rijksuniversiteit groningen

faculteit Wiskunde en Natuurwetenschappen

Edwards Elliptic Curves

Bachelor Thesis Mathematics

August 2012

Student: M.R. Dam

First supervisor: Prof.dr. J. Top

Second supervisor: Prof.dr. H.L. Trentelman

Abstract

Due to its complete addition law, the Edwards form for elliptic curves is in some applications a more convenient form than the well-known Weierstrass form. In this thesis, the difference between both forms is described and special properties of the Edwards curves are treated. A rational map between both forms is constructed in order to show Edwards curves are birationally equivalent to Weierstrass curves if and only if the Weierstrass curve has a point of order 4. Using this map, it can be shown that an Edwards curve is supersingular if and only if the corresponding Legendre form is supersingular.

Contents

Chapter 1

Introduction

An elliptic curve is a curve that can be written in the Weierstrass form. It is also naturally a group with a special addition defined on it. Recently H.M. Edwards introduced a new form to represent a class of elliptic curves, called the *Edwards curves*. Elliptic curves are often used in cryptography, and this is where Edwards elliptic curves have their advantages: addition, doubling and tripling can be done faster on Edwards curves than on curves given by a Weierstrass equation. This is because the addition law on Edwards curves does not have exceptions, while the addition on Weierstrass curves distinguishes several special cases.

This thesis will focus on Edwards curves, the group law and special cases for which an Edwards curve has special properties, in particular when an Edwards curve is supersingular. Although the main goal is to understand Edwards curves, the Weierstrass form will always be close for comparison.

The second chapter treats the basics of elliptic curves in Weierstrass form. In the third chapter, Edwards curves and the addition on them will be introduced. The goal of the fourth chapter is to find the relation between Weierstrass and Edwards curves. The fifth chapter treats supersingular Edwards curves.

Chapter 2

Elliptic curves

2.1 Definition

For elliptic curves, different definitions are given in different books. To prevent having to treat all theory behind elliptic curves, this thesis will use the following definition of elliptic curves:

Definition 2.1. An elliptic curve over a field K is a non-singular curve which can be written in Weierstrass form[1]:

$$v^2 + a_1uv + a_3v = u^3 + a_2u^2 + a_4u + a_6 \tag{2.1}$$

where $a_1, a_2, a_3, a_4, a_6 \in K$.

If *char(K)* is not 2, the Weierstrass equation can be simplified to:

$$E : v^2 = u^3 + au^2 + bu + c \tag{2.2}$$

where $a, b, c \in K$. This is done by replacing $\tilde{v} = v + \frac{1}{2}u + \frac{1}{2}a_3$.

Curves of the form 2.2 will be called *Weierstrass curves* from here on, or just elliptic curves when there is no confusion whether a Weierstrass or an Edwards curve is meant. Also, a curve will always denote an elliptic curve, unless explicitly stated otherwise.

For a curve to be non-singular, it is necessary and sufficient that the *discriminant* D of a curve is nonzero. Recall that the discriminant is a function of its coefficients that gives information about its roots. For a curve of the form (2.2), the discriminant is given by $D = 16(a^2b^2 - 4b^3 - 4a^3c + 18abc - 27c^2)$. If the discriminant is zero, then the curve has a node or a cusp, so it has a singularity.

Another important quantity of an elliptic curve is the *j-invariant*. This is an invariant of the isomorphism class of the curve: two curves are isomorphic

[1]More generally, a curve is an elliptic curve if it is birationally equivalent to an elliptic curve in Weierstrass form. However, since birational equivalence will be introduced in chapter 4, until then an elliptic curve is assumed to have the Weierstrass form.

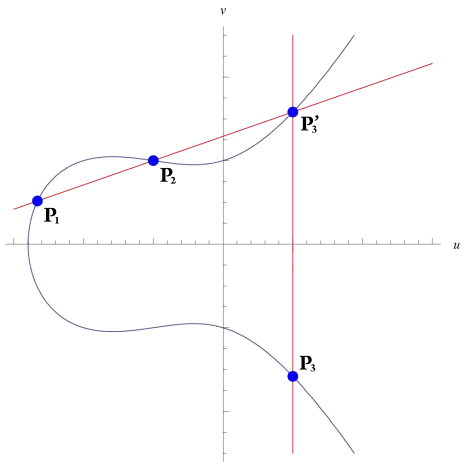

Figure 2.1: Addition of two points on a Weierstrass curve: $P_1 + P_2 = P_3$.

if and only if they have the same j-invariant. For the curve of 2.2, the j-invariant is $j = (16a^2 - 48b)^3/D$, where D is the discriminant.

To a Weierstrass curve also belongs a point O at infinity. The purpose of this point will be explained in the next section. The set $E(K)$ denotes all points (u, v) with $u, v \in K$ that satisfy the equation of the elliptic curve E, together with the point O. So, when E is written as in (2.2):

$$E(K) = \{(u, v) : u, v \in K \text{ and } v^2 = u^3 + au^2 + bu + c\} \cup \{O\}.$$

The set $E(K)$ is a subgroup of E. The elliptic curve E is said to be *defined over* K, written E/K, if E is defined over K as a curve and $O \in E(K)$.

2.2 The group law on Weierstrass curves

Elliptic curves are naturally an abelian group, since there can be a group law defined on it. This is defined geometrically. The idea is that any straight line through two points on a cubic curve intersects the curve in a third point.

A point P on a Weierstrass curve E is represented by $P = (u, v)$, and $-P = (u, -v)$. Now, choose two points on E, say $P_1 = (u_1, v_1)$ and $P_2 = (u_2, v_2)$. Addition of P_1 and P_2 with $P_1 \neq P_2$ and $P_1 \neq -P_2$, on a curve is done by connecting those points by a straight line. This line will intersect the curve at another point P_3'. Drawing the vertical line through P_3' gives another intersection with the curve, P_3. See figure 2.1. This point is *the sum of* P_1 *and* P_2 *on* E, denoted by $P_1 + P_2$, the special meaning of $+$ here being understood.

Some modifications in this method are needed when $P_1 = P_2$ or $P_1 = -P_2$. In the first case, $P_1 = P_2$, assume for now that the tangent line is

not vertical. Then addition can be seen as adding a point P_2 to P_1 which lies infinitely close to P_1 itself. This means that the tangent line is drawn through P_1, which will again intersect the curve E in a point P_3'. Then the vertical line through P_3' can be drawn. The new intersection with this line and E is the point $2P_1$.

The only remaining case is the case where $P_1 = -P_2$ or the tangent line is vertical. The tangent line now does not seem to intersect E in a third point. Hence, it is defined as the point O. So, O is a point at infinity, but it is defined to be a point at infinity *on every vertical line*. It is the *direction* of all vertical lines of $\mathbb{P}^2$, the projective plane[2].

Recall that for a group law, the properties of the following definition need to hold.

Definition 2.2. A group is a triple $(E, +, O)$, where E is a set, $O \in E$, and $+ : E \times E \longrightarrow E$ such that $(P, Q) \longmapsto P + Q$, for which:

1. $P + O = O + P = P$ for all $P \in E$
2. $P + -P = O$ for all $P \in E$
3. $P + (Q + R) = (P + Q) + R$ for all $P, Q, R \in E$

The group is an *abelian group* if in addition the following holds:

4. $P + Q = Q + P$ for all $P, Q \in E$.

For the addition law on Weierstrass curves, all properties are easy to check, except the third one. This associative law can be checked with a long computation of the formulas for this addition. Then it follows that a Weierstrass curve with the above described group law defines an abelian group on E with O as its identity element.

2.2.1 Formulas for addition

As seen in the previous chapter, addition is defined geometrically. It is shown how to draw the sum of two point on an elliptic curve E. It is useful to represent this addition in formulas, so the sum can be calculated explicitly. The following algorithm gives the formulas for addition on a Weierstrass curve:

Group law algorithm 2.3. *Let E be a curve given by*

$$E : v^2 = u^3 + au^2 + bu + c.$$

- *Let $P_0 = (u_0, v_0) \in E$, then $-P_0 = (u_0, -v_0)$.*

Now, let $P_1 + P_2 = P_3$ with $P_i = (u_i, v_i) \in E$ for $i = 1, 2, 3$.

[2] An explanation of $\mathbb{P}^2$ can be found in appendix A.

- *If* $u_1 = u_2$ *and* $v_1 + v_2 = 0$, *then* $P_1 + P_2 = O$.
- *Otherwise:*

  If $u_1 \neq u_2$, *let*

  $$\lambda = \frac{v_2 - v_1}{u_2 - u_1} \qquad \nu = \frac{v_1 u_2 - v_2 u_1}{u_2 - u_1}$$

  If $u_1 = u_2$ *(but* $v_1 \neq -v_2$*), let*

  $$\lambda = \frac{3u_1^2 + 2au_1 + b}{2v_1} \qquad \nu = \frac{-u_1^3 + bu_1 + 2c}{2v_1}$$

  Then $P_3 = P_1 + P_2$, *with* $P_3 = (u_3, v_3)$ *is given by:*

  $$\begin{aligned} u_3 &= \lambda^2 - a - u_1 - u_2 \\ v_3 &= -\lambda u_3 - \nu. \end{aligned}$$

Chapter 3

Edwards curves

In 2007, Harold M. Edwards introduced a new form for elliptic curves over fields of characteristic $\neq 2$ (see [Edw07]), and showed that this form simplifies formulas for curves, especially the addition law. He proved that every elliptic curve over a field K, if K is algebraically closed (i.e. it contains a root for every non-constant polynomial in $K[x]$), can be expressed as:

$$x^2 + y^2 = c^2(1 + x^2y^2).$$

However, over a finite field, there are only a few curves that can be expressed in this form.

These curves were then studied by Daniel J. Bernstein and Tanja Lange. They found that for finite fields there are considerably more elliptic curves when curves of the following form are used:

$$x^2 + y^2 = c^2(1 + dx^2y^2).$$

Then, they proved that all curves of that form are isomorphic to curves of the form(see [BL07]):

$$x^2 + y^2 = 1 + dx^2y^2. \tag{3.1}$$

Curves of this form are called *Edwards curves*. The addition law Edwards introduced for his form is adapted to suit this form. In this chapter, the Edwards curve will be introduced. The definition, addition law and some special properties are studied.

3.1 Definition

Definition 3.1. An Edwards curve over K, with *char(K)* $\neq 2$ is a curve given by:

$$x^2 + y^2 = 1 + dx^2y^2 \tag{3.2}$$

where $d \in K\backslash\{0, 1\}$.

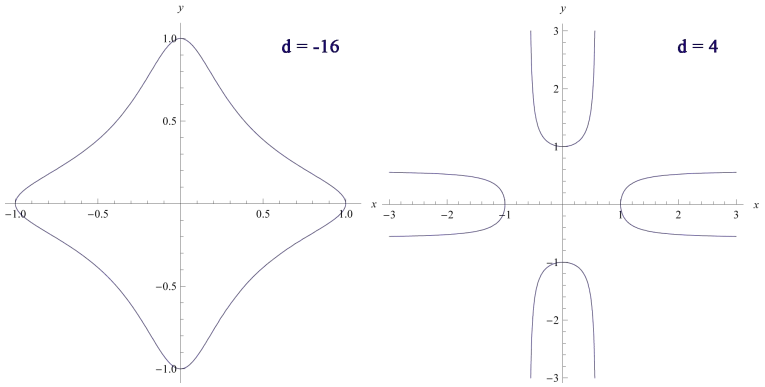

Figure 3.1: Edwards curves for $d = -16$ and $d = 4$.

Figure 3.1 shows two examples of Edwards curves over $\mathbb{R}$ for $d = -16$ and $d = 4$. If $d = 0$, equation 3.2 describes the unit circle, and for $d = 1$ it describes four lines at $x = \pm 1$ and $y = \pm 1$. In both cases, it is not an elliptic curve (see also remark 4.2).

3.2 The group law on Edwards curves

On Edwards curves also an addition law can be defined, but this differs from the law on Weierstrass curves. This addition law also can be interpreted geometrically. To do this, look at the unit circle and add angles on it as if it were a clock. Then, the identity element is $(0, 1)$ (while usually on a unit circle, one starts in $(1, 0)$), so use $x_i = \sin(\alpha_i), y_1 = \cos(\alpha_i)$. With the regular addition of angles on a circle it follows:

$$\begin{aligned} x_3 &= \sin(\alpha_1 + \alpha_2) \\ &= \sin(\alpha_1)\cos(\alpha_2) + \cos(\alpha_1)\sin(\alpha_2) \\ &= x_1 y_2 + x_2 y_1 \end{aligned}$$

$$\begin{aligned} y_3 &= \cos(\alpha_1 + \alpha_2) \\ &= \cos(\alpha_1)\cos(\alpha_2) + \sin(\alpha_1)\sin(\alpha_2) \\ &= y_1 y_2 - x_1 x_2 \end{aligned}$$

This is illustrated in figure 3.2. This does define a group, called the *clock group*, but the unit circle is not an elliptic curve. Hence, a term dx^2y^2 is added. This makes it elliptic, as will be shown in chapter 4 (remark 4.2).

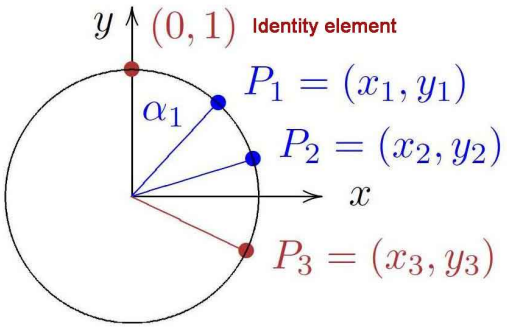

Figure 3.2: Addition on a clock, $P_1 + P_2 = P_3$.

3.2.1 A formula for addition

As introduced in the previous section, when $dx_1x_2y_1y_2 \neq \pm 1$, the group law on Edwards curves is given in the next algorithm:

Group law algorithm 3.2. *Let E_d be an Edwards curve given by:*

$$E_d : x^2 + y^2 = 1 + dx^2y^2$$

Let $P_0 = (x_0, y_0) \in E_d$, then $-P_0 = (-x_0, y_0)$. Now, let $P_1 + P_2 = P_3$ with $P_i = (x_i, y_i) \in E_d$ for $i = 1, 2, 3$. Then:

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3) = \Big(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}\Big).$$

Here, the point $(0, 1)$ is the identity element and $-(x_1, y_1) = (-x_1, y_1)$, note that this differs from the identity element and inverse of the Weierstrass form. For all (x_1, y_1) and (x_2, y_2) in $E_d(K)$, this law is complete and strongly unified when $dx_1x_2y_1y_2 \neq \pm 1$: the denominators are never zero and it has no exceptions for doublings, inverses, etc. whereas the addition on the Weierstrass form distinguished four different cases. For example, doubling a point on an Edwards curve is given simply by:

$$2(x_1, y_1) = \Big(\frac{2x_1y_1}{1 + dx_1^2y_1^2}, \frac{y_1^2 - x_1^2}{1 - dx_1^2y_1^2}\Big).$$

To see that this addition law indeed defines a group law, one has to check that the sum of any two points is a point that lies on the curve itself:

Theorem 3.3. *Let K be a field with char(K)$\neq 2$ and let $d \in K\backslash\{0, 1\}$. Let x_1, y_1, x_2, y_2 be elements of K such that $x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$ and $x_2^2 + y_2^2 = 1 + dx_2^2y_2^2$. Assume $dx_1x_2y_1y_2 \notin \{-1, 1\}$ Define $x_3 = (x_1y_2 + x_2y_1)/(1 + dx_1x_2y_1y_2), y_3 = (y_1y_2 - x_1x_2)/(1 - dx_1x_2y_1y_2)$. Then $x_3^2 + y_3^2 = 1 + dx_3^2y_3^2$.*

Proof. Define a polynomial $T = (x_1y_2 + y_1x_2)^2(1 - dx_1x_2y_1y_2)^2 + (y_1y_2 - x_1x_2)^2(1 + dx_1x_2y_1y_2)^2 - d(x_1y_2 + y_1x_2)^2(y_1y_2 - x_1x_2)^2$, which equals:

$$T = (x_1^2 + y_1^2 - (x_2^2 + y_2^2)dx_1^2y_1^2)(x_2^2 + y_2^2 - (x_1^2 + y_1^2)dx_2^2y_2^2).$$

Now, use the hypotheses for (x_1, y_1) and (x_2, y_2). Subtract $(x_2^2+y_2^2)dx_1^2y_1^2 = (1 + dx_2^2y_2^2)dx_1^2y_1^2$ from $x_1^2 + y_1^2 = 1 + dx_1^2y_1^2$ to see that

$$x_1^2 + y_1^2 - (x_2^2 + y_2^2)dx_1^2y_1^2 = 1 - d^2x_1^2y_1^2x_2^2y_2^2.$$

Similarly,

$$x_2^2 + y_2^2 - (x_1^2 + y_1^2)dx_2^2y_2^2 = 1 - d^2x_1^2y_1^2x_2^2y_2^2.$$

Hence, $T = 1 - d^2x_1^2x_2^2y_1^2y_2^2$.

Now the addition law is used: (x_3, y_3) is expressed in terms of x_1, y_1, x_2 and y_2. It gives:

$$\begin{aligned} x_3^2 + y_3^2 - dx_3^2y_3^2 &= \frac{(x_1y_2 + x_2y_1)^2}{(1 + dx_1x_2y_1y_2)^2} + \frac{(y_1y_2 - x_1x_2)^2}{(1 - dx_1x_2y_1y_2)^2} \\ &\quad - \frac{d(x_1y_2 + x_2y_1)^2(y_1y_2 - x_1x_2)^2}{(1 + dx_1x_2y_1y_2)^2(1 - dx_1x_2y_1y_2)^2} \\ &= \frac{T}{(1 + dx_1x_2y_1y_2)^2(1 - dx_1x_2y_1y_2)^2} \\ &= \frac{T}{1 - d^2x_1^2x_2^2y_1^2y_2^2} = 1. \end{aligned}$$

Thus it follows that $x_3^2 + y_3^2 = 1 + dx_3^2y_3^2$. □

Also, the properties of a group law (see definition 2.2) need to hold, but these properties can easily be verified.

As said, the group law is complete when $dx_1x_2y_1y_2 \neq \pm 1$. This is the case when d is not a square in K, as stated in the next theorem:

Theorem 3.4. *Let E_d be an Edwards curve over a field K with char(K)$\neq 2$, with the corresponding addition law. Then, the addition law is complete if d is not a square in K.*

Proof. Let (x_1, y_1) and (x_2, y_2) be on the curve, i.e.: $x_i^2 + y_i^2 = 1 + dx_i^2y_i^2$ for $i = 1, 2$. Define $\epsilon = dx_1x_2y_1y_2$ and suppose $\epsilon \in \{-1, 1\}$. Then $x_1, x_2, y_1, y_2 \neq 0$ and

$$\begin{aligned} dx_1^2y_1^2(x_2^2 + y_2^2) &= dx_1^2y_1^2(1 + dx_2^2y_2^2) \\ &= dx_1^2y_1^2 + d^2x_1^2y_1^2x_2^2y_2^2 \\ &= dx_1^2y_1^2 + \epsilon^2 \\ &= 1 + dx_1^2y_1^2 \qquad \text{because } \epsilon = \pm 1 \\ &= x_1^2 + y_1^2 \end{aligned}$$

Thus, it follows: $(*)$ $dx_1^2y_1^2(x_2^2+y_2^2) = x_1^2+y_1^2$. Now,

$$\begin{aligned}(x_1+\epsilon y_1)^2 &= x_1^2+y_1^2+2\epsilon x_1y_1\\ &= dx_1^2y_1^2(x_2^2+y_2^2)+2x_1y_1dx_1y_1x_2y_2 \quad \text{using } (*)\\ &= dx_1^2y_1^2(x_2^2+2x_2y_2+y_2^2)\\ &= dx_1^2y_1^2(x_2+y_2)^2\end{aligned}$$

Now it can be seen:

- If $x_2+y_2 \neq 0$ then it follows: $d = ((x_1+\epsilon y_1)/x_1y_1(x_2+y_2))^2$, so d is a square in K.
- Likewise, if $x_2-y_2 \neq 0$ then $d = ((x_1-\epsilon y_1)/x_1y_1(x_2-y_2))^2$, and again d is a square in K.
- If $x_2+y_2 = 0$ and $x_2-y_2 = 0$, then it follows that $x_2 = y_2 = 0$, but this is a contradiction to the assumption that $\epsilon \in \{-1,1\}$.

This proves that $\epsilon = dx_1x_2y_1y_2 = \pm 1$ implies that d is a square. So, the denominators are never zero if d is not a square in K and hence the addition law is complete. □

So, an Edwards curve together with the group law algorithm (3.2) defines an abelian group when d is not a square in K.

3.3 Four special points

Looking at the equation of an Edwards curve, it is seen that it is symmetric in the sense that the roles of x and y can be interchanged. If one has a solution (x,y), it will follow that $(\pm x, \pm y)$ and $(\pm y, \pm x)$ are solutions as well. Four solutions of the equation are easily found to be $(0,1)$, $(0,-1)$, $(1,0)$ and $(-1,0)$. With these four points, a D_4-group of automorphisms can be made, given by:

$$S : P \longmapsto \pm P + Q, \text{ where } Q \in \{(0,1),(0,-1),(1,0),(-1,0)\}.$$

This group consists of reflections in the lines through $(0,0)$ and the points of Q and the lines $x=y$ and $x=-y$, and rotations over an angle of $\frac{k\pi}{2}$ for $0 \leq k < 4$. So, D_4 consists of 8 elements.

The operations of S can be seen as the two operations changing the roles of x and y & changing the signs of x and/or y. The eight outcomes for $S(x,y)$ are:

- $(x,y)+(0,1) = (x,y)$ and $(-x,y)+(0,1) = (-x,y)$
- $(x,y)+(0,-1) = (-x,-y)$ and $(-x,y)+(0,-1) = (x,-y)$

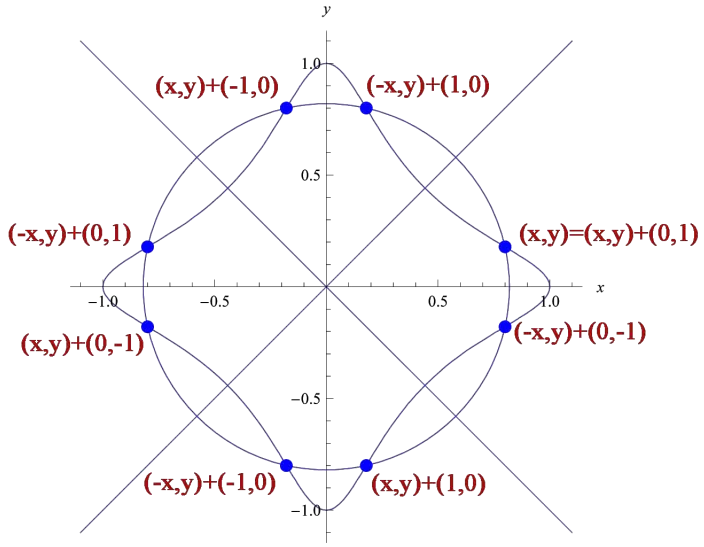

Figure 3.3: The Edwards curve for $d = -16$ with the 8 points resulting from rotation of (x, y) over an angle of $\frac{k\pi}{2}$ for $0 \leq k < 4$ and reflections of (x, y) in the $y-$ and $x-$axis and the lines $y = x$, $y = -x$.

- $(x, y) + (1, 0) = (y, -x)$ and $(-x, y) + (1, 0) = (y, x)$
- $(x, y) + (-1, 0) = (-y, x)$ and $(-x, y) + (-1, 0) = (-y, -x)$

See also figure 3.3, where all the points are drawn. So S consists of reflections in the lines through $(0, 0)$ and the points of Q and the lines $x = y$ and $x = -y$, and rotations over an angle of $\frac{k\pi}{2}$ for $0 \leq k < 4$, hence it is a D_4-group of automorphisms.

In the previous chapter, $(0, 1)$ was said to be the identity element with the addition law 3.2. However, one can choose any of the four points of Q as identity element. By adding the new identity element to each point on the curve, the addition law will change slightly, but the curve is an abelian group again.

In particular, the points

$$\{(0, 1), (0, -1), (1, 0), (-1, 0)\} \subset \{\text{Edwards curve}\}$$

form a cyclic group of order 4, the generator of the group being $(-1, 0)$ or $(1, 0)$. This is shown for $(1, 0)$, but works the same way for $(-1, 0)$:

$$\begin{aligned} 2(1,0) = (1,0) + (1,0) &= (0,-1) \\ 3(1,0) = (1,0) + (0,-1) &= (-1,0) \\ 4(1,0) = (1,0) + (-1,0) &= (0,1) \\ 5(1,0) = (1,0) + (0,1) &= (1,0). \end{aligned}$$

Chapter 4

Constructing a map from Edwards to Weierstrass curves

At the end of the previous chapter, it is shown that an Edwards curve has points of order 4. This is the essential key to construct a map that maps points on an Edwards curve to points on a Weierstrass curve (or vice versa). This is the main goal in this chapter, and will be done in the following way: first, Weierstrass curves with a point of order 4 are constructed. Then it will be checked that having a point of order four means that the curve is birationally equivalent to an Edwards curve. While doing this, an explicit map between the curves is found. Using this it will be shown that the Edwards addition law corresponds to the addition law on a birationally equivalent Weierstrass curve.

From here on, to avoid confusions, a Weierstrass curve will be denoted by coordinates (u, v) and corresponding addition $\oplus$, while an Edwards curve will be denoted by (x, y) and addition $+$.

4.1 Points of order 4 on Weierstrass curves

In this section, a Weierstrass curve with a point of order 4 on it will be constructed. Suppose a Weierstrass curve is given together with a point of order 4 on it. This point is denoted by (α, β). Then the curve can be shifted such that $(0, \beta)$ is the point of order 4. So, the equation was:

$$v^2 = u^3 + au^2 + bu + c,$$

and after the shift, using the coordinates (w, v) with $w = u - \alpha$, this becomes:

$$v^2 = w^3 + \bar{a}w^2 + \bar{b}w + \beta^2. \tag{4.1}$$

With this equation, restrictions can be found on $\bar{a}, \bar{b}$ and β, following from the assumption that $(0, \beta)$ has order 4, such that the Weierstrass curve has a point of order 4 on it.

Since the point $P = (0, \beta)$ has order 4, it follows that $\beta \neq 0$ and $v(-2P) = 0$. The next step is to calculate the v-coordinate of $-2P$. By a straightforward computation we get the formula for the tangent line at the point $(0, \beta)$:

$$v = \lambda w + \nu$$

where:

$$\lambda = \frac{dv}{dw}\bigg|_{(0,\beta)} = \frac{3w^2 + 2\bar{a}x + \bar{b}}{2v}\bigg|_{(0,\beta)} = \frac{\bar{b}}{2\beta}.$$

Since the line passes through $(0, \beta)$ it follows $\nu = \beta$. Now, the tangent line is given by:

$$v = \frac{b}{2\beta}w + \beta.$$

Putting this in the original equation 4.1 gives:

$$\bar{b}w + \frac{\bar{b}^2}{4\beta^2}w^2 + \beta^2 = w^3 + \bar{a}w^2 + \bar{b}w + \beta^2,$$

$$\left(\frac{\bar{b}^2}{4\beta^2} - \bar{a}\right)w^2 = w^3.$$

Here, $w = 0$ (this was the point that was already known) or $w = (\frac{\bar{b}^2}{4\beta^2} - \bar{a})$. Now use $v(-2P) = 0$, so set $v = 0$ in equation 4.1 and substitute $w = \left(\frac{\bar{b}^2}{4\beta^2} - \bar{a}\right)$. This gives:

$$\left(\frac{\bar{b}^2}{4\beta^2} - \bar{a}\right)^3 + \bar{a}\left(\frac{\bar{b}^2}{4\beta^2} - \bar{a}\right)^2 + \bar{b}\left(\frac{\bar{b}^2}{4\beta^2} - \bar{a}\right) + \beta^2 = 0.$$

The expression simplifies to:

$$-\bar{b}^3 + 4\bar{b}\bar{a}\beta^2 - 8\beta^4 = 0.$$

We know that $\beta \neq 0$ because $(0, \beta)$ was the point of order 4. The case $\bar{b} = 0$ cannot happen, because then the above equation reads $-8\beta^4 = 0$, implying that $\beta = 0$, which is a contradiction. So, it follows that:

$$\bar{a} = \frac{8\beta^4 + \bar{b}^3}{4\bar{b}\beta^2}.$$

Substituting this into equation 4.1 and multiplying both sides by $(4\bar{b}\beta^2)^6$ gives:

$$\begin{aligned}\big((4\bar{b}\beta^2)^3 v\big)^2 &= \big((4\bar{b}\beta^2)^2 w\big)^3 + (8\beta^4 + \bar{b}^3)(4\bar{b}\beta^2)\big((4\bar{b}\beta^2)^2 w\big)^2 \\ &\quad + \bar{b}(4\bar{b}\beta^2)^4\big((4\bar{b}\beta^2)^2 w\big) + \beta^2(4\bar{b}\beta^2)^6.\end{aligned}$$

Using new coordinates $(g, h) = ((4\bar{b}\beta^2)^2 w, (4\bar{b}\beta^2)^3 v)$ gives:

$$h^2 = g^3 + (8\beta^4 + \bar{b}^3)(4\bar{b}\beta^2)g^2 + \bar{b}(4\bar{b}\beta^2)^4 g + \beta^2(4\bar{b}\beta^2)^6. \tag{4.2}$$

Setting $g = 0$ shows that the point $(0, \beta(4\bar{b}\beta^2)^3)$ lies on this curve. This is again a point of order 4, as will be checked below. Applying the same change of coordinates to the previously found tangent line gives a new tangent line at the point $(0, \beta(4\bar{b}\beta^2)^3)$:

$$h = 2\bar{b}^2\beta g + \beta(4\bar{b}\beta^2)^3.$$

Using the same steps as before, this can be substituted in equation 4.2, and so one can find $g = -32\bar{b}\beta^6$. Substituting g in equation 4.2 gives:

$$\begin{aligned}(-32\bar{b}\beta^6)^3 + (8\beta^4 + \bar{b}^3)(4\bar{b}\beta^2)(-32\bar{b}\beta^6)^2 + \bar{b}(4\bar{b}\beta^2)^4(-32\bar{b}\beta^6) + \beta^2(4\bar{b}\beta^2)^6 \\ = -32768\beta^{18}\bar{b}^3 - 4096\beta^{14}\bar{b}^6 + 4096\beta^{14}\bar{b}^3(8\beta^4 + \bar{b}^3) \\ = 0.\end{aligned}$$

Since the h-coordinate of $2(0, \beta(4\bar{b}\beta^2)^3)$ is 0, it follows that the curve of the form 4.2 is indeed a curve with a point of order 4.

In conclusion, a Weierstrass curve with a point of order 4 on it is constructed. A curve of the form of 4.2 will do, where $(0, \beta(4\bar{b}\beta^2)^3)$ is a point of order 4. But what are the restrictions on β and $\bar{b}$? The cases $\beta = 0, \bar{b} = 0$ were already excluded. In addition, the discriminant of a curve may not be zero. The discriminant D of 4.2 is:

$$D = -2^{24}\beta^{28}\bar{b}^9(32\beta^4 - \bar{b}^3) \neq 0.$$

From this, it follows $\beta \neq 0, \bar{b} \neq 0$ (but this was already known), $2^{24} \neq 0$ (but the curve lies in a field with *char(K)*> 2, so this is indeed the case), and β and $\bar{b}$ must satisfy $32\beta^4 \neq \bar{b}^9$.

So, a curve contains points of order 4 if it is of the following form:

$$h^2 = g^3 + (8\beta^4 + \bar{b}^3)(4\bar{b}\beta^2)g^2 + \bar{b}(4\bar{b}\beta^2)^4 g + \beta^2(4\bar{b}\beta^2)^6.$$

where $\beta, \bar{b} \in K\backslash\{0\}$, and $\bar{b}^3 \neq 32\beta^4$. The curve can be shifted to make the $\beta^2(4\bar{b}\beta^2)^6$-term disappear. This is done by using the transformation $u = g - 32\beta^6\bar{b}$, and gives (also renaming $h = v$ for notational convenience):

$$v^2 = u^3 + (4\beta^2\bar{b}^4 - 64\beta^6\bar{b})u^2 + 1024\beta^{12}\bar{b}^2 u.$$

The point of order 4 is now $(32\beta^6\bar{b}, \beta(4\bar{b}\beta^2)^3) = (u_4, v_4)$. The curve can be rewritten in terms of (u_4, v_4) and gives the form of a curve with a point of order 4:

$$v^2 = u^3 + (v_4^2/u_4^2 - 2u_4)u^2 + u_4^2 u. \tag{4.3}$$

4.2 From Weierstrass to Edwards curves

With equation 4.3, the next question can be investigated: if a curve has a point of order 4 on it, is it birationally equivalent to an Edwards curve?

Definition 4.1. Two elliptic curves E_1 and E_2 are called *birational equivalent* if there exist rational maps $\psi : E_1 \longrightarrow E_2$ and $\pi : E_2 \longrightarrow E_1$ such that $\psi \circ \pi$ is the identity on E_2 for all, but finitely many points and $\pi \circ \psi$ is the identity on E_1 for all, but finitely many points.

A rational map between a Weierstrass curve E of the form 4.3 and an Edwards curve E_d can be constructed. This is done in [BL08], and gives the following birational equivalence from E to E_d (with $d = 1 - 4u_4^3/v_4^2$).

$$\begin{aligned} \psi : (u, v) &\longmapsto (x, y) = \left(\frac{v_4 u}{u_4 v}, \frac{u - u_4}{u + u_4}\right) \\ \pi : (x, y) &\longmapsto (u, v) = \left(\frac{u_4(1 + y)}{1 - y}, \frac{v_4(1 + y)}{(1 - y)x}\right) \end{aligned}$$

It can be checked that $\psi \circ \pi(x, y) = (x, y)$ for almost all $(x, y) \in E_d(K)$ and $\pi \circ \psi(u, v) = (u, v)$ for almost all $(u, v) \in E(K)$. The rational maps are undefined for only finitely many points and those points can easily be found.

4.3 From Edwards to Weierstrass curves

Now, starting with an Edwards curve, the goal of this section is to find the Weierstrass curve birational equivalent to it. The map from the previous section cannot be used, since this makes use of the known point of order 4 on the Weierstrass curve. The idea is to write the Edwards curve as a Weierstrass curve with coefficients expressed in d. This can be done using the recipe from [Cas91, Chapter 8], which works for quartic curves in x with a rational point on it (so, for an Edwards curve).

The first step is to rewrite the equation for an Edwards curve:

$$\begin{aligned} x^2 + y^2 &= 1 + dx^2y^2 \\ (dx^2 - 1)y^2 &= x^2 - 1. \end{aligned}$$

Multiplying both sides by $(dx^2 - 1)$ gives $((dx^2 - 1)y)^2 = (dx^2 - 1)(x^2 - 1)$. Set $z = (dx^2 - 1)y$, then:

$$z^2 = dx^4 - (d + 1)x^2 + 1.$$

Now, replace $\eta = \frac{1}{x}$ and $\zeta = \frac{z}{x^2}$ (note that this is a rational map). This can be seen as "writing the polynomal backwards", making it a monic polynomial:

$$\begin{aligned}\zeta^2 &= \eta^4 - (d+1)\eta^2 + d \\ &= \Big(\eta^2 - \frac{d+1}{2}\Big)^2 + d - \Big(\frac{d+1}{2}\Big)^2 \\ &= G(\eta)^2 + H(\eta).\end{aligned}$$

Here, $G(\eta) = \big(\eta^2 - \frac{d+1}{2}\big)$ and $H(\eta) = d - \big(\frac{d+1}{2}\big)^2$. The equation of the curve is now:

$$(\zeta + G(\eta))(\zeta - G(\eta)) = H(\eta).$$

Set $\zeta + G(\eta) = \tau$, then it follows:

$$\zeta - G(\eta) = \frac{H(\eta)}{\tau}$$

$$2G(\eta) = \tau - \frac{H(\eta)}{\tau}.$$

Multiply by τ^2 and put $\tau\eta = \sigma$. Then:

$$2\sigma^2 = \tau^3 + (d+1)\tau^2 - \Big(d - \Big(\frac{d+1}{2}\Big)^2\Big)\tau.$$

This is almost in Weierstrass form. When both sides are multiplied by 8, the term $2\sigma^2$ will disappear:

$$\begin{aligned}16\sigma^2 &= 8\tau^3 + 8(d+1)\tau^2 - 8\Big(d - \Big(\frac{d+1}{2}\Big)^2\Big)\tau \\ (4\sigma)^2 &= (2\tau)^3 + 2(d+1)(2\tau)^2 - (4d - (d+1)^2)(2\tau).\end{aligned}$$

Using $(u, v) = (2\tau, 4\sigma)$ gives:

$$v^2 = u^3 + 2(d+1)u^2 + (d-1)^2 u. \tag{4.4}$$

Remark 4.2. The discriminant of the elliptic curve (4.4) is $D = 16(1 - 2d + d^2)(d - 2d^2 + d^3)$. This is zero if and only if $d = 0$ or $d = 1$. Thus, the unit circle is not an elliptic curve but, using definition 2.1, an Edwards curve over a field K with *char(K)*$\neq 2$ is indeed an elliptic curve for $d \in K\backslash\{0, 1\}$, since it is birationally equivalent to a Weierstrass curve.

By composing the (rational) maps we used above, a map from the Edwards to the corresponding Weierstrass curve (4.4) is found:

$$
\begin{aligned}
(x, y) &\longmapsto (x, z) = (x, (dx^2 - 1)y) \\
(x, z) &\longmapsto (\eta, \zeta) = (1/x, z/x^2) \\
(\eta, \zeta) &\longmapsto (\eta, \tau) = (\eta, \zeta + \eta^2 - (d+1)/2) \\
(\eta, \tau) &\longmapsto (\tau, \sigma) = (\tau, \eta\tau) \\
(\tau, \sigma) &\longmapsto (u, v) = (2\tau, 4\sigma)
\end{aligned}
$$

In addition, the curve also has to be translated. For all (x, y) on the Edwards curve, the translation $(x, y) \longmapsto (x, y) + (0, -1) = (-x, -y)$ is used. This must be done to make sure that the identity element of a curve is mapped properly onto the identity element of the other. All together, this gives the map:

$$
\begin{aligned}
(x, y) &\longmapsto (u, v) = \Big(\frac{A}{x^2}, \frac{-2A}{x^3}\Big) \\
&\qquad \text{where } A = 2y - (2dy + d + 1)x^2 + 2
\end{aligned}
$$

$$
(u, v) \longmapsto (x, y) = \Big(\frac{-2u}{v}, \frac{v^2 - (2 + 2d)u^2 - 2u^3}{4du^2 - v^2}\Big)
$$

Example 4.3. The point $(x, y) = (1, 0)$ on an Edwards curve is mapped to $(u, v) = (1 - d, 2(d - 1))$. If $d = 4$, this corresponds to $(u, v) = (-3, 6)$ and the corresponding Weierstrass curve is $v^2 = u^3 + 10u^2 + 9u$. This is plotted (in $\mathbb{R}$) in figure 4.1. In this figure, the tangent line at this point is drawn and it can be seen that this line intersects the curve in $(0, 0)$, so $2(-3, 6) = (0, 0)$ (a point of order 2). This shows that $(0, 1)$, a point of order 4 on the Edwards curve, is mapped onto a point of order 4 on the corresponding Weierstrass curve.

4.4 Addition on Edwards is addition on Weierstrass curves

The question now arises whether the outcomes of the addition laws on the two curves correspond. For the rational maps as given in section 4.2, this proof is given in [BL07], but the same can be proven for the map of section 4.3.

It will be proven that it does not matter whether first $(x_1, y_1)+(x_2, y_2) = (x_3, y_3)$ is computed and then the outcome (x_3, y_3) is mapped onto the corresponding Weierstrass curve to a point (u_3, v_3), or first the points (x_1, y_1), (x_2, y_2) are mapped onto the corresponding points $(u_1, v_1), (u_2, v_2)$ and then $(u_1, v_1) \oplus (u_2, v_2) = (u_3', v_3')$ is computed. It will follow that $(u_3, v_3) = (u_3', v_3')$. This is stated in the next theorem:

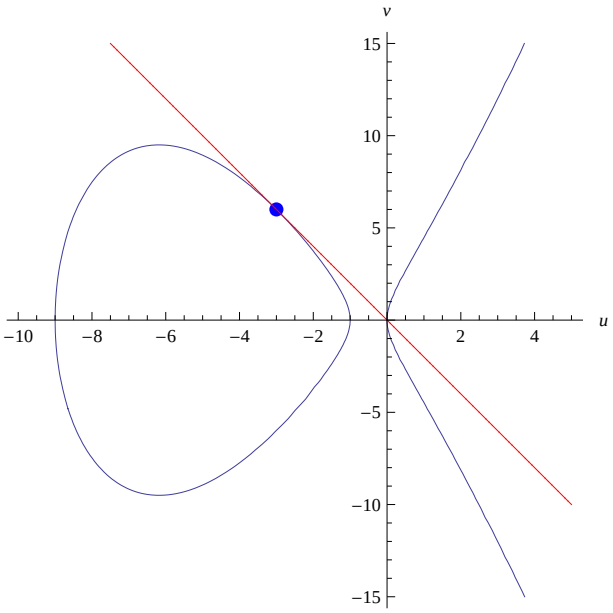

Figure 4.1: For $d = 4$, the point $(0, 1)$ on an Edwards curve is mapped onto $(-3, 6)$, a point of order 4 on the Weierstrass curve $v^2 = u^3 + 10u^2 + 9u$.

Theorem 4.4. *Set* $E : v^2 = u^3 + 2(d+1)u^2 + (d-1)^2u$. *For each* $i \in 1, 2, 3$ *let:*

$$P_i = \begin{cases} O \text{ if } (x_i, y_i) = (0, 1) \\ (0, 0) \text{ if } (x_i, y_i) = (0, -1) \\ (u_i, v_i) \text{ if } x_i \neq 0, \text{ where } u_i = \frac{2y_i - (2dy_i + d + 1)x_i^2 + 2}{x_i^2} \text{ and } v_i = \frac{-2u_i}{x_i}. \end{cases}$$

Then $P_i \in E(K)$ *and* $P_1 \oplus P_2 = P_3$.

Proof. First it is shown that each P_i is in $E(K)$. There are three cases: if $(x_i, y_i) = (0, 1)$, then $P_i = O$ and $O \in E(K)$. If $(x_i, y_i) = (0, -1)$, then $P_i = (0, 0) \in E(K)$. Otherwise, it can be shown that $P_i = (u_i, v_i) \in E(K)$ using Magma (see Appendix B).

Now, all that remains is to show that $P_1 + P_2 = P_3$ in any case. There are seven steps distinguished:

- If $(x_1, y_1) = (0, 1)$, then $(x_2, y_2) = (x_3, y_3)$ and P_1 is the point at infinity. It follows that $P_1 \oplus P_2 = O \oplus P_2 = P_2 = P_3$, and similar when $(x_2, y_2) = (0, 1)$. Assume from now on that $(x_1, y_1) \neq (0, 1)$, $(x_2, y_2) \neq (0, 1)$.

- If $(x_3, y_3) = (0, 1)$, then $(-x_1, y_1) = (x_2, y_2)$ and $P_3 = O$. It should follow that $-P_1 = P_2$. Since $P_2 = \left(\frac{2y_2 - (2dy_2 + d + 1)x_2^2 + 2}{x_2^2}, \frac{-2u_2}{x_2}\right) =$

$\left(\frac{2y_1-(2dy_1+d+1)x_1^2+2}{x_1^2}, \frac{-2u_1}{-x_1}\right) = (u_1, -v_1)$, it follows that $-P_1 = P_2$. From now on, assume $(x_3, y_3) \neq (0, 1)$.

- If $(x_1, y_1) = (0, -1)$, then $(x_3, y_3) = (-x_2, -y_2)$. Now $(x_2, y_2) \neq (0, -1)$ since then $(x_3, y_3) = (0, 1)$ and $(x_2, y_2) \neq (0, 1)$, so $x_2 \neq 0$. Also, $P_1 = (0, 0)$ and $P_2 = (u_2, v_2) = \left(\frac{2y_2-(2dy_2+d+1)x_2^2+2}{x_2^2}, \frac{-2u_2}{-x_2}\right)$. The standard addition law says that $(0, 0) \oplus (u_2, v_2) = (r_3, s_3)$ with $r_3 = \frac{4}{x_2^2} - 2(d+1) - \frac{2y_2-(2dy_2+d+1)x_2^2+2}{x_2^2} = \frac{-2y_2+(2dy_2-d-1)x_2^2-2}{x_2^2} = \frac{2y_3-(2dy_3+d+1)x_3^2-2}{x_3^2} = u_3$ and $s_3 = \frac{2s_3}{x_2} = \frac{-2u_3}{x_3} = v_3$. Similar when $(x_2, y_2) = (0, -1)$. From now on, $x_1 \neq 0$ and $x_2 \neq 0$.

- If $(x_3, y_3) = (0, -1)$, then $(x_1, y_1) = (x_2, -y_2)$ so $u_1 = \frac{2y_1-(2dy_1+d+1)x_1^2+2}{x_1^2} = \frac{-2y_2-(-2dy_2+d+1)x_2^2+2}{x_2^2}$ and $v_1 = \frac{-2u_1}{x_1} = \frac{-2u_2}{x_2}$. Since $P_3 = (0, 0)$, the addition law states that $-P_3 \oplus P_2 = (0, 0) + P_2 = -P_1$. Let $(0, 0) \oplus P_2 = (r_1, s_1)$. Now the standard addition law says that $\lambda = \frac{-2}{x_2}$ and $\nu = 0$, such that $r_1 = \frac{4}{x_2^2} - 2(d+1) - \frac{2y_2-(2dy_2+d+1)x_2^2+2}{x_2^2} = \frac{-2y_2+(2dy_2-d-1)x_2^2+2}{x_2^2} = u_1$ and $s_1 = \frac{2r_1}{x_2} = \frac{2u_1}{x_1} = -v_2$, so $(r_1, s_1) = -P_1$. Assume from now on that $x_3 \neq 0$.

- If $P_2 = -P_1$ then $u_2 = u_1$ and $v_2 = -v_1$, so $x_2 = -x_1$ and $y_2 = \frac{v_2^2-(2+2d)u_2^2-2u_2^3}{4du_2^2-v_2^2} = \frac{v_1^2-(2+2d)u_1^2-2u_1^3}{4du_1^2-v_1^2} = -y_1$, so $(x_3, y_3) = (0, 1)$ which is already handled above.

- If $u_2 = u_1$ and $v_2 \neq v_1$, the standard addition law says that $(u_1, v_1) \oplus (u_2, v_2) = (s_3, r_3)$ where, $\lambda = \frac{3u_1^2+4(d+1)u_1-(d-1)^2}{2v_1}$, $\nu = \frac{-u_1^3-(d-1)^2x_1}{2v_1}$, $r_3 = \lambda^2 - 2(d+1) - 2u_1$, $s_3 = \lambda u_3 - \nu$. Using Magma, this case can be checked (see appendix B).

- The only remaining case is when $u_2 \neq u_1$. Now the standard addition law says that $(u_1, v_1) \oplus (u_2, v_2) = (s_3, r_3)$ where $\lambda = \frac{v_2-v_1}{u_2-u_1}, \nu = \frac{v_1u_2-v_2u_1}{u_2-u_1}, r_3 = \lambda^2 - 2(d+1) - u_1 - u_2, s_3 = \lambda u_3 - \nu$. Again, using Magma, this can be checked (see appendix B). So, $P_1 \oplus P_2 = P_3$ in any case.

□

In conclusion, the following theorem was proved in this chapter:

Theorem 4.5. *Fix a field K with $char(K) \neq 2$. Let E a Weierstrass curve over K. The group $E(K)$ has an element of order 4 if and only if E is birationally equivalent over K to an Edwards curve.*

The proof consists of checking that the addition laws correspond (section 5), and noting that the Edwards curve hase a point of order 4 (for example $(1, 0)$), so the Weierstrass curve has a point of order 4 as well. Conversely, it must be checked that if E has a point of order 4, there is a rational map between E and E_d with inverse, such that it is a birational equivalence between the two curves (section 3 and 4).

Chapter 5

Supersingular Edwards curves

Supersingular elliptic curves arise naturally. They have certain properties that other, so-called ordinary elliptic curves, do not have. Only finitely many curves are supersingular, as will be shown later on. Note that being supersingular has nothing to do with being singular, since an elliptic curve is by definition non-singular. In this chapter, supersingular curves will be introduced and it will be investigated for which d an Edwards curve is supersingular.

5.1 Definition

There are several equivalent conditions for a curve to be supersingular. Here, the next definition is used:

Definition 5.1. Let E an elliptic curve over a field K with characteristic p. Let $[n] : E \longrightarrow E$ be the multiplication by n-map with kernel $E[n]$, then:

$$E[p^r] \simeq \begin{cases} 0 \\ \mathbb{Z}/p^r\mathbb{Z} \end{cases} \text{ or}$$

for all $r \geq 1$. If the first holds, E is called E **supersingular**. Otherwise, E is ordinary.

The proof that either one of these properties is true, can be found in [Sil86].

5.2 The Legendre form

A Weierstrass equation over a field K is in *Legendre form* if it can be written as:

$$\tilde{E}_\lambda : v^2 = u(u-1)(u-\lambda).$$

Here, $\lambda \in K\backslash\{0,1\}$. In this section it is shown that the previously found Weierstrass curve E corresponding to an Edwards curve E_d, is related to an elliptic curve in Legendre form. The equation was:

$$E : v^2 = u^3 + 2(d+1)u^2 + (d-1)^2 u.$$

Now, use the homomorphism as described in [ST92, Chapter III.4]. This is a homomorphism between E and $\bar{E} : v^2 = u^3 + \bar{a}u^2 + \bar{b}u$ where $\bar{a} = -2a = -4(d+1)$ and $\bar{b} = a^2 - 4b = 4(d+1)^2 + 4(d-1)^2$. So:

$$\bar{E} : v^2 = u^3 - 4(1+d)u^2 + (4(d+1)^2 - 4(d-1)^2)u.$$

This homomorphism sends exactly O and $(0,0)$ on E to $\bar{O}$, the identity element of $\bar{E}$. All other elements are mapped onto $\bar{E}\backslash\{\bar{O}\}$. Factoring $\bar{E}$ gives:

$$\bar{E} : v^2 = u(u-4)(u-4d).$$

Dividing both sides by 64 gives:

$$\left(\frac{v}{8}\right)^2 = \frac{u}{4}\left(\frac{u}{4} - 1\right)\left(\frac{u}{4} - d\right).$$

Replacing $\tilde{v} = v/8$ and $\tilde{u} = u/8$ gives an elliptic curve in the Legendre form:

$$\tilde{E}_d : \tilde{v}^2 = \tilde{u}(\tilde{u}-1)(\tilde{u}-d).$$

To summarize, now an Edwards curve E_d is birationally equivalent to a Weierstrass curve E. There is a non-constant homomorphism from E to a curve in Legendre form $\tilde{E}_d$. So, there is a non-constant rational map from E_d to $\tilde{E}_d$.

5.3 Supersingular Edwards curves

With the previously found Legendre form, the theory of supersingular Legendre curves can be used to find supersingular Edwards curves. The next theorem will be useful.

Theorem 5.2. *Let E_1 and E_2 be elliptic curves over a finite field $\mathbb{F}_q$, where $q = p^n$ for some prime p.*

- *If $\phi : E_1 \to E_2$ is a non-constant rational map (defined over $\mathbb{F}_q$), then:*

$$\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$$

- *As a result, $\#E_1(\mathbb{F}_{q^n}) = \#E_2(\mathbb{F}_{q^n})$ for all $n \geq 1$*
- *As a result, E_1 supersingular if and only if E_2 supersingular.*

The proof can be found in [Cas66, lemma 15.1]. Now, from theorem (5.2) it follows that an Edwards curve E_d is supersingular if and only if the corresponding curve in Legendre form $\tilde{E}_d$ is supersingular.

The next theorem gives conditions for $\tilde{E}_\lambda$ to be supersingular.

Theorem 5.3. *Let K be a finite field of characteristic $p > 2$.*

1. *Let $m = (p-1)/2$. Define the polynomial $H_p(t) = \sum_{i=0}^{m} \binom{m}{i}^2 t^i$, let $\lambda \in K$, $\lambda \neq 0, 1$. Then $\tilde{E}_\lambda : v^2 = u(u-1)(u-\lambda)$ is supersingular if and only if $H_p(\lambda) = 0$.*
2. *The polynomial $H_p(\lambda)$ has distinct roots in $\bar{K}$. Up to isomorphism, there are exactly $[p/12] + \epsilon_p$ supersingular curves in characteristic p, where $\epsilon_3 = 1$ and for $p \geq 5$,*

$$\epsilon_p = 0, 1, 1, 2 \text{ if } p \equiv 1, 5, 7, 11 \bmod 12.$$

The proof can be found in [Sil86].

It turns out that all zeros of the polynomial $H_p(\lambda) \in \mathbb{F}_p[\lambda]$ (these are called the *Legendre parameter*) are in $\mathbb{F}_{p^2}$, as is proven in [AT02, Prop 2.2]. Sometimes there are zeros of $H_p(\lambda)$ in $\mathbb{F}_p$. A condition for this is given in the next theorem.

Theorem 5.4. *Fix a finite field $\mathbb{F}_p$ with $p > 3$ prime. Then an elliptic curve $E/\mathbb{F}_p$ is supersingular if and only if $\#E(\mathbb{F}_p) = p + 1$.*

Proof. From the Hasse inequality (see e.g. [Sil86, Chapter V.1]) it follows that $\#E(\mathbb{F}_p) = p + 1 - a$ with $a \leq 2\sqrt{p}$. But since E is supersingular, it follows that $p|a$ as well (this follows from the proof of Thm. 4.1 in [Sil86, Chapter V.4]). So a is an integer and can be written as $a = pm$ for some integer m. But then $|pm| \leq 2\sqrt{p}$, and this is only true for $m = 0$ if $p > 3$, so $a = 0$. Hence, it follows that $\#E(\mathbb{F}_p) = p + 1$. □

With this result, it can be shown that $H_p(\lambda) \in \mathbb{F}_p[\lambda]$ has roots in $\mathbb{F}_p$ if and only if $p \equiv 3 \bmod 4$.

Theorem 5.5. *Let $\tilde{E}_\lambda$ be an elliptic curve in Legendre form over a finite field $\mathbb{F}_p$. The polynomial $H_p(\lambda)$ has at least one zero in $\mathbb{F}_p$ if and only if $p \equiv 3 \bmod 4$.*

Proof. ($\Rightarrow$) First, it is proven that there exists a λ such that $\tilde{E}_\lambda$ is supersingular in $\mathbb{F}_p$ if $p \equiv 3 \bmod 4$. Since $\tilde{E}_\lambda : v^2 = u(u-1)(u-\lambda)$, the following is a subgroup of $\tilde{E}_\lambda(\mathbb{F}_q)$:

$$\{O, (0,0), (1,0)(\lambda, 0)\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

This is a subgroup, since all elements are in $\tilde{E}_\lambda(\mathbb{F}_q)$ and, using the standard addition on elliptic curves, one can check that adding any two elements gives an element of the subgroup again.

Since this subgroup has four elements, it follows that 4 is a divisor of $\#\tilde{E}_\lambda(\mathbb{F}_p)$, so (using theorem 5.4), $4|p+1$, and thus $p \equiv 3 \bmod 4$.

($\Leftarrow$) Otherwise, it will be shown that if $p \equiv 3 \bmod 4$, then $H_p(-1) = 0$. If $p \equiv 3 \bmod 4$, then $m = \frac{p-1}{2}$ is odd. Use

$$\binom{m}{i} = \binom{m}{m-i},$$

and note that if i is odd, then $m - i$ is even. Then:

$$\binom{m}{i}^2 (-1)^i + \binom{m}{m-i}^2 (-1)^{m-i} = \binom{m}{i}^2 (-1+1) = 0.$$

Hence:

$$H_p(-1) = \sum_{i=0}^{m} \binom{m}{i}^2 (-1)^i = 0.$$

So $H_p(\lambda)$ has at least one zero in $\mathbb{F}_p$ if $p \equiv 3 \bmod 4$, namely $\lambda = -1$, which completes the proof of the theorem. □

This theorem states that if $p \equiv 1 \bmod 4$, then there are no $\lambda \in \mathbb{F}_p$ such that $\tilde{E}_\lambda$ is supersingular. If $p \equiv 3 \bmod 4$, then for $\lambda = -1$ the elliptic curve $\tilde{E}_\lambda$ is supersingular, so then there is at least one $\lambda \in \mathbb{F}_p$ such that $\tilde{E}_\lambda$ is supersingular. There can be more values for λ for which $\tilde{E}_\lambda$ is supersingular in $\mathbb{F}_p$, as stated in the next theorem:

Theorem 5.6. *The number of Legendre parameters λ in $\mathbb{F}_p$ satisfies:*

$$\#\{\lambda \in \mathbb{F}_p : H_p(\lambda) = 0\} = \begin{cases} 0 \text{ if and only if } p = 1 \bmod 4 \\ 1 \text{ if } p = 3 \\ 3h(-p) \text{ if } p > 3 \text{ and } p \equiv 3 \bmod 4, \end{cases}$$

where $h(-p)$ is the class number of $\mathbb{Q}(\sqrt{-p})$.[1]

The proof can be found in [AT02, Prop 3.2].

When $H_p(d)$ is calculated, the polynomial has always $(p-1)/2$ distinct roots. However, the formula of theorem 5.3.2 states that up to isomorphism, there are less than $(p-1)/2$ supersingular curves. This is due to the following theorem:

Theorem 5.7. *Let E_λ and E_μ be elliptic curves in Legendre form over a field K with char(K)$\neq 2$, then E_μ and E_λ have the same j-invariant if and only if*

$$\mu \in \left\{ \lambda, \frac{1}{\lambda}, 1-\lambda, \frac{1}{1-\lambda}, \frac{\lambda}{\lambda-1}, \frac{\lambda-1}{\lambda} \right\}.$$

[1] i.e. the number of elements of the class group of $\mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$.

The proof can be found in [Sil86, Chapter III.1].

Example 5.8. If for example $p = 13$, then $p \equiv 1 \bmod 4$ and

$$H_{13}(d) = (d^2 + 4d + 9)(d^2 + 12d + 3)(d^2 + 7d + 1).$$

This has no roots in $\mathbb{F}_{13}$, but it has roots in $\mathbb{F}_{13^2}$.

On the other hand, if $p = 11$, then $p \equiv 3 \bmod 4$. When $H_{11}(d)$ is calculated, this gives:

$$H_{11}(d) = (d + 1)(d + 9)(d^2 + 10d + 1)(d + 5).$$

The solutions are $d = 2, 6, 10, -5 \pm 2\sqrt{6}$. It seems like there are five supersingular curves in $\mathbb{F}_{11}$, while theorem 5.3 states that up to isomorphism, there are only two. This can be seen using theorem 5.7. Let $\lambda = 10$, then $1 - \lambda = -9 \equiv 2 \bmod 11$ and $\frac{\lambda}{\lambda - 1} = \frac{10}{9} \equiv 6 \bmod 11$.[2] So these three solutions for d give isomorphic curves. Also, when $\lambda = -5 + 2\sqrt{6}$, then $\frac{1}{\lambda} = -5 - 2\sqrt{6}$, so these are isomorphic as well.

Clearly, this polynomial has roots in $\mathbb{F}_{11}$, namely $d = 2, 6, 10$. It follows that $E : v^2 = u^3 + 2(10 + 1)u^2 + (10 - 1)^2 u$ defines a supersingular curve and thus $\#E(\mathbb{F}_{11}) = 12$. This can be checked by calculating $u^3 + 22u^2 + 81u$ for all elements of $\mathbb{F}_{11}$ and then checking if the outcome is a square in $\mathbb{F}_{11}$. For example, $u = 1$ gives $v^2 = 5$ and 5 is a square in $\mathbb{F}_{11}$ since $(\pm 4)^2 \equiv 5 \bmod 11$. This gives two points on the curve: $(1, 4)$ and $(1, 7)$. Continuing this way gives:

$$\begin{aligned} E(\mathbb{F}_{11}) &= \{O, (0, 0), (1, 4), (1, 7), (2, 4), (2, 7), \\ &\quad (4, 5), (4, 6), (6, 3), (6, 8), (8, 4), (8, 7)\}. \end{aligned}$$

So there are exactly 12 elements. This is a cyclic group of order 12: $(6, 3)$, $(6, 8)$, $(8, 4)$ and $(8, 7)$ are the points of order 12. The corresponding Edwards curve is $E_{10} : x^2 + y^2 = 1 + 10x^2y^2$. Mapping all points of $E(\mathbb{F}_{11})$ onto $E_{10}(\mathbb{F}_{11})$ (using the map of chapter 4) gives the elements:

$$\begin{aligned} E_{10}(\mathbb{F}_{11}) &= \{(0, 1), (0, 10), (1, 0), (4, 5), (4, 6), (5, 4), \\ &\quad (5, 7), (6, 4), (6, 7), (8, 5), (8, 6), (10, 0)\}. \end{aligned}$$

It can easily be checked that these 12 elements are indeed all elements of $E_{10}(\mathbb{F}_{11})$. So, for $d = 10$, the Edwards curve is supersingular in $\mathbb{F}_{11}$. This is again a cyclic group of order 12.

In conclusion, in this chapter it is shown that there is a non-constant rational map from an Edwards curve to an elliptic curve in Legendre form $\tilde{E}_d : v^2 = u(u - 1)(u - d)$, which means that an Edwards curve is supersingular if and only if $\tilde{E}_d$ is supersingular. Whether $\tilde{E}_d$ is supersingular, can be checked using theorem 5.3.

[2] Note that $\frac{a}{b} \equiv c \bmod d$ means $a \equiv bc \bmod d$ for integers a, b, c, d such that $\gcd(b, d) = 1$.

Chapter 6

Conclusion

Edwards curves are elliptic curves of the form $E_d : x^2 + y^2 = 1 + dx^2y^2$, where $d \in K\backslash\{0, 1\}$. The addition law is given by:

$$(x_1, y_1) + (x_2, y_2) = (x_3, y_3) = \Big(\frac{x_1y_2 + x_2y_1}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 - dx_1x_2y_1y_2}\Big).$$

The addition law is complete if d is not a square in K. It is also strongly unified: the formulas work for *all* pairs of input on the curve, so also for doublings etc. Edwards curves naturally have points of order 4, for instance $(1, 0)$.

If a Weierstrass curve has a point of order 4 on it, then it is birationally equivalent to an Edwards curve, since rational maps between the curves can be found. Using these maps, it follows that the addition laws on both curves correspond. Since also every Edwards curve can be put in Weierstrass form, an Edwards curve is birationally equivalent to a Weierstrass curve if and only if the Weierstrass curve has a point of order 4 on it. The rational map with inverse between E_d and a Weierstrass curve $E : v^2 = u^3+2(d+1)u^2+(d-1)^2u$ given by:

$$\begin{aligned}(x, y) &\longmapsto (u, v) = \Big(\frac{A}{x^2}, \frac{-2A}{x^3}\Big) \\ &\qquad \text{where } A = 2y - (2dy + d + 1)x^2 + 2\end{aligned}$$

$$(u, v) \longmapsto (x, y) = \Big(\frac{-2u}{v}, \frac{v^2 - (2 + 2d)u^2 - 2u^3}{4du^2 - v^2}\Big)$$

is a birational equivalence from E_d to E.

There is a rational map from an Edwards curve to an elliptic curve in Legendre form $\tilde{E}_d : v^2 = u(u - 1)(u - d)$, which implies that an Edwards curve is supersingular if and only if $\tilde{E}_d$ is supersingular. The elliptic curve in Legendre form $\tilde{E}_d$ is supersingular if and only if d is a root of the polynomial $H_p(d) = \sum_{i=0}^{m} \binom{m}{i}^2 d^i$. For $p > 2$, this polynomial has all roots in $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$ if $p \equiv 3 \bmod 4$ and only has roots in $\mathbb{F}_{p^2}$ if $p \equiv 1 \bmod 4$.

Appendix A

The projective plane

This appendix introduces the projective plane and shows where the point O on a Weierstrass curve comes from.

Recall that the affine plane over a field K, denoted by $\mathbb{A}^2$, is given by:

$$\mathbb{A}^2 = \{(x, y) : x, y \in K\}.$$

The *projective plane*, denoted $\mathbb{P}^2$, can be seen as an extension of $\mathbb{A}^2$. If the field $\mathbb{R}$ is taken, then in $\mathbb{A}^2$ two lines intersect in exactly one point, except when they are parallel. In $\mathbb{P}^2$ every two lines intersect, *even if* they are parallel. This can be explained from an algebraic or a geometric view.

At first, say we want to find the solutions of

$$x^N + y^N = 1 \tag{A.1}$$

in rational numbers. It can be shown that any solution has the form $(a/c, b/c)$. This can be written in homogeneous coordinates by using $x = X/Z$ and $y = Y/Z$:

$$X^N + Y^N = Z^N, \tag{A.2}$$

which has solutions of the form (a, b, c). But now the problem arises that for example the point $(1, -1, 0)$ for N is odd, is a solution of equation A.2, but not of equation A.1. But what happens if a sequence of solutions is taken, such that $(a_i, b_i, c_i) \to (1, -1, 0)$ for $i = 1, 2, 3, \ldots$ and $c_i \neq 0$ for all i? Then $(a_i/c_i, b_i/c_i)$ goes to $(\infty, -\infty)$. Somehow, the extra solution $(1, -1, 0)$ corresponds to a solution of equation A.1 'at infinity'. This leads to the definition of the projective plane $\mathbb{P}^2$ as the set of triples $[a, b, c]$, not all zero, where $[a, b, c] \sim [a', b', c']$ if there is a t (not zero) such that $a = ta', b = tb', c = tc'$. Or:

$$\mathbb{P}^2 = \{[a, b, c] : a, b, c \text{ not all } 0\}/\sim .$$

The other way of looking at it, is geometrically. As said before, parallel lines do not have an intersection in $\mathbb{A}^2$, but in $\mathbb{P}^2$ they do. This means that there

are some 'points at infinity' added to $\mathbb{A}^2$, points where two parallel lines intersect. This cannot be just one point, because if two couples of parallel lines $P\&P'$ and $L\&L'$ are taken, where P and L are not parallel, then $P\&P'$ intersect at a point O_1 and $L\&L'$ intersect at a point O_2. Because P and L are not parallel, this means they intersect at some point $\{Q\} = P \cap L$. If $O_1 = O_2$, this would mean that P and L intersect again in O_1, which contradicts the fact that they can only intersect once. So, there are more points at infinity. In fact, there is a point at infinity for every *direction* in $\mathbb{A}^2$. Two point are said to have the same direction if and only if they are parallel. So, a direction is a collection of all lines parallel to a given line. The associated point at infinity is a point that is not in $\mathbb{A}^2$, so $\mathbb{P}^2$ can be defined as:

$$\mathbb{P}^2 = \mathbb{A}^2 \cup \{ \text{ set of all directions in } \mathbb{A}^2\}.$$

It can be shown that these definitions of $\mathbb{P}^2$ are equivalent, see [ST92].

Now, back to elliptic curves: every elliptic curve can be written as the set of points in $\mathbb{P}^2$ that satisfies a cubic equation with only one point on the line at ∞. After scaling X and Y, it can be written in the Weierstrass form, i.e.:

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_5Z^3.$$

The basepoint is $O = [0, 1, 0]$. If non-homogeneous coordinates $x = X/Z$ and $y = Y/Z$ are used, this becomes:

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

If all $a_i \in K$ for $1 \leq i \leq 6$, E is said to be *defined over* K, written E/K.

Appendix B

Checking the addition law

The next Magma-script checks that for $u_1 \neq u_2$ and $v_1 \neq v_2$ the addition law holds:

```
{K<d,x1,x2>:=FieldOfFractions(PolynomialRing(Rationals(),3));
R<y1,y2>:=PolynomialRing(K,2);
S:=quo<R|x1^2+y1^2-(1+d*x1^2*y1^2),x2^2+y2^2-(1+d*x2^2*y2^2)>;
// the Edwards addition law:
x3:=(x1*y2+y1*x2)/(1+d*x1*x2*y1*y2);
y3:=(y1*y2-x1*x2)/(1-d*x1*x2*y1*y2);
// map to the Weierstrass curve:
u1:=((-2*d*y1-d-1)*x1^2+2*y1+2)/(x1^2); v1:=-2*u1/x1;
   S!(v1^2-u1^3-2*(d+1)*u1^2-(d-1)^2*u1);
u2:=((-2*d*y2-d-1)*x2^2+2*y2+2)/(x2^2); v2:=-2*u2/x2;
   S!(v2^2-u2^3-2*(d+1)*u2^2-(d-1)^2*u2);
u3:=((-2*d*y3-d-1)*x3^2+2*y3+2)/(x3^2); v3:=-2*u3/x3;
   S!(v3^2-u3^3-2*(d+1)*u3^2-(d-1)^2*u3);
// add on the Weierstrass curve:
lambda:=(v2-v1)/(u2-u1);
nu:= (v1*u2-v2*u1)/(u2-u1);
r3:=lambda^2-2*(d+1)-u1-u2; s3:=-lambda*r3-nu;
// check the answer:
S!(u3-r3); S!(v3-s3);
```

Here, the output will be five times a 0, implying that all (u_i, v_i) satisfy the Weierstrass equation in S, and that the two different ways of computing (u_3, v_3) coincide.

When $u_1 = u_2$ but $v_1 \neq -v_2$, the next script checks the addition law (note that this is in fact doubling):

```
K<d,x1>:=FieldOfFractions(PolynomialRing(Rationals(),2));
R<y1>:=PolynomialRing(K,1);
```

```
S:=quo<R|x1^2+y1^2-(1+d*x1^2*y1^2)>;
x2:=x1; y2:=y1;
// the Edwards addition law:
x3:=(x1*y2+y1*x2)/((1+d*x1*x2*y1*y2));
y3:=(y1*y2-x1*x2)/((1-d*x1*x2*y1*y2));
// map to the Weierstrass curve:
u1:=((-2*d*y1-d-1)*x1^2+2*y1+2)/(x1^2); v1:=-2*u1/x1;
   S!(v1^2-u1^3-2*(d+1)*u1^2-(d-1)^2*u1);
u2:=((-2*d*y2-d-1)*x2^2+2*y2+2)/(x2^2); v2:=-2*u2/x2;
   S!(v2^2-u2^3-2*(d+1)*u2^2-(d-1)^2*u2);
u3:=((-2*d*y3-d-1)*x3^2+2*y3+2)/(x3^2); v3:=-2*u3/x3;
   S!(v3^2-u3^3-2*(d+1)*u3^2-(d-1)^2*u3);
// double on the Edwards curve:
lambda:=(3*u1^2+2*(2*d+2)*u1+(d-1)^2)/(2*v1);
r3:=lambda^2-(2*d+2)-u1-u2; s3:=lambda*(u1-r3)-v1;
// check the answer:
S!(u3-r3); S!(v3-s3);
```

Again, the output will be five times a 0, implying the same thing as above.

Bibliography

[AT02] R. Auer and J. Top. Legendre elliptic curves over finite fields. *Journal of Number Theory*, 95:303–312, 2002.

[BL07] D.J. Bernstein and T. Lange. Faster addition and doubling on elliptic curves. *Advances in cryptology - ASIACRYPT 2007*, pages 29–50, 2007.

[BL08] D.J. Bernstein and T. Lange. Twisted Edwards Curves. *Progress in cryptology - AFRICACRYPT 2008*, pages 389–405, 2008.

[Cas66] J.W.S. Cassels. Diophantine equations with special reference to elliptic curves. *Journal of the London Mathematical Society*, 41:193–291, 1966.

[Cas91] J.W.S. Cassels. *Lectures on Elliptic Curves*. Cambridge University Press, 1991.

[Edw07] H.M. Edwards. A normal form for elliptic curves. *Bulletin of the American Mathematical Society*, 44:393–422, 2007.

[Pet11] Christiane Peters. *Curves, Codes, and Cryptography*. PhD thesis, Technische Universiteit Eindhoven, the Netherlands, 2011.

[Sil86] J.H. Silverman. *The Arithmetic of Elliptic Curves*. Springer Verlag, 1986.

[ST92] J.H. Silverman and J. Tate. *Rational Points on Elliptic Curves*. Springer Verlag, 1992.