BACHELOR

Transformation from Weierstrass curves to Jacobi curves

Smeets, C.J.C.

Award date:
2014

Transformation from Weierstrass curves to Jacobi curves

Supervisor: Tanja Lange

Bachelor thesis
Technical University Eindhoven
Applied Mathematics

Anne Smeets
0678115
c.j.c.smeets@student.tue.nl

April 23, 2014

Preface

First of all, I want to thank Tanja Lange for accepting me as a bachelor student who wants to do a thesis with her, because she didn't know what to expect and do, since I was her first bachelor student doing a thesis with her. It was a good experience exploring this together. I have enjoyed working on my thesis and learning the new information she has given me. I also want to thank Dan Bernstein for his nice intermezzos whilst talking with Tanja about my thesis. I have learned a lot about the NSA, cryptology and of course elliptic curves from both of them.

I also want to thank my boyfriend Mike Mouthaan for pushing me to finish my project. He made me work on it by doing all my chores and forcing me to work. But he also made me take breaks when I didn't know what to do anymore and was frustrated by the project. Without him, I don't think I would have finished.

As last, I want to thank you, my dear reader. Let this project not be in vain and read it carefully. I hope you will learn a lot by it, just as I did researching this.

Contents

Summary

This project studies elliptic curves in different representations. In chapter 1, it is explained that the name elliptic curve comes from the fact that the curve is the arc length of an ellipse. In this chapter we also see that Elliptic Curve Cryptography (ECC) has advantages, such as higher speed and less space, over RSA, the most widely used cryptosystem nowadays. In the last part of this chapter, we discuss that we need different kind of curves, because some curves are faster or safer than other curves.

In chapter 2 the Weierstrass affine form $E_W : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ is discussed and we show how we can add points P and Q, denoted $R = P \oplus Q$, and double on the Weierstrass curve:

$$\lambda = \begin{cases} \frac{y_P - y_Q}{x_P - x_Q} & \text{if } P \neq \pm Q \\ \frac{3x_P^2 + 2a_2x_P + a_4 - a_1y_P}{2y_P + a_1x_P + a_3} & \text{if } P = Q \neq -Q \end{cases}$$

$$x_R = \lambda^2 + a_1\lambda - a_2 - x_P - x_Q,$$

$$y_R = \lambda(x_P - x_R) - y_P - a_1x_R - a_3.$$

Besides the points (x, y) satisfying E_W there exists a further point, P_∞ on the curve; it can be pictured far out on the y-axis. If $P = P_\infty$, we have that $P \oplus Q = Q$. If $P = -Q$, we have that $R = P \oplus Q = -Q \oplus Q = P_\infty$, the neutral element. In the end of chapter 2 an example over $\mathbb{Q}$ and in a finite field are shown.

In chapter 3 the Jacobi form $E_J : v^2 = au^4 + cu^2 + q^2$ and a special kind of Jacobi quartic $E_S : v^2 = u^4 + 2c_0u^2 + 1$ are discussed. We also see how to add points P and Q on a Jacobi quartic:

$$u_R = \frac{u_Pv_Q + v_Pu_Q}{1 - a(u_Pu_Q)^2},$$

$$v_R = \frac{(1 + a(u_Pu_Q)^2)(v_Pv_Q + cu_Pu_Q) + 2au_Pu_Q(u_P^2 + u_Q^2)}{(1 - a(u_Pu_Q)^2)^2}.$$

As last we show how to double a point P on a Jacobi quartic:

$$u_{2P} = \frac{2u_P v_P}{1 - u_P^4},$$
$$v_{2P} = \frac{(1 + u_P^4)(v_P^2 + 2c_0 u_P^2) + 4u_P^4}{(1 - u_P^4)^2}.$$

For both cases, the Jacobi quartic and the special Jacobi quartic, an example over $\mathbb{Q}$ and an example over a finite field is given.

In chapter 4, we show that there exists a birational equivalence between a general Jacobi quartic curve $E_Q : v^2 = au^4 + bu^3 + cu^2 + du + q^2$ and a Weierstrass curve $E_W : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ with:

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

where

$$a_1 = \frac{d}{q}, \qquad a_2 = c - \frac{d^2}{4q^2},$$
$$a_3 = 2qb, \qquad a_4 = -4q^2a,$$

$$a_6 = a_2a_4 = a(d^2 - 4q^2c).$$

And we see how we can invert this:

$$u = \frac{2q(x + c) - \frac{d^2}{2q}}{y},$$
$$v = -q + \frac{u(ux - d)}{2q}.$$

The addition and doubling formulae are for a more restricted kind of curve than the mapping is. We are able to devise the adding and doubling formulae for the general Jacobi curve by symbolically using first the map from the Jacobi curve to a Weierstrass curve, add symbolically on the Weierstrass curve and then map back to the Jacobi curve, but I have not done this yet, because the formulae would grow much longer. This could be done in a future paper.

Chapter 1

Introduction

1.1 Name elliptic curves

Elliptic curves were first discovered when people wanted to calculate the arc length of an ellipse. For an arc length, one takes $\int_a^b \sqrt{1 + (f'(x))^2}\ \mathrm{d}x$, with starting point $x = a$ and end point $x = b$ and $f(x)$ the formula given for the ellipse. These integrals can be written as the primitive of $y = \sqrt{1 + (f'(x))^2}$ with begin point $x = a$ and end point $x = b$. These integrals (without the begin and end point) yield the elliptic curves we know nowadays. Note: Ellipses themselves are conic sections, not elliptic curves.

1.2 RSA versus ECC

One of the most widely used cryptosystems in the world at the moment is RSA. This cryptosystem is named after **R**ivest, **S**hamir and **A**dleman, the designers [9]. RSA is mathematically easily to understand. The security of RSA is dependent on the factorization of integers into primes. Factorization is still a hard task if the numbers are big enough and well chosen, so the system is quite secure at the moment. RSA uses a secret key and a public key, which have to be unique per person. This secret key is only known to the sender. RSA consists out of two algorithms, one for signing the message and one for encrypting the message. These can use the same key and implementation. The verification of signatures with RSA can be done fairly fast, with a lot of ECDSA (Elliptic curve digital signature algorithm) verifications per second (To refresh your memory on RSA, read [9]).

Another cryptosystem is Elliptic Curve Cryptography (ECC). The security of ECC is dependent on the assumption that finding the discrete logarithm of a random elliptic curve element with respect to a publicly known base point is hard. The entire security is based on the ability to compute a point multiplication and the inability to compute the multiplicand, given the original and product points. There are shorter keys for ECC which are just as secure as the longer keys for RSA. Another good property of ECC is that it uses a lot less CPU power and memory than RSA. So it takes less space and is faster.

Third, we can use different kind of shapes with the same operations and the code can be widely optimized if we stick to a specific shape known when the code was written. There is no security issue in using the same curve for many distinct people with distinct key pairs. Unfortunately, the mathematics is a lot more complicated than RSA and there can be done a lot less ECDSA verifications per second. Fortunately, public-key operations are rarely a bottleneck and more than enough verifications can be done. More information on the comparison between RSA and ECC can be found in [12].

When we compare RSA to ECC, we see that ECC the advantage that we can use shorter keys, use less memory and a lot less CPU power. But because the patents of RSA have expired and those of ECC have not, legally speaking it is easier to use RSA than ECC. We can do more signature verifications for RSA than for ECC. But fortunately, public key operations are rarely a bottleneck and ECC can still do a lot of verifications per second. And although the mathematics for ECC are harder than on RSA, implementation is hard for both algorithms.

At the moment there is a lot of political push for the adoption of elliptic curves in cryptography, by both academic researchers and institutional organizations. For instance, Google uses ECC and the German government uses ECC in their passports. In the US, ECC is the only supported algorithm for government applications.

1.3 Why different kinds of curves?

In mathematics, we have a lot of shapes of elliptic curves. All these shapes have a lot of different properties. On some we can do faster addition and on some others point counting is easier. Also, some curves are more secure against certain types of attacks, such as side channel attacks (SCA). Luckily, transforming one elliptic curve into a different elliptic curve appears not to be too hard. In chapter 4, I will transform a Weierstrass curve into a quartic elliptic curve and back.

We have a standard form for elliptic curves, the Weierstrass equation, see chapter 2. On this curve, point counting already has been defined, whilst this is not yet done for Jacobi curves, see chapter 3. So when we transform a Jacobi curve to a Weierstrass curve, we can count the points and output this as an answer.

Next to this, we know that Jacobi curves are safer from the simple and differential power analysis style (SPA and DPA, respectively) attacks of side-channel attacks (SCA), because the addition formulae can be used for doubling. This is not possible on a Weierstrass curve, this can be read in chapter 2.1 and chapter 2.2. Because of the fact that doubling and adding is the same on the Jacobi quartic, it has unified point addition formulae. This is explained in [1].

We also know that arithmetic operations, such as addition and doubling, are a lot faster on Jacobi curves than on Weierstrass curves. When we start on a Jacobi quartic, because it has all these nice properties, we want everybody to use this. But sometimes there still are people who use Weierstrass curves. If we then want to compare if the speed of adding and doubling on a Jacobi quartic is that much faster, even for the ones using the Weierstrass curves, we need to add the time to transform from Weierstrass curves to Jacobi curves and back.

Chapter 2

Weierstrass curves

When speaking of elliptic curves, the most general elliptic curve shape is the Weierstrass curve E, here given in its affine form:

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

The coefficients a_i are in a field K and $E_W(K)$ denotes the set of all solutions $(x, y) \in K \times K$, together with the point P_∞ "at infinity", defined as the neutral element of this group of points. One of the properties of Weierstrass curves is that if a line intersects two points, it will intersect a third one (counting with multiplicity). So if we have a line that is tangent to the curve, it will have to go through a third. But this is not generally the case when we just draw the curve. For this, we need the point at infinity. This is needed for addition and doubling, see section 2.1 and section 2.2, respectively.

We can think of the Weierstass curve as the equation being in a graded ring, where x has weight 2, y has weight 3 and a_i has weight i. In this way, every term in the equation has weight 6. We require the curve to be non-singular, geometrically, this means that the graph has no cusps, self-intersections or isolated points. A slightly more abstract definition for elliptic curves is: "a plane nonsingular cubic with a distinguished rational point". This means that there are points defined over the field K. This does not refer to the rational field $\mathbb{Q}$, unless $K = \mathbb{Q}$.

If we have a field K with $\text{char}(K) \neq 2$ or 3, we can transform the curve into the short Weierstrass form. For a field of $\text{char}(K) \neq 2$ we can use computations to transform the equation in the Weierstrass normal form, which looks like this:

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

In this equation $a_1 = a_3 = 0$. This is done as follows: we put $\eta = y + \frac{(a_1 x + a_3)}{2}$ in the equation and complete the square. This yields:

$$\eta^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}$$

with $b_2 = a_1^2 + 4a_2, b_4 = a_1 a_3 + 2a_4$ and $b_6 = a_3^2 + 4a_6$. Now, if we have a field with $\mathrm{char}(K) \neq 3$ (and, of course, still $\mathrm{char}(K) \neq 2$), we can transform the curve to the short Weierstrass form, with the subsitution $\zeta = x + \frac{b_2}{12}$. This yields us the short Weierstrass form:

$$\eta^2 = \zeta^3 - \frac{c_4}{48}\zeta - \frac{c_6}{864}$$

with $c_4 = b_2^2 - 24b_4$ and $c_6 = -b_2^3 + 36b_2 b_4 - 216b_6$.

For curves in Weierstrass form the computeralgebra system Sage[1] has implementation for addition, computing the j-invariant, listing all points, counting points and computing the characteristic polynomial. These are properties we do not have in Sage for other elliptic curves. So we use a mapping from any other elliptic curve to the Weierstrass curve, calculate and use a mapping from the Weierstrass curve to any other elliptic curve if necessary. But not every elliptic curve has an isomorphism with the Weierstrass curve. Fortunately, this is not needed. Only a birational equivalence (for more information, read [4]) is enough for these mappings to exist. We have a birational equivalence when we have a rational transformation $\phi : E \to E'$ and its rational inverse $\psi : K' \to K$. These maps need not be defined for all points on E and E', but they should be each others inverses when defined and they should preserve the group structure of the elliptic curve. Also there should be only finitely many failure cases.

[1] Sage is a free open-source mathematics software system licensed under the GPL. It combines the power of many existing open-source packages into a common Python-based interface. For more information go to www.sagemath.org.

2.1 Addition on Weierstrass curves

In the beginning of this chapter, we have seen the following curve:

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

With the coefficients a_i in a field K and $E_W(K)$ denotes the set of all solutions $(x, y) \in K \times K$, together with the point P_∞ "at infinity", defined as the neutral element of this group of points. We now want to turn the set of points E_W into a group with the group operation "point addition" denoted by $\oplus$. This is illustrated by the following picture over the reals:

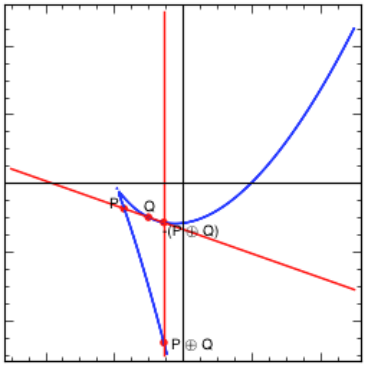

Figure 2.1: Addition on a Weierstrass curve

To add two points $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ in general one draws a line connecting them. There is a third point of intersection. Finding the other point with the same x-coordinate gives the sum $P \oplus Q$. The same construction can be applied to double a point, where the connecting line is replaced by the tangent at P, see section 2.2.

We also need to define the sum of two points with the same x-coordinate, since for them the group operation cannot be performed as stated. As $y^2 + a_1xy + a_3y = f(x)$ there are at most 2 such points (x_P, y_P) and $(x_P, -y_P - a_1x - a_3)$. Furthermore, we have to find the neutral element of the group.

The way out is to include a further point P_∞, called the "point at infinity". It can be visualized as lying really far out on the y-axis, such that any line $x = c$ for some constant c, parallel to the y-axis passes through it. This point is the neutral element of the group. Hence, the line connecting (x_P, y_P) and $(x_P, -y_P - a_1x - a_3)$ passes through P_∞, see picture 2.2. As it serves as the neutral element, we know that $(x_P, y_P) \oplus (x_P, -y_P - a_1x - a_3) = P_\infty$, i.e. $(x_P, -y_P - a_1x - a_3) = -P$. This is illustrated by the picture below.

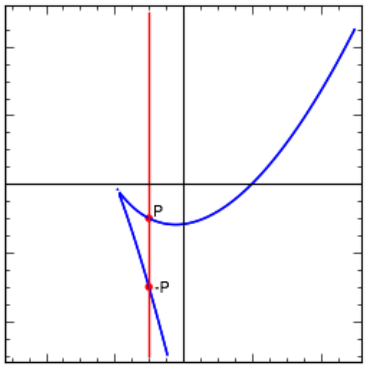

Figure 2.2: Inverse points on a Weierstrass curve

Now we derive the addition formula for an arbitrary field K. Take $P \neq Q$, with $x_P \neq x_Q$ and let us compute the coordinates of $R = P \oplus Q = (x_R, y_R)$:

$$\lambda = \frac{y_P - y_Q}{x_P - x_Q},$$

$$x_R = \lambda^2 + a_1\lambda - a_2 - x_P - x_Q,$$

$$y_R = \lambda(x_P - x_R) - y_P - a_1 x_R - a_3.$$

Where a_1, a_2 and a_3 are the curve coefficients in front of xy, x^2 and y, respectively, in our elliptic field and λ is the slope between point P and point Q. These addition formulae can be found in [2, 10, 6].

2.2 Doubling on Weierstrass curves

Now remains the question how to add a point to itself. The formulas above cannot be used, for they use the slope of the line between the two different points. Since we are adding P to P and thus create $2P = (x_{2P}, y_{2P})$, we need to find the line joining P to P. This is illustrated by the following picture:

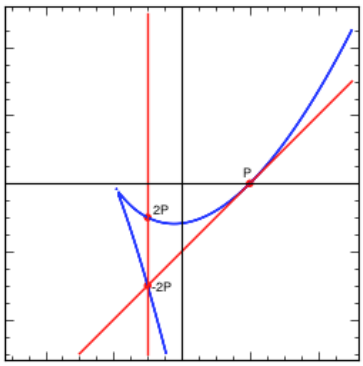

Figure 2.3: Doubling on a Weierstrass curve

Well, from the recipe above it follows that the line connecting P to P is the tangent line to the cubic at P. From the relation $y^2 + (a_1x + a_3)y = f(x)$ we find by implicit differentiation that

$$\lambda := \frac{dy}{dx} = \frac{f'(x_P)}{2y_P + a_1x + a_3} = \frac{3x_P^2 + 2a_2x_P + a_4 - a_1y_P}{2y_P + a_1x_P + a_3},$$

and this is the λ we will use to double a point. The formulas for x_{2P} and y_{2P} are as follows:

$$x_{2P} = \lambda^2 + a_1\lambda - a_2 - 2x_P,$$
$$y_{2P} = \lambda(x_P - x_{2P}) - y_P - a_1x_{2P} - a_3.$$

So we can also denote addition and doubling in one notation, if $P \neq P_\infty$ and $P \neq -Q$:

$$\lambda = \begin{cases} \frac{y_P - y_Q}{x_P - x_Q} & \text{if } P \neq \pm Q \\ \frac{dy}{dx} = \frac{3x_P^2 + 2a_2x_P + a_4 - a_1y_P}{2y_P + a_1x_P + a_3} & \text{if } P = Q \end{cases}$$
$$x_R = \lambda^2 + a_1\lambda - a_2 - x_P - x_Q,$$
$$y_R = \lambda(x_P - x_R) - y_P - a_1x_R - a_3.$$

Here a_1, a_2 and a_3 are the coefficients in front of xy, x^2 and y, respectively, in our elliptic curve and λ is the slope. If $P = P_\infty$, we have that $R = P \oplus Q = Q$. If $P = -Q$, we have that $R = P \oplus Q = -Q \oplus Q = P_\infty$, the neutral element. The doubling formulae can be found in [2, 10, 6].

2.3 Example over $\mathbb{Q}$

Now we have the Weierstrass curve $y^2 + 4xy + 8y = x^3 + 2x^2 - 4x - 8$ over $\mathbb{Q}$. We want to find a point on the curve. We choose for $x = -1$ and fill this in:

$$y^2 - 4y + 8y = -1 + 2 + 4 - 8,$$
$$y^2 + 4y + 3 = 0,$$
$$y = -1 \wedge y = -3.$$

We pick the point $(-1, -1)$ for our calculations. We do the same for $x = -2$ and $x = 2$ and find $(-2, 0), (2, 0)$ and $(2, 16)$.

Now we want to add the points $(x_P, y_P) = (-1, -1)$ and $(x_Q, y_Q) = (-2, 0)$. First we calculate λ:

$$\lambda = \frac{y_P - y_Q}{x_P - x_Q} = \frac{-1 - 0}{-1 - (-2)} = -1.$$

Now we calculate our (x_R, y_R):

$$x_R = \lambda^2 + a_1\lambda - a_2 - x_P - x_Q = (-1)^2 + 4 \cdot (-1) - 2 - (-1) - (-2) = -2,$$
$$y_R = \lambda(x_P - x_R) - y_P - a_1 x_R - a_3 = -1 \cdot (-1 - (-2)) - (-1) - 4 \cdot (-2) - 8 = 0.$$

So we see that adding $(-1, -1)$ to $(-2, 0)$ yields the point $(-2, 0)$.

Now we want to double the point $(x_S, y_S) = (2, 0)$. We first calculate the matching λ:

$$\lambda = \frac{3x_P^2 + 2a_2 x_P + a_4 - a_1 y_P}{2y_P + a_1 x_P + a_3} = \frac{16}{16} = 1.$$

Then we calculate x_{2S} and y_{2S}:

$$x_{2S} = \lambda^2 + a_1\lambda - a_2 - 2x_P = -1,$$
$$y_{2S} = \lambda(x_P - x_{2S}) - y_P - a_1 x_{2S} - a_3 = -1.$$

And we see that the doubling of $(x_S, y_S) = (2, 0)$ ends up in $(x_P, y_P) = (-1, -1)$.

2.4 Example over $\mathbb{Z}/17\mathbb{Z}$

Now we have the Weierstrass curve $y^2 = x^3 + 11x^2 + 2x + 5$ over $\mathbb{Z}/17\mathbb{Z}$. We want to find a point on the curve. We choose for $x = 1$ and substitute:

$$y^2 \equiv 1 + 11 + 2 + 5 \mod 17,$$
$$y^2 \equiv 2 \mod 17,$$
$$y \equiv 6 \mod 17 \wedge y \equiv 11 \mod 17.$$

We pick the point $(1, 6)$ for our calculations. We do the same for $x = 4$ and $x = 12$. We find the points $(4, 7), (4, 10), (12, 3)$ and $(12, 14)$.

We want to add the points $(x_P, y_P) = (4, 7)$ and $(x_Q, y_Q) = (1, 6)$. First we calculate λ with the help of the Extended Euclidean Algorithm:

$$\lambda \equiv \frac{y_P - y_Q}{x_P - x_Q} \equiv \frac{10 - 6}{4 - 1} \equiv \frac{4}{3} \equiv 7 \mod 17.$$

Now we calculate our (x_R, y_R):

$$x_R \equiv \lambda^2 + a_1\lambda - a_2 - x_P - x_Q \equiv 7^2 + 0 \cdot 7 - 11 - 4 - 1 \equiv 16 \mod 17,$$
$$y_R \equiv \lambda(x_P - x_R) - y_P - a_1 x_R - a_3 \equiv 7 \cdot (4 - 16) - 10 - 0 - 0 \equiv 8 \mod 17.$$

So we see that adding $(4, 7)$ to $(1, 6)$ yields the point $(16, 8)$.

Now we want to double the point $(x_S, y_S) = (12, 3)$. We first calculate the matching λ:

$$\lambda = \frac{3x_P^2 + 2a_2x_P + a_4 - a_1y_P}{2y_P + a_1x_P + a_3} \equiv \frac{1}{6} \equiv 3 \mod 17.$$

Then we calculate x_{2S} and y_{2S}:

$$x_{2S} = \lambda^2 + a_1\lambda - a_2 - 2x_P \equiv 3^2 + 0 \cdot 3 - 11 - 2 \cdot 12 \equiv 8 \mod 17,$$
$$y_{2S} = \lambda(x_P - x_{2S}) - y_P - a_1x_{2S} - a_3 \equiv 3 \cdot (12 - 3) - 3 - 0 - 0 \equiv 9 \mod 17.$$

And we see that the doubling of $(x_S, y_S) = (12, 3)$ ends up in $(x_P, y_P) = (8, 9)$.

Chapter 3

Jacobi Quartics

Another shape of elliptic curves are the Jacobi quartics, here given in its affine form:

$$E_J : v^2 = au^4 + cu^2 + q^2$$

where we require $a(\frac{1}{4}c^2 - a) \neq 0$, so it is non-singular, and a, c and q are in a field K. There are two points at infinity, which can be obtained as the blow up of $(0 : 1 : 0)$ in projective coördinates. $E(K)$ denotes the set of all solutions $(u, v) \in K \times K$. The field K has $\text{char}(K) \neq 2$ or 3.

For most uses, the form

$$v^2 = a'u^4 + c'u^2 + 1$$

is more convenient. This is easily accomplished by dividing all the constants by q^2 and renaming $a' = \frac{a}{q^2}$ and $c' = \frac{c}{q^2}$. We will use this form for addition and doubling of points.

3.1 Addition on Jacobi Quartics

Addition on Jacobi Quartics is also point addition, same as for Weierstrass curves, see section 2.1. In this case we add a point $P = (u_P, v_P)$ to a point $Q = (u_Q, v_Q)$ and we gain point $R = (u_R, v_R)$, using the formulas below:

$$u_R = \frac{u_P v_Q + v_P u_Q}{1 - a(u_P u_Q)^2},$$

$$v_R = \frac{(1 + a(u_P u_Q)^2)(v_P v_Q + c u_P u_Q) + 2a u_P u_Q (u_P^2 + u_Q^2)}{(1 - a(u_P u_Q)^2)^2},$$

where a and c are the coefficients in front of u^4 and u^2, respectively, in our elliptic curve. The identity element becomes the point $(0, 1)$. The negative of a point (u, v) is $(-u, v)$. The point $(0, -1)$ is of order 2. These are generally defined formulas, such that an attacker cannot see the difference between addition and doubling[2, 5, 8].

We want to show that for every curve with a point $P = (u_P, v_P)$, that $P + (0, 1) = P$. We put this into the formulae:

$$u_R = \frac{u_P + 0}{1 - 0} = u_P,$$

$$v_R = \frac{(1 + 0)(v_P + 0) + 0}{(1 - 0)^2} = v_P,$$

and we see that we indeed end up in $P = (u_P, v_P)$. We also want to show that for every curve we have $P + (-P) = (u_P, v_P) + (-u_P, v_P) = (0, 1)$. We once more plug this in the formulae:

$$u_R = \frac{u_P v_P - v_P u_P}{1 - a(-u_P u_P)^2} = 0,$$

$$v_R = \frac{(1 + a(-u_P u_P)^2)(v_P v_P - c u_P u_P) - 2a u_P u_P (u_P^2 + (-u_P)^2)}{(1 - a(-u_P u_P)^2)^2} = \frac{(1 + a u_P^2)(v_P^2 - c u_P^2) - 4a u_P^4}{(1 - a u_P^2)^2}.$$

We plug in $v_P^2 = a u_P^4 + c u_P^2 + 1$ in v_R:

$$v_R = \frac{(1 + a u_P^2)(a u_P^4 + c u_P^2 + 1 - c u_P^2) - 4a u_P^4}{(1 - a u_P^2)^2} = \frac{(1 + a u_P^2)(a u_P^4 + 1) - 4a u_P^4}{(1 - a u_P^2)^2} =$$

$$\frac{1 + 2a u_P^2 + a^2 u_P^8 - 4a u_P^4}{(1 - a u_P^2)^2} = \frac{1 - 2a u_P^2 + a^2 u_P^8}{(1 - a u_P^2)^2} = 1,$$

and we see that we end up in $(0, 1)$. So we see that $(0, 1)$ is indeed the identity element.

3.2 Doubling on Jacobi Quartics

We know that usually $1 - au_P^4 \neq 0$, so the addition formulae work for $Q = P$. If we try to use the above formulae for doubling, we get:

$$u_{2P} = \frac{u_P v_P + u_P v_P}{1 - a(u_P u_P)^2} = \frac{2u_P v_P}{1 - au_P^4},$$

$$v_{2P} = \frac{(1 + a(u_P u_P)^2)(v_P v_P + cu_P u_P) + 2au_P u_P(u_P^2 + u_P^2)}{(1 - a(u_P u_P)^2)^2} = \frac{(1 + au_P^4)(v_P^2 + cu_P^2) + 4au_P^4}{(1 - au_P^4)^2}.$$

where a and c are the multiplication factors in front of u^4 and u^2, respectively, in our elliptic field. These formulae for addition and doubling can be found in [2, 8].

3.3 Example over $\mathbb{Q}$

We have the Jacobi quartic $v^2 = 2u^4 + 6u^2 + 1$ over $\mathbb{Q}$. First we check whether or not the condition $a(\frac{1}{4}c^2 - a) \neq 0$ holds. We see that $2 \cdot (\frac{1}{4} \cdot 6^2 - 2) = 2 \cdot (9 - 2) \neq 0$, so the condition holds. We want to add point $(u_P, v_P) = (1, 3)$ and $(u_Q, v_Q) = (0, 1)$:

$$u_R = \frac{1 + 0}{1 - 2 \cdot (0)^2} = 1,$$

$$v_R = \frac{(1 + 2 \cdot (0)^2)(3 + 0) + 0}{(1 - 2 \cdot (0)^2)^2} = 3.$$

So we end up in the point $(1, 3)$.

Now we want to double the point $(u_S, v_S) = (-1, 3)$:

$$u_{2S} = \frac{-6}{-1} = 6,$$

$$v_{2S} = \frac{53}{1} = 53.$$

And we see that we end up in $(u_{2S}, v_{2S}) = (6, 53)$.

3.4 Example over $\mathbb{Z}/17\mathbb{Z}$

We have the Jacobi quartic $v^2 = 8u^4 + 11u^2 + 1$ over $\mathbb{Z}/17\mathbb{Z}$. First we check whether or not the condition $a(\frac{1}{4}c^2 - a) \neq 0$ holds. We see that $8 \cdot (\frac{1}{4} \cdot 11^2 - 8) \neq 0$, so the condition holds. We want to add point $(u_P, v_P) = (3, 0)$ and $(u_Q, v_Q) = (4, 7)$:

$$u_R \equiv \frac{3 \cdot 7 + 4 \cdot 0}{1 - 8 \cdot (3 \cdot 4)^2} \equiv \frac{4}{5} \equiv 11 \mod 17,$$

$$v_R \equiv \frac{(1 + 8 \cdot (3 \cdot 4)^2)(0 \cdot 7 + 11 \cdot 3 \cdot 4) + 2 \cdot 8 \cdot 3 \cdot 4 \cdot (3^3 + 4^2)}{(1 - 8 \cdot (3 \cdot 4)^2)^2} \equiv \frac{1}{8} \equiv 15 \mod 17.$$

So we end up in $(11, 15)$.

Now we want to double the point $(u_S, v_S) = (4, 10)$:

$$u_{2S} \equiv \frac{12}{10} \equiv 8 \mod 17,$$

$$v_{2S} \equiv \frac{0}{15} \equiv 0 \mod 17.$$

And we see that we end up in $(u_{2S}, v_{2S}) = (8, 0)$.

3.5 Special Jacobi Quartic

We have a special kind of Jacobi Quartic, namely:

$$E_s : v^2 = u^4 + 2c_0u^2 + 1$$

where we require $c_0^2 \neq 1$ and c_0 is in a field K. There are two points at infinity, which can be obtained as the blow up of $(0 : 1 : 0)$ in projective coördinates. $E(K)$ denotes the set of all solutions $(u, v) \in K \times K$. The field K has $\text{char}(K) \neq 2$ or 3.

This curve has the fastest addition we know of (we can have 2M + 5S with the right parameterization, see [7] for more information). So it is quite handy to map to this curve, add (or double) on this curve and then map back to the original curve. This curve is also a safe curve against SPA and SCA attacks. For more on this, see [7].

3.5.1 Addition

Addition on this curve is the same as on the general Jacobi Quartics, but simplified with $a = 1$, and looks like this:

$$u_R = \frac{u_P v_Q + v_P u_Q}{1 - (u_P u_Q)^2},$$
$$v_R = \frac{(1 + (u_P u_Q)^2)(v_P v_Q + 2c_0 u_P u_Q) + 2u_P u_Q(u_P^2 + u_Q^2)}{(1 - (u_P u_Q)^2)^2}.$$

Where c_0 is the coefficient in front of u^2, in our elliptic curve.

3.5.2 Doubling

And also for the doubling holds that it is the same as on the other Jacobi Quartics:

$$u_{2P} = \frac{2u_P v_P}{1 - u_P^4},$$
$$v_{2P} = \frac{(1 + u_P^4)(v_P^2 + 2c_0 u_P^2) + 4u_P^4}{(1 - u_P^4)^2}.$$

These formulae for addition and doubling can be found in [7].

3.5.3 Example over $\mathbb{Q}$

Now we have the curve $v^2 = u^4 + 8u^2 + 1$ in $\mathbb{Q}$ and we want to add two points together, namely $(u_P, v_P) = (2, 7)$ and $(u_Q, v_Q) = (-2, 7)$. First we check if they are on the curve:

$$49 = 16 + 8 \cdot 4 + 1$$

and see that the points are on the curve. We calculate (u_R, v_R) as follows:

$$u_R = \frac{u_P v_Q + v_P u_Q}{1 - (u_P u_Q)^2} = \frac{0}{-15} = 0,$$
$$v_R = \frac{(1 + (u_P u_Q)^2)(v_P v_Q + 8u_P u_Q) + 2u_P u_Q(u_P^2 + u_Q^2)}{(1 - (u_P u_Q)^2)^2} = \frac{225}{225} = 1.$$

And we see that we end up in $(u_R, v_R) = (0, 1)$.

Now we want to double the point $(u_S, v_S) = (0, -1)$. We calculate this as follows:

$$u_{2S} = \frac{2u_P v_P}{1 - u_P^4} = 0,$$
$$v_{2S} = \frac{(1 + u_P^4)(v_P^2 + 8u_P^2) + 4u_P^4}{(1 - u_P^4)^2} = 1.$$

And we see that we end up in $(u_{2S}, v_{2S}) = (0, 1)$. $(0, -1)$ appears to be a point of order 2.

3.6 Example over $\mathbb{Z}/17\mathbb{Z}$

Now we have the curve $v^2 = u^4 + 10u^2 + 1$ in $\mathbb{Z}/17\mathbb{Z}$ and we want to add two points together, namely $(u_P, v_P) = (3, 6)$ and $(u_Q, v_Q) = (4, 3)$. We calculate (u_R, v_R) as follows:

$$u_R \equiv \frac{u_P v_Q + v_P u_Q}{1 - (u_P u_Q)^2} \equiv \frac{16}{10} \equiv 5 \mod 17,$$
$$v_R \equiv \frac{(1 + (u_P u_Q)^2)(v_P v_Q + 8u_P u_Q) + 2u_P u_Q(u_P^2 + u_Q^2)}{(1 - (u_P u_Q)^2)^2} \equiv \frac{6}{15} \equiv 14 \mod 17.$$

And we see that we end up in $(u_R, v_R) = (5, 14)$.

Now we want to double the point $(u_S, v_S) = (3, 11)$. We calculate this as follows:

$$u_{2S} \equiv \frac{2u_P v_P}{1 - u_P^4} \equiv \frac{15}{5} \equiv 3 \mod 17,$$
$$v_{2S} \equiv \frac{(1 + u_P^4)(v_P^2 + 8u_P^2) + 4u_P^4}{(1 - u_P^4)^2} \equiv \frac{14}{8} \equiv 6 \mod 17.$$

And we see that we end up in $(u_{2S}, v_{2S}) = (3, 6)$.

Chapter 4

Quartic curves to Weierstrass curves

In the first part of this chapter we are going to examine the transformation from Weierstrass curves into quartic curves and the transformation from quartic curves to Weierstrass curves. We want to know if there are certain conditions on E, such that it can be represented, and if it is possible if the addition and doubling laws are compatible with the map, which will be examined in the second part of the chapter. The mapping will be more general than the addition and doubling, because the addition and doubling for the general Jacobi quartics are not known yet. These can easily be calculated by symbolically using the addition on the Weierstrass curve and transforming the results back to the Jacobi quartic, but I have chosen not to do so, because the formulae tend to get very long. This can be done in a future paper. The diagram below illustrates the mapping, where P_1 is the starting point, P_2 is the end point, C_1 is the Jacobi quartic, C_2 is the Weierstrass curve and $\phi(P_1)$ and $\phi(P_2)$ are the transformed points:

$$\begin{array}{ccc} P_1/C_1 & \xrightarrow{\text{Transformation to Weierstrass curve}} & \phi(P_1)/C_1 \\ \Big\downarrow \text{Addition/doubling on Jacobi curve} & & \Big\downarrow \text{Addition/doubling on Weierstrass curve} \\ P_2/C_1 & \xrightarrow[\text{Transformation to Weierstrass curve}]{} & \phi(P_2)/C_2 \end{array}$$

4.1 From quartic curves to Weierstrass curves

If K is a field, K^* denotes the multiplicative group and $\overline{K}$ denotes an algebraic closure. Let K be a field of characteristic $\neq 2$, and consider the curve defined by an equation over K of the form $v^2 =$ a quartic polynomial in u with a rational point $P = (u_P, v_Q)$. If we replace u by $u + u_P$ we can assume $u_P = 0$, and create the following curve with $v_Q^2 = q^2$:

$$E_Q : v^2 = au^4 + bu^3 + cu^2 + du + q^2.$$

Such a curve is birationally equivalent to a curve given by a Weierstrass equation. To prove this, we use the following proposition, which can be found in [3]:

Proposition 4.1.1 *Let K be a field with char(K) $\neq 2$ and u, v trancendentals over K satifying*

$$v^2 = au^4 + bu^3 + cu^2 + du + q^2,$$

where $a, b, c, d \in K$ and $q \in K^*$. Then

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

satisfy the Weierstrass equation with

$$a_1 = \frac{d}{q}, \qquad a_2 = c - \frac{d^2}{4q^2},$$
$$a_3 = 2qb, \qquad a_4 = -4q^2a,$$

$$a_6 = a_2a_4 = a(d^2 - 4q^2c).$$

The inverse transformation is given by

$$u = \frac{2q(x+c) - \frac{d^2}{2q}}{y} \text{ and } v = -q + \frac{u(ux - d)}{2q}.$$

In this birational correspondence, the point $(u, v) = (0, -q)$ *on the curve* $v^2 = au^4 + bu^3 + cu^2 + du + q^2$ *corresponds to the point* $(x, y) = (-a_2, a_1a_2 - a_3)$ *on the Weierstrass curve and the point* $(u, v) = (0, q)$ *on the curve* $v^2 = au^4 + bu^3 + cu^2 + du + q^2$ *corresponds to the point at infinity on the Weierstrass curve.*

Proof: The proof of the transformation for any point, except for $(0, q)$ and $(0, -q)$, can be found in appendix A. This chapter contains the code that shows us the transformations are right.

To obtain the image of $(0, -q)$, one cannot simply substitute $u = 0$ and $v = -q$ in the formulas for x and y, for this yields the undetermined form $\frac{0}{0}$. L'Hôpital's rule gives us the quickest way to obtain the answer: we differentiate the numerator and denominator of x twice with respect to u, and those of y three times, using $\frac{dv}{du} = \frac{(4au^3+3bu^2+2cu+d)}{2v}$ obtained by differentiating $v^2 = au^4 + bu^3 + cu^2 + du + q^2$. Note that this only works for curves in $\mathbb{R}$ and $\mathbb{C}$. Then cancel the common factors, such as 3! from the numerator and denominator of the resulting fractions. The validity of the method for all K with $\mathrm{char}(K) \neq 2$ depends on the fact that the functions have perfectly usable Taylor expansions. This means that there is no problem with factorials in denominators. These Taylor expansions are most easily described in the field of formal power series as follows.

Regard u as an indeterminate and use that the field of rational functions $K(u)$ is a subfield of the field $K((u))$ of formal power series, i.e., series of the form $\sum_N^\infty k_n u^n$ for some $N \in \mathbb{Z}, k_n \in K$. Now $v^2 = au^4 + bu^3 + cu^2 + du + q^2$ defines a quadratic extension $L = K(u)(v)$ of $K(u)$ and there are two embeddings $\phi : L \to K((u))$ corresponding to the two square roots of $au^4 + bu^3 + cu^2 + du + q^2$. We pick

$$\begin{aligned}\phi(v) &= -q(1 + \frac{d}{q^2}u + \frac{c}{q^2}u^2 + \frac{b}{q^2}u^3 + \frac{a}{q^2}u^4)^{\frac{1}{2}} \\ &= -q - \frac{d}{2q}u + \Big[\frac{d^2}{8q^3} - \frac{c}{2q}\Big]u^2 + \cdots .\end{aligned}$$

Since q is nonzero in our field, all its powers are nonzero too.

Regrouping and substitution yields:

$$\begin{aligned}x &= \Big[\frac{d^2}{4q^2} - c\Big] + \Big[\frac{-d^3}{8q^4} - \frac{cd}{2q^2} - b\Big]u + \cdots , \\ y &= \Big[\frac{-d^3}{4q^3} + \frac{cd}{q} - 2bq\Big] + \Big[\frac{5d^4}{32q^5} - \cdots\Big]u + \cdots .\end{aligned}$$

When $u = 0$ we get

$$x = \frac{d^2}{4q^2} - c,$$
$$y = \frac{-d^3}{4q^3} + \frac{cd}{q} - 2bq = \frac{d}{q}(c - \frac{d^2}{4q^2}) - 2qb.$$

Now we fill in the expressions for the coefficients of the Weierstrass curve and see that these expressions reduce to $x = -a_2$ and $y = a_1a_2 - a_3$.

We can do the same for the other square root of $au^4 + bu^3 + cu^2 + du + q^2$. This yields:

$$\begin{aligned}\phi(v) &= q(1 + \frac{d}{q^2}u + \frac{c}{q^2}u^2 + \frac{b}{q^2}u^3 + \frac{a}{q^2}u^4)^{\frac{1}{2}} \\ &= q - \frac{d}{2q}u + \Big[\frac{d^2}{8q^3} - \frac{c}{2q}\Big]u^2 + \cdots .\end{aligned}$$

Since q is nonzero in our field, all its powers are nonzero too. Thus this is a valid statement.

Regrouping and substitution yields:

$$\begin{aligned}x &= \frac{2q}{u^2} + \Big[\frac{d^2}{4q^2} - c\Big] + \Big[\frac{-d^3}{8q^4} - \frac{cd}{2q^2} - b\Big]u + \cdots , \\ y &= \frac{2q}{u^3} + \Big[\frac{-d^3}{4q^3} + \frac{cd}{q} - 2bq\Big] + \Big[\frac{5d^4}{32q^5} - \cdots\Big]u + \cdots .\end{aligned}$$

For $u = 0$ we map the point to P_∞ on E_W. This can be motivated by taking the limit for $u \to 0$:

$$\begin{aligned}\lim_{u\to 0} x &= \lim_{u\to 0}(\frac{2q}{u^2} + \Big[\frac{d^2}{4q^2} - c\Big] + \Big[\frac{-d^3}{8q^4} - \frac{cd}{2q^2} - b\Big]u + \cdots) = \infty, \\ \lim_{u\to 0} y &= \lim_{u\to 0}(\frac{2q}{u^3} + \Big[\frac{-d^3}{4q^3} + \frac{cd}{q} - 2bq\Big] + \Big[\frac{5d^4}{32q^5} - \cdots\Big]u + \cdots) = \infty.\end{aligned}$$

So we end up in the point at ∞ on the Weierstrass curve. ■

Remarks: This proposition essentially covers all cases where $q \neq 0$, as we can indicate now by assuming some definitions and relying on some result that will be given later. Consider the following curve:

$$v^2 = au^4 + bu^3 + cu^2 + du + q^2$$

where at least on of the a, b is nonzero and the polynomial on the right has no repeated roots in $\overline{K}$. This curve is then birationally equivalent over K to a Weierstrass curve if and only if this curve has a rational point, which means that either

- there is an affine rational point $(u, v) = (u_P, v_P)$. We transform this to $(0, q)$. This means that either
  - (i) $q \neq 0$. This yields a function treated by the proposition above; or
  - (ii) $q = 0$: replace u by $\frac{1}{u}$ and v by $\frac{v}{u^2}$. This gives the function $\frac{v^2}{u^4} = \frac{a}{u^4} + \frac{b}{u^3} + \frac{c}{u^2} + \frac{d}{u}$. Now we multiply by u^4 to obtain an equation of the type dealt in (iv) below;
- or there is a rational place at ∞. This means that either
  - (iii) $a = q^2 \in K^{*2}$: there are two rational places at ∞: replace u by $\frac{1}{u}$ and v by $\frac{v}{u^2}$. This yields a function treated by the proposition above; or
  - (iv) $a = 0$: then the function is essentially already in Weierstrass form: take $u = \frac{x}{b}$ and $v = \frac{y}{b}$. When $e = q^2 \in K^{*2}$, this gives a Weierstrass equation different from that of the proposition. But this Weierstrass curve can be transformed into the the Weierstrass curve of the proposition, because they are isomorphic to each other.

When we look at the meaning of the inverse transformation we can see it as follows: if x, y satisfy the Weierstrass curve, then u, v defined as rational functions in x, y in the way stated above satisfy $v^2 = au^4 + bu^3 + cu^2 + du + q^2$.

Proposition 2 can also be applied in the reverse direction: given a point $Q_0 = (x_0, y_0)$ satisfying a Weierstrass equation E with order divisible by 4, one can write down an equation: $v^2 = au^4 + bu^3 + cu^2 + du + q^2$ as in the proposistion and birational transformations between E and this equation, such that Q_0 corresponds to $(0, -q)$. The first step is to transform the equation of E to a new Weierstrass equation E' whose coefficients satisfy $a'_6 = a'_2 a'_4$ and such that Q_0 is transformed to $(-a'_2, a'_1 a'_2 - a'_3)$ as in the proposition. We put this in a corollary, so referencing is easier.

Corollary 4.1.2 *Let K be a field of characteristic $\neq 2$, let E be a Weierstrass curve with coefficients $a_1, ..., a_6 \in K$ and let $Q = (x_0, y_0) \in E(K)$.*

(a) *Define*

$$x' = x + \frac{x_0 + a_2}{2}, \qquad\qquad y' = y + (y_0 + a_1 x_0 + a_3).$$

Then x', y' satisfy the Weierstrass equation with coefficients

$$\begin{aligned} a_1' &= a_1, \\ a_2' &= -\frac{3x_0 + a_2}{2} = -x_0', \\ a_3' &= -(\frac{2y_0 + a_1(5x_0 + a_2)}{2} + a_3) = -y_0' + a_1' a_2', \\ a_4' &= a_1 y_0 + \frac{a_1^2 + a_2}{2} x_0 + \frac{3x_0^2}{4} + a_1 a_3 - \frac{a_2^2}{4} + a_4, \\ a_6' &= a_2' a_4'. \end{aligned}$$

In terms of the new x', y'-coordinates,

$$Q_0 = (x_0', y_0') = (a_2', a_1' a_2' - a_3').$$

(b) *Define*

$$\begin{aligned} u &= \frac{2(x - x_0)}{y + y_0 + a_1 x_0 + a_3}, \\ v &= \frac{2x + x_0 + a_2}{4} u^2 - \frac{a_1}{2} u - 1. \end{aligned}$$

Then

$$v^2 = au^4 + bu^3 + cu^2 + du + 1,$$

where

$$a = -\frac{a_4'}{4}, \qquad b = \frac{a_3'}{2},$$
$$c = \frac{{a_1'}^2}{4} + a_2', \qquad d = a_1'.$$

The inverse transformations are

$$x = \frac{2(v+1) + du}{u^2} - \frac{x_0 + a_2}{2},$$
$$y = \frac{4(v+1) + 2(du + cu^2) - \frac{d^2u^2}{2}}{u^3} - (y_0 + a_1x_0 + a_3).$$

In this birational correspondence, Q_0 corresponds to the point $(u, v) = (0, -1)$ on $v^2 = au^4 + bu^3 + cu^2 + du + 1$.

Proof: The verification of (a) amounts to some easy calculations, see chapter A.1. The verification of (b) amounts to applying the formulas in the proposition where we have chosen $v_Q = 1$. There is no loss of generality in the proposition if we take $q = 1$. If we replace v with qv and divide by q^2 we have $v^2 = \frac{au^4}{q^2} + \frac{bu^3}{q^2} + \frac{cu^2}{q^2} + \frac{du}{q^2} + 1$. Which is equal to $v^2 = \frac{a}{q^2}u^4 + \frac{b}{q^2}u^3 + \frac{c}{q^2}u^2 + \frac{d}{q^2}u + 1$. If we rename $a' = \frac{a}{q^2}, b' = \frac{b}{q^2}, c' = \frac{c}{q^2}$ and $d' = \frac{d}{q^2}$. Then we have $v^2 = a'u^4 + b'u^3 + c'u^2 + d'u + 1$, which has the same form as the standard quartic elliptic curve, so we have no loss of generality. ■

4.2 Example over $\mathbb{Q}$

We start with the following quartic curve:

$$v^2 = u^4 + 4u^3 + 6u^2 + 4u + 1.$$

We then calculate x and y for a non-specific point (u, v):

$$x = \frac{2(2u + v + 1)}{u^2},$$
$$y = \frac{4(u^2 + u + v + 1)}{u^3}.$$

Now we calculate $a_1, ..., a_6$:

$$a_1 = \frac{4}{1} = 1, \qquad a_2 = 6 - \frac{16}{4} = 2,$$
$$a_3 = 2 \cdot 1 \cdot 4 = 8, \qquad a_4 = -4 \cdot 1 \cdot 1 = -4,$$

$$a_6 = a_2 a_4 = -8$$

and see that the curve $y^2 + 4xy + 8y = x^3 + 2x^2 - 4x - 8$ is the Weierstrass curve that should be birationally equivalent to our chosen quartic curve. To check this, we pick a point on the quartic curve, say $(-2, 1)$, calculate (x, y) and check if this lays on this curve.

$$x = \frac{2(2 \cdot -2 + 1 + 1)}{(-2)^2} = -1,$$
$$y = \frac{4((-2)^2 - 2 + 1 + 1)}{(-2)^3} = -1.$$

So we put $(-1, -1)$ in $y^2 + 4xy + 8y = x^3 + 2x^2 - 4x - 8$. Both sides give -3, so this point is on the Weierstrass curve and our transformation from a quartic curve to a Weierstrass curve was successful.

Now we also want to know if it works when we transform the Weierstrass curve back to a quartic curve. Now we pick the non-specific point (x, y) and calculate u and v:

$$u = \frac{2q(x+c) - \frac{d^2}{2q}}{y} = \frac{2(x+2)}{y},$$
$$v = -q + \frac{u(ux-d)}{2q} = -1 + \frac{u(ux-4)}{2}.$$

We now pick $(x, y) = (-1, -1)$ on the Weierstrass curve and put this in the equitations for u and v:

$$u = \frac{2(-1+2)}{-1} = -2,$$
$$v = -1 + \frac{-2(-2 \cdot -1 - 4)}{2} = 1,$$

which is the point we started with on the quartic curve.

4.3 Example over $\mathbb{Z}/17\mathbb{Z}$

We start with the following quartic curve with $b \equiv d \equiv 0 \mod 17$, which we also used in section 3.4:

$$v^2 = 8u^4 + 11u^2 + 1.$$

We then calculate x and y for a non-specific point (u, v):

$$x \equiv \frac{2(v+1)}{u^2} \mod 17,$$
$$y \equiv \frac{4(v+1) + 5 \cdot u^2}{u^3} \mod 17.$$

Now we calculate $a_1, ..., a_6$:

$$a_1 \equiv 0 \mod 17, \qquad a_2 \equiv 11 \mod 17,$$
$$a_3 \equiv 0 \mod 17, \qquad a_4 \equiv 2 \mod 17,$$

$$a_6 \equiv a_2 a_4 \equiv 5 \mod 17$$

and see that the curve $y^2 = x^3 + 11x^2 + 2x + 5$ is the Weierstrass curve that should be birationally equivalent to our chosen quartic curve. This is the curve we also have used in section 2.4.

Now we also want to know if it works when we transform the Weierstrass curve back to a quartic curve. Now we pick the non-specific point (x, y) and calculate u and v:

$$u \equiv \frac{2q(x+c) - \frac{d^2}{2q}}{y} \equiv \frac{2(x+11)}{y} \mod 17,$$
$$v \equiv -q + \frac{u(ux-d)}{2q} \equiv -1 + \frac{u(ux)}{2} \equiv 16 + \frac{u^2 x)}{2} \mod 17.$$

We now pick $(x, y) = (4, 10)$ on the Weierstrass curve and put this in the equitations for u and v:

$$u \equiv \frac{2(4+11)}{10} \equiv 3 \mod 17,$$
$$v \equiv 16 + \frac{3^2 \cdot 4)}{2} \equiv 0 \mod 17,$$

which is the point we started with on the quartic curve.

Since we are already using the curves from section 2.4 and section 3.4, we could also show with this example that the addition and doubling laws hold. In section 3.4 we added $(3, 0)$ to $(4, 7)$ and this yielded $(11, 15)$. We already have transformed the point $(3, 0)$ from the Jacobi curve into $(4, 10)$ on the Weierstrass curve. Now we need to transform $(4, 7)$:

$$x \equiv \frac{2(7+1)}{4^2} \equiv 1 \mod 17,$$
$$y \equiv \frac{4(7+1) + 5 \cdot 4^2}{4^3} \equiv 6 \mod 17$$

and see that we end up in $(1, 6)$. In section 2.4 we already added $(4, 10)$ to $(1, 6)$. This yielded $(16, 8)$. We now want to transform $(11, 15)$ to the Weierstrass curve to see if this is equal to $(16, 8)$:

$$x \equiv \frac{2(15+1)}{11^2} \equiv 16 \mod 17,$$
$$y \equiv \frac{4(15+1)+5\cdot 11^2}{11^3} \equiv 8 \mod 17.$$

So we see that addition ends up in the same point. Now we want to check if doubling a point on the Jacobi quartic and then transforming to the Weierstrass curve ends up in the same point as first transforming to the Weierstrass curve and then double. Doubling $(4, 10)$ on the Jacobi quartic yields $(8, 0)$, see section 3.4. So we transform $(4, 10)$ to the Weierstrass curve:

$$x \equiv \frac{2(10+1)}{4^2} \equiv 12 \mod 17,$$
$$y \equiv \frac{4(10+1)+5\cdot 4^2}{4^3} \equiv 3 \mod 17.$$

So this ends up in $(12, 3)$. We already doubled this point in section 2.4 and see that doubling yields $(8, 9)$. Now we transform $(8, 0)$ from the Jacobi quartic to the Weierstrass curve:

$$x \equiv \frac{2(0+1)}{8^2} \equiv 8 \mod 17,$$
$$y \equiv \frac{4(0+1)+5\cdot 8^2}{8^3} \equiv 9 \mod 17$$

and we see that we end up in $(8, 9)$. So the doubling laws also hold under the transformation.

Appendix A

Sage code

In this chapter the code can be found for checking the mapping and if adding and doubling works. These code snippets should be copy-pasted into Sage, if the reader would like to check the code. The first code snippet needed is the fastfrac snippet, this I found in the EFD [7]. After that comes the mapping snippet or the adding and doubling snippet. I found the general structure on which the code is based in the EFD [7].

A.1 Mapping

This code snippet gives us the initialization of the ring and checks if the mapping is correct. The output of the code is "True, True, True", which tells us that the mapping is correct.

```
1  def mynumerator(x):
2    if parent(x) == R:
3      return x
4    return numerator(x)
5
6  def isidentity(x):
7    return x.iszero()
8
9  # initializing the polynomial ring for the curve
10 R.<ua,ub,uc,ud,uq,uu1,uv1> = PolynomialRing(QQ,7,order='invlex')
11 I = R.ideal([
12   mynumerator((uv1^2)-(ua*uu1^4+ub*uu1^3+uc*uu1^2+ud*uu1+uq^2))])
13
14 # Jacobi coefficients
15 ua = fastfrac(ua)
16 ub = fastfrac(ub)
17 uc = fastfrac(uc)
18 ud = fastfrac(ud)
19 uq = fastfrac(uq)
20
21 # Jacobi variables
22 uu1 = fastfrac(uu1)
23 uv1 = fastfrac(uv1)
```

```
24
25  # Weierstrass coefficients
26  a0 = fastfrac(1)
27  a1 = fastfrac(ud/uq)
28  a2 = fastfrac(uc - ud^2/(fastfrac(4)*uq^2))
29  a3 = fastfrac(fastfrac(2)*uq*ub)
30  a4 = fastfrac(fastfrac(-4)*uq^2*ua)
31  a6 = fastfrac(a2*a4)
32
33  # Weierstrass variables stated in terms of Jacobi variables
34  xx1 = ((fastfrac(2)*uq*(uv1 + uq) + ud*uu1)/(uu1^2)).reduce().sreduce()
35  xy1 = ((fastfrac(4)*uq^2*(uv1+uq) + fastfrac(2)*uq*(ud*uu1 + uc*(uu1^2)) -
        ((ud^2*uu1^2)/(fastfrac(2)*uq)))/(uu1^3)).reduce().sreduce()
36
37  # Checking if the points are on the Weierstrass curve
38  print isidentity(a0*(xy1^2)+a1*(xx1*xy1)+a3*xy1-(xx1^3 + a2*xx1^2 + a4*xx1
        + a6))
39
40  # Checking if transformation back to Jacobi curve works
41  print isidentity(uu1-(((fastfrac(2)*uq*(xx1+uc)-ud^2/(fastfrac(2)*uq))/xy1
        )))
42  print isidentity(uv1-(fastfrac(-1)*uq+(uu1*(uu1*xx1-ud))/(fastfrac(2)*uq))
        )
```

Listing A.1: Code in Sage for checking the mapping

A.2 Addition and doubling

This part of the code is added to the code above to check whether or not adding on the quartic curve and then mapping to the Weierstrass curve gives the same as mapping from the quartic curve to the Weierstrass curve and then adding. It does the same for doubling. The output of the code is "True, True, True, True", which tells us that doing addition or doubling first and then map to the other curve is the same as first map to the other curve and then doing addition or doubling. This can only be checked for a certain kind of Jacobi curve, as stated before.

```
1   def mynumerator(x):
2     if parent(x) == R:
3       return x
4     return numerator(x)
5
6   def isidentity(x):
7     return x.iszero()
8
9   R.<ua,uc,uq,uu1,uv1,uu2,uv2> = PolynomialRing(QQ,7,order='invlex')
10  I = R.ideal([
11    mynumerator((uv1^2)-(ua*uu1^4+uc*uu1^2+1))
12  , mynumerator((uv2^2)-(ua*uu2^4+uc*uu2^2+1))
13  ])
```

```
14
15  # Jacobi coefficients
16  ua = fastfrac(ua)
17  ub = fastfrac(0)
18  uc = fastfrac(uc)
19  ud = fastfrac(0)
20  uq = fastfrac(1)
21
22  # Jacobi variables
23  uu1 = fastfrac(uu1)
24  uv1 = fastfrac(uv1)
25  uu2 = fastfrac(uu2)
26  uv2 = fastfrac(uv2)
27
28  # Weierstrass coefficients
29  a0 = fastfrac(1)
30  a1 = fastfrac(0)
31  a2 = fastfrac(uc)
32  a3 = fastfrac(0)
33  a4 = fastfrac(fastfrac(-4)*ua)
34  a6 = fastfrac(a2*a4)
35
36  # Weierstrass variabels
37  xx1 = ((fastfrac(2)*(uv1+fastfrac(1)))/(uu1^2)).reduce().sreduce()
38  xy1 = ((fastfrac(4)*(uv1+fastfrac(1)) + fastfrac(2)*uc*(uu1^2))/(uu1^3)).
        reduce().sreduce()
39
40  # Jacobi variables with addition
41  uu3 = (fastfrac((uu1*uv2 + uv1*uu2)/(fastfrac(1) - ua*(uu1*uu2)^2))).
        reduce().sreduce()
42  uv3 = (fastfrac(((fastfrac(1) + ua*(uu1*uu2)^2)*(uv1*uv2 + uc*uu1*uu2) +
        fastfrac(2)*ua*uu1*uu2*(uu1^2 + uu2^2))/((fastfrac(1) - ua*(uu1*uu2)^2)
        ^2))).reduce().sreduce()
43
44  # Jacobi variables with doubling
45  uu4 = (fastfrac((fastfrac(2)*uu1*uv1)/(fastfrac(1) - ua*uu1^4))).reduce().
        sreduce()
46  uv4 = (fastfrac(((fastfrac(1) + ua*uu1^4)*(uv1^2 + uc*uu1^2) + fastfrac(4)
        *ua*uu1^4)/((fastfrac(1) - ua*uu1^4)^2))).reduce().sreduce()
47
48  # Weierstrass variables stated in terms of Jacobi variables
49  xx2 = ((fastfrac(2)*(uv2+fastfrac(1)))/(uu2^2)).reduce().sreduce()
50  xy2 = ((fastfrac(4)*(uv2+fastfrac(1)) + fastfrac(2)*uc*(uu2^2))/(uu2^3)).
        reduce().sreduce()
51  xx3 = ((fastfrac(2)*(uv3+fastfrac(1)))/(uu3^2)).reduce().sreduce()
52  xy3 = ((fastfrac(4)*(uv3+fastfrac(1)) + fastfrac(2)*uc*(uu3^2))/(uu3^3)).
        reduce().sreduce()
53  xx4 = ((fastfrac(2)*(uv4+fastfrac(1)))/(uu4^2)).reduce().sreduce()
54  xy4 = ((fastfrac(4)*(uv4+fastfrac(1)) + fastfrac(2)*uc*(uu4^2))/(uu4^3)).
        reduce().sreduce()
55
```

```
56  # Addition on the Weierstrass curve and checking if it is the same as on
        the Jacobi curve
57  slope = ((xy1 - xy2)/(xx1 - xx2)).reduce().sreduce()
58  print isidentity(xx3 - (slope^2 + a1*slope - a2 - xx1 - xx2))
59  print isidentity(xy3 - (slope*(xx1 - xx3) - xy1 - a1*xx3 - a3))
60
61  # Doubling on the Weierstrass curve and checking if it is the same as on
        the Jacobi curve
62  slope2 = (fastfrac((fastfrac(3)*xx1^2 + fastfrac(2)*a2*xx1 + a4 -
63  a1*xy1)/(fastfrac(2*xy1 + a1*xx1 + a3)))).reduce().sreduce()
64  print isidentity(xx4 - (slope2^2 + a1*slope2 - a2 - fastfrac(2)*xx1))
65  print isidentity(xy4 - (slope2*(xx1 - xx4) - xy1 - a1*xx4 - a3))
```

Listing A.2: Code in Sage for checking addition and doubling in the map

A.3 Fastfrac code

For adding the newly defined variables, constants and numbers to the ring, we need the code for fastfrac. Unfortunately, Sage is not capable to do this on it's own. I have found this in the EFD[7].

```
1   def mynumerator(x):
2     if parent(x) == R:
3       return x
4     return numerator(x)
5
6   class fastfrac:
7     def __init__(self,top,bot=1):
8       if parent(top) == ZZ or parent(top) == R:
9         self.top = R(top)
10        self.bot = R(bot)
11      elif top.__class__ == fastfrac:
12        self.top = top.top
13        self.bot = top.bot * bot
14      else:
15        self.top = R(numerator(top))
16        self.bot = R(denominator(top)) * bot
17    def reduce(self):
18      return fastfrac(self.top / self.bot)
19    def sreduce(self):
20      return fastfrac(I.reduce(self.top),I.reduce(self.bot))
21    def iszero(self):
22      return self.top in I and not (self.bot in I)
23    def isdoublingzero(self):
24      return self.top in J and not (self.bot in J)
25    def __add__(self,other):
26      if parent(other) == ZZ:
27        return fastfrac(self.top + self.bot * other,self.bot)
28      if other.__class__ == fastfrac:
```

```
29          return fastfrac(self.top * other.bot + self.bot * other.top,self.bot
                * other.bot)
30        return NotImplemented
31      def __sub__(self,other):
32        if parent(other) == ZZ:
33          return fastfrac(self.top - self.bot * other,self.bot)
34        if other.__class__ == fastfrac:
35          return fastfrac(self.top * other.bot - self.bot * other.top,self.bot
                * other.bot)
36        return NotImplemented
37      def __neg__(self):
38        return fastfrac(-self.top,self.bot)
39      def __mul__(self,other):
40        if parent(other) == ZZ:
41          return fastfrac(self.top * other,self.bot)
42        if other.__class__ == fastfrac:
43          return fastfrac(self.top * other.top,self.bot * other.bot)
44        return NotImplemented
45      def __rmul__(self,other):
46        return self.__mul__(other)
47      def __div__(self,other):
48        if parent(other) == ZZ:
49          return fastfrac(self.top,self.bot * other)
50        if other.__class__ == fastfrac:
51          return fastfrac(self.top * other.bot,self.bot * other.top)
52        return NotImplemented
53      def __pow__(self,other):
54        if parent(other) == ZZ:
55          return fastfrac(self.top ^ other,self.bot ^ other)
56        return NotImplemented
```

Listing A.3: The code for the function “Fastfrac”

Bibliography

[1] Billet, O. & Joye, M. (2003), "The Jacobi model of an elliptic curve and side-channel analysis". New York, NY: Springer-Verlag.

[2] Cohen, Henri & Frey, Gerhard (2006), "Handbook of Elliptic and Hyperelliptic Curve Cryptography". Boca Raton, FL: Chapman & Hall/CRC, Taylor & Francis Group.

[3] Connell, Ian (1999), "Elliptic Curve Handbook". Montréal, CA: McGill University.

[4] Dolgachev, I.V. & Iskovskikh V.A., Encyclopedia of Mathematics, "Birational Mapping",
http://www.encyclopediaofmath.org/index.php/Birational_mapping retrieved on saturday 21-12-2013.

[5] Huseyin Hisil, Kenneth Koon-Ho Wong, Gary Carter & Ed Dawson (5 november 2009), "Jacobi Quartic Curves Revisited". New York, NY: Springer-Verlag.

[6] Lange, Tanja (Fall 2013), College notes from the class "2WC09 Coding Theory and Cryptology I",
http://hyperelliptic.org/tanja/teaching/CCI13/ retrieved on saturday 21-12-2013.

[7] Lange, Tanja and Bernstein, Daniel J., "Explicit-Formulas Database",
http://hyperelliptic.org/EFD/index.html retrieved on saturday 21-12-2013.

[8] Moody, Dustin (2011), "Division Polynomial for Jacobi Quartics". Gaithersburg, MD: National Institute of Standards and Technology.

[9] Rivest, R.L., Shamir, A. & Adleman, L. (1977), "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". Cambridge, MA: Laboratory for Computer Science, Massachusetts Institute of Technology.

[10] Silverman, Joseph H. & Tate, John (1992), "Rational Points on Elliptic Curves". New York, NY: Springer-Verlag.

[11] Stein, William A., "Why Use Elliptic Curves?",
http://modular.math.washington.edu/edu/124/lectures/lecture29/lecture29/node6.html retrieved on saturday 21-12-2013.

[12] Various authors, "Why is elliptic curve cryptography not widely used, compared to RSA?",
http://crypto.stackexchange.com/questions/1190/why-is-elliptic-curve-cryptography-not-widely-used-compared-to-rsa retrieved on saturday 21-12-2013.