P$. In general, when we write $[n]P$, it means we add P to itself n times.

3.2 Points of order three

Elliptic curves are groups that have points of finite order. We are particularly interested in points of order three. Notice that for points of order 3, we get $[3]P = \mathcal{O}$, or equivalently, $[2]P = -P$. This last expression is easier to deal with since we have clear and explicit duplication and inversion formulas. Also, we do not need to deal with homogeneous coordinates, since we have $Z = 1$ on both sides. If the x-coordinates are matching, that gives us two values of y, because we have $y^2 = f(x)$. Hence, we only really need to consider the x-coordinates.

Something else that we need to introduce that is related to points of order 3 are flex points. Flex points, also known as inflection points, will be useful later on. It allows us to look at points of order 3 in a different way, where we can also make use

of the tangent line of the point.

Definition 3.2. A flex point on an elliptic curve is a point whose tangent line intersects that point, with multiplicity 3 exactly.

In particular, $\mathcal{O}$ is always a flex point, which is of order 1.

Lemma 3.3. A point $P \neq \mathcal{O}$ on an elliptic curve is a flex point if and only if it is of order 3.

Proof. Let P be a flex point. By definition, this means that $P * P = P$. Hence, $P + P = (P * P) * \mathcal{O} = P * \mathcal{O}$. Then, $P + P + P = (P * \mathcal{O}) * P * \mathcal{O}$. We know that $(P * \mathcal{O}) * P = \mathcal{O}$, so $P + P + P = \mathcal{O} * \mathcal{O} = \mathcal{O}$, and thus P is of order 3. This reasoning is the exact same in the opposite direction. □

It follows immediately that if P is a flex point, $-P$ is also a flex point: $-P + -P + -P = -(P + P + P) = \mathcal{O}$.

A final observation to make about flex points is that if P is in some field extension L of K, it remains a flex points under field automorphisms in the Galois group. A field automorphism σ in the Galois group is K-linear, so it always maps 1 to 1, hence for the point $\mathcal{O} = [0 : 1 : 0]$ it is clear that we get $\sigma(\mathcal{O}) = \mathcal{O}$.

For a flex point of order 3, $P = [x : y : 1]$, we find $\sigma(P) = [\sigma(x) : \sigma(y) : 1]$. We thus need to only look at the affine coordinates. Then,

$$\begin{aligned} x([2]\sigma(P)) &= \frac{\sigma(x)^4 - b_4\sigma(x)^2 - 2b_6\sigma(x) - b_8}{4\sigma(x)^3 + b_2\sigma(x)^2 + 2b_4\sigma(x) + b_6} \\ &= \sigma\left(\frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6}\right) \\ &= \sigma(x([2]P)) \\ &= \sigma(x(-P)) \\ &= x(-\sigma(P)) \end{aligned}$$

using the facts that σ acts trivially on the b_i coefficients and that $[2]P = -P$. Thus, because the x-coordinates are matching, $\sigma(P)$ must be a point of order 3, and thus a flex point.

3.3 The m-torsion subgroup

We can also consider the points of order 3 as points of the 3-torsion subgroup of E. This gives us a slightly more theoretical overview, which will tell us what to expect for order 3 points in characteristic 3.

Definition 3.4. For $m \in \mathbb{Z}$, the m-torsion subgroup $E[m]$ of an elliptic curve E is the set of points of order m in E,

$$E[m] = \{P \in E : [m]P = \mathcal{O}\}$$

It is quite clear that this is a subgroup of E. For two points $P, Q \in E[m]$,

$$\underbrace{(P+Q) + \ldots + (P+Q)}_{\text{m times}} = \underbrace{P + \ldots + P}_{\text{m times}} + \underbrace{Q + \ldots + Q}_{\text{m times}} = \mathcal{O} + \mathcal{O} = \mathcal{O}$$

Hence $P + Q \in E[m]$.

If we restrict ourselves to p-torsion groups, that is, m-torsion groups with p a prime number, we can look at one interesting result, adapted from [2].

Theorem 3.5. Let E be an elliptic curve over a field K. Let p be a prime number. Then,

- If $\text{char}(K) \neq p$,
$$E[p] \cong (\mathbb{Z}/p\mathbb{Z}) \oplus (\mathbb{Z}/p\mathbb{Z})$$
- If $\text{char}(K) = p$, we have one of
$$E[p] \cong \{\mathcal{O}\}$$
$$E[p] \cong \mathbb{Z}/p\mathbb{Z}$$

Proving this theorem is beyond the scope of this article. It involves something called the Frobenius morphism and a multiplication-by-p map. The details of this can be found in [2]. A more elementary proof is done by Washington can be found in [5], which involves division polynomials. We are not too concerned about the details of the proof, however.

From this theorem it follows that in the case $p = 3$, for any characteristic but 3, we have $E[3] \cong (\mathbb{Z}/3\mathbb{Z}) \oplus (\mathbb{Z}/3\mathbb{Z})$. Only in characteristic 3 does this not hold, which is the reason this case was ignored in previous works. The techniques used rely on this particular structure of the 3-torsion subgroup. For this reason, we will need to use different methods.

In characteristic 3, we have either $E[3] \cong \{\mathcal{O}\}$ or $E[3] \cong \mathbb{Z}/3\mathbb{Z}$. The set of flex points is exactly equal to $E[3]$, as we showed in section 3.2. This means that either there are no flex points besides $\mathcal{O}$, or we have three flex points, namely $\mathcal{O}, P$ and $-P$, for $P \neq \mathcal{O}$ a flex point. It is good to keep this in mind, as we now know what kinds of order 3 points we can expect on an elliptic curve over characteristic 3, assuming these points exist.

4 Curve over characteristic 3

4.1 The two forms

We will now be shifting our focus to elliptic curves defined over fields of characteristic 3. In characteristic 3 the general Weierstrass form can be reduced to a simpler form. By distinguishing between a zero and a nonzero j-invariant, we are reduced to two cases, as described by Silverman in appendix A of [2].

Theorem 4.1. Let K be a field of characteristic 3, and let E be an elliptic curve defined over K, given in Weierstrass form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Then, we can rewrite the Weierstrass equation as follows:

1. If $j(E) \neq 0$, then we can rewrite to the form $y^2 = x^3 + a_2x^2 + a_6$.
2. If $j(E) = 0$, then we can rewrite to the form $y^2 = x^3 + a_4x + a_6$.

Proof. To start, we can get rid of the a_1 and a_3 terms by completing the square:

$$y^2 + a_1xy + a_3y = \left(y + \frac{a_1x + a_3}{2}\right)^2 - \left(\frac{a_1x + a_3}{2}\right)^2$$

By taking $\tilde{y} = y + \frac{a_1x+a_3}{2}$, rewriting and moving terms to the right side, we can then relabel our coefficients for the quadratic, linear and constant term back to a_2, a_4 and a_6 respectively to get to the form

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

This works regardless of the value of $j(E)$.

With $a_1 = a_3 = 0$, we can compute $j(E)$ in characteristic 3, resulting in $j(E) = \frac{a_2^6}{\Delta}$. Hence, for the case $j(E) = 0$, it instantly follows that $a_2 = 0$ and case 2 is proven.

In the case $j(E) \neq 0$, it then holds that $a_2 \neq 0$. Thus, we can make the substitution $x = x' + \frac{a_4}{a_2}$. Plugging this in, for the linear term this results in $(2a_4 + a_4)x'$, which in characteristic 3 is indeed 0. We finally relabel our constant term to a_6 again. We have then reached our desired form, proving case 1. □

This rewritten form makes computation significantly easier. Regardless of the value of $j(E)$, we have $a_1 = a_3 = 0$. We can also use the fact that in characteristic 3, we have $3 = 0$. This allows us to greatly simplify the quantities that we defined in section 2.2.

For clarity, in characteristic 3 our quantities will become:

$$\begin{aligned} b_2 &= a_2 \\ b_4 &= 2a_4 \\ b_6 &= a_6 \\ b_8 &= a_2a_6 - a_4^2 \\ c_4 &= a_2^2 \\ \Delta &= a_2^2a_4^2 - a_2^3a_6 - a_4^3 \\ j(E) &= \frac{a_2^6}{\Delta} \end{aligned}$$

For any value of $j(E)$, we get for $P = (x, y)$

$$x([2]P) = \frac{x^4 + a_4x^2 + a_6x - a_2a_6 + a_4^2}{x^3 + a_2x^2 + a_4x + a_6}$$

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

With these simplified formulas for doubling and inversion, we can move on to making explicit computations for order 3 points.

4.2 Points of order 3 in characteristic 3

Which types of elliptic curves have points of order 3? The two types of reduced Weierstrass form based on the value of $j(E)$ turn out to exactly answer this question. We will get a little computational to find the solution.

Theorem 4.2. An elliptic curve E over a perfect field of characteristic 3 has a point of order 3 if and only if $j(E) \neq 0$.

Proof. Let us start with case 2, where $j(E) = 0$. Here, we have $a_1 = a_2 = a_3 = 0$. Consider a point $P = (x, y) \in E$. Then, $-P = (x, -y)$. Now, using the duplication formula, we can compute $x([2]P)$.

$$\begin{aligned} x([2]P) &= \frac{x^4 + a_4x^2 + a_6x + a_4^2}{x^3 + a_4x + a_6} \\ &= \frac{x(x^3 + a_4x + a_6)}{x^3 + a_4x + a_6} + \frac{a_4^2}{x^3 + a_4x + a_6} \\ &= x + \frac{a_4^2}{x^3 + a_4x + a_6} \end{aligned}$$

For a point of order 3 we set $-P = [2]P$. Then, for the x-coordinate we must have that $\frac{a_4^2}{x^3+a_4x+a_6} = 0$, and so a_4^2 must be 0. But this would mean $\Delta = 0$ which would mean we don't have an elliptic curve. Thus, a point of order 3 can not exist in case 2.

We can now continue with case 1, where $j(E) \neq 0$. Here, we have $a_1 = a_3 = a_4 = 0$. With a point $P = (x, y) \in E$, we again have $-P = (x, -y)$. On the other hand,

$$x([2]P) = \frac{x^4 + a_6x - a_2a_6}{x^3 + a_4x + a_6}$$

Again, setting the x-coordinates equal, we get

$$\begin{aligned} \frac{x^4 + a_6x - a_2a_6}{x^3 + a_4x + a_6} &= x \\ x^4 + a_6x - a_2a_6 &= x^4 + a_2x^3 + a_6x \\ a_2(x^3 + a_6) &= 0 \end{aligned}$$

Since $a_2 \neq 0$, we must have that $x = -\sqrt[3]{a_6}$. Notice that this is where we make use of the fact that our field is perfect. Then, for our the y-coordinate, we can plug it into our equation, yielding two options:

$$y^2 = (-\sqrt[3]{a_6})^3 + a_2(-\sqrt[3]{a_6})^2 + a_6 = a_2\sqrt[3]{a_6}^2$$

So, the order 3 points are of the form $(-\sqrt[3]{a_6}, \sqrt{a_2}\sqrt[3]{a_6})$ and $(-\sqrt[3]{a_6}, -\sqrt{a_2}\sqrt[3]{a_6})$. □

We need to be careful with our points of order 3. In their paper [4], Smart and Westwood make the assumption that a_2 is a square in K so that their order 3 points are guaranteed to have coordinates in K.

However, we aim to extend the result by dropping this assumption. Thus, if a_2 is not a square, we need to extend our field K by $\sqrt{a_2}$, with P living in $E(K(\sqrt{a_2}))$. When trying to classify elliptic curves with points of order 3, it would be nice to ensure that if a_2 is a square, meaning the extension is trivial, the family of curves reduces exactly to the one given by Smart and Westwood, where the points of order 3 can only be in $E(K)$.

From this proof, we can also say something about the flex points on an elliptic curve. In the case $j(E) = 0$, there is one flex point $\mathcal{O}$. In the case $j(E) \neq 0$, there are three flex points, namely $\mathcal{O}$, P and $-P$, for P one of the points of order 3. This aligns exactly with what we know from theorem 3.5, but we now also know when exactly these cases hold.

5 Classifying curves with points of order 3

5.1 Points only in $E(K)$

The work of Smart and Westwood [4] gives a family for elliptic curves over perfect fields of characteristic 3 that have points of order 3 in $E(K)$:

$$x^3 + y^3 + z^3 = \lambda xyz \tag{1}$$

where $\lambda \in K^\times$. This formula is not in the familiar Weierstrass form. Rather, it is written in something known as the Hessian form. Any curve in Weierstrass form can be written in Hessian form by making appropriate transformations. The group law is the same, but the formulas to compute point doubling and point addition are different.

The reason they use this form is because these computations are more efficient to perform, making them useful in applications in cryptography. However, we are not particularly interested in efficiency, so we will not mind if our result is in the Weierstrass form.

5.2 Extending the result

To generalise the above formula to also include points that might only exist in $E(K(\sqrt{d}))$, it seems logical to expect to find the d that we use for the quadratic extension somewhere in this family. We used a concept called quadratic twist to reach our desired family, but we can introduce it and show that it works after giving the formula. For more details on quadratic twists, see [2].

Theorem 5.1. Let K be a perfect field with $\mathrm{char}(K) = 3$. Let $d \in K^\times$. Let E be an elliptic curve over K containing a point $P = (a, b) \in E$ of order 3. We define $K(\sqrt{d}) = K(a, b)$. Then E is isomorphic as an elliptic curve over K to a curve in E_λ, where E_λ is the family of elliptic curves given by

$$y^2 = x^3 + d\lambda^2 x^2 - d^3\lambda^3$$

for $\lambda \in K^\times$.

Notice that we specifically said $P \in E$. This is because it is not yet clear whether P lies in $E(K)$, or in $E(K(\sqrt{d}))$. We do know it satisfies the equation.

Doing the computations of the order 3 points on this particular form, as done in section 4.2, we can find that for points of order 3, the x coordinate is $-\sqrt[3]{a_6}$, hence we get $x = d\lambda$. Plugging this into the equation, we find that the y coordinates are

$d\lambda^2\sqrt{d}$ and $-d\lambda^2\sqrt{d}$. So, the coordinates of the points of order 3 are $(d\lambda, d\lambda^2\sqrt{d})$ and $(d\lambda, -d\lambda^2\sqrt{d})$.

This gives us quite a specific form that order 3 points can be in within our family. For instance, the x-coordinate of our point has to always exist in K. Only the y-coordinate is allowed to exist in $K(\sqrt{d})$.

It now becomes rather easy to find a curve with a particular order 3 point that one might want, provided it exists. Choose the point you want to be of order 3, then check if it has to extend your field or not. Doing this, you quickly find what value d is supposed to have. After this, the x coordinate forces a value of λ, providing our curve in the family.

Example 5.2. Consider $K = \mathbb{F}_3$ and $P = (2, 2\sqrt{2})$. Then, $K(a, b) = K(2, 2\sqrt{2}) = K(\sqrt{2})$. Thus, we find $d = 2$. Then, the x-coordinate tells us that $\lambda = 1$. So, the curve in E_λ that contains this point as a point of order 3 is the curve

$$y^2 = x^3 + 2x^2 + 1$$

With the points of order 3 being $(2, 2\sqrt{2})$ and $(2, \sqrt{2})$.

Example 5.3. If our extension is trivial (and so $d = 1$), with our point of order 3 existing in $E(K)$, our value of λ will correspond to the value of λ according to the form found by Smart and Westwood, equation (1).

By making the appropriate transformations as outlined in their paper, one finds that, for example, choosing the point of order 3 as $(2, 2)$ in the field $\mathbb{F}_3$ yields $\lambda = 2$. We can easily verify that taking $d = 1$ and $\lambda = 2$ in our family also yields $(2, 2)$ as a point of order 3, and hence we can create an isomorphism between the curves $x^3 + y^3 + z^3 = 2xyx$ and $y^2 = x^3 + x^2 + 1$.

After this discussion, we still need to prove the theorem.

Proof of Theorem 5.1. Let E be the elliptic curve with $P = (a, b)$ the point of order 3. We can write E in Weierstrass form

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

Note that though we have a point of order 3, and hence $j(E) \neq 0$, we will not get rid of the linear term, because this depends on a translation of x, restricting our freedom to translate x later on.

We know that P being a point of order 3 is equivalent to saying P is a flex point. Let us for now assume that $P \in E(K(\sqrt{d}))$, $P \notin E(K)$. We can take the non-trivial automorphism $\sigma \in \mathrm{Gal}(K(\sqrt{d})/K)$ with $\sigma(1) = 1$ and $\sigma(\sqrt{d}) = -\sqrt{d}$. As discussed

earlier, flex points are preserved under automorphisms in the Galois group, and hence we can conclude that $\sigma(P) = (\sigma(a), \sigma(b))$ is also a flex point.

In particular, since σ is non-trivial, $\sigma(P) \neq P$, and also $\sigma(P) \neq \mathcal{O}$. The only other flex point on the curve is $-P$, as we know from Theorem 3.5. Hence, $\sigma(P) = -P = (a, -b)$. This in turn implies that $\sigma(a) = a$ and $\sigma(b) = -b$. Thus, $a \in K$ and $b \in K(\sqrt{d})$ with $b = c\sqrt{d}$ for some $c \in K$. So, our point P is of the form $(a, c\sqrt{d})$.

This form $P = (a, c\sqrt{d})$ also holds in the case $P \in E(K)$. However, then we simply have $d = 1$ and $c = b$. So we no longer need to work with the assumption made above. This was only done to find out what P looks like.

We now make the translation $x = \bar{x} + a$. This will shift our flex point P to the coordinates $(0, c\sqrt{d})$. Plugging this into our equation, we find $c^2 d = a_6$. Thus, we get

$$y^2 = \bar{x}^3 + a_2\bar{x}^2 + a_4\bar{x} + c^2 d$$

Keep in mind that the a_2 and a_4 are not exactly the same as above due to the translation in x, but we can simply relabel them again without any issues. We also keep the name P in use, though this point will be expressed in different coordinates as we make changes to the variables.

We are yet to make use of the fact that P is a flex point. The tangent line l through P is of the form $y = rx + c\sqrt{d}$, with r not yet known. We can easily compute r, however:

$$r = \frac{dy}{d\bar{x}}\Big|_{(0,c\sqrt{d})} = \frac{2a_2\bar{x} + a_4}{2y}\Big|_{(0,c\sqrt{d})} = \frac{a_4}{2c\sqrt{d}}$$

Using this r, and putting l into our equation E, we get

$$\left(\frac{a_4}{2c\sqrt{d}}\bar{x} + c\sqrt{d}\right)^2 - \bar{x}^3 - a_2\bar{x}^2 - a_4\bar{x} - c^2 d = 0$$

$$\frac{a_4^2}{c^2 d}\bar{x}^2 + a_4\bar{x} + c^2 d - \bar{x}^3 - a_2\bar{x}^2 - a_4\bar{x} - c^2 d = 0$$

This equation is supposed to have solution $\bar{x} = 0$ with multiplicity 3. So, we want to get the quadratic, linear and constant terms to 0. We can see that the constant term and the linear term are already equal to 0, which is unsurprising, since this is exactly how l was constructed. For the quadratic term, we find that we need $a_2 = \frac{a_4^2}{c^2 d}$, so we can now plug that into the equation.

We now have the equation

$$y^2 = \bar{x}^3 + \frac{a_4^2}{c^2 d}\bar{x}^2 + a_4\bar{x} + c^2 d$$

If we now multiply both sides by $\frac{a_4^{12}}{c^{18}d^6}$, and we make the substitutions $\tilde{y} = \frac{a_4^6}{c^9 d^3} y$ and $\tilde{x} = \frac{a_4^4}{c^6 d^2}\bar{x}$, we get

$$\tilde{y}^2 = \tilde{x}^3 + \frac{a_4^6}{c^8 d^3}\tilde{x}^2 + \frac{a_4^9}{c^{12}d^4}\tilde{x} + \frac{a_4^{12}}{c^{16}d^5}$$

Rewriting this gives us

$$\tilde{y}^2 = \tilde{x}^3 + d\left(-\frac{a_4^3}{c^4 d^2}\right)^2 \tilde{x}^2 - d^2\left(-\frac{a_4^3}{c^4 d^2}\right)^3 \tilde{x} + d^3\left(-\frac{a_4^3}{c^4 d^2}\right)^4$$

We then make the substitution $\lambda = -\frac{a_4^3}{c^4 d^2}$ to find

$$\tilde{y}^2 = \tilde{x}^3 + d\lambda^2\tilde{x}^2 - d^2\lambda^3\tilde{x} + d^3\lambda^4$$

Finally, by making the substitution $\xi = \tilde{x} + d\lambda$, we reach our desired form

$$\tilde{y}^2 = \xi^3 + d\lambda^2\xi^2 - d^3\lambda^3$$

□

While the final part of the above proof works, it is perhaps not very enlightening or satisfying. It gives an isomorphism that is not at all obvious to find. We can also approach it from a different angle that uses some more general theory to show an isomorphism exists, instead of explicitly computing it.

Alternate proof of theorem 5.1. For the first part, we do the same procedure as above, taking the tangent line of our point P, until we again reach the curve that we will call E, of the form

$$E : y^2 = x^3 + \frac{a_4^2}{c^2 d}x^2 + a_4 x + c^2 d$$

that we would like to show is isomorphic over K to the curve that we will call F, of the form

$$F : y^2 = x^3 + d\lambda^2 x^2 - d^3\lambda^3$$

We know that if two curves have the same j-invariant, they are isomorphic over the algebraic closure of K. As we discussed in section 3.1, two curves with the same j-invariant are isomorphic over a separable extension of degree dividing 24. We can do more than this, however. An equivalent definition for a perfect field is that every extension is separable, so any extension we make will be separable. Furthermore, if the j-invariant is not 0 or 1728, the extension is of degree 2. In characteristic 3,

1728 is the same as 0, and since we know that $j(E) \neq 0$, this is the case that holds for us.

Thus, if we can set the j-invariant of E and F to be the same, we know that E and F are isomorphic over some quadratic extension of K. Let us call this extension $K(\sqrt{e})$ with e a non-square element of K.

Computing the j-invariants, we find $j(E) = -\frac{a_4^9}{c^{12}d^6}$ and $j(F) = \lambda^3$. So, we can set $\lambda = -\frac{a_4^3}{c^4d^2}$ to set the j-invariants equal. Then, if we write $E : y^2 = f(x)$, for $f(x)$ being a third degree polynomial in x, we can write $F : ey^2 = f(x)$, with an isomorphism being defined over $K(\sqrt{e})$.

However, we also know that both on E and F, the coordinates of the point of order 3, $P = (a, b)$, generate exactly $K(\sqrt{d})$. But on F, the point P has $\sqrt{e}$ in its y-coordinate. Indeed, we get $ey^2 = f(a)$, meaning $b = \pm\frac{\sqrt{f(a)}}{\sqrt{e}}$. So, that would make P generate $K(\sqrt{de})$. Thus, $K(\sqrt{de}) = K(\sqrt{d})$, which implies $K(\sqrt{e}) = K$. Thus, the isomorphism from above is already defined over K. This implies that these two curves are isomorphic, finishing the proof. $\square$

6 Conclusion

With the results of this thesis, we have closed the final gap in the work to classify elliptic curves with points of order 3 defined over perfect fields of any characteristic. The method used is a little more explicit and computational than other works, due to the methods used in other characteristics not working in characteristic 3.

First, we introduced basic concepts about elliptic curves and their group law in Weierstrass form, along with related quantities that help us explicitly compute addition of points on elliptic curves. We then discussed some things about points that are specifically of order 3, discussing flex points and the 3-torsion subgroup.

Next, we started looking at curves over perfect fields of characteristic 3. Here, we were able to distinguish these curves to two different types, depending on the value of the j-invariant. This allowed us to explicitly determine the case where curves do have points of order 3.

Finally, we discussed the family of elliptic curves with points of order 3 that have coordinates that may lie inside of our field K, but that may also lie in a quadratic extension $K(\sqrt{d})$ for a non-square element $d \in K$. If this extension is trivial, the family reduces exactly to the family of curves given by Smart and Westwood in [4]. We showed that any elliptic curve over characteristic 3 that has points of order 3 has an isomorphism over K to some curve in this family.

References

[1] Ane S.I. Anema, Jaap Top, and Anne Tuijp. Hesse pencils and 3-torsion structures. *SIGMA*, 14:102–114, 2018.

[2] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer New York, 2nd edition, 2009.

[3] Joseph H. Silverman and John T. Tate. *Rational Points on Elliptic Curves*. Springer Cham, 2nd edition, 2015.

[4] N. P. Smart and E. J. Westwood. Point multiplication on ordinary elliptic curves over fields of characteristic three. *AAECC*, 14:485–497, 2003.

[5] Lawrence C. Washington. *Elliptic Curves: Number Theory and Cryptography*. Chapman & Hall/CRC, 2nd edition, 2008.

[6] Andrew Wiles. Modular elliptic curves and fermat's last theorem. *Annals of Mathematics*, 141:443–551, 1995.