University of Groningen

Faculty of Science and Engineering

Mathematics

Master Thesis

A naive p-adic height function on the Jacobians of curves of genus 2

Manoy Trip

1st supervisors:
dr. J. S. Müller
dr. F. Bianchi

2nd supervisor:
dr. O. Lorscheid

May 2022

Abstract

In this thesis, we introduce a naive p-adic height on the Jacobians of smooth projective curves of genus 2. More generally, we explore both real and p-adic height functions on elliptic curves and on the Jacobians of genus 2 curves. Starting from the more established topic of real-valued height functions on elliptic curves, we discuss how methods can be adapted to the construction of p-adic height functions. A naive p-adic height was defined by Bernadette Perrin-Riou, and it can be used to obtain a quadratic p-adic height using a limit process. We give more details on her arguments. We then move on to the topic of height functions on the Jacobians of genus 2 curves. We discuss existing real height functions in this setting, and a quadratic p-adic height defined using local height functions. Then we turn to the main result of the thesis, which is the existence of a naive p-adic height on the Jacobian of a genus 2 curve that can be used to define a quadratic p-adic height. This height is defined analogously to Perrin-Riou's height. We show that the resulting quadratic p-adic height is equal to the quadratic height obtained using local heights.

Contents

Introduction

Roughly speaking, a real height function is a function from a mathematical structure to the real numbers which measures the complexity of mathematical objects. On projective space, there is a straightforward definition of a real height function that can be used to count points that are rational over a given field, such as a number field, in the sense that there is a finite number of points with height below any given value (even though the total number of projective points over a field may be infinite). Using this function, we can define a real height function on the group of points on an elliptic curve over $\mathbb{Q}$ (or more generally, a number field). The resulting function is also reasonably well-behaved with respect to the group structure of the elliptic curve. In particular, it is close to being a quadratic form, as we will see in Section 2.1.1. We call this the naive real height function on the elliptic curve. This function was for example important in the proof of the Mordell-Weil theorem (see [32, VIII, Theorem 6.7]), which states that the group of rational points on an elliptic curve over a number field is finitely generated.

In 1965, Néron constructed a real height function on elliptic curves in [27] which is actually a quadratic form, by writing it as a sum of local functions. Around that time, Tate defined the same height function as a global height using the naive height and applying a limit construction (unpublished). The resulting height function is called the canonical height or Néron-Tate height. We will discuss both constructions in Section 2.1.2 and Section 2.1.3.

The idea of height functions can be extended to curves of genus higher than 1, or more generally to algebraic varieties. In this thesis, besides height functions on elliptic curves, we look at height functions defined on the Jacobians of smooth projective genus 2 curves. Because the Jacobian is an abelian variety, we can again impose conditions on the behaviour of the height function with respect to the group law. In particular, height functions that are quadratic forms can also be found in this case. We will see such height functions in Section 3.1.

Besides height functions that map to the real numbers, we can define height functions that map to the field of p-adic numbers for a prime p. In this case, we lose the counting property, but it is still possible to define p-adic height functions which are quadratic forms. For elliptic curves, such functions were defined as the sum of local p-adic height functions, similar to Néron's construction of the canonical real height. The local height at p is defined using a so-called p-adic sigma function, which can be defined up to a choice of a parameter in $\mathbb{Q}_p$. Different sigma functions give rise to different p-adic heights. Such sigma functions have been constructed by Bernardi [3], Néron [26] and Mazur–Tate [24]. We will see Bernardi's sigma function and a general description of the possible sigma functions in Section 2.2.2.

Alternatively, in 1984 Perrin-Riou [28] constructed two quadratic p-adic height functions on elliptic curves using an analogue of the method of Tate, namely as limits of naive p-adic height functions. She compared these functions with the one that was constructed using local p-adic

heights. We discuss her construction and the comparison at length in Section 2.3.

On the Jacobians of genus 2 curves, p-adic height functions constructed using local p-adic heights have also recently been described. This construction also needs a p-adic sigma function, which is defined by Blakestad in [8] and generalized by Bianchi in [5]. The main goal of this thesis is to give an alternative construction analogous to Perrin-Riou's construction for elliptic curves. In Section 3.3, we define a naive p-adic height on the Jacobian of a genus 2 curve and show that a limit construction applied to this height, similar to the construction of Tate and Perrin-Riou, results in a quadratic p-adic height. We show that the resulting height is the same function as the one that was obtained using local p-adic heights.

Real-valued height functions on elliptic curves and more generally on abelian varieties arise in the Birch and Swinnerton-Dyer conjecture (see [2, Conjecture 1.1]), which is one of the Millenium Prize Problems. The p-adic height functions on abelian varieties in turn appear in a p-adic analogue of the Birch and Swinnerton-Dyer conjecture (see [25], [2, Conjecture 1.3, 1.4]). Besides this, p-adic heights are also used in the quadratic Chabauty method (see [1]). This is a method for computing the rational points on a curve of genus > 1 over the rational numbers, when the rank of the Mordell-Weil group of its Jacobian is equal to the genus of the curve. The method extends the Chabauty-Coleman method, which requires this rank to be strictly smaller than the genus. An exploration of such applications for the discussed height functions is outside the scope of this thesis.

We start this thesis by defining the necessary preliminaries to understand the theory behind the topics outlined above. In Section 1.1, we define the field of p-adic numbers, and the p-adic logarithm function which appears in the definitions of p-adic heights. In Section 1.2, we introduce the Riemann-Roch theorem for curves. We then define elliptic curves and some useful properties of these curves in Section 1.3. In Section 1.4 we see a general description of smooth genus 2 curves, and we define the corresponding Jacobians and Kummer surfaces in Section 1.5. To prove results about p-adic height functions, we make frequent use of properties of formal groups. We define the general notion of a formal group in Section 1.6, and use it to construct formal groups associated to elliptic curves and Jacobians of curves of genus 2. We conclude the section by introducing the formal group logarithm, a formal power series which shows up frequently in arguments in later chapters.

In the second chapter, we explore the topic of height functions on elliptic curves. We start by introducing the naive real height function and the Néron-Tate height in Section 2.1. We present both Tate's limit construction and Néron's construction using local height functions. In Section 2.2, we discuss the definition of p-adic quadratic heights as the sum of local p-adic height functions. Then we discuss the alternative construction by Perrin-Riou, using naive p-adic height functions, in Section 2.3. We go through her arguments showing the existence and quadraticity of the limit heights, giving more details where useful. We then compare these quadratic p-adic heights to the quadratic p-adic heights from Section 2.2.

In the final chapter we treat height functions on the Jacobians of genus 2 curves. The structure of this chapter is comparable to that of the previous one. In Section 3.1, we discuss real-valued height functions on the Jacobians of genus 2 curves defined by Uchida [35]. Then, in Section 3.2, we discuss a p-adic height that is defined using local p-adic height functions by Bianchi [4]. Finally, in Section 3.3 we introduce a naive p-adic height on the Jacobian. This naive height can be used to define a quadratic p-adic height, as we show in this section. We then show that the resulting quadratic height is the same as the quadratic p-adic height from Section 3.2.

Chapter 1

Preliminaries

1.1 p-adic numbers

Traditionally, height functions on curves were defined as functions mapping into the real numbers. The real numbers are the completion of $\mathbb{Q}$ with respect to the standard absolute value. In this section we will see that it is also possible to define other absolute values on the field $\mathbb{Q}$, which can be used to define the field of p-adic numbers for a prime p. The main references used for this section are [33, Section 2, 3], [15, Chapter 3, 4, 5] and [21, Chapter I, VI].

Definition 1.1.1 ([11, p. 2]). Let K be a field. A *discrete valuation* on K is a surjective map $v\colon K \to \mathbb{Z} \cup \{\infty\}$ with the properties

1. $v(a) = \infty \iff a = 0$.
2. $v(ab) = v(a) + v(b)$ for all $a, b \in K$.
3. $v(a + b) \geq \min\{v(a), v(b)\}$ for all $a, b \in K$.

The subring $\mathcal{O}_K = \{a \in K \mid v(a) \geq 0\}$ is a principal ideal domain with exactly one nonzero maximal ideal, which is a *discrete valuation ring (DVR)* by definition (see [11, p. 4, Proposition 2]).

Definition 1.1.2. An *absolute value* on a field K is a map $|\cdot|\colon K \to \mathbb{R}_{\geq 0}$ with the properties:

1. $|a| = 0 \iff a = 0$.
2. $|ab| = |a| \cdot |b|$ for all $a, b \in K$.
3. $|a + b| \leq |a| + |b|$ for all $a, b \in K$ (the triangle inequality).

If the map satisfies the stronger property

4. $|a + b| \leq \max\{|a|, |b|\}$ for all $a, b \in K$,

the absolute value is called *non-archimedean*. Otherwise it is called *archimedean*. The absolute value satisfying $|a| = 1$ for all $a \neq 0$ is called the *trivial absolute value*.

Lemma 1.1.3 ([15, Proposition 2.3.4]). *Let $|\cdot|$ be a non-archimedean absolute value. If $|a| \neq |b|$, we have $|a+b| = \max\{|a|, |b|\}$. Similarly, if v is a discrete valuation and $v(a) \neq v(b)$, we have $v(a+b) = \min\{v(a), v(b)\}$.*

An absolute value on a field K induces a metric $d(a,b) = |a-b|$, which turns K into a metric space.

Definition 1.1.4. Two absolute values on a field K are called *equivalent* if they induce the same topology on K. An equivalence class of absolute values is called a *place* of K.

Proposition 1.1.5 ([15, Proposition 3.1.3]). *Two absolute values $|\cdot|_1$ and $|\cdot|_2$ on a field K are equivalent if and only if there exists $\alpha \in \mathbb{R}_{>0}$ such that for every $a \in K$, $|a|_1 = |a|_2^{\alpha}$.*

Let K be a field with a discrete valuation v. Then we can define a non-archimedean absolute value $|\cdot|_v$ on K by

$$|a|_v = \begin{cases} 0 & \text{if } a = 0 \\ \alpha^{v(a)} & \text{if } a \neq 0 \end{cases}$$

for some $0 < \alpha < 1$. For different choices of α these absolute values are in the same equivalence class.

Lemma 1.1.6 ([15, Lemma 3.2.2]). *Let $|\cdot|$ be a non-archimedean absolute value on a field K. A sequence (a_n) is Cauchy if and only if $\lim_{n\to\infty} |a_{n+1} - a_n| = 0$.*

Lemma 1.1.7 (Generalization of [15, Corollary 5.1.2]). *Let K be a field which is complete with respect to the metric induced by a non-archimedean absolute value $|\cdot|$. Then a series $\sum_{n=0}^{\infty} a_n$ with $a_n \in K$ converges in K if and only if $\lim_{n\to\infty} a_n = 0$. In that case we have $|\sum_{n=0}^{\infty} a_n| \leq \max_n\{|a_n|\}$.*

1.1.1 Absolute values on $\mathbb{Q}$

The most well-known absolute value on $\mathbb{Q}$ is defined by

$$|a|_\infty = \begin{cases} a & \text{if } a \geq 0 \\ -a & \text{if } a < 0. \end{cases}$$

This is an archimedean absolute value.

Let p be a prime number. We can write each $a \in \mathbb{Q}^\times$ as $a = \frac{r_1}{r_2} p^n$ for some unique $n \in \mathbb{Z}$, and some $r_1, r_2 \in \mathbb{Z}$ such that $p \nmid r_1 r_2$. Then we assign $\operatorname{ord}_p(a) = n$, and $\operatorname{ord}_p(0) = \infty$. This defines a discrete valuation ord_p on $\mathbb{Q}$, which we call the *p-adic valuation.* This valuation defines a non-archimedean absolute value $|\cdot|_p$ on $\mathbb{Q}$:

$$|a|_p = \begin{cases} 0 & \text{if } a = 0 \\ p^{-\operatorname{ord}_p(a)} & \text{if } a \neq 0, \end{cases}$$

which we call the *p-adic absolute value.* It can be shown that $|\cdot|_p$ and $|\cdot|_q$ are not equivalent for primes p and q when $p \neq q$. Furthermore, $|\cdot|_\infty$ is not equivalent to $|\cdot|_p$ for any prime p [21, p. 7, Exercise 7, 9].

Theorem 1.1.8 (Ostrowski's Theorem, [21, p. 3, Theorem 1]). *Every nontrivial absolute value on $\mathbb{Q}$ is equivalent to $|\cdot|_\infty$ or to $|\cdot|_p$ for a prime p.*

Definition 1.1.9. We define the *set of standard absolute values* on $\mathbb{Q}$ by

$$M_{\mathbb{Q}} = \{\infty\} \cup \{p \in \mathbb{Z}_{>0} \mid p \text{ a prime number}\}.$$

This set defines a choice of representative for every place of $\mathbb{Q}$.

Theorem 1.1.10 ([32, VIII, Product Formula 5.3]). *Let $x \in \mathbb{Q}^\times$. Then*

$$\prod_{v \in M_{\mathbb{Q}}} |x|_v = 1.$$

The field $\mathbb{Q}$ is not complete with respect to the metric induced by each of the standard absolute values (see [15, Lemma 3.2.3]). The completion of $\mathbb{Q}$ with respect to $|\cdot|_\infty$ is the field of real numbers $\mathbb{R}$. With respect to the p-adic absolute value for a prime p, the completion of $\mathbb{Q}$ is called the *field of p-adic numbers* and is denoted by $\mathbb{Q}_p$. Explicitly, we have

$$\mathbb{Q}_p = \{(a_n) \mid (a_n) \text{ is a Cauchy sequence in } \mathbb{Q} \text{ w.r.t. } |\cdot|_p\}/\{(a_n) \mid \lim_{n\to\infty} |a_n|_p = 0\}.$$

We can extend the p-adic valuation and absolute value to $\mathbb{Q}_p$. Let $a \in \mathbb{Q}_p$ be represented by the Cauchy sequence (a_n). We define $\mathrm{ord}_p(a) = \lim_{n\to\infty} \mathrm{ord}_p(a_n)$ and $|a|_p = \lim_{n\to\infty} |a_n|_p$ (for the existence of these limits, see [21, p. 10]). Then ord_p is a discrete valuation on $\mathbb{Q}_p$, and $|\cdot|_p$ is a non-archimedean absolute value on $\mathbb{Q}_p$.

Definition 1.1.11. We define the ring of *p-adic integers* as

$$\begin{aligned}\mathbb{Z}_p &= \{a \in \mathbb{Q}_p \mid |a|_p \leq 1\} \\ &= \{a \in \mathbb{Q}_p \mid \mathrm{ord}_p(a) \geq 0\}.\end{aligned}$$

The ring $\mathbb{Z}_p$ is a DVR with field of fractions $\mathbb{Q}_p$ and maximal ideal $p\mathbb{Z}_p$. Note that $\mathbb{Z} \subseteq \mathbb{Z}_p$.

Definition 1.1.12. On $\mathbb{Z}_p$, there is a natural reduction map

$$\mathbb{Z}_p \to \mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p.$$

We denote the image of $a \in \mathbb{Z}_p$ under this map by $\tilde{a} \in \mathbb{F}_p$. For a polynomial $g \in \mathbb{Z}_p[x_1, \ldots, x_n]$, we use the notation $\tilde{g}$ for the polynomial in $\mathbb{F}_p[x_1, \ldots, x_n]$ obtained by reducing all of its coefficients modulo p.

Theorem 1.1.13 (Hensel's lemma, [21, p. 16, Theorem 3]). *Let $f \in \mathbb{Z}_p[x]$ with formal derivative f'. Let $a_0 \in \mathbb{Z}_p$ such that $f(a_0) \in p\mathbb{Z}_p$ and $f'(a_0) \notin p\mathbb{Z}_p$. Then there exists a unique $a \in \mathbb{Z}_p$ such that $f(a) = 0$ and $a_0 - a \in p\mathbb{Z}_p$.*

1.1.2 The p-adic exponential and logarithm

On $\mathbb{R}$ we have an exponential function, which can be described by the power series

$$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!} \tag{1.1}$$

which converges on all of $\mathbb{R}$. We can define a *p-adic exponential function* on a subset of $\mathbb{Q}_p$ using the same power series. On $\mathbb{Q}_p$, we need $\mathrm{ord}_p(x) > \frac{1}{p-1}$ for this series to converge, and in that case it converges to a value in $\mathbb{Z}_p$ (see [32, IV, Lemma 6.3(b)]). When p is odd, this means its domain of convergence is $p\mathbb{Z}_p$. We denote this function by $\exp_p \colon p\mathbb{Z}_p \to \mathbb{Z}_p$ (or $\exp_2 \colon 4\mathbb{Z}_2 \to \mathbb{Z}_2$ for $p = 2$).

Lemma 1.1.14. *If $x \in p^k\mathbb{Z}_p$ for some $k \in \mathbb{Z}$, $k > \frac{1}{p-1}$, then $\exp_p(x) \in 1 + p^k\mathbb{Z}_p$.*

Proof. This follows from [32, IV, Lemma 6.3(b)]. ∎

Similarly we have the standard (natural) logarithm function on $\mathbb{R}$, which can be described by the power series

$$\log(x) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n}(x-1)^n \tag{1.2}$$

which converges for $0 < x \leq 2$. We can define a *p-adic logarithm* on $\mathbb{Q}_p$ by starting out from the same power series. On $\mathbb{Q}_p$ equipped with the p-adic absolute value, the series (1.2) converges for $x \in 1 + p\mathbb{Z}_p$, i.e. when $|x-1|_p < 1$ (see [32, IV, Lemma 6.3(a)]).

Lemma 1.1.15 ([15, Corollary 5.8.3]). *Let $a \in \mathbb{Q}_p^\times$. Then we can write $a = rbp^n$ for some unique $n \in \mathbb{Z}$, $r \in \mathbb{Z}_p^\times$ a root of unity satisfying $r^{p-1} = 1$, and $b \in 1 + p\mathbb{Z}_p$.*

Proof. We already know that we can write $a = up^n$ for a unique $n \in \mathbb{Z}$ and some $u \in \mathbb{Z}_p^\times$. From Hensel's lemma applied to the polynomial $x^{p-1} - 1$, we get that there exists a unique $r \in \mathbb{Z}_p$ satisfying $r^{p-1} = 1$ such that $u \equiv r \bmod p\mathbb{Z}_p$. This shows that $ur^{p-2} \equiv r^{p-1} \equiv 1 \bmod p\mathbb{Z}_p$, or in other words, $ur^{p-2} \in 1 + p\mathbb{Z}_p$. If we set $b = ur^{p-2}$, we get $u = rb$ and hence $a = rbp^n$. Because our choices of n and r were unique, this factorization is uniquely determined. ∎

We want to define a p-adic logarithm $\log_p \colon \mathbb{Q}_p^\times \to \mathbb{Q}_p$ in such a way that for all $a, b \in \mathbb{Q}_p^\times$, we have the property $\log_p(ab) = \log_p(a) + \log_p(b)$. For $b \in 1 + p\mathbb{Z}_p$, we can define

$$\log_p(b) = \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n}(b-1)^n \tag{1.3}$$

because this series converges at b. For $r \in \mathbb{Z}_p^\times$ satisfying $r^{p-1} = 1$, we need

$$(p-1)\log_p(r) = \log_p(1) = 0,$$

and hence $\log_p(r) = 0$. We thus get

$$\log_p(rbp^n) = \log_p(b) + n\log_p(p).$$

Hence when we fix a value for $\log_p(p)$, this completely defines $\log_p$ on $\mathbb{Q}_p^\times$. A common choice, which we adopt, is to set $\log_p(p) = 0$. For this choice, the resulting logarithm is called the Iwasawa logarithm ([15, p. 155]). To see that it indeed satisfies the desired property, let $r_1, r_2 \in \mathbb{Z}_p$ be $(p-1)$-st roots of unity, $b_1, b_2 \in 1 + p\mathbb{Z}_p$ and $n_1, n_2 \in \mathbb{Z}$. Then $r_1 r_2 \in \mathbb{Z}_p$ is also a $(p-1)$-st root of unity and $b_1 b_2 \in 1 + p\mathbb{Z}_p$. Hence

$$\begin{aligned}\log_p(r_1 b_1 p^{n_1} \cdot r_2 b_2 p^{n_2}) &= \log_p(r_1 r_2 b_1 b_2 p^{n_1+n_2}) \\ &= \log_p(b_1 b_2) \\ &= \log_p(b_1) + \log_p(b_2).\end{aligned}$$

This last step uses that the original power series (1.2) satisfies $\log_p(b_1 b_2) = \log_p(b_1) + \log_p(b_2)$ for $b_1, b_2 \in 1 + p\mathbb{Z}_p$ (see [15, Proposition 5.7.3]).

The p-adic logarithm has the following useful property.

Lemma 1.1.16. *If $x \in 1 + p^k\mathbb{Z}_p$ for some $k \in \mathbb{Z}_{>0}$, then $\log_p(x) \in p^k\mathbb{Z}_p$.*

Proof. Because $x \in 1 + p\mathbb{Z}_p$, we have by definition $\log_p(x) = \sum_{i=1}^{\infty} \frac{(-1)^{i+1}}{i}(x-1)^i$. We know $\mathrm{ord}_p(x-1) \geq k$. Also $\mathrm{ord}_p(i) \leq i-1$ for all $i \geq 1$. Hence for all $i \geq 1$, we have

$$\begin{aligned}\mathrm{ord}_p\left(\frac{(-1)^{i+1}}{i}(x-1)^i\right) &\geq ik - (i-1) \\ &= k + (k-1)(i-1) \geq k.\end{aligned}$$

This shows that $\log_p(x) \in p^k\mathbb{Z}_p$. ■

In particular, this shows that the image of the function $\log_p$ actually lies in $p\mathbb{Z}_p$, so we have $\log_p \colon \mathbb{Q}_p^\times \to p\mathbb{Z}_p$.

As formal power series, we have $\log_p(\exp_p(x)) = x$ and $\exp_p(\log_p(x)) = x$. Hence Lemma 1.1.14 and Lemma 1.1.16 imply that for all $k > \frac{1}{p-1}$, the map $\exp_p \colon p^k\mathbb{Z}_p \to 1 + p^k\mathbb{Z}_p$ is a bijection with inverse $\log_p$.

We deduce a variation on the product formula involving the p-adic logarithm, which will be useful multiple times.

Lemma 1.1.17. *Let $x \in \mathbb{Q}^\times$. Then*

$$\log_p(x) + \sum_{\substack{q \text{ prime} \\ q \neq p}} \log_p |x|_q = 0.$$

Proof. Note that for $x \in \mathbb{Q}^\times$, we have $|x|_v \in \mathbb{Q}^\times \subseteq \mathbb{Q}_p^\times$ for all $v \in M_\mathbb{Q}$. From the product formula (Theorem 1.1.10), we then know that

$$\sum_{v \in M_\mathbb{Q}} \log_p |x|_v = 0.$$

Note that $\log_p(-1) = 0$ and hence $\log_p(a) = \log_p(-a)$ for all $a \in \mathbb{Q}_p^\times$. In particular, we have $\log_p |x|_\infty = \log_p(x)$. Furthermore, we note that $|x|_p$ is an integer power of p by definition, and hence $\log_p |x|_p = 0$. This implies the result. ■

1.2 The Riemann-Roch theorem

This section gives an overview of some general theory about algebraic curves. We use the word *curve* for a geometrically irreducible projective variety of dimension 1. We aim to introduce all concepts necessary to understand the Riemann-Roch theorem for curves. This section is mainly based on [32, Chapter II]. We restrict to curves over *perfect fields*, which are fields for which every algebraic extension is separable. In particular, all fields of characteristic 0 and all finite fields are perfect fields, and these are the only types of fields we will need to consider. For more general fields the arguments we discuss work in the same way when we replace the algebraic closure by the separable closure.

1.2.1 Divisors

Let us consider a curve $\mathcal{C}$ defined over a perfect field K. Then the *divisor group* of $\mathcal{C}$, denoted by $\mathrm{Div}_{\mathcal{C}}$, is the free abelian group generated by the points of $\mathcal{C}$. A *divisor* D is thus a finite formal sum of points of $\mathcal{C}$, of the form $D = \sum_{P \in \mathcal{C}} n_P \, P$ for some $n_P \in \mathbb{Z}$, where all but finitely many n_P are equal to zero. We define the degree of a divisor D to be $\deg(D) = \sum_{P \in \mathcal{C}} n_P$. We define the set $\mathrm{Div}^0_{\mathcal{C}} = \{D \in \mathrm{Div}_{\mathcal{C}} \mid \deg(D) = 0\}$, which is a subgroup of $\mathrm{Div}_{\mathcal{C}}$.

Consider any algebraic extension field $K \subseteq L \subseteq \overline{K}$, where $\overline{K}$ denotes a fixed algebraic closure of K. If $\mathrm{Gal}(\overline{K}/L)$ is the Galois group of $\overline{K}/L$, there is an action of this group on $\mathrm{Div}_{\mathcal{C}}$ and $\mathrm{Div}^0_{\mathcal{C}}$, defined for $\sigma \in \mathrm{Gal}(\overline{K}/L)$ as

$$\left(\sum_{P \in \mathcal{C}} n_P \, P \right)^{\sigma} := \sum_{P \in \mathcal{C}} n_P \, \sigma(P),$$

where $\sigma(P)$ represents the image under the coordinate-wise action of σ on P as a point in projective space. We define $\mathrm{Div}_{\mathcal{C}}(L) = \{D \in \mathrm{Div}_{\mathcal{C}} \mid \forall \sigma \in \mathrm{Gal}(\overline{K}/L), D^{\sigma} = D\}$ and we say that such $D \in \mathrm{Div}_{\mathcal{C}}(L)$ is *defined over* L. The set $\mathrm{Div}_{\mathcal{C}}(L)$ is a subgroup of $\mathrm{Div}_{\mathcal{C}}$. We similarly define the group $\mathrm{Div}^0_{\mathcal{C}}(L) = \{D \in \mathrm{Div}^0_{\mathcal{C}} \mid \forall \sigma \in \mathrm{Gal}(\overline{K}/L), D^{\sigma} = D\}$.

Now let us assume that $\mathcal{C}$ is a smooth curve, and let $\overline{K}(\mathcal{C})$ be its function field. For $f \in \overline{K}(\mathcal{C})^{\times}$, we define an associated divisor

$$\mathrm{div}(f) = \sum_{P \in \mathcal{C}} \mathrm{ord}_P(f) \, P,$$

with ord_P as defined in [32, p. 18, Definition]. We say that a divisor $D \in \mathrm{Div}_{\mathcal{C}}$ is *principal* if $D = \mathrm{div}(f)$ for some $f \in \overline{K}(\mathcal{C})^{\times}$. We can now define an equivalence relation on $\mathrm{Div}_{\mathcal{C}}$. We say D_1 and D_2 are *linearly equivalent* if their difference is a principal divisor. In this case, we write $D_1 \sim D_2$. The principal divisors from a subgroup, which we denote by $\mathrm{Princ}_{\mathcal{C}} \subseteq \mathrm{Div}_{\mathcal{C}}$. We can thus define the quotient group $\mathrm{Pic}_{\mathcal{C}} = \mathrm{Div}_{\mathcal{C}} \,/\, \mathrm{Princ}_{\mathcal{C}}$, which is called the *Picard group*. Furthermore, all principal divisors have degree zero (see [32, II, Proposition 3.1]), and hence $\mathrm{Princ}_{\mathcal{C}} \subseteq \mathrm{Div}^0_{\mathcal{C}}$. We can thus also define $\mathrm{Pic}^0_{\mathcal{C}} = \mathrm{Div}^0_{\mathcal{C}} \,/\, \mathrm{Princ}_{\mathcal{C}}$. We denote the class of a divisor D in these factor groups by $[D]$. By definition we have $[D_1] = [D_2]$ precisely when $D_1 \sim D_2$.

For $f \in \overline{K}(\mathcal{C})^{\times}$ and $\sigma \in \mathrm{Gal}(\overline{K}/K)$, let us denote by f^{σ} the function we obtain when we replace each coefficient in f by its image under σ. We have

$$\begin{aligned} (\mathrm{div}(f))^{\sigma} &= \sum_{P \in \mathcal{C}} \mathrm{ord}_P(f) \, \sigma(P) \\ &= \sum_{P \in \mathcal{C}} \mathrm{ord}_P(f^{\sigma}) \, P \\ &= \mathrm{div}(f^{\sigma}), \end{aligned}$$

which follows from the observation that $f(P) = 0 \iff f^{\sigma}(\sigma(P)) = 0$. In particular, this shows that $(\mathrm{div}(f))^{\sigma} \in \mathrm{Princ}_{\mathcal{C}}$. Hence there are well-defined actions of $\mathrm{Gal}(\overline{K}/K)$ on $\mathrm{Pic}_{\mathcal{C}}$ and $\mathrm{Pic}^0_{\mathcal{C}}$ defined by $[D]^{\sigma} = [D^{\sigma}]$ for $\sigma \in \mathrm{Gal}(\overline{K}/K)$. For an extension field $K \subseteq L \subseteq \overline{K}$ we can hence define

$$\mathrm{Pic}_{\mathcal{C}}(L) = \{[D] \in \mathrm{Pic}_{\mathcal{C}} \mid \forall \sigma \in \mathrm{Gal}(\overline{K}/L), [D]^{\sigma} = [D]\}$$

and

$$\mathrm{Pic}^0_{\mathcal{C}}(L) = \{[D] \in \mathrm{Pic}^0_{\mathcal{C}} \mid \forall \sigma \in \mathrm{Gal}(\overline{K}/L), [D]^{\sigma} = [D]\}.$$

1.2.2 Differentials

The space of *differentials* $\Omega_{\mathcal{C}}$ on $\mathcal{C}$ is a $\overline{K}(\mathcal{C})$-vector space generated by symbols of the form df for $f \in \overline{K}(\mathcal{C})$, subject to the relations

1. $d(f+g) = df + dg$ for all $f, g \in \overline{K}(\mathcal{C})$,
2. $d(fg) = f\ dg + g\ df$ for all $f, g \in \overline{K}(\mathcal{C})$,
3. $dc = 0$ for all $c \in \overline{K}$.

Let $P \in \mathcal{C}$, and fix a uniformizer $t \in \overline{K}(\mathcal{C})$ at P. Then for each differential $\omega \in \Omega_{\mathcal{C}}$, there is a unique function $g \in \overline{K}(\mathcal{C})$ such that $\omega = g dt$. If $\omega \neq 0$, we can define $\mathrm{ord}_P(\omega) = \mathrm{ord}_P(g)$, because this value is independent of the choice of t (see [32, II, Proposition 4.3]). We define the *divisor associated to a nonzero differential* ω as

$$\mathrm{div}(\omega) = \sum_{P \in \mathcal{C}} \mathrm{ord}_P(\omega)\, P.$$

The space $\Omega_{\mathcal{C}}$ is a 1-dimensional vector space ([32, II, Proposition 4.2]), which implies that all differentials $\omega \in \Omega_{\mathcal{C}}$ are in the same divisor class in $\mathrm{Pic}_{\mathcal{C}}$. We call this class the *canonical divisor class* on $\mathcal{C}$. Any divisor in this class is called a *canonical divisor*.

1.2.3 The Riemann-Roch theorem

We say a divisor $D = \sum_{P \in \mathcal{C}} n_P\, P$ is *effective* when $n_P \geq 0$ for all $P \in \mathcal{C}$. We then write $D \geq 0$. Similarly, we write $D_1 \geq D_2$ when $D_1 - D_2$ is effective. For any divisor $D \in \mathrm{Div}_{\mathcal{C}}$, we can define a finite-dimensional $\overline{K}$-vector space

$$\mathcal{L}(D) = \{f \in \overline{K}(C)^{\times} \mid \mathrm{div}(f) \geq -D\} \cup \{0\}.$$

We write $\ell(D) = \dim_{\overline{K}} \mathcal{L}(D)$.

Theorem 1.2.1 (Riemann-Roch, [32, II, Theorem 5.4]). *Let $\mathcal{C}$ be a smooth curve and let $K_{\mathcal{C}}$ be a canonical divisor. There is an integer $g \geq 0$ (called the genus of $\mathcal{C}$) such that for every divisor $D \in \mathrm{Div}_{\mathcal{C}}$, we have*

$$\ell(D) - \ell(K_{\mathcal{C}} - D) = \deg(D) - g + 1.$$

Corollary 1.2.2 ([32, II, Corollary 5.5]).

1. $\ell(K_{\mathcal{C}}) = g$.
2. $\deg(K_{\mathcal{C}}) = 2g - 2$.
3. *If* $\deg(D) > 2g - 2$, *then* $\ell(D) = \deg(D) - g + 1$.

There exist generalizations of the Riemann-Roch Theorem to smooth projective varieties of higher dimensions. We do not treat them here, but see for example [17, V, Theorem 1.6] for a version on surfaces or [17, Appendix A] for a treatment of Riemann-Roch on varieties of arbitrary dimension.

1.3 Elliptic curves

We introduce the concept of elliptic curves, and we state some properties that we use in this thesis. A more elaborate introduction can be found in [32, Chapter III].

Let K be a perfect field. An *elliptic curve* over K is a smooth projective curve E over K of genus 1, together with a point $\mathcal{O} \in E$. Any elliptic curve can be given as the zero set in $\mathbb{P}^2$ of a *Weierstrass equation*, which is an equation of the form

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

with $a_i \in K$, and $\mathcal{O} = [0 : 1 : 0]$. Such a specific equation is also called a Weierstrass *model* for E. We say E is defined over K, and we write E/K. For any algebraic extension field $K \subseteq L \subseteq \overline{K}$, we denote by $E(L)$ the points of E which can be represented with coordinates in L. We can dehomogenize by setting $x = \frac{X}{Z}$ and $y = \frac{Y}{Z}$ to represent E by an affine equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1.4}$$

We call $\mathcal{O}$ the *point at infinity*. When the characteristic of K is not 2 or 3, it is possible to perform a change of coordinates to represent E by an equation of the form

$$y^2 = x^3 + Ax + B$$

with $A, B \in K$, called a *short Weierstrass equation* [32, Section III.1]. We can define an addition operation on an elliptic curve, which turns it into an abelian group with identity $\mathcal{O}$, and more specifically an abelian variety. The explicit group law can be found in [32, Section III.2].

Elliptic curves are smooth by definition. For a curve represented by a Weierstrass equation (1.4), being smooth is equivalent to the nonvanishing of the quantity Δ defined in [32, p. 42], called the *discriminant* of the Weierstrass equation. A curve given by an equation of the form (1.4) can also be singular. In that case it has exactly one singular point, and the subset E_{ns} of nonsingular points still has a group structure where the addition operation is defined in the same way as on elliptic curves (see [32, III, Proposition 2.5]).

We denote the sum of m copies of a point $P \in E(\overline{K})$ by $[m]P$. We write E_{tors} for the subgroup of *torsion points* on E, that is

$$E_{\text{tors}} = \{P \in E(\overline{K}) \mid [m]P = \mathcal{O} \text{ for some } m \in \mathbb{Z}_{>0}\}.$$

Similarly we write $E_{\text{tors}}(K) = E_{\text{tors}} \cap E(K)$.

In this thesis, we mostly consider elliptic curves over $\mathbb{Q}$ given by an equation (1.4) with $a_i \in \mathbb{Z}$ (for any arbitrary Weierstrass equation over $\mathbb{Q}$ we can perform a coordinate transformation to achieve $a_i \in \mathbb{Z}$, see [32, Section III.1]).

Proposition 1.3.1. *Let $E/\mathbb{Q}$ be an elliptic curve given by a Weierstrass equation* (1.4) *with $a_i \in \mathbb{Z}$. Then for any $P \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}$, we can write the coordinates of P uniquely as*

$$x(P) = \frac{a(P)}{d(P)^2} \quad \text{and} \quad y(P) = \frac{b(P)}{d(P)^3}$$

for some $a(P), b(P) \in \mathbb{Z}$, $d(P) \in \mathbb{Z}_{>0}$ such that $\gcd(a(P), d(P)) = \gcd(b(P), d(P)) = 1$.

Proof. Because $a_i \in \mathbb{Z}$, we have $\operatorname{ord}_q(a_i) \geq 0$ for all i and all primes q. Let us consider any point $P = (x, y) \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}$. If $\operatorname{ord}_q(y) < 0$ for a prime q, we can compare the q-adic valuations of the left- and right-hand side of (1.4), and we find that

$$\begin{aligned} 2\operatorname{ord}_q(y) &= \operatorname{ord}_q(y^2 + a_3y - a_6) && \text{(using Lemma 1.1.3)} \\ &= \operatorname{ord}_q(x^3 + a_2x^2 + a_4x - a_1xy), && (1.5) \end{aligned}$$

which implies that we must also have $\operatorname{ord}_q(x) < 0$. Then $\operatorname{ord}_q(x^3) < \operatorname{ord}_q(a_2x^2 + a_4x)$. We consider three cases.

1. If $\operatorname{ord}_p(x^3) > \operatorname{ord}_p(a_1xy)$, we have $2\operatorname{ord}_p(x) > \operatorname{ord}_p(a_1y)$. But Lemma 1.1.3 and (1.5) then imply that $2\operatorname{ord}_q(y) = \operatorname{ord}_q(a_1xy)$, and hence

   $$2\operatorname{ord}_q(x) = 2\operatorname{ord}_q(y) - 2\operatorname{ord}_q(a_1) < \operatorname{ord}_q(a_1y).$$

   This is a contradiction.

2. If $\operatorname{ord}_q(x^3) = \operatorname{ord}_q(a_1xy)$, we have $\operatorname{ord}_q(y) = 2\operatorname{ord}_q(x) - \operatorname{ord}_q(a_1)$. But from (1.5) we get

   $$2\operatorname{ord}_q(y) \geq \min\{\operatorname{ord}_q(x^3), \operatorname{ord}_q(a_2x^2), \operatorname{ord}_q(a_4x), \operatorname{ord}_1(a_1xy)\} = \operatorname{ord}_p(x^3).$$

   We obtain $4\operatorname{ord}_p(x) - 2\operatorname{ord}_p(a_1) \geq 3\operatorname{ord}_p(x)$ which is again a contradiction.

3. We must thus have $\operatorname{ord}_p(x^3) < \operatorname{ord}_p(a_1xy)$. Using Lemma 1.1.3, this implies that

   $$\operatorname{ord}_q(x^3 + a_2x^2 + a_4x - a_1xy) = \operatorname{ord}_q(x^3) = 3\operatorname{ord}_q(x).$$

   We conclude that $2\operatorname{ord}_q(y) = 3\operatorname{ord}_q(x)$.

Conversely, if $\operatorname{ord}_q(x) < 0$, similar reasoning again shows that $2\operatorname{ord}_q(y) = 3\operatorname{ord}_q(x)$. This shows that we can write the coordinates of P uniquely as $x(P) = \frac{a(P)}{d(P)^2}$ and $y(P) = \frac{b(P)}{d(P)^3}$ for some $a(P), b(P) \in \mathbb{Z}$, $d(P) \in \mathbb{Z}_{>0}$ such that $\gcd(a(P), d(P)) = \gcd(b(P), d(P)) = 1$. ■

1.3.1 The Kummer variety

For a general abelian variety A, if we identify all points P on A with their additive inverse $-P$, the corresponding quotient of A is again a variety called the *Kummer variety* (see [7, Section 4.8]). Let us consider an elliptic curve E/K given by a Weierstrass model (1.4). Because an elliptic curves is an abelian variety, we can consider its Kummer variety. Let us consider the surjective morphism

$$\begin{aligned} \kappa\colon E &\to \mathbb{P}^1 \\ (x, y) &\mapsto [x : 1] \\ \mathcal{O} &\mapsto [1 : 0] \end{aligned} \qquad (1.6)$$

(see [32, II, Example 2.2, Theorem 2.3]). We see that $\kappa(P) = \kappa(Q)$ precisely when $P, Q \neq \mathcal{O}$ and $x(P) = x(Q)$, or when $P = Q = \mathcal{O}$. From the group law on E, we can deduce that $x(P) = x(Q)$ precisely when $P = \pm Q$. This shows that κ exactly identifies each point with its inverse, and thus the map κ identifies the Kummer variety of E with $\mathbb{P}^1$.

1.3.2 Reduction of elliptic curves

Let q be a prime. When we have an elliptic curve E given by a model of the form (1.4) with coefficients in $\mathbb{Z}$, we can view E as an elliptic curve defined over $\mathbb{Q}_q$. Each coefficient $a \in \mathbb{Z}_q$ in the defining equation (1.4) of E can be reduced modulo q via the natural reduction in Definition 1.1.12. The resulting equation defines a (possibly singular) Weierstrass curve over $\mathbb{F}_q$, given by

$$\widetilde{E}\colon y^2 + \tilde{a}_1 xy + \tilde{a}_3 y = x^3 + \tilde{a}_2 x^2 + \tilde{a}_4 x + \tilde{a}_6,$$

which is the *reduction of* (1.4) *modulo* q. Each $P \in E(\mathbb{Q}_q)$ can be written in the form $[X : Y : Z]$ with $X, Y, Z \in \mathbb{Z}_q$ such that at least one of the coordinates is in $\mathbb{Z}_q^\times$. Then the *reduction of* P *modulo* q is defined as $\widetilde{P} = [\widetilde{X} : \widetilde{Y} : \widetilde{Z}]$, which is a point on $\widetilde{E}$. When $\widetilde{E}$ is nonsingular (that is, when $q \nmid \Delta(E)$), we say E has *good reduction at* q with respect to the model (1.4). Otherwise, E has *bad reduction at* q with respect to the model. This may be dependent on the chosen Weierstrass equation for E. It is possible to define the notion of a minimal Weierstrass equation for E, and we say E has *good reduction at* q if it has good reduction at q with respect to this minimal equation (see [32, Section VII.1]). In particular, if E has good reduction at q with respect to some Weierstrass equation with integer coefficients, it has good reduction with respect to a minimal equation as well.

We define the following sets, which are actually groups:

$$\begin{aligned}
\widetilde{E}_{\mathrm{ns}}(\mathbb{F}_q) &= \{P \in \widetilde{E}(\mathbb{F}_q) \mid P \text{ is nonsingular}\}.\\
E_0(\mathbb{Q}_q) &= \{P \in E(\mathbb{Q}) \mid \widetilde{P} \in \widetilde{E}_{\mathrm{ns}}(\mathbb{F}_q)\}\\
E_1(\mathbb{Q}_q) &= \{P \in E(\mathbb{Q}) \mid \widetilde{P} = \widetilde{\mathcal{O}}\}.
\end{aligned}$$

These groups form an exact sequence

$$\{\mathcal{O}\} \to E_1(\mathbb{Q}_q) \to E_0(\mathbb{Q}_q) \to \widetilde{E}_{\mathrm{ns}}(\mathbb{F}_q) \to \{\mathcal{O}\}$$

where the map on the left is inclusion, and the map on the right is reduction modulo q (see [32, VII, Proposition 2.1]). We also use the notation $E_0^{(q)}(\mathbb{Q}) = E_0(\mathbb{Q}_q) \cap E(\mathbb{Q})$ and $E_1^{(q)}(\mathbb{Q}) = E_1(\mathbb{Q}_q) \cap E(\mathbb{Q})$.

1.3.3 Division polynomials

Given a Weierstrass curve E, we define a collection of polynomials called division polynomials. These are useful when looking at the coordinates of multiples of points on the curve.

Definition 1.3.2 ([32, Exercise 3.7]). Let E/K be a curve over a field K given by a Weierstrass equation (1.4) (we include singular curves). The division polynomials corresponding to E are polynomials $\psi_n \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6, x, y]$, defined inductively as

$$\begin{aligned}
\psi_0 &= 0,\\
\psi_1 &= 1,\\
\psi_2 &= 2y + a_1 x + a_3,\\
\psi_3 &= 3x^4 + b_2 x^3 + 3b_4 x^2 + 3b_6 x + b_8,\\
\psi_4 &= \psi_2 \left(2x^6 + b_2 x^5 + 5b_4 x^4 + 10b_6 x^3 + 10b_8 x^2 + (b_2 b_8 - b_4 b_6)x + (b_4 b_8 - b_6^2)\right),\\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \quad \text{for } m \geq 2,\\
\psi_{2m} &= \frac{\psi_m}{\psi_2}(\psi_{m-1}^2\psi_{m+2} - \psi_{m-2}\psi_{m+1}^2) \quad \text{for } m \geq 3.
\end{aligned}$$

with $b_i \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$ as defined in [32, Section III.1]. We furthermore define polynomials

$$\phi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1} \quad \text{for } m \geq 1. \tag{1.7}$$

Proposition 1.3.3 ([28, p. 248], [37, Lemma 3.3, 3.4, 3.5, 3.6], [36, Proposition 4.9]). *For all $m \geq 1$, the polynomials ψ_m and ϕ_m satisfy the following properties:*

(i) $\phi_m, \psi_m^2 \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6, x]$.

(ii) *ϕ_m is homogeneous of degree $2m^2$ and ψ_m^2 of degree $2(m^2-1)$ if we give a_i weight i and x weight 2.*

(iii) *As polynomials in $\mathbb{Z}[a_1, \ldots, a_6][x]$, ϕ_m has degree m^2 and ψ_m^2 has degree m^2-1. Moreover, ϕ_m is monic, and the leading coefficient of ψ_m^2 is m^2.*

(iv) *Let $P \neq \mathcal{O}$ be a nonsingular point on E. When $\psi_m^2(x(P)) = 0$, we have $[m]P = \mathcal{O}$. Otherwise,*

$$x([m]P) = \frac{\phi_m(x(P))}{\psi_m^2(x(P))}. \tag{1.8}$$

(v) *For a nonsingular point $P \neq \mathcal{O}$ and all $m, n \geq 1$ such that $[n]P \neq \mathcal{O}$, we have*

$$\psi_{mn}(P) = \psi_n(P)^{m^2}\psi_m([n]P).$$

(vi) *We have*

$$\begin{aligned}
\phi_{2n} &= \psi_n^8 \cdot \phi_2\left(\frac{\phi_n}{\psi_n^2}\right) \\
&= \phi_n^4 - b_4\phi_n^2\psi_n^4 - 2b_6\phi_n\psi_n^6 - b_8\psi_n^8, &(1.9)\\
\psi_{2n}^2 &= \psi_n^8 \cdot \psi_2^2\left(\frac{\phi_n}{\psi_n^2}\right) \\
&= \psi_n^2(4\phi_n^3 + b_2\phi_n^2\psi_n^2 + 2b_4\phi_n\psi_n^4 + b_6\psi_n^6). &(1.10)
\end{aligned}$$

1.4 Curves of genus 2

Let K be a perfect field with characteristic different from 2. Every smooth curve of genus 2 over K can be described by an affine equation of the form

$$\mathcal{C}\colon y^2 = f(x) = f_6x^6 + f_5x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0, \tag{1.11}$$

where $f \in K[x]$ has degree 5 or 6, and it has no multiple factors (otherwise the curve is singular) (see [10, p. 1]). In particular, every smooth genus 2 curve is a *hyperelliptic curve*. For a general introduction on this class of curves, see [33].

We cannot complete the affine curve (1.11) by homogenizing the equation in the usual way to obtain a smooth projective curve in $\mathbb{P}^2$. The resulting equation would be of the form $Y^2Z^4 = F(X, Z)$ where F is a homogeneous polynomial of total degree 6 in X and Z. The projective point $[0 : 1 : 0]$ is a zero of this equation, but it is a singular point, so the projective equation defines a singular curve. Instead, we embed the affine curve in a modified projective plane.

Definition 1.4.1 ([33, Definition 2.1]). The *weighted projective plane* $\mathbb{P}^2_{(1,3,1)}$ is the geometric object whose points over a field L are triples $(X, Y, Z) \in L^3 \setminus \{(0,0,0)\}$ modulo the equivalence relation $\sim$, where $(X, Y, Z) \sim (X', Y', Z')$ if there exists some element $c \in \overline{L}^\times$ such that $(X', Y', Z') = (cX, c^3Y, cZ)$. We denote the corresponding equivalence class by $[X : Y : Z]$.

The *coordinate ring of* $\mathbb{P}^2_{(1,3,1)}$ *over* L is the ring $L[X, Y, Z]$ graded such that X and Z have degree 1 and Y has degree 3.

If we homogenize (1.11) to a polynomial in the coordinate ring of $\mathbb{P}^2_{(1,3,1)}$ over K, we obtain the equation

$$Y^2 = f_6X^6 + f_5X^5Z + f_4X^4Z^2 + f_3X^3Z^3 + f_2X^2Z^4 + f_1XZ^5 + f_0Z^6, \tag{1.12}$$

where $x = \frac{X}{Z}$ and $y = \frac{Y}{Z^3}$. This equation defines $\mathcal{C}$ as a smooth subvariety of $\mathbb{P}^2_{(1,3,1)}$.

If $f(x)$ has degree 6 and it has a root in K, it is possible to apply a coordinate transformation over K such that f becomes monic of degree exactly 5 (see [10, p. 1]). In this thesis we restrict to curves that can be written in this form. These curves have an affine equation of the form

$$\mathcal{C}\colon y^2 = f(x) = x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0 \tag{1.13}$$

for some $f_i \in K$ such that f has no multiple factors. If we denote the (distinct) roots of f by $r_1, \ldots, r_5 \in \overline{K}$, we can alternatively write

$$f(x) = \prod_{i=1}^{5}(x - r_i).$$

Looking at the curve via its embedding in $\mathbb{P}^2_{(1,3,1)}$, we note that it has one point at infinity $\infty = [1 : 0 : 0]$.

Note that when $[X : Y : Z] \in \mathcal{C}$, we also have $[X : -Y : Z] \in \mathcal{C}$. So there is an automorphism of $\mathcal{C}$ defined by

$$\begin{aligned} \iota\colon \mathcal{C} &\to \mathcal{C} \\ [X : Y : Z] &\mapsto [X : -Y : Z], \end{aligned}$$

called the *hyperelliptic involution*. We also have a quotient map

$$\begin{aligned} \pi\colon \mathcal{C} &\to \mathbb{P}^1 \\ [X : Y : Z] &\mapsto [X : Z]. \end{aligned}$$

Note that this map is well-defined, because $[0 : 1 : 0] \notin \mathcal{C}$. This map is a 2-1 cover, branched precisely on the fixed points of ι (i.e. the points with $Y = 0$). These points are called the *Weierstrass points* of $\mathcal{C}$. Explicitly, these are the points $(r_1, 0), \ldots, (r_5, 0)$ and ∞.

1.4.1 Divisors on genus 2 curves

We introduce a few important divisors on $\mathcal{C}$. To find divisors, it is useful to first fix a uniformizer at every point in $\mathcal{C}$. We distinguish three types of points.

1. Let $P = (x_0, y_0)$ with $y_0 \neq 0$. In this case, the maximal ideal of the local ring $\mathcal{O}_{\mathcal{C},P}$ at P is of the form $\mathfrak{m}_P = (x - x_0, y - y_0)$, but we notice that

$$\begin{aligned}(y - y_0)(y + y_0) &= y^2 - y_0^2 \\ &= (x - x_0)^5 + \cdots + f_1(x - x_0) \\ &= (x - x_0)^k g(x),\end{aligned}$$

   where $g \in \overline{K}[x]$ satisfies $g(x_0) \neq 0$, and the value of $k \in \mathbb{Z}_{>0}$ depends on which of the f_i equal 0. We conclude that

$$y - y_0 = (x - x_0)^k \frac{g(x)}{y + y_0},$$

   where $\frac{g(x)}{y+y_0} \in \mathcal{O}_{\mathcal{C},P}^{\times}$. This implies that $\mathfrak{m}_P = (x - x_0)$, so $x - x_0$ is a uniformizer at P.

2. Let $P = (r_k, 0)$ for some $k \in \{1, \ldots, 5\}$. We know $f(x) = (x - r_k)g(x)$ with $g \in \overline{K}[x]$. We have that $\mathfrak{m}_P = (x - r_k, y)$, but $y^2 = f(x)$ and hence $x - r_k = \frac{y^2}{g(x)}$. Because f has no multiple roots we know that $\frac{1}{g(x)} \in \mathcal{O}_{\mathcal{C},P}^{\times}$, and hence this implies that $\mathfrak{m}_P = (y)$. We conclude that y is a uniformizer at P.

3. Let $P = \infty$. We perform a change of variables to the affine patch corresponding to $X \neq 0$, which results in the $w^2 = z + \cdots + f_0 z^6$ with $z = \frac{1}{x}$ and $w = \frac{y}{x^3}$. We can also write it as $w^2 = \prod_{i=1}^{6}(z - \rho_i)$, where the $\rho_i \in \overline{K}$ are the roots of $z + \cdots + f_0 z^6$. We fix $\rho_1 = 0$. When we represent points Q by coordinates $(w(Q), z(Q))$, we have $\infty = (0, 0)$. We have $\mathfrak{m}_\infty = (w, z)$. We note that

$$z = \frac{w^2}{\prod_{i=2}^{6}(z - \rho_i)}$$

   and $\frac{1}{\prod_{i=2}^{6}(z - r_i)} \in \mathcal{O}_{\mathcal{C},\infty}^{\times}$. Hence $\mathfrak{m}_\infty = (w)$, so w is a uniformizer at ∞.

We use this information to find a canonical divisor on $\mathcal{C}$.

Lemma 1.4.2. *The divisor 2∞ is a canonical divisor.*

Proof. We will show that $\operatorname{div}\left(\frac{dx}{y}\right) = 2\infty$. First, we determine $\operatorname{div}(dx) = \sum_{P \in \mathcal{C}} \operatorname{ord}_P(dx)\, P$. We find $\operatorname{ord}_P(dx)$ for all $P \in \mathcal{C}$ again by considering the three different types of points.

1. If $P = (x_0, y_0)$ with $y_0 \neq 0$, we found that $x - x_0$ is a uniformizer. We conclude that $\operatorname{ord}_P(dx) = \operatorname{ord}_P(d(x - x_0)) = \operatorname{ord}_P(1) = 0$.

2. If $P = (r_k, 0)$ for some $k \in \{1, \ldots, 5\}$, then y is a uniformizer at P. We can derive that

$$2y dy = dx \sum_{i=1}^{5} \prod_{j \neq i} (x - r_j),$$

   and hence

$$\operatorname{ord}_P(dx) = \operatorname{ord}_P\left(\frac{2y}{\sum_{i=1}^{5} \prod_{j \neq i}(x - r_j)} dy\right) = 1.$$

3. At $P = \infty$, we saw that w is a uniformizer. Using $x = \frac{1}{z}$, we find

$$\begin{aligned} dx &= -x^2 dz \\ &= \frac{-2wx^2}{\sum_{i=1}^{6} \prod_{j \neq i} (z - \rho_j)} dw. \end{aligned}$$

This implies that

$$\operatorname{ord}_P(dx) = \operatorname{ord}_P \left(\frac{-2wx^2}{\sum_{i=1}^{6} \prod_{j \neq i} (z - \rho_j)} \right) = -3.$$

In conclusion, we have found that $\operatorname{div}(dx) = \sum_{i=1}^{5} (r_i, 0) - 3\infty$.

Now we determine $\operatorname{div}(y)$. It is easy to see that $\operatorname{ord}_P(y) = 0$ when $P = (x_0, y_0)$ with $y_0 \neq 0$, and $\operatorname{ord}_P(y) = 1$ when $P = (r_k, 0)$. Finally we note that $\operatorname{ord}_\infty(y) = \operatorname{ord}_\infty(\frac{w}{z^3}) = -5$. Hence $\operatorname{div}(y) = \sum_{i=1}^{5} (r_i, 0) - 5\infty$. We conclude that $\operatorname{div}(\frac{dx}{y}) = \operatorname{div}(dx) - \operatorname{div}(y) = 2\infty$. Because $\frac{dx}{y}$ is a differential, we conclude that 2∞ is a canonical divisor. ■

Lemma 1.4.3. *Let $P \in \mathcal{C}$. Then $P + \iota(P) - 2\infty$ is a principal divisor.*

Proof. If $P = \infty$, this divisor becomes trivial and the result is clear. Now assume $P = (x_0, y_0)$ for some $x_0, y_0 \in \overline{K}$. Let us determine the divisor of the function $x - x_0$. First of all, for points $Q = (x_1, y_1) \in \mathcal{C}$ with $x_1 \neq x_0$, we have $\operatorname{ord}_Q(x - x_0) = 0$. The only points with x-coordinate x_0 are $P = (x_0, y_0)$ and $\iota(P) = (x_0, -y_0)$. We have to distinguish two cases.

1. If $y_0 \neq 0$, we have $P \neq \iota(P)$. We saw that $x - x_0$ is a uniformizer at P and $\iota(P)$. This shows that $\operatorname{ord}_P(x - x_0) = \operatorname{ord}_{\iota(P)}(x - x_0) = 1$.

2. If $y_0 = 0$, we have $P = \iota(P)$. We know that y is a uniformizer at P, and that $x - x_0 = \frac{y^2}{g(x)}$ for some function $g(x)$ such that $g(x_0) \neq 0$. Hence $\operatorname{ord}_P(x - x_0) = 2$.

Finally, at ∞ we saw that w is a uniformizer. We have $x - x_0 = \frac{1 - x_0 z}{z}$ and hence $\operatorname{ord}_\infty(x - x_0) = -\operatorname{ord}_\infty(z) = -2$. We conclude that $\operatorname{div}(x - x_0) = P + \iota(P) - 2\infty$. The latter is therefore a principal divisor. ■

Corollary 1.4.4. *Let $P \in \mathcal{C}$. Then $P + \iota(P)$ is a canonical divisor.*

Proof. We know from Lemma 1.4.2 that 2∞ is a canonical divisor, so the result is true for $P = \infty$. If $P = (x_0, y_0)$, using Lemma 1.4.3 we see that

$$\begin{aligned} [2\infty] &= [2\infty + \operatorname{div}(x - x_0)] \\ &= [P + \iota(P)]. \end{aligned}$$

This shows that $P + \iota(P)$ is also a canonical divisor. ■

1.5 The Jacobian of a genus 2 curve and its Kummer surface

In this section, we introduce the concept of the Jacobian variety J of a smooth curve $\mathcal{C}$ of genus 2, which is an abelian variety. We treat everything in the setting of Section 1.4. We also define the Kummer surface of the Jacobian, and see how operations on J carry over to this surface.

As in Section 1.4, we consider a smooth curve $\mathcal{C}$ of genus 2 over a perfect field K with $\mathrm{char}(K) \neq 2$, represented by an equation of the form

$$\begin{aligned} \mathcal{C}\colon y^2 = f(x) &= x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0 \\ &= \prod_{i=1}^{5}(x - r_i) \end{aligned} \tag{1.14}$$

where $f_i \in K$, such that f has no multiple roots, and $r_i \in \overline{K}$ are the distinct roots of f. The *Jacobian* corresponding to $\mathcal{C}$ is an abelian variety J of dimension 2 over the field K, such that as abelian groups we have $J(K) = \mathrm{Pic}^0_{\mathcal{C}}(K)$ (and more generally, for any field $K \subseteq L \subseteq \overline{K}$, $J(L) = \mathrm{Pic}^0_{\mathcal{C}}(L)$) ([33, Theorem 4.8]). The following result shows that each nonzero point on J can be represented by a unique pair of points on $\mathcal{C}$. The first part of the proof is based on the proof of a more general statement for hyperelliptic curves in [33, Corollary 4.14].

Proposition 1.5.1. *Let $K \subseteq L \subseteq \overline{K}$ be a field. For all $P \in \mathrm{Pic}^0_{\mathcal{C}}(L) \setminus \{0\}$, there are unique points $P_1, P_2 \in \mathcal{C}(L')$ for some algebraic extension field $L \subseteq L'$ with $[L' : L] \leq 2$, such that $P = [P_1 + P_2 - 2\infty]$.*

Proof. Consider any $P = [D] \in \mathrm{Pic}^0_{\mathcal{C}}(L)$ where $D \in \mathrm{Div}^0_{\mathcal{C}}$ is a divisor representing P. The Riemann-Roch theorem (Theorem 1.2.1), together with Lemma 1.4.2, gives us that

$$\ell(2\infty + D) = \ell(-D) + 1 \geq 1.$$

In other words, there exists a function $\phi \in \mathcal{L}(2\infty + D)$ such that $2\infty + D + \mathrm{div}(\phi) \geq 0$. Let us write $\widetilde{D} = 2\infty + D + \mathrm{div}(\phi)$. Then we know $\widetilde{D} \geq 0$ and $\deg(\widetilde{D}) = 2$, hence it is of the form $\widetilde{D} = P_1 + P_2$ for some $P_1, P_2 \in \mathcal{C}(\overline{K})$. We have $P = [D] = [\widetilde{D} - 2\infty] = [P_1 + P_2 - 2\infty]$.

Now let us show uniqueness. For this we need that $P \neq 0$. Let us assume that

$$P = [P_1 + P_2 - 2\infty] = [Q_1 + Q_2 - 2\infty].$$

Then

$$\begin{aligned} P_1 + P_2 - Q_1 - Q_2 &\sim 0 \\ P_1 + P_2 + \iota(Q_1) + \iota(Q_2) - 4\infty &\sim 0, \end{aligned}$$

where we used $Q_i + \iota(Q_i) - 2\infty \sim 0$ for $i = 1, 2$ (Lemma 1.4.3). This shows that

$$P_1 + P_2 + \iota(Q_1) + \iota(Q_2) - 4\infty \in \mathrm{Princ}_{\mathcal{C}}$$

and hence there exists a function $\psi \in \overline{K}(\mathcal{C})^\times$ such that $\mathrm{div}(\psi) = P_1 + P_2 + \iota(Q_1) + \iota(Q_2) - 4\infty$. In particular, we see that $\psi \in \mathcal{L}(4\infty)$. Corollary 1.2.2 implies that $\ell(4\infty) = 3$. Because $\mathrm{ord}_P(x) \geq 0$ for all $P \neq \infty$, and $\mathrm{ord}_\infty(x) = \mathrm{ord}_\infty(1/z) = -2$, we deduce that $\mathcal{L}(4\infty) = \langle 1, x, x^2 \rangle$. Hence we can write $\psi = a_0 + a_1x + a_2x^2$ for some $a_i \in \overline{K}$. In particular, ψ does not depend on y. We consider a few cases:

1. If $P_1 = (x_0, y_0)$ with $y_0 \neq 0$, we know that ψ has a zero at P_1. But because ψ is a polynomial in x, ψ then also has a zero at $\iota(P_1) = (x_0, -y_0)$.

2. If $P_1 = (r_k, 0)$ for some k, recall that y is a uniformizer at P_1. We know $\psi \in \overline{K}[x]$ has a zero at P_1. Hence $\psi(x) = (x - r_k)g(x)$ for some $g(x) \in \overline{K}[x]$. In the proof of Lemma 1.4.2 we saw that $\mathrm{ord}_{P_1}(x - r_k) = 2$, hence $\mathrm{ord}_{P_1}(\psi) \geq 2$.

3. If $P_1 = \infty$, recall that w is a uniformizer at P_1 and $\mathrm{ord}_{P_1}(z) = 2$. We have $\psi = \frac{a_0 z^2 + a_1 z + a_2}{z^2}$. We have $\mathrm{ord}_{P_1}(\psi) \geq -3$, so $\mathrm{ord}_{P_1}(a_0 z^2 + a_1 z + a_2) \geq 1$. But because $a_0 z^2 + a_1 z + a_2 \in \overline{K}[z]$ and $\mathrm{ord}_{P_1}(z) = 2$, this implies $\mathrm{ord}_{P_1}(a_0 z^2 + a_1 z + a_2) \geq 2$ and hence $\mathrm{ord}_{P_1}(\psi) \geq -2$.

In each case, we see that $\iota(P_1)$ has to be one of the points $P_2, \iota(Q_1), \iota(Q_2)$ appearing in $\mathrm{div}(\psi)$. We cannot have $\iota(P_1) = P_2$, because then Lemma 1.4.3 tells us that $P = 0$. Hence $\iota(P_1) = \iota(Q_i)$ for $i \in \{1, 2\}$. Because ι is an involution we conclude $P_1 = Q_i$. We can repeat the entire reasoning for P_2 to get $\iota(P_2) = \iota(Q_i)$ for $i \in \{1, 2\}$. Hence $\{P_1, P_2\} \subseteq \{Q_1, Q_2\}$. The symmetric counterpart of this argument shows that we must have $\{P_1, P_2\} = \{Q_1, Q_2\}$ and hence $P_1 + P_2 - 2\infty = Q_1 + Q_2 - 2\infty$, which shows uniqueness.

Now we show the last part of the proposition. Because $P \in \mathrm{Pic}^0_{\mathcal{C}}(L)$, we must have that the class of $P_1 + P_2 - 2\infty$ is fixed under the action of $\mathrm{Gal}(\overline{K}/L)$. Note that ∞ is fixed under this action because $\infty \in \mathcal{C}(L)$. Therefore, we need

$$\begin{aligned}[P_1 + P_2 - 2\infty] &= [P_1 + P_2 - 2\infty]^\sigma \\ &= [\sigma(P_1) + \sigma(P_2) - 2\infty]\end{aligned}$$

for all $\sigma \in \mathrm{Gal}(\overline{K}/L)$. By the uniqueness we just showed, we conclude $P_1 + P_2 = \sigma(P_1) + \sigma(P_2)$, or in other words, each $\sigma \in \mathrm{Gal}(\overline{K}/L)$ permutes P_1 and P_2. In particular, $\sigma^2(P_i) = P_i$ for all $\sigma \in \mathrm{Gal}(\overline{K}/L)$ for $i = 1, 2$. If $P_1, P_2 \in \mathcal{C}(L)$, then the statement is immediate. Let us assume that $P_1 \notin \mathcal{C}(L)$, so there exists $\tau \in \mathrm{Gal}(\overline{K}/L)$ such that $\tau(P_1) = P_2 \neq P_1$. We then also have $\tau(P_2) = P_1$, so also $P_2 \notin \mathcal{C}(L)$. Then $P_1 \neq \infty$, so $P_1 = (x_1, y_1)$ for some $x_1, y_1 \in \overline{K}$, and $\sigma^2(P_1) = P_1$ for all $\sigma \in \mathrm{Gal}(\overline{K}/L)$. This implies that x_1 and y_1 have a minimal polynomial of degree 2 over L. Using the defining equation of $\mathcal{C}$, we deduce that $x_1 \in L(y_1)$. We then have $x_1, y_1, \tau(x_1), \tau(y_1) \in L(y_1)$, so $P_1, P_2 \in \mathcal{C}(L(y_1))$ with $[L(y_1) : L] = 2$. ■

Because the Jacobian is a group, we introduce similar notation as for elliptic curves. We denote the sum of m copies of a point $P \in J$ by $[m]P$, and we write J_{tors} for the subgroup of torsion points on J.

1.5.1 Algebraic variety structure of the Jacobian

For a fixed $P \in \mathcal{C}$, we define the map $\Phi_P \colon \mathcal{C} \to \mathrm{Pic}^0_{\mathcal{C}}$ by $Q \mapsto [Q - P]$. It follows from Proposition 1.5.1 that Φ_∞ is injective. We denote the image of Φ_∞ by Θ. Then because Φ_∞ is an embedding and $\mathrm{Pic}^0_{\mathcal{C}}$ can be identified with the Jacobian J, we can view Θ as a subvariety of J of dimension 1 (because it is isomorphic to $\mathcal{C}$). The variety Θ is then a divisor on J (see [17, Section II.6] for a general introduction). The space $\mathcal{L}(3\Theta)$ corresponding to J is a 9-dimensional $\overline{K}$-vector space (see [16, p. 100]). Proposition 1.5.1 shows that we can identify J with the 2-fold symmetric product of $\mathcal{C}$, where the points corresponding to $\mathcal{O}$ on J are blown down to a single point (that is, all points of the form $\{P, \iota(P)\}$). Points on Θ then correspond to points of the form $\{P, \infty\}$ for some $P \in \mathcal{C}$. Under this identification, $\mathcal{L}(3\Theta)$ corresponds to a space of symmetric functions on $\mathcal{C} \times \mathcal{C}$. These functions are in $K(x_1, y_1, x_2, y_2)^\times$ (where $y_1^2 = f(x_1)$ and $y_2^2 = f(x_2)$) such

that they have at most a triple pole at ∞ in both coordinates. This space is a $\overline{K}$-vector space which has a basis $1, \wp_{11}, \wp_{12}, \wp_{22}, \wp_{111}, \wp_{112}, \wp_{122}, \wp_{222}, \wp$ of functions that are defined over K, described explicitly in [16, p. 99]. We note that $\wp_{11}$, $\wp_{12}$, $\wp_{22}$ and $\wp$ are even functions, and $\wp_{111}$, $\wp_{112}$, $\wp_{122}$ and $\wp_{222}$ are odd. It follows from a theorem of Lefschetz ([7, Theorem 4.5.1]) that the following map defines an embedding of the Jacobian into $\mathbb{P}^8$, which makes its projective variety structure explicit:

$$\begin{aligned} \mathcal{J}\colon \operatorname{Pic}^0_{\mathcal{C}} &\to \mathbb{P}^8 \\ [P_1 + P_2 - 2\infty] &\mapsto [1 : \wp_{11} : \wp_{12} : \wp_{22} : \wp_{111} : \wp_{112} : \wp_{122} : \wp_{222} : \wp]. \end{aligned} \tag{1.15}$$

The image of this map is the Jacobian as an algebraic variety embedded in $\mathbb{P}^8$, and we denote it by J. Explicit equations defining the Jacobian variety can be found in [16, Corollary 2.15], and we reproduced them adapted to our notation in the Appendix of this thesis. For the nine projective coordinates of J in $\mathbb{P}^8$, we use the notation $X_0, X_{11}, X_{12}, X_{22}, X_{111}, X_{112}, X_{122}, X_{222}, X$ in this order, after [16]. As coordinate functions, we then have

$$\wp_{ij} = \frac{X_{ij}}{X_0},\ \wp_{ijk} = \frac{X_{ijk}}{X_0},\ \wp_{ij} = \frac{X_{ij}}{X_0} \text{ and } \wp = \frac{X}{X_0}. \tag{1.16}$$

We note that $\mathcal{J}([0]) = [0:0:0:0:1:0:0:0] =: \mathcal{O}$.

1.5.2 The Kummer surface

If we identify all points P on the Jacobian with their additive inverse $-P$, the corresponding quotient of J is again a variety called the *Kummer surface*.

The Kummer surface can be embedded in $\mathbb{P}^3$ using a basis of $\mathcal{L}(2\Theta)$ (see [7, Theorem 4.8.1]). The even functions $1, \wp_{11}, \wp_{12}$ and $\wp_{22}$ form such a basis ([13, §2]), and as such define a map into $\mathbb{P}^3$ as follows:

$$\begin{aligned} \mathcal{K}\colon \operatorname{Pic}^0_{\mathcal{C}} &\to \mathbb{P}^3 \\ [P_1 + P_2 - 2\infty] &\mapsto [1 : \wp_{22} : -\wp_{12} : \wp_{11}]. \end{aligned} \tag{1.17}$$

The image of this map is the Kummer surface embedded in $\mathbb{P}^3$. We denote it by $\mathbb{K}$. Because the map $\mathcal{J}$ is an embedding, there exists an inverse map from J to $\operatorname{Pic}^0_{\mathcal{C}}$ and hence we can define a map $\mathcal{K}\mathcal{J}^{-1}$ from the Jacobian to the Kummer surface. Explicitly it can be described as a morphism of varieties:

$$\begin{aligned} \kappa\colon J &\to \mathbb{K} \\ [X_0 : X_{11} : X_{12} : X_{22} : X_{111} : X_{112} : X_{122} : X_{222} : X] &\mapsto \left[1 : \frac{X_{22}}{X_0} : -\frac{X_{12}}{X_0} : \frac{X_{11}}{X_0}\right]. \end{aligned} \tag{1.18}$$

In particular, we have $\kappa(\mathcal{O}) = [0:0:0:1]$. The Kummer surface is a projective variety defined by a homogeneous equation of the form

$$G(X,Y,Z,W) := R(X,Y,Z)W^2 + S(X,Y,Z)W + T(X,Y,Z) = 0, \tag{1.19}$$

where R, S and T are homogeneous polynomials with coefficients in $\mathbb{Z}[f_0, \ldots, f_4]$ of total degree 2, 3, and 4, respectively, and X, Y, Z, W are the coordinates of the considered projective space $\mathbb{P}^3$. The explicit equation can be found in [13, Appendix A]. We note that in [13], Flynn uses an embedding of the Jacobian in $\mathbb{P}^{15}$ rather than $\mathbb{P}^8$ to construct the Kummer surface. This embedding works more generally for genus 2 curves defined by an equation of degree 5 or 6, but because we restrict to degree 5 curves we can use Grant's embedding into $\mathbb{P}^8$ instead. The same Kummer construction is applicable in this case.

1.5.3 Computations on the Kummer surface

For a point $P \in J$ let us write $\kappa(P)$ for its image on the Kummer surface. In general, when we consider the projective Kummer coordinates of two points $\kappa(P), \kappa(Q) \in \mathbb{K}$, we do not have enough information to deduce the coordinates of $\kappa(P+Q)$, because we cannot distinguish $\pm P$ and $\pm Q$ from only their Kummer coordinates. We can thus not in general find a formula for addition on $\mathbb{K}$. We do however have the following theorem:

Theorem 1.5.2 ([10, Theorem 3.4.1]). *For $i, j \in \{1,2,3,4\}$, there exist polynomials B_{ij} with coefficients in $\mathbb{Z}[f_0, \ldots, f_4]$, which are biquadratic in two sets of variables $k_1, \ldots, k_4$ and $l_1, \ldots, l_4$, with the following property. For any $P, Q \in J$, let us fix Kummer coordinates*

$$\kappa(P) = [x_1 : \ldots : x_4], \kappa(Q) = [y_1 : \ldots : y_4], \kappa(P+Q) = [z_1 : \ldots : z_4], \kappa(P-Q) = [w_1 : \ldots : w_4].$$

Then there exists a constant $c \in \overline{K}^\times$ such that for all $i, j \in \{1,2,3,4\}$, we have

$$z_i w_j + w_i z_j = 2cB_{ij}((x_1, x_2, x_3, x_4), (y_1, y_2, y_3, y_4)).$$

The constant c makes sure that we work projectively, which is necessary because the Kummer coordinates in projective space are only well-defined up to a scalar multiple in $\overline{K}^\times$. Explicit formulas for the polynomials B_{ij} can be found in [12].

Using this result, it is possible to define a multiplication-by-m map μ_m on the Kummer surface for any $m \in \mathbb{Z}$, such that the following diagram is commutative:

$$\begin{array}{ccc} J & \xrightarrow{[m]} & J \\ \downarrow{\scriptstyle \kappa} & & \downarrow{\scriptstyle \kappa} \\ \mathbb{K} & \xrightarrow{\mu_m} & \mathbb{K} \end{array}$$

Such a map μ_m is well-defined, because if $\kappa(P) = \kappa(Q)$, this implies that $Q = \pm P$, and hence $\kappa([m]Q) = \kappa(\pm[m]P) = \kappa([m]P)$. Using Theorem 1.5.2, we can find explicit formulas defining the multiplication-by-2 map.

Proposition 1.5.3. *There exist polynomials $\delta_1, \ldots, \delta_4$ in $\mathbb{Z}[f_0, \ldots, f_4][k_1, k_2, k_3, k_4]$, each homogeneous of total degree 4, such that for all $P \in J$ with $\kappa(P) = [x_1 : x_2 : x_3 : x_4]$, we have*

$$\kappa([2]P) = [\delta_1(x_1, x_2, x_3, x_4) : \delta_2(x_1, x_2, x_3, x_4) : \delta_3(x_1, x_2, x_3, x_4) : \delta_4(x_1, x_2, x_3, x_4)]\,.$$

Proof. Let $P \in J$ with $\kappa(P) = [x_1 : x_2 : x_3 : x_4]$. Let us write $\kappa([2]P) = [y_1 : y_2 : y_3 : y_4]$. If we apply Theorem 1.5.2 for $P = Q$ using $\kappa(\mathcal{O}) = [0:0:0:1]$, we get

$$y_i = \begin{cases} 2cB_{i,4}((x_1, \ldots, x_4), (x_1, \ldots, x_4)) & \text{if } i = 1,2,3, \\ cB_{4,4}((x_1, \ldots, x_4), (x_1, \ldots, x_4)) & \text{if } i = 4, \end{cases}$$

for some $c \in \overline{K}^\times$. So if we define $\delta_i \in \mathbb{Z}[f_0, \ldots, f_4][k_1, k_2, k_3, k_4]$ as

$$\delta_i(k_1, k_2, k_3, k_4) = \begin{cases} 2B_{i,4}((k_1, k_2, k_3, k_4), (k_1, k_2, k_3, k_4)) & \text{if } i = 1,2,3, \\ B_{4,4}((k_1, k_2, k_3, k_4), (k_1, k_2, k_3, k_4)) & \text{if } i = 4, \end{cases}$$

then $\kappa([2]P) = [\delta_1(x_1, \ldots, x_4) : \delta_2(x_1, \ldots, x_4) : \delta_3(x_1, \ldots, x_4) : \delta_4(x_1, \ldots, x_4)]$. ∎

Explicit formulas for the polynomials δ_i can be found in [13, Appendix C]. For general multiples, we have the following result by Uchida:

Theorem 1.5.4 ([35, Theorem 3.3, Proposition 3.6, Lemma 3.8]). *For any $m \geq 0$ and $i = 1, 2, 3, 4$, there exist homogeneous polynomials $\mu_{m,i} \in \mathbb{Z}[f_0, \ldots, f_4][k_1, k_2, k_3, k_4]$ of total degree m^2 such that:*

$$\begin{aligned} \mu_{0,1} = \mu_{0,2} = \mu_{0,3} = 0,\ \mu_{0,4} = 1, \\ \mu_{1,i} = k_i, \\ \mu_{2m,i} = \delta_i(\mu_m) \qquad & \text{for } m \geq 1, \\ \mu_{2m+1,i} k_i = B_{ii}(\mu_{m+1}, \mu_m) \quad & \text{for } m \geq 1 \end{aligned}$$

in $\mathbb{Q}(f_0, \ldots, f_4)[k_1, k_2, k_3, k_4]/(G)$ (where G is the defining equation (1.19) of the Kummer surface $\mathbb{K}$ as a projective variety in $\mathbb{P}^3$), where we write $\mu_m = (\mu_{m,1}, \ldots, \mu_{m,4})$. For all $P \in J(\mathbb{Q})$ with $\kappa(P) = [x_1 : x_2 : x_3 : x_4]$, we have

$$\kappa([m]P) = [\mu_{m,1}(x_1, \ldots, x_4) : \ldots : \mu_{m,4}(x_1, \ldots, x_4)].$$

In other words, scalar multiplication on J descends to $\mathbb{K}$, and we have an inductive definition for the image on $\mathbb{K}$ of multiples of points in $J(\mathbb{Q})$.

1.5.4 Reduction of varieties

Let q be a prime number. Consider a projective variety $V \subseteq \mathbb{P}^n$ defined by a set of equations with coefficients in $\mathbb{Z}$. Then we can view V as a variety defined over $\mathbb{Q}_q$ for a prime q. We can reduce V modulo q by reducing the coefficients of the defining equations with the map in Definition 1.1.12, the same way we did in Section 1.3.2 for elliptic curves, to obtain a possibly singular variety $\widetilde{V}$ over $\mathbb{F}_q$. For a curve in the weighted projective space $\mathbb{P}^2_{(1,3,1)}$, for example a smooth genus 2 curve $\mathcal{C}$ defined by an equation of the form (1.12) with coefficients in $\mathbb{Z}$, we define the reduction modulo q analogously, by reducing each of the coefficients modulo q. The resulting equation then also defines a possibly singular curve $\widetilde{\mathcal{C}}$ over $\mathbb{F}_q$ in $\mathbb{P}^2_{(1,3,1)}$. In each of these cases, we can write a point on V as $P = [X_0 : \cdots : X_n]$ with $X_i \in \mathbb{Z}_p$ such that at least one of the coordinates is in $\mathbb{Z}_p^\times$, and we define $\widetilde{P} = [\widetilde{X}_0 : \cdots : \widetilde{X}_n] \in \widetilde{V}$.

As in Section 1.3.2, we define the following sets:

$$\begin{aligned} \widetilde{V}_{\mathrm{ns}}(\mathbb{F}_q) &= \{P \in \widetilde{V}(\mathbb{F}_q) \mid P \text{ is nonsingular}\}, \\ V_0(\mathbb{Q}_q) &= \{P \in V(\mathbb{Q}) \mid \widetilde{P} \in \widetilde{V}_{\mathrm{ns}}(\mathbb{F}_q)\}. \end{aligned}$$

When V is an abelian variety with identity $\mathcal{O}$ (for example when V is a Jacobian), we also define

$$V_1(\mathbb{Q}_q) = \{P \in V(\mathbb{Q}) \mid \widetilde{P} = \widetilde{\mathcal{O}}\}.$$

Furthermore we write $V_0^{(q)}(\mathbb{Q}) = V_0(\mathbb{Q}_q) \cap V(\mathbb{Q})$ and $V_1^{(q)}(\mathbb{Q}) = V_1^{(q)}(\mathbb{Q}_q) \cap V(\mathbb{Q})$.

For a smooth curve $\mathcal{C}$ of genus 2 given by (1.14) with $f_i \in \mathbb{Z}$, the reduction modulo q is a curve $\widetilde{\mathcal{C}}$ over $\mathbb{F}_q$, which is singular precisely when q divides the *discriminant* of f (see [9, Section 16]). It follows that $\mathcal{C}$ has bad reduction at only a finite number of primes. For such a curve $\mathcal{C}$, the embedding of its Jacobian J in $\mathbb{P}^8$ is also defined by equations with coefficients in $\mathbb{Z}$ (see the Appendix). Hence we can also reduce J modulo q. When $\mathcal{C}$ has good reduction at a prime q, so does J. The reduction $\widetilde{J}$ is the Jacobian variety corresponding to $\widetilde{\mathcal{C}}$, and we have a commutative diagram

$$\begin{array}{ccc} \mathrm{Pic}^0_{\mathcal{C}}(\mathbb{Q}_q) & \xrightarrow{\mathcal{J}} & J(\mathbb{Q}_q) \\ \downarrow & & \downarrow \\ \mathrm{Pic}^0_{\tilde{\mathcal{C}}}(\mathbb{F}_q) & \xrightarrow{\mathcal{J}} & \widetilde{J}(\mathbb{F}_q) \end{array}$$

where $\mathcal{J}$ is the map (1.15), the vertical map on the left is defined by

$$[P_1 + P_2 - 2\infty] \mapsto [\widetilde{P}_1 + \widetilde{P}_2 - 2\infty],$$

and the vertical map on the right is the reduction map described above (see [33, Lemma 4.20]). The sets $\widetilde{J}(\mathbb{F}_q)$ and $J_1(\mathbb{Q}_q)$ are then also groups.

Similarly we can reduce points on the Kummer surface, and this reduction also fits in a commutative diagram

$$\begin{array}{ccc} J(\mathbb{Q}_q) & \xrightarrow{\kappa} & \mathbb{K}(\mathbb{Q}_q) \\ \downarrow & & \downarrow \\ \widetilde{J}(\mathbb{F}_q) & \xrightarrow{\kappa} & \widetilde{\mathbb{K}}(\mathbb{F}_q) \end{array} \tag{1.20}$$

where the vertical maps are reduction modulo q.

1.5.5 Division polynomials on J

Like for elliptic curves (Section 1.3.3), we can define division polynomials on the Jacobian of a genus 2 curve of the form (1.14). These were defined by Kanayama in [20, 19] for curves over $\mathbb{C}$, so in particular this works when our curve is defined over $\mathbb{Q}$. A Jacobian over $\mathbb{C}$ can be identified with $\mathbb{C}^2/\Lambda$ for some lattice Λ, and on this lattice there is a σ-function of dimension 2 (see [20, p. 400]), much like the Weierstrass σ-function of dimension 1 on elliptic curves. There is an identification between J and $\mathbb{C}^2/\Lambda$ and we denote the image of the subvariety Θ under this map by Θ'. We have the following definition.

Definition 1.5.5 ([20, p. 402, Definition]). For all $n \in \mathbb{Z}$, we define functions ϕ_n on $(\mathbb{C}^2/\Lambda) \setminus \Theta'$ by

$$\phi_n(\boldsymbol{u}) = \frac{\sigma(n\boldsymbol{u})}{\sigma(\boldsymbol{u})^{n^2}}.$$

We define $\phi_n^{(i)} := \frac{\partial \phi_n}{\partial u_i}$, $\phi_n^{(ij)} := \frac{\partial \phi_n^{(i)}}{\partial u_j}$, and $\phi_n^{(ijk)} := \frac{\partial \phi_n^{(ij)}}{\partial u_k}$ for $i, j, k \in \{1, 2\}$.

In [36, Proposition 4.3], Uchida notes that for any $n \in Z$, we have

$$\phi_{-n}(\boldsymbol{u}) = -\phi_n(\boldsymbol{u}). \tag{1.21}$$

Each $\boldsymbol{u} \in (\mathbb{C}^2/\Lambda) \setminus \Theta'$ corresponds to a point $[1 : \wp_{11} : \wp_{12} : \wp_{22} : \wp_{111} : \wp_{112} : \wp_{122} : \wp_{222} : \wp]$ on J. Under this identification, we can consider ϕ_n, $\phi_n^{(i)}$, $\phi_n^{(ij)}$ and $\phi_n^{(ijk)}$ for $i, j, k \in \{1, 2\}$ as a functions on J. Let us denote the set of points that lie on the subvariety of J defining the divisor Θ by $\mathrm{supp}(\Theta)$, the *support* of the divisor Θ.

Proposition 1.5.6 ([20, Proposition 2], [36, Theorem 5.8], [16, Equation (3.4)]). *For all $n \in \mathbb{Z}$, the function ϕ_n on $J \setminus \mathrm{supp}(\Theta)$ is a polynomial in the coordinates $\wp_{ij}$ and $\wp_{ijk}$ with coefficients in $\mathbb{Z}[\frac{1}{2}, f_0, \ldots, f_4]$. As a result, also the functions $\phi_n^{(i)}, \phi_n^{(ij)}$ and $\phi_n^{(ijk)}$ for $i, j, k \in \{1, 2\}$ are polynomials in $\mathbb{Z}[\frac{1}{2}, f_0, \ldots, f_4][\wp_{ij}, \wp_{ijk}]$.*

We call ϕ_n the *n-th division polynomial*. In particular, we have

$$\begin{aligned}\phi_1 &= 1,\\ \phi_2 &= \wp_{12}\wp_{122} - \wp_{22}\wp_{112} - \wp_{111}.\end{aligned}$$

The polynomials quickly become more complicated, but they can be determined using a recurrence relation, see [20, 19, Lemma 1, Proposition 3]. The division polynomials can be used to express the coordinates of multiples of a point P on J in terms of the coordinates of P.

Proposition 1.5.7 ([20, Proposition 1]). *Let $n \geq 1$, and $P \in J$ such that $P, [n]P \notin \operatorname{supp}(\Theta)$. Then*

$$\begin{aligned}\wp_{ij}([n]P) &= \wp_{ij}(P) + \frac{\phi_n^{(i)}(P)\phi_n^{(j)}(P) - \phi_n(P)\phi_n^{(ij)}(P)}{n^2\phi_n^2(P)},\\ \wp_{ijk}([n]P) &= \frac{1}{n}\wp_{ijk}(P) - \frac{\phi_n^{(ijk)}\phi_n^2 - \left(\phi_n^{(ij)}\phi_n^{(k)} + \phi_n^{(ki)}\phi_n^{(j)} + \phi_n^{(jk)}\phi_n^{(i)}\right)\phi_n + 2\phi_n^{(i)}\phi_n^{(j)}\phi_n^{(k)}}{n^3\phi_n^3}(P).\end{aligned}$$

1.6 Formal groups

We define the notion of a formal group, and describe ways in which it is useful for the study of elliptic curves and Jacobians of genus 2 curves. This section is based on [32, Chapter IV] for one-dimensional groups, and [5] for more general statements. In this chapter, R denotes a commutative ring with identity.

Definition 1.6.1 ([5, Definition 1.1]). An *n-parameter formal group* $\mathcal{F}$ over R is a collection of n power series

$$F_i(X_1, \ldots, X_n, Y_1, \ldots, Y_n) \in R[[X_1, \ldots, X_n, Y_1, \ldots, Y_n]]$$

in $2n$ variables with the following properties, where we write $\boldsymbol{F} = (F_1, \ldots F_n)$, and define $\boldsymbol{X}$, $\boldsymbol{Y}$ similarly:

1. $F_i(\boldsymbol{X}, \boldsymbol{Y}) = X_i + Y_i + (\text{terms of total degree } \geq 2)$.
2. $\boldsymbol{F}(\boldsymbol{X}, \boldsymbol{F}(\boldsymbol{Y}, \boldsymbol{Z})) = \boldsymbol{F}(\boldsymbol{F}(\boldsymbol{X}, \boldsymbol{Y}), \boldsymbol{Z})$.

$\boldsymbol{F}(\boldsymbol{X}, \boldsymbol{Y})$ is called the *formal group law* of $\mathcal{F}$. We denote the formal group by $(\mathcal{F}, \boldsymbol{F})$ if we want to make the formal group law explicit. If $\boldsymbol{F}$ furthermore satisfies $\boldsymbol{F}(\boldsymbol{X}, \boldsymbol{Y}) = \boldsymbol{F}(\boldsymbol{Y}, \boldsymbol{X})$, we say $\mathcal{F}$ is *commutative*.

Lemma 1.6.2 ([5, p. 1]). *Let $\mathcal{F}$ be an n-parameter (possibly noncommutative) formal group over R with group law $\boldsymbol{F}(\boldsymbol{X}, \boldsymbol{Y})$. It satisfies the following properties:*

1. *$\boldsymbol{F}(\boldsymbol{X}, \boldsymbol{0}) = \boldsymbol{X}$ and $\boldsymbol{F}(\boldsymbol{0}, \boldsymbol{Y}) = \boldsymbol{Y}$.*
2. *There is a unique collection of n power series $\boldsymbol{i}(\boldsymbol{T}) \in R[[T_1, \ldots, T_n]]$, calded the formal inverse, satisfying $\boldsymbol{F}(\boldsymbol{T}, \boldsymbol{i}(\boldsymbol{T})) = \boldsymbol{F}(\boldsymbol{i}(\boldsymbol{T}), \boldsymbol{T}) = \boldsymbol{0}$ and*

$$\boldsymbol{i}(\boldsymbol{T}) = -\boldsymbol{T} + (\textit{terms of total degree} \geq 2).$$

An important example of a commutative formal group, which we will use later, is the *n-parameter formal additive group* $(\hat{\mathbb{G}}_a^n, \boldsymbol{F}_a)$ defined by the formal group law $\boldsymbol{F}_a(\boldsymbol{X}, \boldsymbol{Y}) = \boldsymbol{X} + \boldsymbol{Y}$.

Definition 1.6.3 ([32, Section IV.2], [5, Definition 1.2]). Let $(\mathcal{F}, \boldsymbol{F})$ and $(\mathcal{G}, \boldsymbol{G})$ be an n-parameter and an m-parameter formal group over R, respectively. A *formal group homomorphism* $\boldsymbol{f}$ from $\mathcal{F}$ to $\mathcal{G}$ defined over R is a collection of m power series $f_1, \ldots, f_m \in R[[T_1, \ldots, T_n]]$ with no constant term, that satisfies

$$\boldsymbol{f}(\boldsymbol{F}(\boldsymbol{X}, \boldsymbol{Y})) = \boldsymbol{G}(\boldsymbol{f}(\boldsymbol{X}), \boldsymbol{f}(\boldsymbol{Y})).$$

The homomorphism $\boldsymbol{f}$ is an *isomorphism* if there exists a formal group homomorphism $\boldsymbol{g}$ from $\mathcal{G}$ to $\mathcal{F}$ such that $\boldsymbol{f}(\boldsymbol{g}(\boldsymbol{T})) = \boldsymbol{T}$ and $\boldsymbol{g}(\boldsymbol{f}(\boldsymbol{T})) = \boldsymbol{T}$.

Definition 1.6.4 ([32, Section IV.2]). Let $(\mathcal{F}, \boldsymbol{F})$ be a commutative n-parameter formal group. We define the *multiplication-by-m maps* for $m \in \mathbb{Z}$ inductively as homomorphisms $[m] \colon \mathcal{F} \to \mathcal{F}$ by

$$\begin{aligned} [0](\boldsymbol{T}) &= \boldsymbol{0}, \\ [m+1](\boldsymbol{T}) &= \boldsymbol{F}([m](\boldsymbol{T}), \boldsymbol{T}), \\ [m-1](\boldsymbol{T}) &= \boldsymbol{F}([m](\boldsymbol{T}), \boldsymbol{i}(\boldsymbol{T})). \end{aligned}$$

Proposition 1.6.5 ([32, IV, Proposition 2.3]). *Let $\mathcal{F}$ be a formal group over R and let $m \in \mathbb{Z}$. Then*

$$[m](\boldsymbol{T}) = m\boldsymbol{T} + (\textit{terms of total degree} \geq 2).$$

Furthermore, $[m]$ is an isomorphism precisely when $m \in R^\times$.

Proof. This can be proven using the inductive definition of the map $[m]$. Clearly, we have $[0](\boldsymbol{T}) = \boldsymbol{0} = 0\boldsymbol{T}$. Now let us assume that the result holds for $m = k \geq 0$, so we have $[k](\boldsymbol{T}) = k\boldsymbol{T} + (\text{higher order terms})$. Then

$$\begin{aligned} [k+1](\boldsymbol{T}) &= \boldsymbol{F}([k](\boldsymbol{T}), \boldsymbol{T}) \\ &= [k](\boldsymbol{T}) + \boldsymbol{T} + (\text{terms of total degree} \geq 2) \\ &= k\boldsymbol{T} + \boldsymbol{T} + (\text{terms of total degree} \geq 2) \\ &= (k+1)\boldsymbol{T} + (\text{terms of total degree} \geq 2). \end{aligned}$$

This shows the first statement is true for all $m \geq 0$. A similar induction argument shows the statement for all $m < 0$. For the second part of the proposition, we note that according to [38, Lemma 1.4], $[m]$ is an isomorphism if and only if the matrix $\left(\frac{\partial [m]_i}{\partial T_j}(\boldsymbol{0})\right)$ is invertible over R. By what we just found, we have $\left(\frac{\partial [m]_i}{\partial T_j}(\boldsymbol{0})\right) = (m\delta_{ij})$ (where δ_{ij} is the Kronecker delta function), which is invertible over R precisely when $m \in R^\times$. ∎

1.6.1 Groups associated to formal groups

Let us now assume that R is a complete local commutative ring with maximal ideal $\mathfrak{m}$, and let $(\mathcal{F}, \boldsymbol{F})$ be an n-parameter formal group over R. In this case, if we take $\boldsymbol{r} = (r_1, \ldots, r_n)$ and $\boldsymbol{s} = (s_1, \ldots, s_n)$ in $\prod_{i=1}^n \mathfrak{m}$ (the Cartesian product of n copies of $\mathfrak{m}$), then $\boldsymbol{F}(\boldsymbol{r}, \boldsymbol{s})$ converges in $\prod_{i=1}^n \mathfrak{m}$ by the completeness of R. Similarly, $\boldsymbol{i}(\boldsymbol{r})$ converges in $\prod_{i=1}^n \mathfrak{m}$. Hence we can use $\mathcal{F}$ to define a group.

Definition 1.6.6 (generalization of [32, p. 123, Definition]). The *group associated to* $\mathcal{F}$, which we denote by $\mathcal{F}(\prod_{i=1}^n \mathfrak{m})$, is a group with underlying set $\prod_{i=1}^n \mathfrak{m}$, group operations

$$\boldsymbol{r} + \boldsymbol{s} = \boldsymbol{F}(\boldsymbol{r}, \boldsymbol{s}) \text{ for all } \boldsymbol{r}, \boldsymbol{s} \in \prod_{i=1}^{n} \mathfrak{m},$$
$$-\boldsymbol{r} = \boldsymbol{i}(\boldsymbol{r}) \text{ for all } \boldsymbol{r} \in \prod_{i=1}^{n} \mathfrak{m}$$

and identity element $\mathbf{0} = (0, \ldots, 0) \in \prod_{i=1}^n \mathfrak{m}$.

The fact that this defines a group follows from the properties of the formal group law.

Proposition 1.6.7. *Let $(\mathcal{F}, \boldsymbol{F})$ and $(\mathcal{G}, \boldsymbol{G})$ be an n-parameter and an m-parameter formal group over R, respectively. Let $\boldsymbol{f}$ be a formal group homomorphism from $\mathcal{F}$ to $\mathcal{G}$. Then $\boldsymbol{f}$ converges for all $\boldsymbol{r} \in \prod_{i=1}^n \mathfrak{m}$ and it defines a group homomorphism*

$$\begin{aligned} \boldsymbol{f} \colon \mathcal{F}(\textstyle\prod_{i=1}^n \mathfrak{m}) &\to \mathcal{G}(\textstyle\prod_{i=1}^m \mathfrak{m}) \\ (r_1, \ldots, r_n) &\mapsto \boldsymbol{f}(r_1, \ldots, r_n). \end{aligned}$$

If $\boldsymbol{f}$ is a formal group isomorphism, then this group homomorphism is also an isomorphism.

Proof. The fact that R is complete with respect to $\mathfrak{m}$ ensures that $\boldsymbol{f}$ converges on $\prod_{i=1}^n \mathfrak{m}$. We have $\boldsymbol{f}(\boldsymbol{r} + \boldsymbol{s}) = \boldsymbol{f}(\boldsymbol{F}(\boldsymbol{r}, \boldsymbol{s})) = \boldsymbol{G}(\boldsymbol{f}(\boldsymbol{r}), \boldsymbol{f}(\boldsymbol{s})) = \boldsymbol{f}(\boldsymbol{r}) + \boldsymbol{f}(\boldsymbol{s})$ for all $\boldsymbol{r}, \boldsymbol{s} \in \prod_{i=1}^n \mathfrak{m}$. ■

Proposition 1.6.8. *The group homomorphism induced by $[m]$ on $\mathcal{F}(\prod_{i=1}^n \mathfrak{m})$ is the usual multiplication-by-m homomorphism on a group.*

Proof. Let $\boldsymbol{r} \in \prod_{i=1}^n \mathfrak{m}$, and let us denote by $m\boldsymbol{r}$ the sum of m copies of $\boldsymbol{r}$ in $\mathcal{F}(\prod_{i=1}^n \mathfrak{m})$ if $m \geq 0$, or the sum of $-m$ copies of $-\boldsymbol{r}$ if $m < 0$. We show the result by induction on m. Clearly, $0 \cdot \boldsymbol{r} = \mathbf{0} = [0](\boldsymbol{r})$. Now assume the statement is true for $m = k \in \mathbb{Z}_{\geq 0}$. Then we get

$$\begin{aligned} (k+1)\boldsymbol{r} &= k\boldsymbol{r} + \boldsymbol{r} \\ &= [k](\boldsymbol{r}) + \boldsymbol{r} \\ &= F([k](\boldsymbol{r}), \boldsymbol{r}) \\ &= [k+1](\boldsymbol{r}). \end{aligned}$$

Similarly, if we assume the result holds for $m = k \in \mathbb{Z}_{\leq 0}$, we get

$$\begin{aligned} (k-1)\boldsymbol{r} &= k\boldsymbol{r} - \boldsymbol{r} \\ &= [k](\boldsymbol{r}) + \boldsymbol{i}(\boldsymbol{r}) \\ &= F([k](\boldsymbol{r}), \boldsymbol{i}(\boldsymbol{r})) \\ &= [k-1](\boldsymbol{r}). \end{aligned}$$

■

In this thesis, we often consider the situation where R is the ring of p-adic integers $\mathbb{Z}_p$ for a prime p, which is complete with respect to its maximal ideal $p\mathbb{Z}_p$. In this case we have a result about the image of the multiplication-by-p^m map. We use the notation $(p\mathbb{Z}_p)^n$ for the Cartesian product of n copies of $p\mathbb{Z}_p$, and $p^n\mathbb{Z}_p$ for the n-th power of the ideal $p\mathbb{Z}_p$.

Proposition 1.6.9. *Let p be a prime. Let $(\mathcal{F}, \boldsymbol{F})$ be a commutative n-parameter formal group over $\mathbb{Z}_p$. For all $\boldsymbol{r} \in (p\mathbb{Z}_p)^n$ and $m \in \mathbb{Z}_{\geq 0}$, we have $[p^m](\boldsymbol{r}) \in (p^{m+1}\mathbb{Z}_p)^n$.*

Proof. We prove this by induction on m. Because $\boldsymbol{r} \in (p\mathbb{Z}_p)^n$, the result is true for $m = 0$. Now assume it is true for $m = k \geq 0$. By Proposition 1.6.5, we have

$$[p^{k+1}](\boldsymbol{r}) = [p]([p^k](\boldsymbol{r})) = p[p^k](\boldsymbol{r}) + \boldsymbol{g}([p^k](\boldsymbol{r}))$$

for some $\boldsymbol{g} = (g_1, \ldots, g_n)$ with $g_i \in (r_1, \ldots, r_n)^2\mathbb{Z}_p[[\boldsymbol{r}]]$. Let us denote by $[p^{k+1}]_i(\boldsymbol{r})$ the i-th component of $[p^{k+1}](\boldsymbol{r})$. Then it is of the form $[p^{k+1}]_i(\boldsymbol{r}) = p[p^k]_i(\boldsymbol{r}) + g_i([p^k](\boldsymbol{r}))$. Because $[p^k]_i(\boldsymbol{r}) \in p^{k+1}\mathbb{Z}_p$ by the induction hypothesis, we have $p[p^k]_i(\boldsymbol{r}) \in p^{k+2}\mathbb{Z}_p$. Furthermore, because $g_i \in (r_1, \ldots, r_n)^2\mathbb{Z}_p[[\boldsymbol{r}]]$, we obtain that $g_i([p^k](\boldsymbol{r})) \in p^{2(k+1)}\mathbb{Z}_p \subseteq p^{k+2}\mathbb{Z}_p$. This shows that $[p^{k+1}]_i(\boldsymbol{r}) \in p^{k+2}\mathbb{Z}_p$ for all $i = 1, \ldots, n$, and hence $[p^{k+1}](\boldsymbol{r}) \in (p^{k+2}\mathbb{Z}_p)^n$. ∎

1.6.2 The formal group associated to an elliptic curve

Let E be an elliptic curve over a perfect field K, defined by the homogeneous equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3. \tag{1.22}$$

Let $R = \mathbb{Z}[a_1, \ldots, a_6]$. We can define a formal group associated to E. If we consider the dehomogenization of (1.22) with respect to Y, we get the affine equation

$$w = t^3 + a_1tw + a_2t^2w + a_3w^2 + a_4tw^2 + a_6w^3 =: f(t, w) \tag{1.23}$$

in the variables $w = -\frac{Z}{Y}$ and $t = -\frac{X}{Y}$, corresponding to the affine part of E where $Y \neq 0$. Let us denote the coordinate ring of E by $K[E] := K[t, w]/(f(t, w) - w)$, and its fraction field by $K(E)$. Let us consider the local ring at the point at infinity $\mathcal{O} = [0 : 1 : 0]$, which is the ring

$$\mathcal{O}_{E,\mathcal{O}} = \left\{ \frac{g}{h} \in K(E) \;\middle|\; g, h \in K[E] \text{ with } h(0,0) \neq 0 \right\},$$

and let us denote its maximal ideal by $\mathfrak{m}_{\mathcal{O}} = \{g/h \in \mathcal{O}_{E,\mathcal{O}} \mid g(0,0) = 0\}$. We note that $\mathfrak{m}_{\mathcal{O}} = (w, t) = (t)$, because

$$w = \frac{t^3}{1 - a_1t - a_2t^2 - a_3w - a_4tw - a_6w^2} \in t\mathcal{O}_{E,\mathcal{O}}.$$

Hence $t := -\frac{X}{Y}$ is a uniformiser of $\mathcal{O}_{E,\mathcal{O}}$. Using (1.23) and a general version of Hensel's lemma (see [32, IV, Lemma 1.2]), we get the following result.

Proposition 1.6.10 ([32, IV, Proposition 1.1]). *There exists a unique power series $w^T(T)$ in $K[[T]]$ that satisfies $w^T(0) = 0$ and $w^T(T) = f(T, w^T(T))$. It is of the form*

$$w^T(T) = T^3 + \sum_{i=4}^{\infty} A_iT^i$$

with $A_i \in R$, so $w^T(T) \in R[[T]]$. Explicitly, we have $A_4 = a_1$ and $A_5 = a_1^2 + a_2$.

Using this power series, we define a map between $\mathcal{O}_{E,\mathcal{O}}$ and the power series ring $K[[T]]$.

Proposition 1.6.11. *Let us define the map*

$$\begin{aligned}\varphi\colon\ \mathcal{O}_{E,\mathcal{O}} &\to K[[T]]\\ \frac{g(t,w)}{h(t,w)} &\mapsto g(T,w^T(T))(h(T,w^T(T)))^{-1}.\end{aligned}$$

This map is a well-defined ring homomorphism, which is furthermore injective. In particular, $\mathcal{O}_{E,\mathcal{O}}$ is isomorphic to a subring of $K[[T]]$.

Proof. First of all, we note that if $g/h \in \mathcal{O}_{E,\mathcal{O}}$, then $h(0,0) \neq 0$ and hence $h(T,w^T(T))$ is invertible in $K[[T]]$. Furthermore, if $g_1/h_1 = g_2/h_2$ in $\mathcal{O}_{E,\mathcal{O}}$, then

$$g_1(t,w)h_2(t,w) = g_2(t,w)h_1(t,w) + g(t,w)(f(t,w) - w)$$

for some $g \in K[E]$, and because $f(T,w^T(T)) - w^T(T) = 0$ by Proposition 1.6.10, it follows that $\varphi(g_1/h_1) = \varphi(g_2/h_2)$.

For injectivity, we consider the completion of $\mathcal{O}_{E,\mathcal{O}}$ with respect to its maximal ideal $t\mathcal{O}_{E,\mathcal{O}}$. It follows from the construction of w^T that $w^T(t)$ converges to w in this completion (see [32, Section IV.1]). Hence if $\varphi(g/h) = 0$, we have $g(T,w^T(T)) = 0$ in $K[[T]]$, and so we get $g(t,w^T(t)) = g(t,w) = 0$ in the completion of $\mathcal{O}_{E,\mathcal{O}}$. We conclude that φ is injective. ∎

The function field of E/K, which is the fraction field of $\mathcal{O}_{E,\mathcal{O}}$ is then also isomorphic to a subfield of the fraction field of $K[[T]]$, which is the field of formal Laurent series $K((T))$. An injective homomorphism can be given by

$$\begin{aligned}Q(\mathcal{O}_{E,\mathcal{O}}) = K(E) &\to K((T))\\ \frac{g(t,w)}{h(t,w)} &\mapsto \frac{\varphi(g(t,w))}{\varphi(h(t,w))},\end{aligned}$$

and we also denote it by φ. Hence we can also describe the coordinate functions $x = \frac{X}{Z} = \frac{t}{w}$ and $y = \frac{Y}{Z} = -\frac{1}{w}$ (the affine coordinates when dehomogenized with respect to Z) as Laurent series in $K((T))$. We find

$$\begin{aligned}x^T(T) := \varphi(x) &= \varphi\left(\frac{t}{w}\right) = \frac{T}{w^T(T)} = T^{-2} - a_1T^{-1} - a_2 - a_3T + \dots\\ y^T(T) := \varphi(y) &= \varphi\left(-\frac{1}{w}\right) = -\frac{1}{w^T(T)} = -T^{-3} + a_1T^{-2} + a_2T^{-1} + a_3 + \dots\end{aligned} \tag{1.24}$$

Because $w^T(T) \in R[[T]]$ and has leading coefficient $1 \in R^\times$, both $x^T(T)$ and $y^T(T)$ also have coefficients in R.

From our definition of $w^T(T)$, we deduce that the pair $\big(x^T(T), y^T(T)\big)$ is a solution to the Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ in $K((T))$. Let us specialize to the case $K = \mathbb{Q}_p$ for some prime p, and $a_i \in \mathbb{Z}_p$ (in general, we could choose a complete local field with ring of integers S such that $a_i \in S$, but we will not need this generality). In this case, the series $x^T(T)$ and $y^T(T)$ converge for $T \in p\mathbb{Z}_p \setminus \{0\}$ to a limit in $\mathbb{Q}_p$, and we obtain $\big(x^T(T), y^T(T)\big) \in E(\mathbb{Q}_p)$. We define an injective map

$$\begin{aligned}\psi\colon p\mathbb{Z}_p &\to E(\mathbb{Q}_p)\\ t &\mapsto \begin{cases}\big(x^T(t), y^T(t)\big) & \text{if } t \neq 0\\ \mathcal{O} & \text{if } t = 0.\end{cases}\end{aligned} \tag{1.25}$$

(The map is injective because on the image, an inverse can be given by $(x,y) \mapsto -\frac{x}{y}$, $\mathcal{O} \mapsto 0$.)

It is possible to define a formal group $(\hat{E}, F)$ in such a way that the map ψ in (1.25) becomes a group homomorphism from the group associated to $\hat{E}$ into $E(\mathbb{Q}_p)$. We outline the construction here, more details can be found in [32, Section IV.1]. To define the formal group law of $\hat{E}$ we look at the addition law on $E(\mathbb{Q}_p)$, for which we need to find the third intersection point of the curve with a line through two points. We consider two coordinates T_1 and T_2, and we define a line through $(T_1, w^T(T_1))$ and $(T_2, w^T(T_2))$ in the (t,w)-plane by finding formal power series $\lambda(T_1,T_2)$ and $\nu(T_1,T_2)$ in $R[[T_1,T_2]]$ such that $(T_1, w^T(T_1))$ and $(T_2, w^T(T_2))$ are solutions of the equation $w = \lambda t + \nu$. We also know that $w^T(T_i) = f(T_i, w^T(T_i))$ for $i = 1, 2$ from Proposition 1.6.10. Hence T_1 and T_2 are two roots in $R[[T_1,T_2]]$ of the cubic polynomial

$$\lambda(T_1,T_2)t + \nu(T_1,T_2) - f\left(t, \lambda(T_1,T_2)t + \nu(T_1,T_2)\right)$$

in $R[[T_1,T_2]][t]$. Let us denote the third root by $l(T_1,T_2) \in R[[T_1,T_2]]$. Then in the (t,w)-plane, the point $(l(T_1,T_2), w^T(l(T_1,T_2)))$ is colinear with $(T_1, w^T(T_1))$ and $(T_2, w^T(T_2))$. We define $F(T_1,T_2) := i(l(T_1,T_2))$, where

$$i(T) = \frac{x^T(T)}{y^T(T) + a_1 x^T(T) + a_3} = -T - a_1 T^2 + \cdots \in R[[T]]$$

is the series that gives the t-coordinate of the inverse of $(T, w^T(T))$. From the properties of the addition law on E, we can deduce that $F \in R[[T_1,T_2]]$ and

$$\begin{aligned} F(T_1,T_2) &= F(T_2,T_1) \\ F(T_1,F(T_2,T_3)) &= F(F(T_1,T_2),T_3) \\ F(T,0) &= F(0,T) = T \\ F(T_1,T_2) &= T_1 + T_2 + (\text{terms of degree} \geq 2)). \end{aligned}$$

This shows that F indeed defines a one-parameter commutative formal group over R (and hence over $\mathbb{Z}_p$), denoted by $\hat{E}$. This is the formal group associated to the elliptic curve E.

We can then also define the group $\hat{E}(p\mathbb{Z}_p)$ associated to $\hat{E}$. From the way that F was defined, it follows that the map ψ in (1.25) is a group homomorphism from $\hat{E}(p\mathbb{Z}_p)$ to $E(\mathbb{Q}_p)$ ([32, Example IV.3.1.3]). It turns out ([32, VII, Proposition 2.2]) that the image of ψ in $E(\mathbb{Q}_p)$ is $E_1(\mathbb{Q}_p)$. Hence (1.25) defines an isomorphism

$$\psi \colon \hat{E}(p\mathbb{Z}_p) \to E_1(\mathbb{Q}_p). \tag{1.26}$$

We write $\psi^{-1}(P) = t(P)$ for the inverse map, because it corresponds to the t-coordinate of the point P (where $t = -\frac{X}{Y}$). With this notation we then have $x^T(t(P)) = x(P)$ and $y^T(t(P)) = y(P)$. In particular we use that every $P \in E_1(\mathbb{Q}_p)$ reduces to $[0:1:0]$ modulo p. This implies that $\mathrm{ord}_p(x(P)) > \mathrm{ord}_p(y(P))$, and hence $\mathrm{ord}_p(t(P)) = \mathrm{ord}_p\left(-\frac{x(P)}{y(P)}\right) > 0$. so indeed $t(P) \in p\mathbb{Z}_p$.

Lemma 1.6.12. *For all $P \in E_1(\mathbb{Q}_p)$, we have*

$$t([m]P) = [m](t(P)),$$

where on the left $[m]$ denotes the multiplication-by-m map on $E(\mathbb{Q}_p)$, and on the right we evaluate the power series defining the multiplication-by-m homomorphism $[m] \in \mathbb{Z}_p[[T]]$ from Definition 1.6.4 at $t(P) \in p\mathbb{Z}_p$.

Proof. Because ψ is a group homomorphism, we get

$$\begin{aligned} t([m]P) &= m \cdot t(P) \\ &= [m](t(P)). \qquad \text{(Proposition 1.6.8)} \end{aligned}$$

■

Corollary 1.6.13. *Let $P \in E_1(\mathbb{Q}_p)$. Then for all $n \geq 0$,*

$$\mathrm{ord}_p(t([p^n]P)) \geq n + 1.$$

Proof. Because $t(P) \in \hat{E}(p\mathbb{Z}_p)$, Lemma 1.6.12 and Proposition 1.6.9 imply that for all $n \geq 0$,

$$t([p^n](P)) = [p^n](t(P)) \in p^{n+1}\mathbb{Z}_p.$$

■

1.6.3 The formal group associated to the Jacobian of a genus 2 curve

Assume we are looking at a smooth curve $\mathcal{C}$ of genus 2 over a perfect field K given by an affine equation $y^2 = f(x)$, where f is a polynomial of degree 5 with coefficients in a ring $R \subseteq K$. Then we saw in Section 1.5.1 that the corresponding Jacobian can be embedded in $\mathbb{P}^8$. We can construct a formal group in a similar way as we did for elliptic curves. We have the projective coordinates $X_0, X_{11}, X_{12}, X_{22}, X_{111}, X_{112}, X_{122}, X_{222}, X$ of $\mathbb{P}^8$. Recall that the identity element $\mathcal{O}$ in J has $X_{111} \neq 0$ and all other coordinates equal to 0. Let us then look at the affine part of J where $X_{111} \neq 0$. We can dehomogenize the defining equations of J accordingly. Now let us consider the local ring $\mathcal{O}_{J,\mathcal{O}}$ of J at $\mathcal{O}$. Then if we write $x = \frac{X}{X_{111}}$, $x_0 = \frac{X_0}{X_{111}}$, $x_{ij} = \frac{X_{ij}}{X_{111}}$ and $x_{ijk} = \frac{X_{ijk}}{X_{111}}$, we know that the maximal ideal $\mathfrak{m}$ of $\mathcal{O}_{J,\mathcal{O}}$ is the ideal generated by the functions $x_0, x_{11}, x_{12}, x_{22}, x_{112}, x_{122}, x_{222}, x$. We want to find parameters t_1 and t_2 in $\mathcal{O}_{J,\mathcal{O}}$ such that we can make an identification

$$\widetilde{\mathcal{O}}_{J,\mathcal{O}} \cong K[[t_1, t_2]],$$

where $\widetilde{\mathcal{O}}_{J,\mathcal{O}}$ denotes the completion of $\mathcal{O}_{J,\mathcal{O}}$ with respect to its maximal ideal.

Lemma 1.6.14. *Let $t_1 = -x_{11}$ and $t_2 = -x$. Then t_1 and t_2 form a basis for the K-vector space $\mathfrak{m}/\mathfrak{m}^2$.*

Proof. Recall that $\mathcal{O}_{J,\mathcal{O}}$ is a noetherian local ring. We have $\mathcal{O}_{J,\mathcal{O}}/\mathfrak{m} \cong K$ (via the isomorphism $g + \mathfrak{m} \to g(\mathcal{O})$). This also implies that every $g \in \mathcal{O}_{J,\mathcal{O}}$ is of the form $g = r + h$ for some $r \in K$, $h \in \mathfrak{m}$. We mentioned that the functions $x_0, x_{11}, x_{12}, x_{22}, x_{112}, x_{122}, x_{222}, x$ generate $\mathfrak{m}$ as an ideal, and the observation above implies that they also span $\mathfrak{m}/\mathfrak{m}^2$ as a K-vector space. We use the defining equations of J, which are reproduced in the Appendix, to deduce which of these generators are trivial in $\mathfrak{m}/\mathfrak{m}^2$. Equation F_8 divided by X_{111}^3 gives

$$x_0 = x_{11}^3 + f_2 x_0 x_{11}^2 + f_1 x_0 x_{11} x_{12} - 3 f_0 x_0 x_{11} x_{22} + \ldots$$

which shows that $x_0 \in \mathfrak{m}^3$. By dividing equation F_6 by X_{111}^3 we then deduce that $x_{22}^3 \in \mathfrak{m}^4$, and hence $x_{22} \in \mathfrak{m}^2$. Dividing F_2 by X_{111} implies that $x_{12}^2 \in \mathfrak{m}^3$, and hence $x_{12} \in \mathfrak{m}^2$. In a similar way, we successively deduce by dividing F_{10}, F_{11} and F_9 by X_{111}^2 that $x_{122}, x_{222}, x_{112} \in \mathfrak{m}^2$. Hence they are all trivial in $\mathfrak{m}/\mathfrak{m}^2$, and thus the remaining generators are x_{11} and x. Because J is smooth, $\mathfrak{m}/\mathfrak{m}^2$ has dimension 2 as a K-vector space (see [17, I, Theorem 5.1]). This means that x_{11} and x must be linearly independent generators, and equivalently t_1 and t_2 form a K-basis for $\mathfrak{m}/\mathfrak{m}^2$. ■

Proposition 1.6.15. *The morphism of K-algebras*

$$\varphi_J \colon \widetilde{\mathcal{O}}_{J,\mathcal{O}} \to K[[T_1, T_2]]$$

that sends the local parameters t_1 and t_2 of $\widetilde{\mathcal{O}}_{J,\mathcal{O}}$ to the variables T_1 and T_2 in $K[[T_1, T_2]]$ respectively, is an isomorphism.

Proof. This follows from the Cohen structure theorem, see [23, p. 206, Corollary 2]. ■

In particular, we can find expansions for the coordinate functions x_0, x_{ij}, x_{ijk} as power series in $K[[t_1, t_2]]$. In [16, Theorem 4.2] it is shown that their images under φ_J have expansions in $R[[T_1, T_2]]$ of the following form:

$$\begin{aligned}
\varphi_J(x_0) &= -T_1^3 \left(1 + \sum_{i,j\geq 0,\, i+j\geq 1} \alpha_{ij} T_1^i T_2^j\right) \\
\varphi_J(x_{22}) &= T_1 \left(-2T_1T_2 + \sum_{i,j\geq 0,\, i+j\geq 3} \beta_{ij} T_1^i T_2^j\right) \\
\varphi_J(x_{12}) &= T_1 \left(T_2^2 + \sum_{i,j\geq 0,\, i+j\geq 3} \gamma_{ij} T_1^i T_2^j\right) \\
\varphi_J(x_{112}) &= -T_2^2 + \sum_{\substack{i,j\geq 0 \\ i+j>3}} \delta_{ij} T_1^i T_2^j \\
\varphi_J(x_{122}) &= T_1T_2 + \sum_{\substack{i,j\geq 0 \\ i+j>3}} \epsilon_{ij} T_1^i T_2^j \\
\varphi_J(x_{222}) &= -T_1^2 + \sum_{\substack{i,j\geq 0 \\ i+j>3}} \zeta_{ij} T_1^i T_2^j
\end{aligned} \tag{1.27}$$

with $\alpha_{ij}, \beta_{ij}, \gamma_{ij}, \delta_{ij}, \epsilon_{ij}, \zeta_{ij} \in R$. By definition of φ_J we have

$$\varphi_J(g)(t_1, t_2) = g \text{ for all } g \in \widetilde{\mathcal{O}}_{J,\mathcal{O}}. \tag{1.28}$$

The coordinate functions in (1.16) are not necessarily in $\widetilde{\mathcal{O}}_{J,\mathcal{O}}$, but they are in its field of fractions $Q(\widetilde{\mathcal{O}}_{J,\mathcal{O}})$. We can derive series expansions corresponding to these functions in the field of fractions $Q(K[[T_1, T_2]])$. We use the notation φ_J also for the isomorphism extending the map in Proposition 1.6.15 to the corresponding fields of fractions. For the functions defining the map to the Kummer surface (1.17), we have $\wp_{ij} = \frac{x_{ij}}{x_0}$. To find the corresponding image in $Q(K[[T_1, T_2]])$, we first work out the expansion of $\varphi_J(x_0)$ in a bit more detail.

Lemma 1.6.16. *The expansion $\varphi_J(x_0)$ is of the form*

$$\varphi_J(x_0) = -T_1^3 \alpha(T_1, T_2),$$

where α is of the form $\alpha(T_1, T_2) = 1 + f_2 T_1^2 + (\text{terms of total degree} \geq 4)$.

Proof. We already saw above that $\varphi_J(x_0) = -T_1^3\alpha(T_1,T_2)$ for some $\alpha \in 1+(T_1,T_2)R[[T_1,T_2]]$. Let us look at equation F_8 and divide it by X_{111}^3. It has to vanish on J by definition, so we obtain the equation

$$x_0 = x_{11}^3 + f_2x_0x_{11}^2 + f_1x_0x_{11}x_{12} - 3f_0x_0x_{11}x_{22} - 2f_0x_0^2x - (4f_4f_0 - f_3f_1)x_0^2x_{11} + 3f_3f_0x_0^2x_{12} \\ - (3f_2f_0 - f_1^2)x_0^2x_{22} - (4f_4f_2f_0 + f_1f_0 - f_4f_1^2 - f_3^2f_0)x_0^3.$$

We saw in (1.27) that in the expansions of x_0, x_{12} and x_{22} all nonzero terms have total degree at least 3, and we have $x_{11} = -t_1$. By our observations above, we conclude that all terms on the right-hand side, except the first two, are power series in t_1 and t_2 whose terms all have total degree at least 7. The second term, $f_2x_0x_{11}^2$, only has terms of degree ≥ 5. We then deduce, by comparing coefficients on the left- and right-hand side, that $\alpha_{30} = -1$, $\alpha_{31} = \alpha_{40} = \alpha_{41} = \alpha_{32} = 0$, $\alpha_{50} = f_2\alpha_{30} = -f_2$ and $\alpha_{60} = \alpha_{51} = \alpha_{42} = \alpha_{31} = 0$. This gives the desired result. ∎

The series α is invertible in $R[[T_1,T_2]]$, and its inverse is of the form

$$\alpha^{-1}(T_1,T_2) = 1 - f_2T_1^2 + (\text{terms of total degree} \geq 4).$$

We get

$$\varphi_J(x_0)^{-1} = -T_1^{-3}\alpha^{-1}(T_1,T_2).$$

Using the expansions in (1.27), we then find

$$\begin{aligned} \wp_{22}^T(T) &:= \varphi_J(\wp_{22}) = \varphi_J(x_{22})/\varphi_J(x_0) = T_1^{-2}\left(2T_1T_2 + \sum_{i,j\geq 0,\ i+j\geq 3} \beta'_{ij}T_1^iT_2^j\right) \\ -\wp_{12}^T(T) &:= \varphi_J(-\wp_{12}) = -\varphi_J(x_{12})/\varphi_J(x_0) = T_1^{-2}\left(T_2^2 + \sum_{i,j\geq 0,\ i+j\geq 3} \gamma'_{ij}T_1^iT_2^j\right) \\ \wp_{11}^T(T) &:= \varphi_J(\wp_{11}) = \varphi_J(x_{11})/\varphi_J(x_0) = T_1^{-2}\alpha^{-1}(T_1,T_2) \end{aligned} \tag{1.29}$$

where $\beta'_{ij}, \gamma'_{ij} \in R$.

Now let us look at the case where $K = \mathbb{Q}_p$ and where the coefficients of f are in $\mathbb{Z}_p$. Note that when $P \in J_1(\mathbb{Q}_p)$, we have $\mathrm{ord}_p(X_{11}(P)), \mathrm{ord}_p(X(P)) > \mathrm{ord}_p(X_{111}(P))$, and hence $t_1(P), t_2(P) \in p\mathbb{Z}_p$. It turns out there is a bijection ([16, Corollary 4.5])

$$\begin{aligned} \psi_J\colon J_1(\mathbb{Q}_p) &\to (p\mathbb{Z}_p)^2 \\ P &\mapsto (t_1(P), t_2(P)). \end{aligned} \tag{1.30}$$

Furthermore, this bijection induces a formal group structure on $(p\mathbb{Z}_p)^2$ (see [16, Theorem 4.6]). In other words, using this bijection we can define a pair of power series $\boldsymbol{F}_J(\boldsymbol{X},\boldsymbol{Y})$ which is the group law of a 2-parameter formal group $\hat{J}$ over $\mathbb{Z}_p$. This group law is defined in such a way that ψ_J is a group homomorphism from $J_1(\mathbb{Q}_p)$ to the group $\hat{J}\left((p\mathbb{Z}_p)^2\right)$ associated to the formal group $(\hat{J}, \boldsymbol{F}_J)$. We use the notation $\boldsymbol{t}(P) = (t_1(P), t_2(P))$.

We note that $t_1 = -\frac{\wp_{11}}{\wp_{111}}$ and $t_2 = -\frac{\wp}{\wp_{111}}$ are odd functions, in the sense that $t_i(-P) = -t_i(P)$. This follows from the fact that $\wp_{11}$ and $\wp$ are even functions and $\wp_{111}$ is an odd function on J. This implies that the pair of power series defining the inverse on $\hat{J}$ is simply $\boldsymbol{i}_J(\boldsymbol{T}) = -\boldsymbol{T}$. Because ψ_J is a homomorphism, it furthermore follows that for all $P, Q \in J_1(\mathbb{Q}_p)$, we have

$$\boldsymbol{F}_J(-\boldsymbol{t}(P), -\boldsymbol{t}(Q)) = \boldsymbol{F}_J(\boldsymbol{t}(-P), \boldsymbol{t}(-Q)) = \boldsymbol{t}(-P-Q) = -\boldsymbol{t}(P+Q) = -\boldsymbol{F}_J(\boldsymbol{t}(P), \boldsymbol{t}(Q)).$$

We thus have $\boldsymbol{F}_J(-\boldsymbol{X}, -\boldsymbol{Y}) = -\boldsymbol{F}_J(\boldsymbol{X}, \boldsymbol{Y})$ as series, which implies that $\boldsymbol{F}_J$ is an odd series in the sense that it only has terms of total odd degree.

We have a result analogous to Lemma 1.6.12.

Lemma 1.6.17. *Let $P \in J_1(\mathbb{Q}_p)$. Then*

$$(t_1([m]P), t_2([m]P)) = [m](t_1(P), t_2(P)),$$

where on the left $[m]$ denotes the multiplication-by-m map on $J(\mathbb{Q}_p)$, and on the right we evaluate the power series defining the multiplication-by-m homomorphism $[m] \in \mathbb{Z}_p[[t_1, t_2]]$ at $(t_1(P), t_2(P))$.

Proof. Because ψ_J is a group homomorphism from $J_1(\mathbb{Q}_p)$ to $\hat{J}\left((p\mathbb{Z}_p)^2\right)$, we get

$$\begin{aligned}(t_1([m]P), t_2([m]P) &= \psi_J([m]P) \\ &= m \cdot \psi_J(P) \\ &= [m](t_1(P), t_2(P)). \qquad \text{(by Proposition 1.6.8)}\end{aligned}$$

■

Corollary 1.6.18. *let $P \in J_1(\mathbb{Q}_p)$. For all $n \geq 0$ and for $i = 1, 2$ we have*

$$\mathrm{ord}_p(t_i([p^n]P)) \geq n + 1.$$

Proof. Because $\boldsymbol{t}(P) \in \hat{J}\left((p\mathbb{Z}_p)^2\right)$, Lemma 1.6.17 and Proposition 1.6.9 imply that for all $n \geq 0$,

$$\boldsymbol{t}([p^n]P) = [p^n](\boldsymbol{t}(P)) \in \left(p^{n+1}\mathbb{Z}_p\right)^2.$$

■

1.6.4 The formal logarithm

Let $(\mathcal{F}, \boldsymbol{F})$ be an n-parameter commutative formal group over a commutative ring R with identity. We define *differential forms* as expressions of the form $\omega(\boldsymbol{T}) = \sum_{i=1}^n P_i(\boldsymbol{T})dT_i$, where $P_i(\boldsymbol{T}) \in R[[\boldsymbol{T}]]$. We say ω is an *invariant differential* if it satisfies $\omega(\boldsymbol{F}(\boldsymbol{T}, \boldsymbol{S})) = \omega(\boldsymbol{T})$. Explicitly, this is the case if for all $i = 1, \ldots, n$, we have

$$\sum_{j=1}^{n} P_j(\boldsymbol{F}(\boldsymbol{T}, \boldsymbol{S}))\frac{\partial F_j}{\partial T_i}(\boldsymbol{T}, \boldsymbol{S}) = P_i(\boldsymbol{T})$$

(see [5, Equation (1)]). The collection of invariant differentials form an R-module of rank n (see [5, Corollary 1.4]). We consider a specific basis $\omega_1, \ldots, \omega_n$ as defined in [5, Remark 1.7].

Theorem 1.6.19 ([5, Theorem 1.6]). *Let R be a $\mathbb{Q}$-algebra. Let $\mathcal{L}_i(\boldsymbol{T}) \in R[[\boldsymbol{T}]]$ be the unique power series satisfying*

$$d\mathcal{L}_i(\boldsymbol{T}) = \sum_{j=1}^{n} \frac{\partial \mathcal{L}_i}{\partial T_j} dT_j = \omega_i(\boldsymbol{T}) \quad \textit{and} \quad \mathcal{L}_i(0) = 0.$$

Then $\mathcal{L} = (\mathcal{L}_1, \ldots, \mathcal{L}_n)$ is a formal group isomorphism from $\mathcal{F}$ to $\hat{\mathbb{G}}_a^n$. We call $\mathcal{L}$ the strict formal logarithm.

We denote the inverse of $\mathcal{L}$ by $\mathcal{E}\colon \hat{\mathbb{G}}_a^n \to \mathcal{F}$, and call it the *strict formal exponential*.

Proposition 1.6.20 ([5, Proposition 1.8]). *Let $\mathcal{F}$ be an n-parameter commutative formal group over $\mathbb{Z}$. Then the strict formal logarithm and exponential of $\mathcal{F}$ as a formal group over $\mathbb{Q}$ are of the form*

$$\mathcal{L}_i = T_i + \sum_{\substack{j_1,\ldots,j_n \geq 0 \\ j_1+\cdots+j_n \geq 2}} \frac{a_{j_1,\ldots,j_n}}{\gcd\{j_1,\ldots,j_n\}} T_1^{j_1}\cdots T_n^{j_n} \tag{1.31}$$

$$\mathcal{E}_i = T_i + \sum_{\substack{j_1,\ldots,j_n \geq 0 \\ j_1+\cdots+j_n \geq 2}} \frac{b_{j_1,\ldots,j_n}}{j_1!\cdots j_n!} T_1^{j_1}\cdots T_n^{j_n}$$

with $a_{j_1,\ldots,j_n}, b_{j_1,\ldots,j_n} \in \mathbb{Z}$.

The following theorem is a generalization of [32, IV, Theorem 6.4(a)].

Theorem 1.6.21. *Let p be a prime. Let $(\mathcal{F}, \boldsymbol{F})$ be an n-parameter commutative formal group defined over $\mathbb{Z}$, and hence over $\mathbb{Z}_p$. Then the formal group logarithm $\mathcal{L}(\boldsymbol{T})$ converges for $\boldsymbol{T} \in (p\mathbb{Z}_p)^n$, and it induces a group homomorphism*

$$\mathcal{L}\colon \mathcal{F}\left((p\mathbb{Z}_p)^n\right) \to (\mathbb{Q}_p)^n \tag{1.32}$$

where the group law on $(\mathbb{Q}_p)^n$ is addition.

Proof. Let us consider $\boldsymbol{T} \in (p\mathbb{Z}_p)^n$, and hence $\mathrm{ord}_p(T_i) \geq 1$ for each $i = 1,\ldots,n$. Let us look at a general term of the series (1.31) evaluated at $\boldsymbol{T}$, and write $m = j_1 + \ldots + j_n$. We get

$$\begin{aligned} \mathrm{ord}_p\left(\frac{a_{j_1,\ldots,j_n}}{\gcd\{j_1,\ldots,j_n\}} T_1^{j_1}\cdots T_n^{j_n}\right) &\geq m - \mathrm{ord}_p(\gcd\{j_1,\ldots,j_n\}) \\ &\geq m - \log_{(p)}(m) \end{aligned}$$

where $\log_{(p)}$ denotes the real logarithm with base p. Because this last expression approaches infinity as $m \to \infty$, we conclude that the series (1.31) converges for each i. The fact that $\mathcal{L}$ is a formal group homomorphism then implies that (1.32) is a group homomorphism. ∎

1.6.5 Torsion in formal groups over $\mathbb{Z}_p$

In Section 1.6.2 and Section 1.6.3, we saw that the groups $E_1(\mathbb{Q}_p)$ for an elliptic curve E and $J_1(\mathbb{Q}_p)$ for the Jacobian of a genus 2 curve are both isomorphic to a group associated to a formal group over $\mathbb{Z}_p$. We will show that this means that the groups have trivial torsion subgroups. We first show two more general lemmas that we use to prove the statement.

Lemma 1.6.22. *Let $(\mathcal{F}, \boldsymbol{F})$ be an n-parameter commutative formal group over R with basis of normalized invariant differentials $\omega_1,\ldots,\omega_n$ as in the previous section. Let $\boldsymbol{f}\colon \mathcal{F} \to \mathcal{F}$ be a homomorphism. Then for all $k = 1,\ldots,n$, we have*

$$\omega_k \circ \boldsymbol{f} = \sum_{i=1}^{n} \frac{\partial f_k}{\partial T_i}(\boldsymbol{0})\,\omega_i.$$

Proof. Let us fix $k \in \{1, \ldots, n\}$. Let us write $\omega_k(\boldsymbol{T}) = \sum_{i=1}^{n} P_i^{(k)}(\boldsymbol{T}) dT_i$ with $P_i^{(k)} \in R[[\boldsymbol{T}]]$. First, we show that $\omega_k \circ \boldsymbol{f}$ is an invariant differential. Indeed, we have

$$\begin{aligned}(\omega_k \circ \boldsymbol{f})(\boldsymbol{F}(\boldsymbol{T}, \boldsymbol{S})) &= \omega_k(\boldsymbol{F}(\boldsymbol{f}(\boldsymbol{T}), \boldsymbol{f}(\boldsymbol{S}))) && \text{(because } \boldsymbol{f} \text{ is a homomorphism)} \\ &= \omega_k(\boldsymbol{f}(\boldsymbol{T})). && \text{(because } \omega_k \text{ is an invariant differential)}\end{aligned}$$

Because the ω_i form a basis for R-module of invariant differentials, we thus have

$$\omega_k \circ \boldsymbol{f} = \sum_{i=1}^{n} d_i^{(k)} \omega_i$$

for some $d_i^{(k)} \in R$. The left-hand side can be expanded as

$$\begin{aligned}(\omega_k \circ \boldsymbol{f})(\boldsymbol{T}) &= \sum_{i=1}^{n} P_i^{(k)}(\boldsymbol{f}(\boldsymbol{T})) df_i(\boldsymbol{T}) \\ &= \sum_{j=1}^{n} \left[\sum_{i=1}^{n} P_i^{(k)}(\boldsymbol{f}(\boldsymbol{T})) \frac{\partial f_i}{\partial T_j}(\boldsymbol{T}) \right] dT_j. \end{aligned} \tag{1.33}$$

For the right-hand side, we have

$$\begin{aligned}\sum_{i=1}^{n} d_i^{(k)} \omega_i(\boldsymbol{T}) &= \sum_{i=1}^{n} d_i^{(k)} \left[\sum_{j=1}^{n} P_j^{(i)}(\boldsymbol{T}) dT_j \right] \\ &= \sum_{j=1}^{n} \left[\sum_{i=1}^{n} d_i^{(k)} P_j^{(i)}(\boldsymbol{T}) \right] dT_j. \end{aligned} \tag{1.34}$$

Because (1.33) and (1.34) are equal, each pair of corresponding component functions evaluated at $\mathbf{0}$ must also be equal. Theorem 1.6.19 and Proposition 1.6.20 imply that $P_j^{(i)}(\mathbf{0}) = \frac{\partial \mathcal{L}_i}{\partial T_j}(\mathbf{0}) = \delta_{ij}$ for all $i, j \in \{1, \ldots, n\}$ (where δ_{ij} is the Kronecker delta function). We also have $\boldsymbol{f}(\mathbf{0}) = \mathbf{0}$. We thus get for each $j = 1, \ldots, n$ that

$$\sum_{i=1}^{n} d_i^{(k)} P_j^{(i)}(\mathbf{0}) = \sum_{i=1}^{n} P_i^{(k)}(\boldsymbol{f}(\mathbf{0})) \frac{\partial f_i}{\partial T_j}(\mathbf{0}) \;\Rightarrow\; d_j^{(k)} = \frac{\partial f_k}{\partial T_j}(\mathbf{0}).$$

■

Lemma 1.6.23. *Let $\mathcal{F}$ be an n-parameter commutative formal group over R and let $p \in \mathbb{Z}_{>0}$ be a prime. There are power series $g_k, h_k \in R[[\boldsymbol{T}]]$ with $g_k \in T_k + (T_1, \ldots, T_n)^2 R[[\boldsymbol{T}]]$ and $h_k(\mathbf{0}) = \mathbf{0}$ such that*

$$[p]_k(\boldsymbol{T}) = p \cdot g_k(\boldsymbol{T}) + h_k(T_1^p, \ldots, T_n^p),$$

where $[p]_k$ denotes the k-th component of the multiplication-by-p homomorphism.

Proof. From Proposition 1.6.5, we deduce that $\frac{\partial [p]_i}{\partial T_j}(\mathbf{0}) = \delta_{ij}\, p$. Then Lemma 1.6.22 gives $p\, \omega_k(\boldsymbol{T}) = (\omega_k \circ [p])(\boldsymbol{T})$. Expanding both sides and using the same notation as in Lemma 1.6.22, for each $i = 1, \ldots, n$ we get the equality

$$p \cdot P_i^{(k)}(\boldsymbol{T}) = \sum_{j=1}^{n} P_j^{(k)}([p](\boldsymbol{T})) \frac{\partial [p]_j}{\partial T_i}(\boldsymbol{T}). \tag{1.35}$$

Note that for $j \neq k$, we have $P_j^{(k)}([p](\boldsymbol{T})) \in pR[[\boldsymbol{T}]]$, and $P_k^{(k)}([p](\boldsymbol{T})) \in 1 + (T_1, \ldots, T_n)R[[\boldsymbol{T}]]$. Then $P_k^{(k)}([p](\boldsymbol{T}))$ has a multiplicative inverse which is also in $1 + (T_1, \ldots, T_n)R[[\boldsymbol{T}]]$. Using these facts, (1.35) implies that $\frac{\partial [p]_k}{\partial T_i}(\boldsymbol{T}) \in pR[[\boldsymbol{T}]]$ for each i. If we write

$$[p]_k = \sum_{i_1,\ldots,i_n \geq 0} d_{i_1,\ldots,i_n} T_1^{i_1} \cdots T_n^{i_n}$$

for some $d_{i_1,\ldots,i_n} \in R$, then for each term $d_{i_1,\ldots,i_n} T_1^{i_1} \cdots T_n^{i_n}$ we either have $d_{i_1,\ldots,i_n} \in pR$, or $p \mid \gcd(i_1, \ldots, i_n)$. Hence we can write $[p]_k(\boldsymbol{T}) = pg_k(\boldsymbol{T}) + h_k(T_1^p, \ldots, T_n^p)$ for some $g_k, h_k \in R[[\boldsymbol{T}]]$. The requirement on the coefficients of g_k and h_k follows from Proposition 1.6.5. ■

Theorem 1.6.24 (generalization of [32, IV, Example 6.1.1]). *Let p be an odd prime. For any n-parameter commutative formal group $(\mathcal{F}, \boldsymbol{F})$ over $\mathbb{Z}_p$, the associated group $\mathcal{F}((p\mathbb{Z}_p)^n)$ has a trivial torsion group.*

Proof. We first show that all torsion elements must have a power of p as order. Let $m \in \mathbb{Z}_{>0}$ such that $p \nmid m$. Then $m \in \mathbb{Z}_p^\times$, and hence $[m]$ is a formal group isomorphism by Proposition 1.6.5. But then also the multiplication-by-m map on $\mathcal{F}((p\mathbb{Z}_p)^n)$ is an isomorphism by Proposition 1.6.7 and Proposition 1.6.8, so $[m](\boldsymbol{r}) = \boldsymbol{0}$ precisely when $\boldsymbol{r} = \boldsymbol{0}$. Hence no point can have order exactly m. But if a point $\boldsymbol{r}$ has order mp^n for some $n \geq 0$, then $p^n\boldsymbol{r}$ has order m which is not possible. We conclude that all torsion points have order p^n for some $n \geq 0$.

Now assume $\boldsymbol{r}$ has exact order p. Then we must have $[p](\boldsymbol{r}) = \boldsymbol{0}$. Using Lemma 1.6.23, this becomes

$$[p]_k(\boldsymbol{r}) = p \cdot g_k(\boldsymbol{r}) + h_k(r_1^p, \ldots, r_n^p) = 0$$

for all $k = 1, \ldots, n$, with g_k and h_k as in Lemma 1.6.23. By comparing the order at p of the terms, we deduce that the only possibility for this expression to be 0 is that

$$\operatorname{ord}_p(r_k) \geq 2 \operatorname{ord}_p(r_i)$$

for some $i \in \{1, \ldots, n\}$. However, this cannot be satisfied for all k simultaneously unless $\boldsymbol{r} = \boldsymbol{0}$. We conclude that a point of exact order p cannot exist. But if $\boldsymbol{r}$ has exact order p^n for some $n \geq 1$, then $p^{n-1}\boldsymbol{r}$ has exact order p which is not possible. Hence there can be no nontrivial torsion points. ■

Corollary 1.6.25. *Let p be an odd prime, and let $E/\mathbb{Q}_p$ be an elliptic curve given by a Weierstrass equation with coefficients in $\mathbb{Z}_p$. Then $E_1(\mathbb{Q}_p) \cap E_{\text{tors}} = \{\mathcal{O}\}$.*

Proof. This follows from Theorem 1.6.24 and the isomorphism ψ in (1.26). ■

Corollary 1.6.26. *Let p be an odd prime, and let $\mathcal{C}$ be a smooth curve of genus 2 over $\mathbb{Q}_p$ defined by an affine equation $y^2 = f(x)$ where f is a polynomial of degree 5 with coefficients in $\mathbb{Z}_p$, with Jacobian J. Then $J_1(\mathbb{Q}_p) \cap J_{\text{tors}} = \{\mathcal{O}\}$.*

Proof. This follows from Theorem 1.6.24 and the isomorphism ψ_J in (1.30). ■

Chapter 2

Height functions on elliptic curves

We apply the general theory that we discussed to the study of height functions. First, we discuss the development of height functions on elliptic curves, starting with real-valued functions and comparing these with the introduction of p-adic height functions.

2.1 Real-valued height functions on elliptic curves

We start by looking at a real valued height function on elliptic curves, which was found by Tate, and by Néron [27] as a sum of local contributions at each place of $\mathbb{Q}$. This section is largely based on [32, Chapter VIII] and [31, Chapter VI].

2.1.1 A naive real height function

First, we define a naive height function on projective N-space over $\mathbb{Q}$. Let $P \in \mathbb{P}^N(\mathbb{Q})$. Then we can write $P = [x_0 : \cdots : x_N]$ with $x_0, \ldots, x_N \in \mathbb{Z}$ and $\gcd(x_0, \ldots, x_N) = 1$, uniquely up to sign. We define a function $H \colon \mathbb{P}^N(\mathbb{Q}) \to \mathbb{R}$ by

$$H(P) := \max\{|x_0|_\infty, \ldots, |x_N|_\infty\}. \tag{2.1}$$

Note that this definition is independent of the choice of sign. We use this function to define a height function on points of elliptic curves. Let us consider an elliptic curve $E/\mathbb{Q}$. Recall that we have the map κ in (1.6) from E to its Kummer variety $\mathbb{P}^1$. We define a height function $H \colon E(\mathbb{Q}) \to \mathbb{R}$ by setting

$$H(P) = H(\kappa(P)).$$

For $P \neq \mathcal{O}$ we can write $x(P) = \frac{x_1(P)}{x_2(P)}$ with $\gcd(x_1(P), x_2(P)) = 1$, and then the map H can alternatively be described as

$$H(P) = \begin{cases} 0 & \text{if } P = \mathcal{O} \\ \max\{|x_1(P)|_\infty, |x_2(P)|_\infty\} & \text{otherwise.} \end{cases}$$

We consider the (natural) logarithm of this function to obtain a height function that behaves additively.

Definition 2.1.1. Let $E/\mathbb{Q}$ be an elliptic curve. The *naive real height function* on E is the function $h \colon E(\mathbb{Q}) \to \mathbb{R}$ given by

$$h(P) = \log H(\kappa(P)).$$

The naive real height function satisfies the following properties.

Proposition 2.1.2 ([32, VIII, Theorem 6.2, Corollary 6.4, Proposition 6.1]). *Let $E/\mathbb{Q}$ be an elliptic curve. There exists a constant $C_1 = C_1(E) \in \mathbb{R}$, and for all $m \in \mathbb{Z}$, a constant $C_2(m) = C_2(E, m) \in \mathbb{R}$, such that*

(a) For all $P, Q \in E(\mathbb{Q})$, we have

$$|h(P+Q) + h(P-Q) - 2h(P) - 2h(Q)|_\infty \leq C_1.$$

(b) Let $m \in \mathbb{Z}$. For all $P \in E(\mathbb{Q})$, we have

$$|h([m]P) - m^2 h(P)|_\infty \leq C_2(m).$$

(c) For any constant $C \in \mathbb{R}$, the set

$$\{P \in E(\mathbb{Q}) \mid h(P) \leq C\}$$

is finite.

2.1.2 A canonical real height function

We now define what it means for a function to be a quadratic form. Proposition 2.1.2(a) then says that h is not quite a quadratic form, but it is close in a sense.

Definition 2.1.3 ([32, p. 85, Definition]). Let G be an abelian group and let K be a field. A function $f\colon G \to K$ is a *quadratic form* if it satisfies:

1. $f(g) = f(-g)$ for all $g \in G$ (we say f is *even*).
2. The pairing $G \times G \to K$ given by $(g_1, g_2) \mapsto f(g_1 + g_2) - f(g_1) - f(g_2)$ is bilinear.

Proposition 2.1.4 ([32, VIII, proof of Theorem 9.3(c)]). *Let G be an abelian group and let K be a field. Let $f\colon G \to K$ be a function satisfying the parallelogram law:*

$$f(g_1 + g_2) + f(g_1 - g_2) = 2f(g_1) + 2f(g_2). \tag{2.2}$$

Then f is a quadratic form.

Proposition 2.1.5. *Let G be an abelian group, let K be a field, and let $f\colon G \to K$ be a function satisfying the parallelogram law (2.2). Then for all $g \in G$ and all $m \in \mathbb{Z}$, we have*

$$f(mg) = m^2 f(g). \tag{2.3}$$

Proof. This can be shown by induction. From the parallelogram law applied to $g_1 = g_2 = 0$, we conclude that $f(0) = 0$. For $m = 1$ the statement is trivial. Now let $m \geq 1$ and assume the result holds for all integers i such that $0 \leq i \leq m$. Then for all $g \in G$, we have

$$\begin{aligned} f((m+1)g) &= 2f(mg) + 2f(g) - f((m-1)g) && \text{(parallelogram law)} \\ &= 2m^2 f(g) + 2f(g) - (m-1)^2 f(g) && \text{(induction hypothesis)} \\ &= (m+1)^2 f(g) \end{aligned}$$

which shows the result for $m+1$. Hence the statement is true for all $m \in \mathbb{Z}_{\geq 0}$. Finally, according to Proposition 2.1.4 f is even, so for $m < 0$ and all $g \in G$ we have $f(mg) = f(-mg) = m^2 f(g)$. ∎

We say that a function satisfying (2.3) is a *quadratic function* (not to be confused with a quadratic form).

Proposition 2.1.2(a) tells us that the naive height function h has a bounded difference from being a quadratic form. We can use h to construct an actual quadratic form, which differs from h by a bounded amount.

Definition 2.1.6. The *canonical real height* (or *Néron-Tate height*) on $E/\mathbb{Q}$ is the function

$$\hat{h}(P) = \lim_{n\to\infty} \frac{1}{4^n} h\left([2^n]P\right).$$

The existence of this limit is proven in [32, VIII, Proposition 9.1].

Proposition 2.1.7 ([32, VIII, Theorem 9.3]). *Let $E/\mathbb{Q}$ be an elliptic curve.*

(a) For all $P, Q \in E(\mathbb{Q})$ we have

$$\hat{h}(P+Q) + \hat{h}(P-Q) = 2\hat{h}(P) + 2\hat{h}(Q).$$

(b) For all $P \in E(\mathbb{Q})$ and all $m \in \mathbb{Z}$,

$$\hat{h}([m]P) = m^2\hat{h}(P).$$

(c) $\hat{h}$ is a quadratic form on E.

(d) Let $P \in E(\mathbb{Q})$. Then $\hat{h}(P) \geq 0$, and $\hat{h}(P) = 0$ if and only if P is a torsion point.

(e) $|\hat{h} - h|_\infty \leq C$, where $C \in \mathbb{R}$ depends only on E.

Alternatively, we can describe the canonical height by a different limit:

Proposition 2.1.8.

$$\hat{h}(P) = \lim_{n\to\infty} \frac{1}{n^2} h([n]P).$$

Proof. From Proposition 2.1.7(e), we know that there exists a constant $C \in \mathbb{R}$, only depending on E, such that

$$|\hat{h}([n]P) - h([n]P)|_\infty \leq C \text{ for all } P \in E(\mathbb{Q}) \text{ and all } n \in \mathbb{Z}_{>0}.$$

Using Proposition 2.1.7(b), this becomes

$$|n^2\hat{h}(P) - h([n]P)|_\infty \leq C$$
$$|\hat{h}(P) - \frac{1}{n^2}h([n]P)|_\infty \leq \frac{C}{n^2}.$$

This implies the result. ∎

2.1.3 Local real height functions

Consider $P \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}$. Let us write $x(P) = \frac{x_1(P)}{x_2(P)}$ with $\gcd(x_1(P), x_2(P)) = 1$. Then

$$\begin{aligned} h(P) &= \log H(\kappa(P)) \\ &= \log \max\{|x_1(P)|_\infty, |x_2(P)|_\infty\} \\ &= \log \prod_{v \in M_\mathbb{Q}} \max\{|x_1(P)|_v, |x_2(P)|_v\} \qquad (2.4) \\ &= \log \prod_{v \in M_\mathbb{Q}} |x_2(P)|_v \max\{|x(P)|_v, 1\} \\ &= \log \prod_{v \in M_\mathbb{Q}} \max\{|x(P)|_v, 1\} \qquad \text{(by Theorem 1.1.10)} \\ &= \sum_{v \in M_\mathbb{Q}} \log \max\{|x(P)|_v, 1\}. \end{aligned}$$

The equality in (2.4) follows from the fact that $\max\{|x_1(P)|_q, |x_2(P)|_q\} = 1$ for all primes q, because $x_1(P)$ and $x_2(P)$ are coprime. This shows that away from $\mathcal{O}$, the naive height can be expressed as a sum over local contributions, one for every place of $\mathbb{Q}$.

Definition 2.1.9. Let $v \in M_\mathbb{Q}$. The *naive local real height function associated to* v,

$$\lambda_v \colon E(\mathbb{Q}_v) \setminus \{\mathcal{O}\} \to \mathbb{R},$$

is defined by

$$\lambda_v(P) = \log \max\{|x(P)|_v, 1\}.$$

We saw that $h(P) = \sum_{v \in M_\mathbb{Q}} \lambda_v(P)$ for all $P \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}$. Similarly, we can express the canonical height on $E(\mathbb{Q}) \setminus \{\mathcal{O}\}$ as a sum of local contributions. For all $v \in M_\mathbb{Q}$, we denote by $\mathbb{Q}_v$ the completion of $\mathbb{Q}$ with respect to $|\cdot|_v$. We construct functions $\hat{\lambda}_v \colon E(\mathbb{Q}_v) \setminus \{\mathcal{O}\} \to \mathbb{R}$ for each v, which are almost quadratic in the sense of Proposition 2.1.10 property 3 below, such that the equality

$$\hat{h}(P) = \sum_{v \in M_\mathbb{Q}} \hat{\lambda}_v(P)$$

holds for all $P \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}$.

Proposition 2.1.10 ([31, VI, Theorem 1.1]). *Let v be a place of $\mathbb{Q}$. There exists a unique function $\hat{\lambda}_v \colon E(\mathbb{Q}_v) \setminus \{\mathcal{O}\} \to \mathbb{R}$ with the following properties:*

1. *$\hat{\lambda}_v$ is continuous on $E(\mathbb{Q}_v) \setminus \{\mathcal{O}\}$ and is bounded on the complement of any v-adic neighborhood of $\mathcal{O}$.*
2. *The limit $\lim_{P \to \mathcal{O}} \{\hat{\lambda}_v(P) - \log |x(P)|_v\}$ exists.*
3. *For all $P \in E(\mathbb{Q}_v)$ with $[2]P \neq \mathcal{O}$,*

$$\hat{\lambda}_v([2]P) = 4\hat{\lambda}_v(P) - 2\log |\psi_2(P)|_v,$$

where ψ_2 is the divison polynomial defined in Definition 1.3.2.

The continuity in property 1 is with respect to the v-adic topology on $E(\mathbb{Q}_v)$, a definition of which can be found in [31, p. 455]. We call $\hat{\lambda}_v$ the *local Néron height function associated to* v.

Proposition 2.1.11 ([31, VI, Theorem 2.1]). *Let $\hat{\lambda}_v \colon E(\mathbb{Q}_v) \setminus \{\mathcal{O}\} \to \mathbb{R}$ be the local Néron height function associated to v. Then*

$$\hat{h}(P) = \sum_{v \in M_{\mathbb{Q}}} \hat{\lambda}_v(P)$$

for all $P \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}$.

It is possible to find explicit formulas for the local heights. The local height corresponding to the archimedean absolute value $|\cdot|_\infty$ can be defined using the Weierstrass σ-function (see [32, Chapter VI] for a general introduction). The explicit formula for $\hat{\lambda}_\infty$ can be found in [31, VI, Theorem 3.2].

For the non-archimedean absolute values $|\cdot|_p$, we can consider a Weierstrass equation for $E/\mathbb{Q}$ with integral coefficients, and reduce the curve modulo p. For points on E that reduce to a smooth point, we can describe the local height function as follows.

Theorem 2.1.12 ([31, VI, Theorem 4.1]). *Let p be a prime. For all $P \in E_0(\mathbb{Q}_p) \setminus \{\mathcal{O}\}$, the local Néron height function associated to p is given by*

$$\hat{\lambda}_p(P) = \lambda_p(P) = \log \max\{|x(P)|_p, 1\}.$$

In particular, when E has good reduction at p, we have $E_0(\mathbb{Q}_p) = E(\mathbb{Q}_p)$, and thus in that case we have $\hat{\lambda}_p = \lambda_p$ on all of $E(\mathbb{Q}_p) \setminus \{\mathcal{O}\}$.

2.2 p-adic height functions on elliptic curves

Let us fix an odd prime number p. Instead of defining a height function mapping into $\mathbb{R}$, we can also define a height function that maps into the field of p-adic numbers $\mathbb{Q}_p$, which we want to be a quadratic form. This can be done by defining local p-adic height functions that sum to a height with the desired properties, in a similar way as the real local height functions in Section 2.1.3. The theory in this section follows [6, Section 2.2].

Let us look at an elliptic curve $E/\mathbb{Q}$ with Weierstrass equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.5}$$

with $a_1, \ldots, a_6 \in \mathbb{Z}$. We furthermore assume that E has good reduction at p.

Our goal is to define local height functions $\lambda_v \colon E(\mathbb{Q}_v) \setminus \{\mathcal{O}\} \to \mathbb{Q}_p$ for all $v \in M_{\mathbb{Q}}$ such that $h_p := \sum_{v \in M_{\mathbb{Q}}} \lambda_v$ is a well defined function on $E(\mathbb{Q}) \setminus \{\mathcal{O}\}$ which is a quadratic form. It turns out that we can take $\lambda_\infty = 0$. For primes different from p, we define local height functions in Section 2.2.1 that look very similar to the local real heights from Proposition 2.1.10. To define a local p-adic height at p, we need some p-adic analysis. We will do this in Section 2.2.2. In Section 2.2.3 we combine the local p-adic heights into global p-adic heights that are quadratic forms.

2.2.1 Local p-adic heights at primes different from p

For primes $q \neq p$, we have a result similar to Proposition 2.1.10. Recall that we write $\log_p$ for the p-adic logarithm as defined in Section 1.1.2.

Proposition 2.2.1 ([6, p. 14]). *Let $q \neq p$ be a prime. There exists a unique function $\hat{\lambda}_q^{(p)} \colon E(\mathbb{Q}_q) \setminus \{\mathcal{O}\} \to \mathbb{Q}_p$ with the following properties:*

(a) $\hat{\lambda}_q^{(p)}$ is continuous on $E(\mathbb{Q}_q) \setminus \{\mathcal{O}\}$ and bounded on the complement of any neighborhood of $\mathcal{O}$ with respect to the q-adic topology.

(b) $\lim_{P \to \mathcal{O}} (\hat{\lambda}_q^{(p)}(P) - \log_p |x(P)|_q)$ exists.

(c) For all $P, Q \in E(\mathbb{Q}_q)$ such that $P, Q, P+Q, P-Q \neq \mathcal{O}$, we have

$$\hat{\lambda}_q^{(p)}(P+Q) + \hat{\lambda}_q^{(p)}(P-Q) = 2\hat{\lambda}_q^{(p)}(P) + 2\hat{\lambda}_q^{(p)}(Q) - 2\log_p |x(P) - x(Q)|_v.$$

This function also has the property

(d) For all $P \in E(\mathbb{Q}_q)$ and all $n \geq 1$ such that $P, [n]P \neq \mathcal{O}$, we have

$$\hat{\lambda}_q^{(p)}([n]P) = n^2 \hat{\lambda}_q^{(p)}(P) - 2\log_p |\psi_n(P)|_q,$$

where ψ_n denotes the n-th division polynomial defined in Definition 1.3.2.

For points of good reduction we also get a result similar to the real case.

Lemma 2.2.2 ([6, Lemma 2.2.2]). *Let $q \neq p$. If $P \in E_0(\mathbb{Q}_q) \setminus \{\mathcal{O}\}$, then*

$$\hat{\lambda}_q^{(p)}(P) = \log_p \max\{|x(P)|_q, 1\}.$$

The p-adic local heights at primes different from p are thus very similar to the real local heights, with the real logarithm replaced by the p-adic logarithm.

2.2.2 Local p-adic heights at p

For the local p-adic height at p, we want to mimic the properties of the Weierstrass σ-function, so we need a p-adic analogue of this function. First of all, the Weierstrass $\wp$- and σ-function corresponding to an elliptic curve are defined for a curve in short Weierstrass form (see [32, Section VI.3]). For a curve E given by (2.5), we can perform a coordinate transformation by substituting

$$y = y' - \frac{1}{2}(a_1 x + a_3) \quad \text{and} \quad x = x' - \frac{a_1^2 + 4a_2}{12} \tag{2.6}$$

to get an isomorphic elliptic curve given by a short Weierstrass equation

$$E \colon (y')^2 = (x')^3 - \tfrac{g_2}{4} x' - \tfrac{g_3}{4} \tag{2.7}$$

for some g_2, g_3 in $\mathbb{Q}$. Such a curve is isomorphic to $\mathbb{C}/\Lambda$ for some lattice Λ in $\mathbb{C}$ (see [32, VI, Proposition 3.6]). We consider the Weierstrass $\wp$- and σ-function relative to Λ defined in [32, p. 165, Definition, p. 167, Definition]. When we talk about the Weierstrass $\wp$- and σ-function in the context of the model (2.5), we mean the functions relative to the lattice Λ corresponding to the model (2.7).

Let $\sigma(z)$ be the Taylor series expansion of the complex Weierstrass σ-function, and $\wp(z)$ the Laurent series for the Weierstrass $\wp$-function around $z = 0$. These satisfy the differential equation ([32, VI, Lemma 3.3(b)])

$$\wp(z) = -\frac{d^2}{dz^2} \log \sigma(z) \tag{2.8}$$

as well as the identity ([32, Exercise 6.3])

$$\frac{\sigma(z_1 + z_2)\sigma(z_1 - z_2)}{\sigma(z_1)^2 \sigma(z_2)^2} = \wp(z_2) - \wp(z_1). \tag{2.9}$$

Lemma 2.2.3. *We have $\wp(z) \in z^{-2} + z^2\mathbb{Q}[[z^2]]$ and $\sigma(z) \in z + z^5\mathbb{Q}[[z]]$. In particular, both power series have coefficients in $\mathbb{Q}$.*

Proof. According to [32, VI, Theorem 3.5(a)] the Laurent series expansion for $\wp(z)$ is of the form

$$\wp(z) = z^{-2} + \sum_{k=1}^{\infty} (2k+1) G_{2k+2} z^{2k},$$

where G_{2k+2} are the Eisenstein series of weight $2k+2$ defined in [32, p. 165, Definition]. In particular, $\wp(z) \in z^{-2} + z^2\mathbb{C}[[z^2]]$. By definition we have $g_2 = 60G_4$ and $g_3 = 140G_6$ ([32, VI, Remark 3.5.1]), so $G_4, G_6 \in \mathbb{Q}$. We have the recurrence relation

$$(4k^2 - 1)(k-3)G_{2k} = 3 \sum_{j=2}^{k-2} (2j-1)(2k-2j-1) G_{2j} G_{2k-2j},$$

for all $k \geq 4$ [30, p. 67, Equation (10.7)]. This implies that all G_{2k+2} for $k \geq 1$ can be computed recursively as a polynomials in G_4 and G_6 with coefficients in $\mathbb{Q}$, and hence they are themselves elements of $\mathbb{Q}$. We conclude that $\wp(z)z^{-2} + z^2\mathbb{Q}[[z^2]]$.

For the expansion of $\sigma(z)$, we use the differential equation (2.8) and similar reasoning as in [6, Proposition 2.2.3]. By integrating the expansion of $\wp(z)$ once, we obtain

$$\frac{d}{dz} \log \sigma(z) \in z^{-1} + C_1 + z^3\mathbb{Q}[[z]]$$

for some $C_1 \in \mathbb{C}$. Note that if we define $\theta(z) = z^{-1}\sigma(z)$, we get

$$\begin{aligned} \frac{d}{dz} \log(\theta(z)) &= \frac{1}{\theta(z)} \frac{d\theta(z)}{dz} \\ &= \frac{z^{-1}\sigma'(z) - z^{-2}\sigma(z)}{z^{-1}\sigma(z)} \\ &= \frac{d}{dz} \log(\sigma(z)) - z^{-1} \in C_1 + z^3\mathbb{Q}[[z]] \end{aligned}$$

Integrating this expression and taking the exponential, we get

$$\sigma(z) = z\theta(z) = z \exp(C_2 + C_1 z + z^4 g(z))$$

for some $C_2 \in \mathbb{C}$ and $g \in \mathbb{Q}[[z]]$. From the definition of the Weierstrass σ-function [32, p. 167, Definition], we see that the coefficient of z in $\sigma(z)$ is equal to 1, and that $\sigma(z)$ is an odd function. The first observation implies that we must have $C_2 = 0$, and the second implies that the coefficient of the z^2 term must be zero, hence $C_1 = 0$. We then conclude that $\sigma(z) = z \exp(z^4 g(z)) \in z + z^5\mathbb{Q}[[z]]$. ∎

We define a series

$$\sigma_p(T) = \sigma(\mathcal{L}(T)) \in \mathbb{Q}[[T]],$$

where $\mathcal{L}$ is the strict formal logarithm corresponding to the formal group $(\hat{E}, F)$, as introduced in Section 1.6.4. We call σ_p the Bernardi p-adic σ-function, because it was introduced by Bernardi in [3, p. 9].

We want to use property (2.9) of σ to derive a similar property for σ_p, but in order for the right-hand side to be meaningful we need to know what we obtain when we compose the series $\wp$ with $\mathcal{L}$. The resulting series is one we have already encountered before.

Proposition 2.2.4. *$\wp(\mathcal{L}(T)) = x^T(T) + \frac{a_1^2+4a_2}{12}$ as series in $\mathbb{Q}((T))$.*

To prove this proposition, we first prove some intermediate results. Consider the elliptic curve E given by the model (2.7) (to ease notation we write x, y for the coordinates rather than x', y'). We can consider E as a curve over $\mathbb{C}$, and then there is a group homomorphism $\phi\colon \mathbb{C} \to E(\mathbb{C})$ given by $a \mapsto [\wp(a) : \frac{1}{2}\wp'(a) : 1]$ (see [32, VI, Proposition 3.6(b)]).

The invariant differential on $E(\mathbb{C})$ is given by $\frac{dx}{2y}$ (see [32, Section III.1]), and we see that $\phi^*(\frac{dx}{2y}) = \frac{d\wp(z)}{\wp'(z)} = dz$. We want to use the map ϕ to define a homomorphism of formal groups $\hat{\mathbb{G}}_a^1 \to \hat{E}$ over $\mathbb{Q}$ given by a power series $h(z)$ which also satisfies $h^*\omega = dz$, where dz is the invariant differential of $\hat{\mathbb{G}}_a^1$ with parameter z, and $\omega = \frac{d(x^T(T))}{2y^T(T)}$ is the invariant differential of $\hat{E}$ with parameter T ([32, p. 118]). Recall that to define the formal group associated to E, we defined a series $w^T(T)$ and used it to define $x^T(T)$ and $y^T(T)$ satisfying $T = -\frac{x^T(T)}{y^T(T)}$. The parameter t we started with corresponds to the coordinate function $-\frac{X}{Y}$ on the elliptic curve, which in our case can be represented by the series $h(z) = -2\frac{\wp(z)}{\wp'(z)}$. We will show that h defines the formal homomorphism we need.

From [32, VI, Theorem 3.5(a)] we know that $\wp(z) \in z^{-2} + z^2\mathbb{Q}[[z]]$ and $\wp'(z) \in -2z^{-3} + z\mathbb{Q}[[z]]$, so we get $h(z) \in z + z^2\mathbb{Q}[[z]]$. It then follows from [32, IV, Lemma 2.4] that there exists a unique inverse power series $k(T) \in \mathbb{Q}[[T]]$ that satisfies $k(h(z)) = z$ and $h(k(T)) = T$.

Lemma 2.2.5. *We have $w^T(h(z)) = -\frac{2}{\wp'(z)}$, $x^T(h(z)) = \wp(z)$ and $y^T(h(z)) = \frac{1}{2}\wp'(z)$ as Laurent series in $\mathbb{Q}((z))$.*

Proof. Recall that $w^T(T)$ is the unique power series in $\mathbb{Q}[[T]]$ that satisfies $w^T(0) = 0$ and $w^T(T) = f(T, w^T(T))$ with $f(t, w) = t^3 - \frac{g_2}{4}tw^2 - \frac{g_3}{4}w^3$ (Proposition 1.6.10). Because $k(T)$ exists such that $h(k(T)) = T$ and $k(h(z)) = z$, this implies that $(w^T \circ h)(z)$ is the unique power series in $\mathbb{Q}[[z]]$ satisfying $(w^T \circ h)(0) = 0$ and $(w^T \circ h)(z) = f(h(z), (w^T \circ h)(z))$. We will show that the series $-\frac{2}{\wp'(z)}$ also satisfies these properties. Namely, $-\frac{2}{\wp'(z)} \in z^3\mathbb{Q}[[z]]$, so $-\frac{2}{\wp'(z)}|_{z=0} = 0$. Furthermore, we know that

$$\begin{aligned}
\frac{\wp'(z)^2}{4} &= \wp(z)^3 - \frac{g_2}{4}\wp(z) - \frac{g_3}{4} \\
-\frac{2}{\wp'(z)} &= -8\frac{\wp(z)^3}{\wp'(z)^3} + 2g_2\frac{\wp(z)}{\wp'(z)^3} + g_3\frac{2}{\wp'(z)^3} \\
&= h(z)^3 - \frac{g_2}{4}h(z)\left(-\frac{2}{\wp'(z)}\right)^2 - \frac{g_3}{4}\left(-\frac{2}{\wp'(z)}\right)^3 = f\left(h(z), -\tfrac{2}{\wp'(z)}\right).
\end{aligned}$$

We conclude that $w^T(h(z)) = -\frac{2}{\wp'(z)}$. Finally we get

$$x^T(h(z)) = \frac{h(z)}{w^T(h(z))} = \wp(z),$$
$$y^T(h(z)) = -\frac{1}{w^T(h(z))} = \tfrac{1}{2}\wp'(z).$$

■

Lemma 2.2.6. *$h(z)$ defines a formal group isomorphism from $\hat{\mathbb{G}}_a^1$ to $(\hat{E}, F)$ as formal groups over $\mathbb{Q}$.*

Proof. We already saw that $h(z) \in z + z^2\mathbb{Q}[[z]]$. We furthermore need to show that we have $h(z_1 + z_2) = F(h(z_1), h(z_2))$. From how F was defined in Section 1.6.2, we know that $h(z_1)$, $h(z_2)$ and $i(F(h(z_1), h(z_2)))$ are the three roots of the cubic polynomial

$$\lambda(h(z_1), h(z_2))T + \nu(h(z_1), h(z_2)) - f(T, \lambda(h(z_1), h(z_2))T + \nu(h(z_1), h(z_2))) \tag{2.10}$$

in $\mathbb{Q}[[z_1, z_2]][T]$. We claim that $i(h(z_1 + z_2))$ is also a root of this polynomial. First of all, we note that

$$\begin{aligned} i(h(z_1 + z_2)) &= \frac{x^T(h(z_1 + z_2))}{y^T(h(z_1 + z_2))} && \text{(by definition of } i\text{)} \\ &= \frac{\wp(z_1 + z_2)}{\frac{1}{2}\wp'(z_1 + z_2)} && \text{(by Lemma 2.2.5)} \\ &= -2\frac{\wp(-z_1 - z_2)}{\wp'(-z_1 - z_2)} && \text{(because } \wp \text{ is even)} \\ &= h(-z_1 - z_2). \end{aligned}$$

Because ϕ is a homomorphism, we have for $a_1, a_2 \in \mathbb{C}$, that the points $\phi(a_1)$, $\phi(a_2)$ and $\phi(-a_1-a_2)$ on $E(\mathbb{C})$ are colinear. When they are on the affine patch $Y \neq 0$, we thus have that the point $\left(-2\frac{\wp(-a_1-a_2)}{\wp'(-a_1-a_2)}, -\frac{2}{\wp'(-a_1-a_2)}\right)$ in the (t, w)-plane must lie on the line through $\left(-2\frac{\wp(a_1)}{\wp'(a_1)}, -\frac{2}{\wp'(a_1)}\right)$ and $\left(-2\frac{\wp(a_2)}{\wp'(a_2)}, -\frac{2}{\wp'(a_2)}\right)$. Recall that as series, we have $h(z) = -2\frac{\wp(z)}{\wp'(z)}$ and $w^T(h(z)) = -\frac{2}{\wp'(z)}$. Thus by taking Taylor expansions, we conclude that the point $(h(-z_1 - z_2), w^T(h(-z_1 - z_2)))$ must lie on the line

$$w = \lambda(h(z_1), h(z_2))\, t + \nu(h(z_1), h(z_2))$$

in the (t, w)-plane. We know from Proposition 1.6.10 that

$$w^T(h(-z_1 - z_2)) = f(h(-z_1 - z_2), w^T(h(-z_1 - z_2))),$$

so this shows that $h(-z_1 - z_2)$ is a root of the polynomial (2.10).

We know that $h(-z_1 - z_2) = i(h(z_1 + z_2))$ is not equal to $h(z_1)$ or $h(z_2)$ because it has nontrivial terms in both variables. Then we must have $i(h(z_1 + z_2)) = i(F(h(z_1), h(z_2)))$, and hence $h(z_1 + z_2) = F(h(z_1), h(z_2))$ (where we use that $i(i(T)) = T$). This shows that h is a formal group homomorphism.

We saw that there exists a unique power series $k(z) \in \mathbb{Q}[[z]]$ that satisfies $k(h(z)) = z$ and $h(k(T)) = T$. It can easily be seen that $k(T)$ is a formal group homomorphism from $\hat{E}$ to $\hat{\mathbb{G}}_a^1$, because the proof of [32, IV, Lemma 2.4] shows that $k(T) \in T\mathbb{Q}[[T]]$ and

$$\begin{aligned} k(T_1) + k(T_2) &= k(h(k(T_1) + k(T_2))) \\ &= k(F(h(k(T_1)), h(k(T_2)))) \\ &= k(F(T_1, T_2)). \end{aligned}$$

Hence h is an isomorphism. ■

Corollary 2.2.7. *$h^*\omega = dz$.*

Proof. We have $\omega = \frac{dx^T(T)}{2y^T(T)}$, and hence

$$h^*\omega = \frac{dx^T(h(z))}{2y^T(h(z))} = \frac{d\wp(z)}{\wp'(z)} = dz.$$

■

Proposition 2.2.8. *We have $k(T) = \mathcal{L}(T)$ as power series in $\mathbb{Q}[[T]]$, where $\mathcal{L}$ is the strict formal logarithm on $\hat{E}$ defined in Section 1.6.4.*

Proof. Recall that $k\colon \hat{E} \to \hat{\mathbb{G}}_a^1$ is a homomorphism satisfying $h(k(T)) = T$. Because $h^*\omega = dz$, we also have $\omega = (h \circ k)^*\omega = k^*(h^*\omega) = k^*dz$. On the other hand, the strict formal logarithm is also defined in such a way that $\omega = \mathcal{L}'(T)dT = \mathcal{L}^*dz$. According to [38, Theorem 1.28], there is a unique homomorphism with this property, so we must conclude that $k(T) = \mathcal{L}(T)$. ■

Proof of Proposition 2.2.4. Because we have $x^T(h(z)) = \wp(z)$, Proposition 2.2.8 implies that

$$\wp(\mathcal{L}(T)) = \wp(k(T)) = x^T(h(k(T))) = x^T(T).$$

Now if we go back to our original curve E given by the model (2.5), we performed the transformation (2.6) to obtain (2.7), hence we conclude

$$\wp(\mathcal{L}(T)) = x^T(T) + \frac{a_1^2 + 4a_2}{12}$$

where $x^T(T)$ is now the series defined with respect to the model (2.5). ■

Convergence of σ_p

Our goal is to use σ_p to construct a local height function, and to do this we want to evaluate it at $t(P)$, where $P \in E_1(\mathbb{Q}_p)$ (see (1.26)). For this to be possible, we need to know something about the convergence of σ_p on $\mathbb{Q}_p$. To show a convergence result, we first need a lemma, which is a one-dimensional version of [5, Lemma 2.3].

Lemma 2.2.9. *Let $g(T) \in \mathbb{Z}_p[[T]]$. Then $g(\mathcal{E}(z))$ is of the form*

$$g(\mathcal{E}(z)) = \sum_{n=0}^{\infty} \frac{d_n}{n!} z^n \quad \textit{with } d_n \in \mathbb{Z}_p.$$

Proof. This is observed using exact same reasoning as in the proof of [5, Lemma 2.3]. ■

We now state a convergence result for σ_p which was shown in [3, p. 9]. We provide a more elaborate proof, adapting the arguments used in the proof of [5, Theorem 2.4].

Proposition 2.2.10. *$\sigma_p(T)$ converges for all $T \in p\mathbb{Z}_p$.*

Proof. Recall from Lemma 2.2.3 that the power series $\sigma(z)$ is of the form $\sigma(z) \in z + z^5\mathbb{Q}[[z]]$. We also have $\mathcal{E}(z) \in z + z^2\mathbb{Q}[[z]]$ from Proposition 1.6.20, so $z^{-1}\mathcal{E}(z) \in 1 + z\mathbb{Q}[[z]]$ and thus there exists a series $g(z) \in 1 + z\mathbb{Q}[[z]]$ such that $z^{-1}\mathcal{E}(z)g(z) = 1$. Hence we can write

$$\sigma(z) = \mathcal{E}(z)u(z)$$

where $u(z) = z^{-1}\sigma(z)g(z) \in 1 + z\mathbb{Q}[[z]]$. We note from Proposition 1.6.20 that $\mathcal{E}$ is of the form $\mathcal{E}(z) = z = \frac{c}{2}z^2 + \dots$ for some $c \in \mathbb{Z}$, so we deduce that u is of the form

$$u(z) = 1 - \frac{c}{2}z + \cdots . \tag{2.11}$$

We write

$$\sigma_p(T) = \sigma(\mathcal{L}(T)) = \mathcal{E}(\mathcal{L}(T))u(\mathcal{L}(T)) = Tu_p(T),$$

where $u_p(T) := u(\mathcal{L}(T))$. We will show the convergence result for σ_p by showing the convergence of u_p first.

We have

$$\begin{aligned}
\frac{d^2}{dz^2}\log(\mathcal{E}(z))(\mathcal{L}(T)) + \frac{d^2}{dz^2}\log(u(z))(\mathcal{L}(T)) &= \frac{d^2}{dz^2}\log(\sigma(z))(\mathcal{L}(T)) \\
&= -\wp(\mathcal{L}(T)) && \text{(by (2.8))} \\
&= -x^T(T) - \frac{a_1^2 + 4a_2}{12} && \text{(by Proposition 2.2.4)}
\end{aligned}$$

as series in $\mathbb{Q}((T))$, and thus

$$\frac{d^2}{dz^2}\log(u(z))(\mathcal{L}(T)) + \frac{a_1^2 + 4a_2}{12} = -x^T(T) - \frac{d^2}{dz^2}\log(\mathcal{E}(z))(\mathcal{L}(T)). \tag{2.12}$$

We want to show that the left-hand side of this equation is in $\mathbb{Z}[[T]]$, so that we can apply Lemma 2.2.9 to find the expansion of $\frac{d^2}{dz^2}\log(u(z))$. First of all, because $u(z) \in 1 + z\mathbb{Q}[[z]]$, we have $\frac{d^2}{dz^2}\log(u(z)) \in \mathbb{Q}[[z]]$. Hence $\frac{d^2}{dz^2}\log(u(z))(\mathcal{L}(T)) + \frac{a_1^2+4a_2}{12} \in \mathbb{Q}[[T]]$, so it has no terms with negative powers of T.

Now let us look at the right-hand side of (2.12). Using the chain rule twice, we find that

$$\begin{aligned}
\frac{d^2}{dz^2}\log(\mathcal{E}(z))(\mathcal{L}(T)) &= \frac{1}{\mathcal{L}'(T)}\frac{d}{dT}\left(\frac{d}{dz}\log(\mathcal{E}(z))(\mathcal{L}(T))\right) \\
&= \frac{1}{\mathcal{L}'(T)}\frac{d}{dT}\left(\frac{1}{\mathcal{L}'(T)}\frac{d\log(T)}{dT}\right) \\
&= \frac{1}{\mathcal{L}'(T)}\frac{d}{dT}\left(\frac{1}{T\mathcal{L}'(T)}\right).
\end{aligned} \tag{2.13}$$

Because $\mathcal{L}(T) = T + \sum_{n=2}^{\infty} \frac{c_{n-1}}{n} T^n$ for some $c_n \in \mathbb{Z}$ by Proposition 1.6.20, we have

$$\mathcal{L}'(T) = 1 + \sum_{n=1}^{\infty} c_n T^n \in 1 + T\mathbb{Z}[[T]].$$

Hence also $\frac{1}{\mathcal{L}'(T)} \in \mathbb{Z}[[T]]$. It then follows from (2.13) that $\frac{d^2}{dz^2} \log(\mathcal{E}(z))(\mathcal{L}(T)) \in \mathbb{Z}((T))$. Furthermore, we also know that $x^T(T) \in \mathbb{Z}((T))$. Hence the right-hand side of (2.12) has coefficients in $\mathbb{Z}$, and then so must the left-hand side. We conclude that

$$\frac{d^2}{dz^2} \log(u(z))(\mathcal{L}(T)) + \frac{a_1^2 + 4a_2}{12} \in \mathbb{Z}[[T]].$$

If we evaluate at $\mathcal{E}(z)$, we find using Lemma 2.2.9 that

$$\begin{aligned} \frac{d^2}{dz^2} \log(u(z)) + \frac{a_1^2 + 4a_2}{12} &= \sum_{n=0}^{\infty} \frac{d_n}{n!} z^n \\ \log(u(z)) + \frac{a_1^2 + 4a_2}{24} z^2 &= C_1 + C_2 z + \sum_{n=2}^{\infty} \frac{d_{n-2}}{n!} z^n \end{aligned} \tag{2.14}$$

for some $d_n \in \mathbb{Z}_p$ and $C_1, C_2 \in \mathbb{Q}_p$. Because $u(z)$ is of the form (2.11), we see from the series expansion of the logarithm that $\log(u(z)) = \frac{c}{2} z + \cdots$, so $C_1 = 0$ and $C_2 = \frac{c}{2} \in \mathbb{Z}_p$ (because $p \neq 2$).

When $T \in p\mathbb{Z}_p$, we have that $\mathcal{L}(T)$ converges and $\mathrm{ord}_p(\mathcal{L}(T)) > 0$ by [32, IV, Lemma 6.3(b)] (where we use that $p \geq 3$). The same Lemma [32, IV, Lemma 6.3(b)] then also implies that the right-hand side of (2.14) converges at $\mathcal{L}(T)$ to a value in $p\mathbb{Z}_p$. Because $\mathrm{ord}_p\left(\frac{a_1^2+4a_2}{24}\mathcal{L}(T)^2\right) > 0$ we conclude that then also $\log(u(\mathcal{L}(T)))$ converges to a value in $p\mathbb{Z}_p$. The Taylor series around 0 of the exponential function converges at this value, again by [32, IV, Lemma 6.3(b)], and hence $u(\mathcal{L}(T)) = u_p(T)$ converges. Then $\sigma_p(T)$ also converges for $T \in p\mathbb{Z}_p$. ■

Recall that if $P \in E_1(\mathbb{Q}_p)$, the kernel of reduction modulo p, then $t(P) = -x(P)/y(P) \in p\mathbb{Z}_p$ and hence σ_p converges at $t(P)$.

Properties of σ_p

From the expansions of σ (see Lemma 2.2.3) and $\mathcal{L}$ (see Proposition 1.6.20), we deduce that $\sigma_p(T) \in T + T^2\mathbb{Q}[[T]]$, and hence for T in the domain of convergence $p\mathbb{Z}_p$, we have $\sigma_p(T) = 0$ precisely when $T = 0$.

From the identity (2.9), we deduce a similar identity for σ_p. Using Proposition 2.2.4, we see that

$$\begin{aligned} \frac{\sigma(\mathcal{L}(T_1) + \mathcal{L}(T_2))\sigma(\mathcal{L}(T_1) - \mathcal{L}(T_2))}{\sigma(\mathcal{L}(T_1))^2\sigma(\mathcal{L}(T_2))^2} &= \wp(\mathcal{L}(T_2)) - \wp(\mathcal{L}(T_1)) \\ \frac{\sigma(\mathcal{L}(F(T_1, T_2))\sigma(\mathcal{L}(F(T_1, i(T_2))))}{\sigma(\mathcal{L}(T_1))^2\sigma(\mathcal{L}(T_2))^2} &= \wp(\mathcal{L}(T_2)) - \wp(\mathcal{L}(T_1)) \\ \frac{\sigma_p(F(T_1, T_2))\sigma_p(F(T_1, i(T_2)))}{\sigma_p(T_1)^2\sigma_p(T_2)^2} &= x^T(T_2) - x^T(T_2). \end{aligned}$$

We saw that Proposition 2.2.10 implies that $\sigma_p(T)$ converges on $t(P)$ for $P \in E_1(\mathbb{Q}_p)$, and we know $x^T(T)$ converges on $t(P)$ for $P \in E_1(\mathbb{Q}_p) \setminus \{\mathcal{O}\}$. So for $P, Q \in E_1(\mathbb{Q}_p) \setminus \{\mathcal{O}\}$, we get the identity

$$\frac{\sigma_p(t(P+Q))\sigma_p(t(P-Q))}{\sigma_p(t(P))^2\sigma_p(t(Q))^2} = x(Q) - x(P). \tag{2.15}$$

Other p-adic σ-functions

For any constant $s \in \mathbb{Q}_p$, we define a series

$$\sigma_p^{(s)}(T) = \sigma_p(T)\exp_p\left(-\frac{s}{2}\mathcal{L}(T)^2\right) \tag{2.16}$$

where $\exp_p$ is the p-adic exponential. Note that $\sigma_p = \sigma_p^{(0)}$. These functions $\sigma_p^{(s)}$ are different p-adic σ-functions. The region of convergence of $\sigma_p^{(s)}$ in $\mathbb{Q}_p$ may depend on s, and we denote it by V_s. We write $\overline{V}_s = \{P \in E_1(\mathbb{Q}_p) \mid t(P) \in V_s\}$.

We use the following general property of $\mathcal{L}$.

Proposition 2.2.11. *The map $E_1(\mathbb{Q}_p) \to \mathbb{Q}_p$ defined by $P \mapsto \mathcal{L}(t(P))^2$ is a quadratic form. Explicitly, for all $P, Q \in E_1(\mathbb{Q}_p)$ and $m \in \mathbb{Z}$ we have*

$$\mathcal{L}(t([m]P))^2 = m^2\mathcal{L}(t(P))^2,$$
$$\mathcal{L}(t(P+Q))^2 + \mathcal{L}(t(P-Q))^2 = 2\mathcal{L}(t(P))^2 + 2\mathcal{L}(t(Q))^2.$$

Proof. This follows from Lemma 1.6.12 and the fact that the maps ψ^{-1} defined in (1.26) and $\mathcal{L}$ from (1.32) are group homomorphisms. ∎

Lemma 2.2.12. *Let $P \in E_1(\mathbb{Q}_p)$ such that $P, -P \in \overline{V}_s$. We have*

$$\sigma_p^{(s)}(t(-P)) = -\sigma_p^{(s)}(t(P)).$$

Proof. We have

$$\begin{aligned}
\sigma_p^{(s)}(t(-P)) &= \sigma_p(t(-P))\exp_p\left(-\frac{s}{2}\mathcal{L}(t(-P))^2\right) && \text{(using (2.16))}\\
&= \sigma(\mathcal{L}(i(t(P))))\exp_p\left(-\frac{s}{2}\mathcal{L}(i(t(P)))^2\right) && \text{(because (1.26) is a homomorphism)}\\
&= \sigma(-\mathcal{L}(t(P)))\exp_p\left(-\frac{s}{2}(-\mathcal{L}(t(P)))^2\right) && \text{(because } \mathcal{L} \text{ is a homomorphism)}\\
&= -\sigma_p(t(P))\exp_p\left(-\frac{s}{2}\mathcal{L}(t(P))^2\right) && \text{(because } \sigma \text{ is odd)}\\
&= -\sigma_p^{(s)}(t(P)).
\end{aligned}$$

∎

Lemma 2.2.13. *Let $s \in \mathbb{Q}_p$, and let $P, Q \in \overline{V}_s \setminus \{\mathcal{O}\}$. Then*

$$\frac{\sigma_p^{(s)}(t(P+Q))\sigma_p^{(s)}(t(P-Q))}{\sigma_p^{(s)}(t(P))^2\sigma_p^{(s)}(t(Q))^2} = x(Q) - x(P).$$

Proof. From (2.16) we get

$$\frac{\sigma_p^{(s)}(t(P+Q))\sigma_p^{(s)}(t(P-Q))}{\sigma_p^{(s)}(t(P))^2\sigma_p^{(s)}(t(Q))^2} = \frac{\sigma_p(t(P+Q))\sigma_p(t(P-Q))}{\sigma_p(t(P))^2\sigma_p(t(Q))^2} \times \exp_p\left(-\frac{s}{2}\left(\mathcal{L}(t(P+Q))^2 + \mathcal{L}(t(P-Q))^2 - 2\mathcal{L}(t(P))^2 - 2\mathcal{L}(t(Q))^2\right)\right).$$

This last factor is equal to 1 by Proposition 2.2.11. The result then follows from (2.15). ■

Lemma 2.2.14 ([6, Lemma 2.2.4(ii)]). *Let $s \in \mathbb{Q}_p$, $P \in \overline{V}_s \setminus \{\mathcal{O}\}$, and $n \in \mathbb{Z}_{>0}$. Then*

$$\sigma_p^{(s)}(t([n]P)) = \sigma_p^{(s)}(t(P))^{n^2}\psi_n(P),$$

with ψ_n as defined in Definition 1.3.2.

We can use the p-adic σ-functions to define local heights $\hat{\lambda}_p^{(s)} \colon \overline{V}_s \setminus \{\mathcal{O}\} \to \mathbb{Q}_p$ by

$$\hat{\lambda}_p^{(s)}(P) = -2\log_p(\sigma_p^{(s)}(t(P))). \tag{2.17}$$

This is only meaningful for values of s for which $\overline{V}_s$ is larger than $\{\mathcal{O}\}$, such as $s = 0$. In this case, we want to extend $\hat{\lambda}_p^{(s)}$ to all nontorsion points of $E(\mathbb{Q}_p)$.

Lemma 2.2.15. *Let V be a neighbourhood of 0 in $\mathbb{Q}_p$. Let $P \in E(\mathbb{Q}_p)$. Then there exists an integer $m > 0$ such that $[m]P \in E_1(\mathbb{Q}_p)$ and $t([m]P) \in V$.*

Proof. We note that $E_1(\mathbb{Q}_p)$ has finite index in $E_0(\mathbb{Q}_p) = E(\mathbb{Q}_p)$ from [32, VII, Proposition 2.1]. Hence, the equivalence class of P in $E(\mathbb{Q}_p)/E_1(\mathbb{Q}_p)$ must have finite order k, which implies that $[k]P \in E_1(\mathbb{Q}_p)$. Because V is a neighborhood of 0 in $\mathbb{Q}_p$, it contains a set of the form $p^n\mathbb{Z}_p$ for some $n \in \mathbb{Z}_{>0}$. Because $[k]P \in E_1(\mathbb{Q}_p)$, we find that $\mathrm{ord}_p(t([p^{n-1}k]P)) \geq n$ by Corollary 1.6.13. Hence $t([p^{n-1}k]P) \in p^n\mathbb{Z}_p \subseteq V$. ■

For the rest of this section, let us fix an $s \in \mathbb{Q}_p$ such that V_s is a neighborhood of 0.

Definition 2.2.16. Let $P \in E(\mathbb{Q}_p) \setminus E_{\mathrm{tors}}$. Let $m \in \mathbb{Z}_{>0}$ such that $t([m]P) \in V_s$. We define $\hat{\lambda}_p^{(s)} \colon E(\mathbb{Q}_p) \setminus E_{\mathrm{tors}} \to \mathbb{Q}_p$ by

$$\hat{\lambda}_p^{(s)}(P) = -\frac{2}{m^2}\left(\log_p(\sigma_p^{(s)}(t([m]P))) - \log_p(\psi_m(P))\right).$$

Note that when $P \in \overline{V}_s \setminus \{\mathcal{O}\}$, we can take $m = 1$ and this definition agrees with (2.17). This definition does not depend on the choice of m, as the following lemma shows.

Lemma 2.2.17. *Let $P \in E(\mathbb{Q}_p) \setminus E_{\mathrm{tors}}$. Let $m, n \in \mathbb{Z}_{>0}$ be such that $t([m]P), t([n]P) \in V_s$. Then*

$$-\frac{2}{m^2}\left(\log_p(\sigma_p^{(s)}(t([m]P))) - \log_p(\psi_m(P))\right) = -\frac{2}{n^2}\left(\log_p(\sigma_p^{(s)}(t([n]P))) - \log_p(\psi_n(P))\right).$$

Proof. From Lemma 2.2.14, we have

$$\sigma_p^{(s)}(t([m]P))^{n^2}\psi_n([m]P) = \sigma_p^{(s)}(t([mn]P)) = \sigma_p^{(s)}(t([n]P))^{m^2}\psi_m([n]P).$$

Using Proposition 1.3.3(v) we obtain

$$\frac{\sigma_p^{(s)}(t([m]P))^{n^2}}{\psi_m(P)^{n^2}} = \frac{\sigma_p^{(s)}(t([n]P))^{m^2}}{\psi_n(P)^{m^2}}.$$

This shows that

$$\frac{1}{m^2}\log_p\left(\frac{\sigma_p^{(s)}(t([m]P))}{\psi_m(P)}\right) = \frac{1}{n^2}\log_p\left(\frac{\sigma_p^{(s)}(t([n]P))}{\psi_n(P)}\right).$$

■

Proposition 2.2.18 ([6, p. 18]). *The local height $\hat{\lambda}_p^{(s)}$ satisfies the following properties:*

(a) For all $P \in E(\mathbb{Q}_p) \setminus E_{\mathrm{tors}}$ and all $n \geq 1$, we have

$$\hat{\lambda}_p^{(s)}([n]P) = n^2\hat{\lambda}_p^{(s)}(P) - 2\log_p(\psi_n(P)).$$

(b) For all $P, Q \in E(\mathbb{Q}_p)$ such that $P, Q, P+Q, P-Q \notin E_{\mathrm{tors}}$, we have

$$\hat{\lambda}_p^{(s)}(P+Q) + \hat{\lambda}_p^{(s)}(P-Q) = 2\hat{\lambda}_p^{(s)}(P) + 2\hat{\lambda}_p^{(s)}(Q) - 2\log_p(x(P) - x(Q)).$$

2.2.3 Global p-adic heights

Again we only consider $s \in \mathbb{Q}_p$ for which V_s is a neighborhood of 0. For such s we define a global height on all of $E(\mathbb{Q})$.

Definition 2.2.19. We define a global height $h_p^{(s)} \colon E(\mathbb{Q}) \to \mathbb{Q}_p$ by

$$h_p^{(s)} = \begin{cases} \hat{\lambda}_p^{(s)} + \sum_{q \neq p} \hat{\lambda}_q^{(p)} & \text{if } P \notin E_{\mathrm{tors}}, \\ 0 & \text{if } P \in E_{\mathrm{tors}}. \end{cases}$$

To see that the sum in this definition is finite, we note that E has good reduction at all but a finite number of primes, and at those primes we have we have $\hat{\lambda}_q^{(p)}(P) = \log_p \max\{|x(P)|_q, 1\}$ (see Lemma 2.2.2). For each $P \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}$, we have $|x(P)|_q = 1$ for all but finitely many primes q. We conclude that $\hat{\lambda}_q^{(p)}(P)$ is nonzero for only finitely many primes.

In order to find a more explicit description of $h_p^{(s)}$, we first consider it on a subset on which the local heights have a simple description. Let us write

$$E^{\mathrm{good}}(\mathbb{Q}) = \bigcap_{q \text{ prime}} E_0^{(q)}(\mathbb{Q})$$

for the set of all $P \in E(\mathbb{Q})$ that reduce to a nonsingular point modulo all primes (with respect to the Weierstrass model (2.5)). Furthermore, we write

$$E_p^{(s)}(\mathbb{Q}) := E^{\mathrm{good}}(\mathbb{Q}) \cap \overline{V}_s.$$

Proposition 2.2.20. *Let $P \in E(\mathbb{Q})$. Then there exists an $m \in \mathbb{Z}_{>0}$ such that $[m]P \in E_p^{(s)}(\mathbb{Q})$.*

Proof. Note that E has bad reduction at a prime q precisely when $q \mid \Delta$, so there are at most a finite number of primes $q_1, \dots, q_r$ for which $P \notin E_0^{(q_i)}(\mathbb{Q})$. But $E_0^{(q_i)}(\mathbb{Q})$ has finite index in $E(\mathbb{Q})$ (see [32, VII, Corollary 6.2]), which implies that there is a positive integer m_i such that $[m_i]P \in E_0^{(q_i)}(\mathbb{Q})$ for each $i \in \{1, \dots, r\}$. Then $[m_1 \cdots m_r]P \in E^{\text{good}}(\mathbb{Q})$. We already saw in Lemma 2.2.15 that there exists a positive integer m_0 such that $[m_0 m_1 \cdots m_r]P \in \overline{V}_s$, which concludes the result. ∎

Proposition 2.2.21. *Let $P \in E(\mathbb{Q}) \setminus E_{\text{tors}}$ and let $m \in \mathbb{Z}_{>0}$ such that $[m]P \in E_p^{(s)}(\mathbb{Q})$. Then*

$$h_p^{(s)}(P) = -\frac{2}{m^2} \log_p \left(\frac{\sigma_p^{(s)}(t([m]P))}{d([m]P)} \right),$$

with $d([m]P)$ as defined in Proposition 1.3.1.

Proof. Note that $[m]P \neq \mathcal{O}$ because $P \notin E_{\text{tors}}$. We have

$$\begin{aligned}
h_p^{(s)}(P) &= \hat{\lambda}_p^{(s)}(P) + \sum_{q \neq p} \hat{\lambda}_q^{(p)}(P) \\
&= -\frac{2}{m^2} \left(\log_p(\sigma_p^{(s)}(t([m]P))) - \log_p(\psi_m(P)) \right) \\
&\qquad + \sum_{q \neq p} \frac{1}{m^2} \left(\hat{\lambda}_q^{(p)}([m]P) + 2 \log_p |\psi_m(P)|_q \right) && \text{(Def. 2.2.16, Prop. 2.2.1)} \\
&= -\frac{1}{m^2} \left[2 \log_p(\sigma_p^{(s)}(t([m]P))) - \sum_{q \neq p} \log_p \max\{|x([m]P)|_q, 1\} \right] && \text{(Lemma 1.1.17, 2.2.2)} \\
&= -\frac{1}{m^2} \left[2 \log_p(\sigma_p^{(s)}(t([m]P))) + \sum_{q \neq p} \log_p |d([m]P)^2|_q \right] \\
&= -\frac{2}{m^2} \log_p \left(\frac{\sigma_p^{(s)}([m]P))}{d([m]P)} \right). && \text{(Lemma 1.1.17)}
\end{aligned}$$

∎

Proposition 2.2.22 ([6, Properties 2.2.7]). *The p-adic height $h_p^{(s)} \colon E(\mathbb{Q}) \to \mathbb{Q}_p$ is a quadratic form. Explicitly:*

(a) For all $P \in E(\mathbb{Q})$ and $n \in \mathbb{Z}$, we have $h_p^{(s)}([n]P) = n^2 h_p^{(s)}(P)$.

(b) For all $P, Q \in E(\mathbb{Q})$, we have $h_p^{(s)}(P+Q) + h_p^{(s)}(P-Q) = 2h_p^{(s)}(P) + h_p^{(s)}(Q)$.

Proof. In general, part (a) follows from part (b) by Proposition 2.1.5. However, to prove (b) on torsion points, we will use part (a), and thus we prove part (a) first.

Part (a) is clearly satisfied when $P \in E_{\text{tors}}(\mathbb{Q})$. For $P \notin E_{\text{tors}}$ and $n \geq 1$, we use Proposition

2.2.18 and Proposition 2.2.1 to get

$$\begin{aligned} h_p^{(s)}([n]P) &= \hat{\lambda}_p^{(s)}([n]P) + \sum_{q\neq p} \hat{\lambda}_q^{(p)}([n]P) \\ &= n^2\hat{\lambda}_p^{(s)}(P) - 2\log_p(\psi_n(P)) + n^2 \sum_{q\neq p} \left[\hat{\lambda}_q^{(p)}(P) - 2\log_p|\psi_n(P)|_q\right] \\ &= n^2 h_p^{(s)}(P). \qquad \text{(Lemma 1.1.17)} \end{aligned}$$

For $n = 0$, the statement is clear because both sides evaluate to 0. Finally, to show the statement for $n < 0$, we note that $h_p^{(s)}(P) = h_p^{(s)}(-P)$ for all $P \in E(\mathbb{Q})$. This clear when $P \in E_{\text{tors}}$, and when $P \notin E_{\text{tors}}$, we can find $m \in \mathbb{Z}_{>0}$ such that $[m]P, [-m]P \in E_p^{(s)}(\mathbb{Q})$. It then follows from Proposition 2.2.21 that $h_p^{(s)}(P) = h_p^{(s)}(-P)$, because $\sigma_p^{(s)}(t(-P)) = -\sigma_p^{(s)}(t(P))$ (Lemma 2.2.12), $d(-P) = d(P)$ and $\log_p(-1) = 0$. Then we have

$$h_p^{(s)}([n]P) = h_p^{(s)}([-n]P) = (-n)^2 h_p^{(s)}(P) = n^2 h_p^{(s)}(P).$$

For part (b), let us first consider $P, Q \in E(\mathbb{Q})$ such that $P, Q, P+Q, P-Q \notin E_{\text{tors}}$. Then we again use Proposition 2.2.18 and Proposition 2.2.1 to find

$$\begin{aligned} h_p^{(s)}(P+Q) + h_p^{(s)}(P-Q) &= \hat{\lambda}_p^{(s)}(P+Q) + \hat{\lambda}_p^{(s)}(P-Q) + \sum_{q\neq p} \hat{\lambda}_q^{(p)}(P+Q) + \sum_{q\neq p} \hat{\lambda}_q^{(p)}(P-Q) \\ &= 2\hat{\lambda}_p^{(s)}(P) + 2\hat{\lambda}_p^{(s)}(Q) - 2\log_p(x(P)-x(Q)) \\ &\qquad + \sum_{q\neq p} \left[2\hat{\lambda}_q^{(p)}(P) + 2\hat{\lambda}_q^{(p)}(Q) - 2\log_p|x(P)-x(Q)|_q\right] \\ &= 2h_p^{(s)}(P) + 2h_p^{(s)}(Q). \qquad \text{(Lemma 1.1.17)} \end{aligned}$$

If $P \in E_{\text{tors}}$ with $[n]P = \mathcal{O}$, we get

$$\begin{aligned} h_p^{(s)}(P+Q) + h_p^{(s)}(P-Q) &= \frac{1}{n^2} h_p^{(s)}([n](P+Q)) + \frac{1}{n^2} h_p^{(s)}([n](P-Q)) \\ &= \frac{1}{n^2} h_p^{(s)}([n]Q) + \frac{1}{n^2} h_p^{(s)}([-n]Q)) \\ &= 2h_p^{(s)}(Q) \\ &= 2h_p^{(s)}(P) + 2h_p^{(s)}(Q). \end{aligned}$$

A similar argument shows that the parallelogram law is satisfied when Q is a torsion point. If $P+Q \in E_{\text{tors}}$ with $[n](P+Q) = \mathcal{O}$, we have $[n]P = -[n]Q$. We get

$$\begin{aligned} h_p^{(s)}(P+Q) + h_p^{(s)}(P-Q) &= h_p^{(s)}(P-Q) \\ &= \frac{1}{n^2} h_p^{(s)}([n]P - [n]Q) \\ &= \frac{1}{n^2} h_p^{(s)}([2n]P) \\ &= \frac{2}{n^2} h_p^{(s)}([n]P) + \frac{2}{n^2} h_p^{(s)}([-n]Q) \\ &= 2h_p^{(s)}(P) + 2h_p^{(s)}(Q). \end{aligned}$$

When $P - Q \in E_{\text{tors}}$ we have a similar argument. ■

Finally, let us derive a relation between the height functions $h_p^{(s)}$ for different values of s.

Proposition 2.2.23. *For all $P \in E_1(\mathbb{Q})$, we have*

$$h_p^{(s)}(P) = h_p^{(0)}(P) + s\mathcal{L}(t(P))^2.$$

Proof. If $P = \mathcal{O}$, both sides evaluate to 0 so the equality is satisfied. Otherwise, $P \notin E_{\text{tors}}$ by Corollary 1.6.25. Let $m \in \mathbb{Z}_{>0}$ such that $[m]P \in E_p^{(s)}(\mathbb{Q})$. We find

$$\begin{aligned} h_p^{(s)}(P) &= -\frac{2}{m^2}\log_p\left(\frac{\sigma_p^{(s)}(t([m]P))}{d([m]P)}\right) && \text{(Proposition 2.2.21)} \\ &= -\frac{2}{m^2}\log_p\left(\frac{\sigma_p^{(0)}(t([m]P))}{d([m]P)}\right) + \frac{s}{m^2}\mathcal{L}(t([m]P))^2 && \text{(using (2.16))} \\ &= h_p^{(0)}(P) + s\mathcal{L}(t(P))^2. && \text{(Proposition 2.2.11)} \end{aligned}$$

■

2.3 Naive p-adic height functions on elliptic curves

We now introduce two naive p-adic height functions, which in a limit converge to quadratic p-adic height functions, similarly to how the real canonical height was defined in Definition 2.1.6. We compare these limits to the previously defined p-adic height function $h_p^{(0)}$. These naive p-adic heights were first described by Perrin-Riou in [28], in the setting of elliptic curves over general number fields, and using idèle class characters. The goal of this section is to give a more in depth description and explanation of the results described in [28], specialized to the case where E is an elliptic curve defined over $\mathbb{Q}$. In this setting there is only one idèle class character up to scaling, and for that reason we do not introduce the corresponding theory but instead do everything explicitly for one normalization.

Let us again fix an odd prime p. We remain in the setting of the previous section, considering an elliptic curve $E/\mathbb{Q}$ defined by (2.5). We focus on the subgroup

$$E_p(\mathbb{Q}) := E_p^{(0)}(\mathbb{Q}) = E^{\text{good}}(\mathbb{Q}) \cap E_1^{(p)}(\mathbb{Q})$$

of points on E. Recall from Proposition 1.3.1 that for any $P \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}$ we can write $x(P) = \frac{a(P)}{d(P)^2}$ and $y(P) = \frac{b(P)}{d(P)^3}$ for some unique integers $a(P), b(P)$ and $d(P)$ with $d(P) > 0$, such that $\gcd(a(P), d(P)) = \gcd(b(P), d(P)) = 1$. We define the following functions from $E_p(\mathbb{Q}) \setminus \{\mathcal{O}\}$ to $\mathbb{Q}_p$:

$$\begin{aligned} H_2(P) &= \log_p(a(P)) \qquad (2.18) \\ H_3(P) &= \frac{2}{3}\log_p\left(d(P)^3(2y(P) + a_1x(P) + a_3)/2\right) \\ &= \frac{2}{3}\log_p\left(b(P) + \frac{a_1}{2}a(P)d(P) + \frac{a_3}{2}d(P)^3\right). \end{aligned}$$

Because $P \in E_p(\mathbb{Q}) \subseteq E_1^{(p)}(\mathbb{Q})$, we know that P reduces to $[0:1:0]$ modulo p. This implies that $\text{ord}_p(y(P)) < 0$ and then also $\text{ord}_p(x(P)) < 0$, so we have $\text{ord}_p(a(P)) = \text{ord}_p(b(P)) = 0$ and $\text{ord}_p(d(P)) > 0$. Hence, since $p \neq 2$, the arguments $a(P)$ and $b(P) + \frac{a_1}{2}a(P)d(P) + \frac{a_3}{2}d(P)^3$ are in $\mathbb{Z}_p^\times$. We call H_2 and H_3 naive p-adic heights. The main result we discuss in this section is the following, which is the main proposition in [28, Section 4].

Theorem 2.3.1 ([28, p. 246, Proposition]). *Let $P \in E_p(\mathbb{Q}) \setminus \{\mathcal{O}\}$. Then the following limits exist in $\mathbb{Q}_p$:*

(a) $h_2(P) = \lim_{n\to\infty} \frac{1}{p^{2n}} H_2([p^n]P)$,

(b) $h_3(P) = \lim_{n\to\infty} \frac{1}{p^{2n}} H_3([p^n]P)$.

The goal in this section is to work out Perrin-Riou's proof of this result in detail, which will be done in Section 2.3.2 and Section 2.3.3. We then show that h_2 and h_3 satisfy the parallelogram law in Section 2.3.4. In section 2.3.5, we show how h_2 and h_3 can be extended from the restricted domain $E_p(\mathbb{Q}) \setminus \{\mathcal{O}\}$ to the entire group $E(\mathbb{Q})$. Finally, in Section 2.3.6 we compare h_2 and h_3 with the quadratic height $h_p^{(s)}$ of Section 2.2.3. In [29], Perrin-Riou proves a comparison result under the assumption that E has good ordinary reduction at p. We present an adapted proof that does not use this assumption.

2.3.1 Some useful lemmas

In order to prove Theorem 2.3.1, we first introduce some lemmas which will become useful multiple times throughout the remainder of this chapter. The first lemma is based on [28, Lemme a], but proven for a bigger class of functions (although stated over $\mathbb{Q}_p$ rather than the more general v-adic completion of a number field). This greater generality will allow us in Section 2.3.6 to compare h_2 and h_3 with the quadratic height $h_p^{(s)}$ from Section 2.2.3 without requiring that E has ordinary reduction at p, which is an assumption Perrin-Riou uses in [29] to obtain such a comparison result.

Lemma 2.3.2. *Let $\boldsymbol{T} = (T_1, \dots, T_r)$ and $g(\boldsymbol{T}) \in 1 + (T_1, \dots, T_r)^k \mathbb{Q}_p[[\boldsymbol{T}]]$ for some $k \in \mathbb{Z}_{>0}$, such that g converges on some neighborhood of $\mathbf{0}$ in $(\mathbb{Q}_p)^r$. Let $(\boldsymbol{x}^{(n)})$ be a sequence of r-tuples in $(\mathbb{Q}_p)^r$, satisfying $\mathrm{ord}_p(x_i^{(n)}) \geq n$ for all $n \geq 0$ and $i = 1, \dots, r$. Then for large enough $n \in \mathbb{Z}_{\geq 0}$, $g(\boldsymbol{x}^{(n)})$ converges, and for $m \in \mathbb{Z}_{<k}$ we have*

$$\lim_{n\to\infty} \frac{1}{p^{mn}} \log_p(g(\boldsymbol{x}^{(n)})) = 0.$$

Proof. Let us write

$$g(\boldsymbol{T}) = 1 + \sum_{\substack{i_1,\dots,i_j \geq 0 \\ i_1+\cdots+i_r \geq k}}^{\infty} a_{i_1,\dots,i_r} T_1^{i_1} \cdots T_r^{i_r}$$

with $a_{i_1,\dots,i_r} \in \mathbb{Q}_p$. Because g converges on a neighborhood of $\mathbf{0}$, we know there exists some $R \in \mathbb{Z}$ such that g converges for all $\boldsymbol{T} \in (\mathbb{Q}_p)^r$ satisfying $\mathrm{ord}_p(T_i) \geq R$ for $i = 1, \dots, r$. In particular, $g(\boldsymbol{x}^{(n)})$ converges for all $n \in \mathbb{Z}_{\geq 0}$ satisfying $n \geq R$.

To prove the second statement, we first show that there exists a constant $C \geq 0$ such that $g(\boldsymbol{x}^{(n)}) \in 1 + p^{k(n-C)}\mathbb{Z}_p$ for all $n \geq C$. Because g converges at $(p^R, \dots, p^R)$, There is a minimal $M \in \mathbb{Z}_{\geq k}$ such that for all $i_1, \dots, i_r \in \mathbb{Z}_{\geq 0}$ with $i_1 + \cdots + i_r \geq M$, we have $\mathrm{ord}_p(a_{i_1,\dots,i_r} p^{(i_1+\cdots+i_r)R}) \geq 0$, and hence

$$\mathrm{ord}_p(a_{i_1,\dots,i_r}) \geq -(i_1 + \cdots + i_r)R. \tag{2.19}$$

If $M > k$, let us define $N = -\min\{\min_{i_1+\cdots i_r<M} \operatorname{ord}_p(a_{i_1,\ldots,i_r}), 0\}$. Consider any $n \geq N$. Then for all $i_1, \ldots, i_r$ with $k \leq i_1 + \cdots + i_r < M$, we get

$$\begin{aligned}\operatorname{ord}_p\left(a_{i_1,\ldots,i_r}(x_1^{(n)})^{i_1}\cdots(x_r^{(n)})^{i_r}\right) &= \operatorname{ord}_p(a_{i_1,\ldots,i_r}) + \sum_{j=1}^{r} i_j \operatorname{ord}_p(x_j^{(n)}) \\ &\geq -N + (i_1+\cdots+i_r)n \\ &\geq -N + kn \\ &\geq k(n-N) \geq 0. \qquad \text{(using } k \geq 1,\ N \geq 0\text{)} \end{aligned} \tag{2.20}$$

Now consider $n \geq R$. For all $i_1, \ldots, i_r$ with $i_1 + \cdots + i_r \geq M \geq k$, we get

$$\begin{aligned}\operatorname{ord}_p\left(a_{i_1,\ldots,i_r}(x_1^{(n)})^{i_1}\cdots(x_r^{(n)})^{i_r}\right) &= \operatorname{ord}_p(a_{i_1,\ldots,i_r}) + \sum_{j=1}^{r} i_j \operatorname{ord}_p(x_j^{(n)}) \\ &\geq -(i_1+\cdots+i_r)R + (i_1+\cdots+i_r)n \qquad \text{(using (2.19))} \\ &\geq k(n-R) \geq 0. \end{aligned} \tag{2.21}$$

We set $C = \max\{N, R\} \geq 0$. Using (2.20) and (2.21) we get that if $n \geq C$, then for all for all $i_1, \ldots, i_r$ with $k \leq i_1 + \cdots + i_r$ we have $\operatorname{ord}_p\left(a_{i_1,\ldots,i_r}(x_1^{(n)})^{i_1}\cdots(x_r^{(n)})^{i_r}\right) \geq k(n-C)$. Hence $g(\boldsymbol{x}^{(n)}) \in 1 + p^{k(n-C)}\mathbb{Z}_p$ (by Lemma 1.1.7). We conclude that

$$\begin{aligned}\operatorname{ord}_p\left(\frac{1}{p^{mn}}\log_p(g(\boldsymbol{x}^{(n)}))\right) &= -mn + \operatorname{ord}_p(\log_p(g(\boldsymbol{x}^{(n)}))) \\ &\geq -mn + k(n-C) \qquad \text{(using Lemma 1.1.16)} \\ &= n(k-m) - kC. \end{aligned}$$

Because $m < k$, this shows that $\operatorname{ord}_p\left(\frac{1}{p^{mn}}\log_p(g(\boldsymbol{x}^{(n)}))\right)$ approaches infinity as $n \to \infty$. This implies the result. ■

Corollary 2.3.3. *Let $P \in E_1(\mathbb{Q}_p)$. Let $g(T) \in 1 + T^k\mathbb{Q}_p[[T]]$ for some $k \in \mathbb{Z}_{>0}$, such that g converges on some neighborhood of 0 in $\mathbb{Q}_p$. Then for large enough $n \in \mathbb{Z}_{\geq 0}$, $g(t([p^n]P))$ converges, and for $m \in \mathbb{Z}_{<k}$ we have*

$$\lim_{n\to\infty} \frac{1}{p^{mn}} \log_p(g(t([p^n]P))) = 0.$$

Proof. We know that $\operatorname{ord}_p(t([p^n]P)) \geq n$ from Corollary 1.6.13. The result then follows immediately from Lemma 2.3.2. ■

Corollary 2.3.4 (variation on [29, Lemme part 1]). *Let $P \in E_1(\mathbb{Q}_p)$. If $g(T) \in 1+T^k\mathbb{Z}_p[[t]]$ for some $k \in \mathbb{Z}_{>0}$, then for $m \in \mathbb{Z}_{<k}$ we have*

$$\lim_{n\to\infty} \frac{1}{p^{mn}} \log_p(g(t([p^n]P))) = 0.$$

Proof. Because $g(T) \in \mathbb{Z}_p[[T]]$, g converges for all $T \in p\mathbb{Z}_p$ by Lemma 1.1.7. The result then follows from Corollary 2.3.3. ■

Lemma 2.3.5 ([29, Lemme part 3]). *Let $P \in E_1(\mathbb{Q}_p)$. If $d \in \mathbb{Q}_p$, then*

$$\lim_{n\to\infty} \frac{1}{p^{2n}} \log_p\left(1 + d\, t([p^n]P)^2\right) = d\, \mathcal{L}(t(P))^2.$$

Proof. The statement is clearly true for $d = 0$. Let us assume $d \neq 0$ and write $C := \mathrm{ord}_p(d)$. Recall from Corollary 1.6.13 that $\mathrm{ord}_p(t([p^n]P)) > n$ for all $n \geq 0$, so $1 - d\, t([p^n]P)^2 \in 1 + p\mathbb{Z}_p$ for all $n \geq 0$ satisfying $2n \geq -C$. For such n, we use (1.3) to obtain

$$\log_p\left(1 + d\, t([p^n]P)^2\right) = d\, t([p^n]P)^2 + t([p^n]P)^3 \sum_{i=2}^{\infty} \frac{(-1)^{i+1}}{i} d^i t([p^n]P)^{2i-3}.$$

Let us look at the terms in the sum for $i \geq 2$ individually. We see that

$$\begin{aligned}\mathrm{ord}_p\left(\frac{(-1)^{i+1}}{i} d^i t([p^n]P)^{2i-3}\right) &\geq -(i-1) + (2i-3) \qquad (\text{using } \mathrm{ord}_p(i) \leq i-1)\\ &= i - 2 \geq 0.\end{aligned}$$

If $C < 0$, we consider $n \geq -2C$, and we get

$$\begin{aligned}\mathrm{ord}_p\left(\frac{(-1)^{i+1}}{i} d^i t([p^n]P)^{2i-3}\right) &\geq -(i-1) + Ci + (2i-3)(n+1)\\ &\geq -(i-1) + Ci + (2i-3)(-2C+1)\\ &= -3Ci + i + 6C - 2\\ &= (i-2)(-3C+1) \geq 0.\end{aligned}$$

Hence for all $n \geq \max\{-2C, 0\}$, we can write

$$\log_p(1 + d\, t([p^n]P)^2) = d\, t([p^n]P)^2 + t([p^n]P)^3\, g(t([p^n]P))$$

with $g(t) = \sum_{i=2}^{\infty} \frac{(-1)^{i+1}}{i} d^i t^{2i-3}$ and $\mathrm{ord}_p(g(t([p^n]P))) \geq 0$. We use this to split the argument of the limit into two terms, after which we will show that the limit of each of these separate terms exists, and thus that their sum is equal to the original limit. Assuming for now the limits indeed exist we obtain the equality

$$\begin{aligned}\lim_{n\to\infty} \frac{1}{p^{2n}} \log_p\left(1 + d\, t([p^n]P)^2\right) &= \lim_{n\to\infty} \left[\frac{d\, t([p^n]P)^2}{p^{2n}} + \frac{t([p^n]P)^3}{p^{2n}} g(t([p^n]P))\right]\\ &= d \cdot \lim_{n\to\infty} \left(\frac{t([p^n]P)}{p^n}\right)^2 + \lim_{n\to\infty} \left[\frac{t([p^n]P)^3}{p^{2n}} g(t([p^n]P))\right]. \quad (2.22)\end{aligned}$$

In order to rewrite the first term, we note that $\mathcal{L}(t([p^n]P)) = p^n \mathcal{L}(t(P))$ for all $n \geq 0$, by Theorem 1.6.21 and because the map ψ in (1.26) is a homomorphism. Hence we have

$$\begin{aligned}\mathcal{L}(t(P)) &= \frac{1}{p^n} \mathcal{L}(t([p^n]P))\\ &= \frac{1}{p^n} \sum_{i=1}^{\infty} \frac{c_{i-1}}{i} t([p^n]P)^i\end{aligned}$$

for some $c_i \in \mathbb{Z}$ with $c_0 = 1$ by Proposition 1.6.20. For $i \geq 1$, we have

$$\mathrm{ord}_p\left(\frac{1}{p^n} \frac{c_{i-1}}{i} t([p^n]P)^i\right) > -n - i + in = (n-1)i - n.$$

We get

$$\begin{aligned}\operatorname{ord}_p\left(\mathcal{L}(t(P)) - \frac{t([p^n]P)}{p^n}\right) &= \operatorname{ord}_p\left(\sum_{i=2}^{\infty}\frac{1}{p^n}\frac{c_{i-1}}{i}t([p^n]P)^i\right)\\ &> 2(n-1) - n = n-2\end{aligned}$$

for $n \geq 1$. This implies that $\lim_{n\to\infty}\left(\mathcal{L}(t(P)) - \frac{t([p^n]P)}{p^n}\right) = 0$, and hence

$$\lim_{n\to\infty}\left(\frac{t([p^n]P)}{p^n}\right)^2 = \mathcal{L}(t(P))^2.$$

For the second term of (2.22), we note that for $n \geq \max\{-2C, 0\}$, we have

$$\operatorname{ord}_p\left(\frac{t([p^n]P)^3}{p^{2n}}g(t([p^n]P))\right) > 3n - 2n = n,$$

and hence $\lim_{n\to\infty}\left[\frac{t([p^n]P)^3}{p^{2n}}g(t([p^n]P))\right] = 0$. Taking everything together, we conclude that

$$\lim_{n\to\infty}\frac{1}{p^{2n}}\log_p(1 + d\,t([p^n]P)^2) = d\,\mathcal{L}(t(P))^2.$$

■

Corollary 2.3.6. *Let $d \in \mathbb{Z}_p$, $P \in E_1(\mathbb{Q}_p)$, and let $g(T) \in 1 + dT^2 + T^3\mathbb{Q}_p[[T]]$ such that g converges on a neighborhood of 0 in $\mathbb{Q}_p$. Then for large enough $n \in \mathbb{Z}_{\geq 0}$, $g(t([p^n]P))$ converges and*

$$\lim_{n\to\infty}\frac{1}{p^{2n}}\log_p\left(g(t([p^n]P))\right) = d\,\mathcal{L}(t(P))^2.$$

Proof. If we view $1 + dT^2$ as a power series in $\mathbb{Z}_p[[T]]$, it is invertible, and its inverse is of the form

$$h(T) \in \sum_{i=0}^{\infty}(-d)^i T^{2i}.$$

For T with $2\operatorname{ord}_p(T) > -\operatorname{ord}_p(d)$, we get $\operatorname{ord}_p((-d)^iT^{2i}) \geq i$ for all $i \geq 0$, and hence $h(T)$ converges at T by Lemma 1.1.7. We conclude that h converges on a neighborhood of 0 in $\mathbb{Q}_p$.

We can write $g(T) = (1+dT^2)h(T)g(T)$, and, because both h and g converge on a neighborhood of 0 in $\mathbb{Q}_p$, the same is true for $k(T) := h(T)g(T)$. Furthermore, from the form of the expansions we conclude that $k(T) \in 1 + T^3\mathbb{Q}_p[[T]]$.

We obtain

$$\begin{aligned}\lim_{n\to\infty}\frac{1}{p^{2n}}\log_p\left(g(t([p^n]P))\right) &= \lim_{n\to\infty}\frac{1}{p^{2n}}\log_p\left(1 + d\,t([p^n]P)^2\right) + \lim_{n\to\infty}\frac{1}{p^{2n}}\log_p\left(k(t([p^n]P))\right)\\ &= d\,\mathcal{L}(t(P))^2\end{aligned}$$

using Lemma 2.3.5 and Corollary 2.3.3. ■

2.3.2 Existence of h_2

We start by proving the existence of the limit in Theorem 2.3.1(a). Our strategy is as follows: Let us write $G(P) := H_2([p]P) - p^2 H_2(P)$. Then if we show

$$\lim_{n\to\infty} \frac{1}{p^{2(n+1)}} G([p^n]P) = 0, \tag{2.23}$$

this implies using Lemma 1.1.6 that the sequence $\left(\frac{1}{p^{2n}} H_2([p^n]P)\right)$ for $n \to \infty$ is Cauchy. This then shows that the limit in Theorem 2.3.1(a) exists, because $\mathbb{Q}_p$ is complete and hence every Cauchy sequence has a limit. To be able to show (2.23), we need to rewrite $G(P)$ in a form for which we can evaluate this limit.

Proposition 2.3.7. *Let $P = \left(\frac{a(P)}{d(P)^2}, \frac{b(P)}{d(P)^3}\right) \in E_p(\mathbb{Q}) \setminus \{\mathcal{O}\}$. For all $m \geq 1$ such that $[m]P \neq \mathcal{O}$, we have*

$$H_2([m]P) - m^2 H_2(P) = \log_p \left(\frac{a([m]P)}{a(P)^{m^2}}\right).$$

Proof. This follows directly from the definition of H_2:

$$\begin{aligned} H_2([m]P) - m^2 H_2(P) &= \log_p(a([m]P)) - m^2 \log_p(a(P)) \\ &= \log_p \left(a([m]P)/a(P)^{m^2}\right). \end{aligned}$$

■

To work with the expression above, we want to express the value $a([m]P)$ in terms of the point P rather than $[m]P$. To be able to do this, we make use of some general properties of the division polynomials, which were introduced in Section 1.3.3.

Lemma 2.3.8 ([28, Lemme b]). *Let E/K be a possibly singular Weierstrass curve* (1.4) *over a field K. Let $P \in E(K) \setminus \{\mathcal{O}\}$ be a nonsingular point. Then $x(P)$ cannot be a common zero of ϕ_m and ψ_m^2 for any $m \geq 1$.*

Proof. By definition, a point $P \neq \mathcal{O}$ is singular when it simultaneously satisfies

$$\psi_2(P) = 2y(P) + a_1 x(P) + a_3 = 0 \quad \text{and} \quad \eta(P) := 3x(P)^2 + 2a_2 x(P) + a_4 - a_1 y(P) = 0.$$

For $m = 1$ we have $\phi_m = \psi_m^2 = 1$, so the statement is trivially true. Next, let us consider the case $m = 2$. Some algebra shows that

$$\begin{aligned} \phi_2(x(P)) &= x^4 - b_4 x^2 - 2b_6 x - b_8 \\ &= \eta(P)^2 - 2x(P)\psi_2^2(x(P)) + a_1 \eta(P)\psi_2(P) - a_2 \psi_2^2(x(P)). \end{aligned}$$

If we assume that $\psi_2(P) = \phi_2(x(P)) = 0$, the above equation implies that also $\eta(P) = 0$, and hence that P is a singular point.

Next we show the statement for arbitrary $m > 2$ by contradiction. Let m be the smallest integer for which P is a common zero of ϕ_m and ψ_m^2. Let us first assume that m is even. Then we can write $m = 2n$. We distinguish two cases.

1. If $\psi_n^2(x(P)) = 0$, we see from (1.9) that $\phi_{2n}(x(P)) = 0$ implies that also $\phi_n(x(P)) = 0$. But this is not possible because of the minimality of m and the fact that $n < m$.

2. If $\psi_n^2(x(P)) \neq 0$, then (1.9), (1.10) and our assumption $\phi_m(x(P)) = \psi_m^2(x(P)) = 0$ imply that

$$\phi_2\left(\frac{\phi_n(x(P))}{\psi_n^2(x(P))}\right) = \phi_2(x([n]P)) = 0 \quad \text{and} \quad \psi_2^2\left(\frac{\phi_n(x(P))}{\psi_n^2(x(P))}\right) = \psi_2^2(x([n]P)) = 0.$$

   But we saw that this implies that $[n]P$ is a singular point, which is not possible because we assumed that P is nonsingular.

Now assume m is odd. Then $\phi_m(x(P)) = \psi_m^2(x(P)) = 0$ together with (1.7) imply that $\psi_{m-1}(P)\psi_{m+1}(P) = 0$. This gives two possibilities. If $\psi_{m+1}(P) = 0$, then from (1.7) we know that $\phi_{m+1}(x(P)) = x(P)\psi_{m+1}^2(x(P)) - \psi_m(P)\psi_{m+2}(P) = 0$. But because $m+1$ is even, we just saw that then also $\phi_{(m+1)/2}(x(P)) = \psi_{(m+1)/2}(P) = 0$. But this contradicts the minimality of m, because $(m+1)/2 < m$ for $m \geq 3$. In a similar way we get a contradiction when $\psi_{m-1}(P) = 0$. Together this proves the lemma. ■

Corollary 2.3.9. *Let E/K be an elliptic curve over a field K. Then ϕ_m and ψ_m^2 have no common zeros in $\overline{K}$, and hence they are coprime polynomials in $K[x]$.*

Proof. Assume $x \in \overline{K}$ is a common zero of ϕ_m and ψ_m^2. Because $\overline{K}$ is algebraically closed, there exists $y \in \overline{K}$ such that $(x, y) \in E(\overline{K})$. This contradicts Lemma 2.3.8. ■

Lemma 2.3.10 ([28, Lemme c]). *Let E/K be an elliptic curve, where K is a field with* $\mathrm{char}(K)$ *not equal to* 2 *or* 3. *Then the coefficient of x^{m^2-1} in the polynomial ϕ_m is zero for all $m \geq 1$.*

Proof. Let us consider the change of coordinates

$$y' = y + \frac{a_1 x + a_3}{2} \quad \text{and} \quad x' = x + \frac{4a_2 + a_1^2}{12}.$$

The corresponding Weierstrass equation $(y')^2 + a_1'x'y' + a_3'y' = (x')^3 + a_2'(x')^2 + a_4'x' + a_6'$ satisfies $a_1' = a_2' = 0$. We consider the polynomials ϕ_m' and $(\psi_m')^2$ corresponding to this equation. We know that ϕ_m' is homogeneous of degree $2m^2$, where x has weight 2 (see Proposition 1.3.3(ii)). The coefficient $d'_{m^2-1} \in \mathbb{Z}[a_1', \ldots a_6']$ of $(x')^{m^2-1}$ therefore needs to have weight 2, but because the a_i' have weight i, and $a_1' = a_2' = 0$, this is not possible and hence we must have $d'_{m^2-1} = 0$.

Now if we set $c = \frac{4a_2+a_1^2}{12}$ so that $x' = x + c$, we see that for all P with $[m]P \neq \mathcal{O}$,

$$\begin{aligned}\frac{\phi_m'(x(P)+c)}{(\psi_m')^2(x(P)+c)} &= \frac{\phi_m'(x'(P))}{(\psi_m')^2(x'(P))} \\ &= x'(mP) \\ &= x(mP) + c \\ &= \frac{\phi_m(x(P)) + c\,\psi_m^2(x(P))}{\psi_m^2(x(P))}.\end{aligned}$$

We conclude that

$$\frac{\phi'_m(x+c)}{(\psi'_m)^2(x+c)} = \frac{\phi_m(x) + c\,\psi_m^2(x)}{\psi_m^2(x)} \tag{2.24}$$

in $K(x)$. It follows from Corollary 2.3.9 that the numerator and denominator of this fraction on the right-hand side cannot have common factors. We also know that $\phi'_m(x+c)$ and $(\psi'_m)^2(x+c)$ have no common factors by the same corollary. Hence we conclude that the numerators in (2.24) are equal, so we have

$$\phi'_m(x') = \phi_m(x'-c) + c\psi_m^2(x'-c).$$

Let us denote by d_{m^2-1} the coefficient of x^{m^2-1} in ϕ_m. By comparing the coefficient of $(x')^{m^2-1}$ in the left- and right-hand side of the above equation, we obtain $d'_{m^2-1} = -m^2c + d_{m^2-1} + cm^2 = d_{m^2-1}$. We conclude that $d_{m^2-1} = d'_{m^2-1} = 0$. ∎

Let us return to our original setting, with the elliptic curve E given by (2.5). Recall that we want to rewrite $a([m]P)$ as an expression in terms of the point P. In order to do this, we introduce the notation

$$\overline{\phi_m}(X,Z) = Z^{m^2}\phi_m(X/Z) \quad \text{and} \quad \overline{\psi_m}^2(X,Z) = Z^{m^2}\psi_m^2(X/Z).$$

Lemma 2.3.11 ([28, Lemme d]). *Let $P = \left(\frac{a(P)}{d(P)^2}, \frac{b(P)}{d(P)^3}\right) \in E^{\mathrm{good}}(\mathbb{Q}) \setminus \{\mathcal{O}\}$. Let $m \geq 1$ such that $[m]P \neq \mathcal{O}$. Then $a([m]P) = \pm\overline{\phi_m}(m_1, m_3^2)$.*

Proof. To ease notation, let us write $m_1 = a(P)$, $m_2 = b(P)$ and $m_3 = d(P)$. We also use the notation $\alpha_m = \overline{\phi_m}(m_1, m_3^2)$ and $\beta_m = \overline{\psi_m}^2(m_1, m_3^2)$. First of all, we note that

$$\alpha_m = m_3^{2m^2}\phi_m(x(P)),$$
$$\beta_m = m_3^{2m^2}\psi_m^2(x(P)),$$

and hence $x([m]P) = \frac{\alpha_m}{\beta_m}$ by (1.8). Note that $\alpha_m, \beta_m \in \mathbb{Z}$. It now suffices to show that $\gcd(\alpha_m, \beta_m) = 1$. In order to do this, let us consider any prime q. If $q \mid m_3$, then $q \nmid m_1$ as $\gcd(m_1, m_3) = 1$. We know that $\phi_m(x)$ is monic in x, so we deduce that $\overline{\phi}_m(X,Z) = X^{m^2} + Zg(X,Z)$ where $g(X,Z) \in \mathbb{Z}[X,Z]$ is homogeneous of degree m^2-1. Hence $\alpha_m = \overline{\phi_m}(m_1, m_3^2) \in m_1^{m^2} + m_3^2\mathbb{Z}$, which implies that $q \nmid \alpha_m$.

If $q \nmid m_3$, this implies that $\tilde{m}_3$ has a multiplicative inverse $\tilde{m}_3^{-1}$ in $\mathbb{F}_q$, and $\widetilde{P} = (\tilde{m}_1\tilde{m}_3^{-2}, \tilde{m}_2\tilde{m}_3^{-3})$ (using the notation in Definition 1.1.12). We observe that

$$\widetilde{\phi}_m(x(\widetilde{P})) = \widetilde{\phi}_m(\tilde{m}_1\tilde{m}_3^{-2}) = \tilde{m}_3^{-2m^2}\,\widetilde{\overline{\phi_m}}(\tilde{m}_1, \tilde{m}_3^2).$$

We thus have $q \mid \alpha_m$ precisely when $\widetilde{\phi}_m(x(\widetilde{P})) = 0$. Similarly, $q \mid \beta_m$ precisely when $\widetilde{\psi}_m^2(x(\widetilde{P})) = 0$. But because $P \in E^{\mathrm{good}}(\mathbb{Q})$, $x(\widetilde{P})$ cannot be a common zero of $\widetilde{\phi}_m$ and $\widetilde{\psi}_m^2$ by Lemma 2.3.8. We conclude that $q \nmid \gcd(\alpha_m, \beta_m)$, and because q is arbitrary we have $\gcd(\alpha_m, \beta_m) = 1$. This implies that $\alpha_m = \pm a([m]P)$. ∎

Lemma 2.3.12. *Let $P = \left(\frac{a(P)}{d(P)^2}, \frac{b(P)}{d(P)^3}\right) \in E_p(\mathbb{Q}) \setminus \{\mathcal{O}\}$. For all $m \geq 1$, there exists a power series $l_m(T) \in 1 + T^4\mathbb{Z}[[T]]$, independent of P, such that $a([m]P)/a(P)^{m^2} = l_m(t(P))$.*

Proof. First of all, note that Because $P \in E_1^{(p)}(\mathbb{Q}) \setminus \{\mathcal{O}\}$, P is a nontorsion point by Corollary 1.6.25. Hence $[m]P \neq \mathcal{O}$ for all $m \geq 1$, so $a([m]P)$ is well-defined.

We again use the notation $m_1 = a(P)$, $m_2 = b(P)$ and $m_3 = d(P)$. For $m = 1$ we get $a([m]P)/a(P)^{m^2} = 1$, so we simply have $l_1(T) = 1$. For $m \geq 2$, we use Lemma 2.3.11 to note that

$$a([m]P)/a(P)^{m^2} = \frac{m_3^{2m^2}}{m_1^{m^2}}\phi_m(m_1/m_3^2) = x(P)^{-m^2}\phi_m(x(P)).$$

Because ϕ_m is monic and using Lemma 2.3.10, we get that $\phi_m(x) = x^{m^2} + \sum_{i=0}^{m^2-2} d_i x^i$ for some $d_i \in \mathbb{Z}$. We obtain

$$a([m]P)/a(P)^{m^2} = 1 + \sum_{i=-m^2}^{-2} d_{i+m^2}\, x(P)^i.$$

Because $P \in E_1(\mathbb{Q})$, we have $x(P) = x^T(t(P))$ where x^T has the expansion (1.24). It follows that $x(P)^{-1} \in t(P)^2\mathbb{Z}[[t(P)]]$. This implies that $a([m]P)/a(P)^{m^2} \in 1 + t(P)^4\mathbb{Z}[[t(P)]]$. The coefficients of this series only depend on E and m and not on P, so indeed there exists a power series $l_m(T) \in 1 + T^4\mathbb{Z}[[T]]$, independent of P, such that $a([m]P)/a(P)^{m^2} = l_m(t(P))$. ∎

Using the above lemmas, we can prove the existence of the limit in Theorem 2.3.1(a).

Proof of Theorem 2.3.1(a). Let $P \in E_p(\mathbb{Q}) \setminus \{\mathcal{O}\}$. Then by Corollary 1.6.25, we also have $[p^n]P \in E_p(\mathbb{Q}) \setminus \{\mathcal{O}\}$ for all $n \geq 0$. Recall that we want to show the limit (2.23). We get

$$\begin{aligned}
&\frac{1}{p^{2(n+1)}}H_2([p^{n+1}]P) - \frac{1}{p^{2n}}H_2([p^n]P) \\
&\qquad = \frac{1}{p^{2(n+1)}}\left(H_2([p]([p^n]P)) - p^2 H_2([p^n]P)\right) \\
&\qquad = \frac{1}{p^{2(n+1)}}\log_p(a([p^{n+1}]P)/a([p^n]P)^{p^2}) && \text{(Proposition 2.3.7)} \\
&\qquad = \frac{1}{p^{2(n+1)}}\log_p(l_p(t([p^n]P))). && \text{(Lemma 2.3.12)}
\end{aligned}$$

It then follows from Corollary 2.3.4 that the limit of this expression as n approaches ∞ is zero, and hence by Lemma 1.1.6 the sequence $\left(\frac{1}{p^{2n}}H_2([p^n]P)\right)$ is Cauchy, as desired. ∎

2.3.3 Existence of h_3 and a relation between h_2 and h_3

Next, we show the existence of the limit in Theorem 2.3.1(b), following Perrin-Riou's argument in [28, pp. 247–248]. First, we find a relation between H_2 and H_3, and make use of the fact that we know the limit h_2 exists to find the limit h_3. We prove the following relation between the two limits.

Theorem 2.3.13 ([28, p. 246, Proposition]). *Let $P \in E_p(\mathbb{Q}) \setminus \{\mathcal{O}\}$. Then*

$$h_3(P) = h_2(P) + \frac{a_1^2 + 4a_2}{12}\mathcal{L}(t(P))^2.$$

Consider $P \in E_p(\mathbb{Q}) \setminus \{\mathcal{O}\}$. We write $m_1 = a(P)$, $m_2 = b(P)$ and $m_3 = d(P)$, so that $P = \left(\frac{m_1}{m_3^2}, \frac{m_2}{m_3^3}\right)$. We have

$$3(H_3(P) - H_2(P)) = \log_p\left(\left(m_2 + \frac{a_1}{2}m_1m_3 + \frac{a_3}{2}m_3^3\right)^2\right) - \log_p(m_1^3). \tag{2.25}$$

To find a relation between h_2 and h_3, we want to manipulate the right-hand side of this equation into an expression at which we can evaluate the appropriate limit using the lemmas in Section 2.3.1.

Recall that because $P \in E_1^{(p)}(\mathbb{Q})$, we have $t(P) = -\frac{x(P)}{y(P)} = -\frac{m_1m_3}{m_2}$. We can rewrite the argument of $\log_p$ in the first term of (2.25) as

$$\left(m_2 + \frac{a_1}{2}m_1m_3 + \frac{a_3}{2}m_3^3\right)^2 = \left(m_2 - \frac{a_1}{2}m_2t(P) - \frac{a_3}{2}\frac{m_2^3}{m_1^3}t(P)^3\right)^2.$$

Because $P \in E_1^{(p)}(\mathbb{Q})$ we know that $\mathrm{ord}_p(y(P)) < \mathrm{ord}_p(x(P)) < 0$, and hence $\mathrm{ord}_p(m_1) = \mathrm{ord}_p(m_2) = 0$. This means that $m_1, m_2 \in \mathbb{Z}_p^\times$. Because $p \neq 2$ we also have $2, 4 \in \mathbb{Z}_p^\times$. We can rewrite the expression above as an element in $\mathbb{Z}_p$ modulo the ideal generated by $t(P)^3$ as follows:

$$\begin{aligned}\left(m_2 - \frac{a_1}{2}m_2t(P) - \frac{a_3}{2}\frac{m_2^3}{m_1^3}t(P)^3\right)^2 &\equiv m_2^2\left(1 - \frac{a_1}{2}t(P)\right)^2 \bmod t(P)^3 \\ &\equiv m_2^2\left((1 - a_1t(P))\left(1 + \frac{a_1^2}{4}t(P)^2\right) + \frac{a_1^3}{4}t(P)^3\right) \bmod t(P)^3 \\ &\equiv m_2^2(1 - a_1t(P))\left(1 + \frac{a_1^2}{4}t(P)^2\right) \bmod t(P)^3. \end{aligned} \tag{2.26}$$

Now let us rewrite the first factor in (2.26). By multiplying both sides of the Weierstrass equation of the curve (2.5) by m_3^6, we obtain

$$\begin{aligned} m_2^2 + a_1m_1m_2m_3 + a_3m_2m_3^3 &= m_1^3 + a_2m_1^2m_3^2 + a_4m_1m_3^4 + a_6m_3^6 \\ m_2^2 - a_1m_2^2t(P) - a_3\frac{m_2^4}{m_1^3}t(P)^3 &= m_1^3 + a_2m_2^2t(P)^2 + a_4\frac{m_2^4}{m_1^3}t(P)^4 + a_6\frac{m_2^6}{m_1^6}t(P)^6. \end{aligned} \tag{2.27}$$

Because $m_1 \in \mathbb{Z}_p^\times$, we thus have

$$m_2^2(1 - a_1t(P)) \equiv m_1^3 + a_2m_2^2t(P)^2 \mod t(P)^3. \tag{2.28}$$

Equation (2.27) furthermore shows that $m_2^2 \equiv m_1^3 \bmod t(P)$, and hence (2.28) becomes

$$m_2^2(1 - a_1t(P)) \equiv m_1^3(1 + a_2t(P)^2) \mod t(P)^3. \tag{2.29}$$

We combine (2.26) and (2.29) to obtain

$$\begin{aligned}\left(m_2 + \frac{a_1}{2}m_1m_3 + \frac{a_3}{2}m_3^3\right)^2 &\equiv m_1^3(1 + a_2t(P)^2)\left(1 + \frac{a_1^2}{4}t(P)^2\right) \bmod t(P)^3 \\ &\equiv m_1^3\left(1 + \frac{a_1^2 + 4a_2}{4}t(P)^2\right) \bmod t(P)^3. \end{aligned}$$

Substituting this into (2.25) gives

$$3(H_3(P) - H_2(P)) = \log_p\left(1 + \frac{a_1^2 + 4a_2}{4}t(P)^2 + e\,t(P)^3\right)$$

for some $e \in \mathbb{Z}_p$. We find

$$\begin{aligned}
&\lim_{n\to\infty} \frac{1}{p^{2n}} H_3([p^n]P) \\
&\quad = \lim_{n\to\infty} \frac{1}{p^{2n}} \left[H_2([p^n]P) + \frac{1}{3}\log_p\left(1 + \frac{a_1^2 + 4a_2}{4}t([p^n]P)^2 + e\,t([p^n]P)^3\right)\right] \\
&\quad = \lim_{n\to\infty} \frac{1}{p^{2n}} H_2([p^n]P) + \frac{1}{3}\lim_{n\to\infty} \frac{1}{p^{2n}} \log_p\left(1 + \frac{a_1^2 + 4a_2}{4}t([p^n]P)^2 + e\,t([p^n]P)^3\right) \\
&\quad = h_2(P) + \frac{a_1^2 + 4a_2}{12}\mathcal{L}(t(P))^2. \qquad \text{(Corollary 2.3.6)}
\end{aligned}$$

This proves both Theorem 2.3.1(b) and Theorem 2.3.13.

2.3.4 Quadraticity of h_2 and h_3

We now show that the functions h_2 and h_3 indeed qualify as height functions, in the sense that they are quadratic functions and satisfy the parallelogram law. Quadraticity follows straightforwardly from the results in Section 2.3.2.

Theorem 2.3.14. *Let $P \in E_p(\mathbb{Q}) \setminus \{\mathcal{O}\}$ and let $m \in \mathbb{Z}$, $m \neq 0$. Then*

$$\begin{aligned}
h_2([m]P) &= m^2 h_2(P), \\
h_3([m]P) &= m^2 h_3(P).
\end{aligned}$$

Proof. Let us first consider $m > 0$. Using the results from Section 2.3.2 we get

$$\begin{aligned}
h_2([m]P) - m^2 h_2(P) &= \lim_{n\to\infty} \frac{1}{p^{2n}} \left(H_2([p^n m]P) - m^2 H_2([p^n]P)\right) \\
&= \lim_{n\to\infty} \frac{1}{p^{2n}} \log_p\left(\frac{a([p^n m]P)}{a([p^n]P)^{m^2}}\right) \qquad \text{(Proposition 2.3.7)} \\
&= \lim_{n\to\infty} \frac{1}{p^{2n}} \log_p\left(l_m(t([p^n]P))\right) = 0. \qquad \text{(Lemma 2.3.12, Corollary 2.3.4)}
\end{aligned}$$

To show the result for $m < 0$, recall that for any $P \in E_p(\mathbb{Q}) \setminus \{\mathcal{O}\}$ we have $x(P) = x(-P)$, and thus $a(P) = a(-P)$ which implies $H_2(P) = H_2(-P)$. We get

$$\begin{aligned}
h_2(-P) &= \lim_{n\to\infty} \frac{1}{p^{2n}} H_2([p^n](-P)) \\
&= \lim_{n\to\infty} \frac{1}{p^{2n}} H_2([p^n](P)) \\
&= h_2(P).
\end{aligned}$$

We conclude that for $m < 0$, we have

$$h_2([m]P) = h_2([-m]P) = (-m)^2 h_2(P) = m^2 h_2(P).$$

This shows the result for h_2. The result for h_3 then follows from Theorem 2.3.13 and Proposition 2.2.11. ∎

We now work out the details of the argument by Perrin-Riou in [28, pp. 251–253], which shows that h_2 satisfies the parallelogram law. This argument follows a standard approach for showing the parallelogram law, it is for example analogous to the argument of Silverman in [32, VIII, Theorem 6.2] showing that the Néron-Tate height satisfies the parallelogram law.

Let us start by introducing a map $H\colon \mathbb{Q}\times\mathbb{Q}\to\mathbb{Z}_p$ as follows. Let $a,b\in\mathbb{Q}$. Then we can write $a=\frac{\alpha_1}{\alpha_3}$ and $b=\frac{\alpha_2}{\alpha_3}$ for some $\alpha_1,\alpha_2,\alpha_3\in\mathbb{Z}$ such that $\gcd(\alpha_1,\alpha_2,\alpha_3)=1$, unique up to sign. Let us define the set $B_p=\{i\ :\ p\nmid\alpha_i\}$. Note that $i\in B_p$ precisely when $\alpha_i\in\mathbb{Z}_p^\times$, and that B_p is nonempty. We define

$$H(a,b)=\frac{2}{\#B_p}\sum_{i\in B_p}\log_p(\alpha_i).$$

Note that this is well-defined because $\log_p(\alpha_i)=\log_p(-\alpha_i)$.

Furthermore, for $a\in\mathbb{Q}^\times$ with $\operatorname{ord}_p(a)<0$, we can write $a=\frac{m_1}{m_2}$ with $m_1,m_2\in\mathbb{Z}$ and $\gcd(m_1,m_2)=1$, again unique up to sign. Then $p\nmid m_1$, and we define

$$H(a)=2\log_p(m_1).$$

Lemma 2.3.15 ([28, p. 251]). *Let $a,b\in\mathbb{Q}^\times$ with $\operatorname{ord}_p(a)<0$ and $\operatorname{ord}_p(b)<0$. Then*

$$H(ab,a+b)=H(a)+H(b).$$

Proof. Let $a=\frac{m_1}{m_3}$ and $b=\frac{m_2}{m_4}$ with $m_i\in\mathbb{Z}$ such that $\gcd(m_1,m_3)=\gcd(m_2,m_4)=1$. We have $ab=\frac{m_1m_2}{m_3m_4}$ and $a+b=\frac{m_1m_4+m_2m_3}{m_3m_4}$. Let $\alpha_1=m_1m_2$, $\alpha_2=m_1m_4+m_2m_3$ and $\alpha_3=m_3m_4$. We want to show that $\gcd(\alpha_1,\alpha_2,\alpha_3)=1$. Assume q is a prime such that $q\mid\alpha_1$ and $q\mid\alpha_3$. Without loss of generality we assume that $q\mid m_1$. But because $\gcd(m_1,m_3)=1$ this implies $q\nmid m_3$. Then $q\mid\alpha_3$ implies that $q\mid m_4$. Again, $\gcd(m_2,m_4)=1$ implies that $q\nmid m_2$. Together this implies that $q\nmid m_1m_4+m_2m_3=\alpha_2$. This shows that $\gcd(\alpha_1,\alpha_2,\alpha_3)=1$. To compute $H(ab,a+b)$ we need to determine $B_p=\{i:p\nmid\alpha_i\}$. From our assumption on a and b we know that $\operatorname{ord}_p(m_1)=\operatorname{ord}_p(m_2)=0$ and $\operatorname{ord}_p(m_3),\operatorname{ord}_p(m_4)>0$. We deduce that $\operatorname{ord}_p(\alpha_1)=0$, $\operatorname{ord}_p(\alpha_2)>0$ and $\operatorname{ord}_p(\alpha_3)>0$, so we have $B_p=\{\alpha_1\}$. We conclude that

$$\begin{aligned}H(ab,a+b)&=2\log_p(m_1m_2)\\&=2\log_p(m_1)+2\log_p(m_2)\\&=H(a)+H(b).\end{aligned}$$

■

For $P\in E_p(\mathbb{Q})\setminus\{\mathcal{O}\}$, we have $\operatorname{ord}_p(x(P))<0$ and $H(x(P))=2H_2(P)$. Hence when $P,Q,P+Q,P-Q\in E_p(\mathbb{Q})\setminus\{\mathcal{O}\}$, Lemma 2.3.15 in particular implies

$$\begin{aligned}2H_2(P+Q)+2H_2(P-Q)&=H(x(P+Q))+H(x(P-Q))\\&=H(x(P+Q)x(P-Q),x(P+Q)+x(P-Q)),&(2.30)\\2H_2(P)+2H_2(Q)&=H(x(P)x(Q),x(P)+x(Q)).&(2.31)\end{aligned}$$

We consider the following standard formulas, which can be derived from the group law on E ([32, III, Algorithm 2.3]). They are valid for any (possibly singular) Weierstrass curve E over a

field K at points $P, Q \in E_{\mathrm{ns}}(K)$ such that $P, Q, P+Q, P-Q \neq \mathcal{O}$.

$$x(P+Q) + x(P-Q) = \frac{(x(P)+x(Q))(b_4 + 2x(P)x(Q)) + b_2 x(P)x(Q) + b_6}{(x(P)-x(Q))^2}, \tag{2.32}$$

$$x(P+Q)x(P-Q) = \frac{(x(P)x(Q))^2 - b_4 x(P)x(Q) - b_6(x(P)+x(Q)) - b_8}{(x(P)-x(Q))^2}. \tag{2.33}$$

Lemma 2.3.16 ([28, Lemme e]). *Consider a Weierstrass curve given by* (1.4) *over a field K. If P and Q are two nonsingular points, then the numerators and denominator in the right-hand side of* (2.32) *and* (2.33) *cannot all be simultaneously equal to zero.*

Proof. Suppose that the denominator of both fractions is equal to 0. Then we have $x(P) = x(Q)$, and the numerator of (2.32) reduces to

$$2x(P)(b_4 + 2x(P)^2) + b_2 x(P)^2 + b_6 = 4x(P)^3 + b_2 x(P)^2 + 2b_4 x(P) + b_6 = \psi_2^2(x(P)).$$

The numerator of (2.33) reduces to

$$x(P)^4 - b_4 x(P)^2 - 2b_6 x(P) - b_8 = \phi_2(x(P)).$$

Because P is nonsingular, we cannot have $\phi_2(x(P)) = \psi_2^2(x(P)) = 0$ by Lemma 2.3.8. Hence the numerators of (2.32) and (2.33) cannot simultaneously be zero when the denominator is zero. ∎

Let us now consider two points $P, Q \in E_p(\mathbb{Q}) \setminus \{\mathcal{O}\}$ such that also $P+Q, P-Q \neq \mathcal{O}$. Let $x(P) = \frac{a(P)}{d(P)^2}$ and $x(Q) = \frac{a(Q)}{d(Q)^2}$. Then the reasoning in the proof of Lemma 2.3.15 shows that if we write

$$\begin{aligned} u_1 &= a(P)d(Q)^2 + a(Q)d(P)^2, \\ u_2 &= a(P)a(Q), \\ u_3 &= d(P)^2 d(Q)^2, \end{aligned}$$

then $x(P) + x(Q) = \frac{u_1}{u_3}$ and $x(P)x(Q) = \frac{u_2}{u_3}$ with $\gcd(u_1, u_2, u_3) = 1$. Then we see from (2.32) that

$$\begin{aligned} x(P+Q) + x(P-Q) &= \frac{w_1}{w_3} \\ x(P+Q)x(P-Q) &= \frac{w_2}{w_3} \end{aligned}$$

with

$$\begin{aligned} w_1 &= b_4 u_1 u_3 + 2u_1 u_2 + b_2 u_2 u_3 + b_6 u_3^2, \\ w_2 &= u_2^2 - b_4 u_2 u_3 - b_6 u_1 u_3 - b_8 u_3^2, \\ w_3 &= u_1^2 - 4u_2 u_3. \end{aligned}$$

Lemma 2.3.17. *We have* $\gcd(w_1, w_2, w_3) = 1$.

Proof. Let q be any prime. We show that $q \nmid \gcd(w_1, w_2, w_3)$. We consider separate cases, depending on whether q divides the denominators of $x(P)$ and $x(Q)$.

1. If $q \mid d(Q)$ and $q \mid d(P)$, we have $q \nmid a(P)a(Q)$. Then $q \mid u_3$ but $q \nmid u_2$, and hence $q \nmid w_2$.
2. If $q \mid d(Q)$ and $q \nmid d(P)$, then $q \nmid a(Q)$ and we get $q \mid u_3$ but $q \nmid u_1$. This shows that $q \nmid w_3$.
3. If $q \nmid d(Q)$ and $q \mid d(P)$, similar reasoning implies that $q \nmid w_3$.
4. If $q \nmid d(P)$ and $q \nmid d(Q)$, we have $\widetilde{P}, \widetilde{Q} \neq \mathcal{O}$ modulo q, but both reductions are nonsingular because $P, Q \in E^{\text{good}}(\mathbb{Q})$. We have that $\tilde{u}_3 \in \mathbb{F}_q^\times$. Plugging in $x(\widetilde{P}) = (\tilde{a}(P)\tilde{d}(P)^{-2})$ and $x(\widetilde{Q}) = (\tilde{a}(Q)\tilde{d}(Q)^{-2})$ into equations (2.32) and (2.33) gives

$$x(\widetilde{P}+\widetilde{Q}) + x(\widetilde{P}-\widetilde{Q}) = \frac{\tilde{u}_3^{-2}\tilde{w}_1}{\tilde{u}_3^{-2}\tilde{w}_3} \quad \text{and} \quad x(\widetilde{P}+\widetilde{Q})x(\widetilde{P}-\widetilde{Q}) = \frac{\tilde{u}_3^{-2}\tilde{w}_2}{\tilde{u}_3^{-2}\tilde{w}_3}.$$

   Lemma 2.3.16 then implies that $\tilde{w}_1$, $\tilde{w}_2$ and $\tilde{w}_3$ cannot simultaneously be 0 modulo q. This implies that $q \nmid \gcd(w_1, w_2, w_3)$.

■

Because $\text{ord}_p(x(P)), \text{ord}_p(x(Q)) < 0$, we deduce that $\text{ord}_p(u_1), \text{ord}_p(u_3) > 0$ and $\text{ord}_p(u_2) = 0$. This shows that $\text{ord}_p(w_1), \text{ord}_p(w_3) > 0$ and $\text{ord}_p(w_2) = 0$.

Let us define the notation

$$\lambda(P,Q) := \frac{w_2}{u_2^2} = 1 - b_4\frac{u_3}{u_2} - b_6\frac{u_1u_3}{u_2^2} - b_8\frac{u_3^2}{u_2^2}.$$

We obtain

$$\begin{aligned}
2H_2(P+Q) + 2H_2(P-Q) &= H\left(\frac{w_2}{w_3}, \frac{w_1}{w_3}\right) && \text{(using (2.30))}\\
&= 2\log_p(w_2)\\
&= 4\log_p(u_2) + 2\log_p(\lambda(P,Q))\\
&= 2H\left(\frac{u_2}{u_3}, \frac{u_1}{u_3}\right) + 2\log_p(\lambda(P,Q))\\
&= 2H\left(x(P)x(Q), x(P)+x(Q)\right) + 2\log_p(\lambda(P,Q))\\
&= 2H(x(P)) + 2H(x(Q)) + 2\log_p(\lambda(P,Q)) && \text{(using (2.31))}\\
&= 4H_2(P) + 4H_2(Q) + 2\log_p(\lambda(P,Q)). && (2.34)
\end{aligned}$$

Recall that $x(P) = x^T(t(P))$ and $x(Q) = x^T(t(Q))$. We use the expansion of x^T in (1.24) to find that

$$\begin{aligned}
\frac{u_3}{u_2} &= (x(P)x(Q))^{-1} \in t(P)^2t(Q)^2\mathbb{Z}[[t(P), t(Q)]]\\
\frac{u_1}{u_3} &= x(P) + x(Q) = t(P)^{-2} + t(Q)^{-2} - a_1t(P)^{-1} - a_1t(Q)^{-1} + \cdots.
\end{aligned}$$

This shows that $\lambda(P,Q) = \lambda^T(t(P), t(Q))$ for some power series $\lambda^T(T_1, T_2) \in 1 + T_1^2T_2^2\mathbb{Z}[[T_1, T_2]]$. We have a result very similar to Corollary 2.3.4 for power series in two variables.

Lemma 2.3.18. *Let $P, Q \in E_1(\mathbb{Q}_p) \setminus \{\mathcal{O}\}$. Let $g(T_1, T_2) \in 1 + (T_1, T_2)^k\mathbb{Z}_p[[T_1, T_2]]$ for some $k \in \mathbb{Z}_{>0}$. For $m \in \mathbb{Z}_{<k}$ we have*

$$\lim_{n\to\infty} \frac{1}{p^{mn}} \log_p(g(t([p^n]P), t([p^n]Q))) = 0.$$

Proof. For $P, Q \in E_1(\mathbb{Q}_p)$ we have $\operatorname{ord}_p(t([p^n]P)), \operatorname{ord}_p(t([p^n]Q)) > n$ for all $n \geq 0$ (Corollary 1.6.13). Because $g \in 1 + (T_1, T_2)^k \mathbb{Z}_p[[T_1, T_2]]$ converges on $(p\mathbb{Z}_p)^2$, the result follows from Lemma 2.3.2. ∎

Theorem 2.3.19 ([28, p. 246, Proposition]). *Let $P, Q \in E_p(\mathbb{Q})$ be such that P, Q, $P+Q$, $P-Q \neq \mathcal{O}$. Then*

$$h_2(P+Q) + h_2(P-Q) = 2h_2(P) + 2h_2(Q) \text{ and}$$
$$h_3(P+Q) + h_3(P-Q) = 2h_3(P) + 2h_3(Q).$$

Proof. Using (2.34), we find

$$\begin{aligned} h_2(P+Q) + h_2(P-Q) &= \lim_{n\to\infty} \frac{1}{p^{2n}} (H_2([p^n]P + [p^n]Q) + H_2([p^n]P - [p^n]Q)) \\ &= \lim_{n\to\infty} \frac{1}{p^{2n}} (2H_2([p^n]P) + 2H_2([p^n]Q) + \log_p(\lambda([p^n]P, [p^n]Q))) \\ &= 2h_2(P) + 2h_2(Q) + \lim_{n\to\infty} \frac{1}{p^{2n}} \log_p(\lambda^T(t([p^n]P), t([p^n]Q))) \\ &= 2h_2(P) + 2h_2(Q). \qquad \text{(using Lemma 2.3.18)} \end{aligned}$$

The result for h_3 then follows from Theorem 2.3.13 and Proposition 2.2.11. ∎

2.3.5 Extension of h_2 and h_3 to $E(\mathbb{Q})$

We use the quadraticity of h_2 and h_3 to extend these functions to the entire group $E(\mathbb{Q})$.

Definition 2.3.20. We define a function $h_2 \colon E(\mathbb{Q}) \to \mathbb{Q}_p$ and $h_3 \colon E(\mathbb{Q}) \to \mathbb{Q}_p$ as follows. For $P \in E_{\text{tors}}(\mathbb{Q})$, we set

$$h_2(P) = h_3(P) = 0.$$

For $P \in E(\mathbb{Q}) \setminus E_{\text{tors}}$, let $m \in \mathbb{Z}_{>0}$ such that $[m]P \in E_p(\mathbb{Q}) \setminus \{\mathcal{O}\}$ (which exists by Proposition 2.2.20). Then

$$h_2(P) = \frac{1}{m^2} h_2([m]P) \quad \text{and} \quad h_3(P) = \frac{1}{m^2} h_3([m]P).$$

The following Proposition shows that the definition does not depend on the choice of m.

Proposition 2.3.21. *Let $P \in E(\mathbb{Q}) \setminus E_{\text{tors}}$, and let m_1 and m_2 be positive integers such that $[m_1]P, [m_2]P \in E_p(\mathbb{Q})$. Then*

$$\frac{1}{m_1^2} h_2([m_1]P) = \frac{1}{m_2^2} h_2([m_2]P) \quad \text{and} \quad \frac{1}{m_1^2} h_3([m_1]P) = \frac{1}{m_2^2} h_3([m_2]P).$$

Proof. Because $E_p(\mathbb{Q})$ is a subgroup, we also have $[m_1 m_2]P \in E_p(\mathbb{Q}) \setminus \{\mathcal{O}\}$. It follows from Theorem 2.3.14 that

$$\frac{1}{m_1^2} h_2([m_1]P) = \frac{1}{m_1^2 m_2^2} h_2([m_1 m_2]P) = \frac{1}{m_2^2} h_2([m_2]P).$$

The same argument shows the statement for h_3. ∎

Definition 2.3.20 agrees with the original definition of h_2 and h_3 on $E_p(\mathbb{Q}) \setminus \{\mathcal{O}\}$, because for $P \in E_p(\mathbb{Q}) \setminus \{\mathcal{O}\}$ we have $P \notin E_{\text{tors}}$ by Corollary 1.6.25, so we can take $m = 1$ in Definition 2.3.20.

Proposition 2.3.22. *h_2 and h_3 are quadratic forms on $E(\mathbb{Q})$. Explicitly, let $P, Q \in E(\mathbb{Q})$ and let $n \in \mathbb{Z}$. Then*

(a) $h_2([n]P) = n^2 h_2(P)$ and $h_3([n]P) = n^2 h_3(P)$.

(b) $h_2(P+Q)+h_2(P-Q) = 2h_2(P)+2h_2(Q)$ and $h_3(P+Q)+h_3(P-Q) = 2h_3(P)+2h_3(Q)$.

Proof. We show the results for h_2. The exact same arguments work for h_3.

Part (a) is clearly satisfied for all $P \in E(\mathbb{Q})$ when $n = 0$, because then both sides evaluate to 0. Now let $n \neq 0$. If P is a torsion point, again both sides evaluate to 0. Now let $P \notin E_{\text{tors}}$ and let $m_1 \in \mathbb{Z}_{>0}$ be such that $[m_1]P \in E_p(\mathbb{Q})\setminus\{\mathcal{O}\}$. For $n \neq 0$, we then also have $[m_1 n]P \in E_p(\mathbb{Q})\setminus\{\mathcal{O}\}$, and we get

$$\begin{aligned} h_2([n]P) &= \frac{1}{m_1^2} h_2([m_1 n]P) && \text{(Definition 2.3.20)} \\ &= \frac{n^2}{m_1^2} h_2([m_1]P) && \text{(Theorem 2.3.14)} \\ &= n^2 h_2(P). && \text{(Definition 2.3.20)} \end{aligned}$$

For (b), let us first assume that $P, Q, P+Q, P-Q \notin E_{\text{tors}}$. Let m_1 be as before and let $m_2 \in \mathbb{Z}_{>0}$ be such that $[m_2]Q \in E_p(\mathbb{Q}) \setminus \{\mathcal{O}\}$. Then $[m_1 m_2]P$, $[m_1 m_2]Q$ and their sum and difference are all in $E_p(\mathbb{Q}) \setminus \{\mathcal{O}\}$. Therefore

$$\begin{aligned} h_2(P+Q) + h_2(P-Q) &= \frac{1}{m_1^2 m_2^2} \left(h_2([m_1 m_2]P + [m_1 m_2]Q) + h_2([m_1 m_2]P - [m_1 m_2]Q)\right) \\ &= \frac{1}{m_1^2 m_2^2} \left(2h_2([m_1 m_2]P) + 2h_2([m_1 m_2]Q)\right) && \text{(Theorem 2.3.19)} \\ &= 2h_2(P) + 2h_2(Q). \end{aligned}$$

If one of $P, Q, P+Q, P-Q$ is a torsion point, we can use arguments like in the proof of Proposition 2.2.22 to obtain the result. ∎

2.3.6 A relation between the p-adic heights h_2, h_3 and $h_p^{(s)}$

Next, we compare the quadratic heights h_2 and h_3 to the p-adic heights $h_p^{(s)}$ described in Section 2.2.3. In [29], Perrin-Riou provides a relation between h_2 and $h_p^{(s)}$ for a specific value of s under the assumption that E has ordinary reduction at p. The proof we provide here uses a similar strategy, but we use the more general Corollary 2.3.6 instead of Corollary 2.3.4 and Lemma 2.3.5 in our argument, which allows us to show the relation without the assumption of ordinary reduction at p.

Theorem 2.3.23 ([29, p. 292]). *Let $s \in \mathbb{Q}_p$ such that V_s is a neighborhood of 0. Let $P \in E_p^{(s)}(\mathbb{Q}) \setminus \{\mathcal{O}\}$. Then*

$$h_p^{(s)}(P) = h_2(P) + \left(s + \frac{a_1^2 + 4a_2}{12}\right) \mathcal{L}(t(P))^2.$$

Proof. Let us consider a point $Q \in E_p^{(s)}(\mathbb{Q}) \setminus \{\mathcal{O}\}$. We write $x(Q) = \frac{a(Q)}{d(Q)^2}$ as before. Recall that $a(Q) \neq 0$ for $Q \in E_1^{(p)}(\mathbb{Q}) \setminus \{\mathcal{O}\}$.

$$\begin{aligned} h_p^{(s)}(Q) &= -2\log_p\left(\frac{\sigma_p^{(s)}(t(Q))}{d(Q)}\right) && \text{(Proposition 2.2.21)} \\ &= -\log_p\left(\sigma_p^{(s)}(t(Q))^2 x(Q)\right) + \log_p(a(Q)) \\ &= -\log_p\left(\sigma_p^{(s)}(t(Q))^2 x^T(t(Q))\right) + H_2(Q). && (2.35) \end{aligned}$$

Using the expansion of σ (Lemma 2.2.3), the expansion of $\exp_p$ in (1.1) and the expansion of $\mathcal{L}$, which can be found using Theorem 1.6.19 and the expansion of the invariant differential ω given in [32, p. 118], we can deduce that the expansion of $\sigma_p^{(s)}$ is of the form

$$\sigma_p^{(s)}(T) = T + \frac{a_1}{2}T^2 + \left(\frac{a_1^2 + a_2}{3} - \frac{s}{2}\right)T^3 + \cdots$$

in $\mathbb{Q}_p[[T]]$. Using the expansion of x^T in (1.24), some algebra shows that

$$\sigma_p^{(s)}(T)^2 x^T(T) = 1 - \left(s + \frac{a_1^2 + 4a_2}{12}\right)T^2 + \cdots \in \mathbb{Q}_p[[T]].$$

Recall from Proposition 2.2.10 that the Bernardi σ-function $\sigma_p^{(0)}(T)$ converges for $T \in p\mathbb{Z}_p$. We also know that $x^T(T)$ converges on $p\mathbb{Z}_p \setminus \{0\}$. From the expansion we see that $\sigma_p^{(0)}(0)x^T(0) = 1$. Together, these facts imply that the series $\sigma_p^{(0)}(T)^2 x^T(T)$ converges on a neighborhood of 0. When $P \in E_p^{(0)}(\mathbb{Q}) \setminus \{\mathcal{O}\}$, then also $[p^n]P \in E_p(\mathbb{Q}) \setminus \{\mathcal{O}\}$ for all $n \geq 0$ because P is a nontorsion point by Corollary 1.6.25. We can thus use (2.35) to derive

$$\begin{aligned} h_p^{(0)}(P) &= \lim_{n\to\infty} \frac{1}{p^{2n}} h_p^{(0)}([p^n]P) && \text{(because } h_p^{(0)} \text{ is quadratic)} \\ &= \lim_{n\to\infty} \frac{1}{p^{2n}} H_2([p^n]P) - \lim_{n\to\infty} \frac{1}{p^{2n}} \log_p(\sigma_p^{(0)}(t([p^n]P))^2 x^T(t([p^n]P))) \\ &= h_2(P) + \frac{a_1^2 + 4a_2}{12}\mathcal{L}(t(P))^2. && \text{(Corollary 2.3.6)} \end{aligned}$$

Finally, using Proposition 2.2.23 we find that for all $P \in E_p^{(s)}(\mathbb{Q}) \setminus \{\mathcal{O}\}$,

$$h_p^{(s)}(P) = h_2(P) + \left(s + \frac{a_1^2 + 4a_2}{12}\right)\mathcal{L}(t(P))^2.$$

■

Comparing this result with Theorem 2.3.13 gives the following Corollary.

Corollary 2.3.24. *Let $P \in E_p(\mathbb{Q}) \setminus \{\mathcal{O}\}$. Then*

$$h_p^{(s)}(P) = h_3(P) + s\mathcal{L}(t(P))^2.$$

In particular, we have $h_3(P) = h_p^{(0)}(P)$.

We can extend this last equality to all of $E(\mathbb{Q})$ using the definition in the previous section.

Proposition 2.3.25. *We have $h_p^{(0)} = h_3$ on $E(\mathbb{Q})$.*

Proof. For $P \in E_{\text{tors}}(\mathbb{Q})$, we have $h_p^{(0)}(P) = h_3(P) = 0$. By Corollary 2.3.24 we know the equality is satisfied for $P \in E_p(\mathbb{Q}) \setminus \{\mathcal{O}\}$. For $P \in E(\mathbb{Q}) \setminus E_{\text{tors}}$, let $m \in \mathbb{Z}_{>0}$ such that $[m]P \in E_p(\mathbb{Q})$. Then

$$\begin{aligned} h_p^{(s)}(P) &= \frac{1}{m^2} h_p^{(s)}([m]P) && \text{(Proposition 2.2.22)} \\ &= \frac{1}{m^2} h_3([m]P) && \text{(Corollary 2.3.24)} \\ &= h_3(P). && \text{(Proposition 2.3.22)} \end{aligned}$$

■

Chapter 3

Height functions on the Jacobians of genus 2 curves

Similarly to how we defined heights for elliptic curves, we can define heights on the Jacobian of a genus 2 curve. In the case of elliptic curves we defined the height functions in such a way that they only depend on the x-coordinate of a point. That way, each point has the same height as its additive inverse. On the Jacobian, we will define heights that only depend on the image of a point on the Kummer surface. Because the map from the Jacobian to the Kummer surface also identifies points with their additive inverse, these height functions will have that same property.

Let us consider a smooth projective curve $\mathcal{C}$ of genus 2 defined over $\mathbb{Q}$ by an equation of the form (1.13), with Jacobian J. A point $P \in J(\mathbb{Q})$ has an image $\kappa(P) \in \mathbb{P}^3$ on the Kummer surface via the map (1.18). We introduce notation for a useful normalization of $\kappa(P)$. We write $\kappa(P) = [x_1(P) : x_2(P) : x_3(P) : x_4(P)]$ for the normalization that satisfies $x_i(P) \in \mathbb{Z}$ and $\gcd(x_1(P), \ldots, x_4(P)) = 1$. This normalization is defined uniquely only up to sign, but we only consider the coordinates in the context of ratios, v-adic absolute values or the p-adic logarithm of the coordinates, in which case the sign does not make a difference. Furthermore we use the notation $x(P) = (x_1(P), x_2(P), x_3(P), x_4(P))$.

3.1 Real-valued heights on the Jacobian of a genus 2 curve

In order to define a naive height function, we take the standard height H on projective space defined in (2.1), and apply it to the projective Kummer coordinates of a point on J.

Definition 3.1.1. We define $h_{\text{naive}} \colon J(\mathbb{Q}) \to \mathbb{R}$ by

$$h_{\text{naive}}(P) = \log H(\kappa(P)),$$

with H as defined in (2.1).

A canonical height is defined analogously to the canonical height for elliptic curves (Proposition 2.1.8).

Definition 3.1.2 ([14, p. 335]). We define the real canonical height $\hat{h} \colon J(\mathbb{Q}) \to \mathbb{R}$ by

$$\hat{h}(P) = \lim_{n \to \infty} \frac{1}{n^2} h_{\text{naive}}([n]P).$$

Proposition 3.1.3 ([14, p. 335]). *The real canonical height $\hat{h}\colon J(\mathbb{Q}) \to \mathbb{R}$ is a quadratic form.*

3.1.1 Local real height functions

In Section 2.1.3 we saw that we could write the naive and canonical real heights on an elliptic curve as the sum of local components. We do a similar thing for the naive height in Definition 3.1.1 and the canonical height in Definition 3.1.2. For elliptic curves, we defined the local heights everywhere except on the identity $\mathcal{O}$ of E. In the genus 2 case, we have to define the local heights away from the support of a divisor on J (this is analogous in the sense that the divisor $\mathcal{O}$ on an elliptic curve E can be seen as the genus 1 analogue of the Θ divisor, see [36, p. 281]). Recall that Θ is a divisor on J, obtained as the image of the map Φ_∞ (Section 1.5.1). We use it to define the following divisors on J:

$$\Theta_1 = 2\Theta, \quad \Theta_2 = \Theta_1 + \operatorname{div} \wp_{22}, \quad \Theta_3 = \Theta_1 + \operatorname{div} \wp_{12}, \quad \Theta_4 = \Theta_1 + \operatorname{div} \wp_{11}.$$

We denote by $\operatorname{supp}(D)$ the support of a divisor D, that is, the set of points that lie on the components of D as subvarieties of J. Then $P \in \operatorname{supp}(\Theta)$ precisely when $x_1(P) = 0$, and we have $\operatorname{supp}(\Theta_1) = \operatorname{supp}(\Theta)$. Furthermore, we have $P \in \operatorname{supp}(\Theta_i)$ precisely when $x_i(P) = 0$. For every point $P \in J$, there thus exists $i \in \{1, 2, 3, 4\}$ such that $P \notin \operatorname{supp}(\Theta_i)$. We introduce the notation $J_D = J \setminus \operatorname{supp}(D)$ for a divisor D.

Definition 3.1.4. Let $v \in M_\mathbb{Q}$. For $i = 1, 2, 3, 4$, we define the naive real local height $\lambda_{i,v}\colon J_{\Theta_i}(\mathbb{Q}_v) \to \mathbb{R}$ by

$$\lambda_{i,v}(P) = \log \max_{1 \le j \le 4} \left\{ \left| \frac{x_j(P)}{x_i(P)} \right|_v \right\}.$$

When v is a prime q, we have $\max_{1 \le j \le 4} \left\{ |x_j(P)|_v \right\} = 1$ because of how the normalization $x(P)$ is defined, and hence

$$\lambda_{i,q}(P) = -\log |x_i(P)|_q.$$

Proposition 3.1.5 ([35, Theorem 5.7]). *Let $P \in J_{\Theta_i}(\mathbb{Q})$. Then*

$$h_{\text{naive}}(P) = \sum_{v \in M_\mathbb{Q}} \lambda_{i,v}(P).$$

Proof. We note that $\lambda_{i,v}(P) = 0$ for all but finitely many v. Using the observation that $\max_{1 \le j \le 4} \{|x_j(P)|_q\} = 1$ for all primes q, we get

$$\begin{aligned} h_{\text{naive}}(P) &= \log \max_{1 \le j \le 4} \{|x_j(P)|_\infty\} = \log \prod_{v \in M_\mathbb{Q}} \max_{1 \le j \le 4} \{|x_j(P)|_v\} \\ &= \log \prod_{v \in M_\mathbb{Q}} \max_{1 \le j \le 4} \left\{ \left| \frac{x_j(P)}{x_i(P)} \right|_v \right\} && \text{(using Theorem 1.1.10)} \\ &= \sum_{v \in M_\mathbb{Q}} \log \max_{1 \le j \le 4} \left\{ \left| \frac{x_j(P)}{x_i(P)} \right|_v \right\}. \end{aligned}$$

■

We want a similar decomposition for the canonical height. To achieve this we introduce a more general theory of Weil functions.

Definition 3.1.6. An $M_{\mathbb{Q}}$-constant is a function $\gamma\colon M_{\mathbb{Q}} \to \mathbb{R}$ such that $\gamma(v) = 0$ for all but finitely many places.

Definition 3.1.7 ([35, p. 118]). Let D be a divisor on J. Consider a collection of functions $\lambda_{D,v}\colon J_D(\mathbb{Q}_v) \to \mathbb{R}$ for $v \in M_{\mathbb{Q}}$. These are called *Weil functions* on J associated to D if the following property holds: Let U be any Zariski open subset of J such that $U \cap \operatorname{supp}(D) \neq \varnothing$ and $D|_U = \operatorname{div}(g)$ for some rational function g on U. Then there exists a collection of functions $\alpha_v\colon \coprod U(\mathbb{Q}_v) \to \mathbb{R}$ that are locally $M_{\mathbb{Q}}$-bounded and continuous (see [35, p. 117] for a definition) such that

$$\lambda_{D,v}(P) = -\log|g(P)|_v + \alpha_v(P)$$

for all $v \in M_{\mathbb{Q}}$ and all $P \in U_D(\mathbb{Q}_v)$.

In particular, the naive local height functions $\lambda_{i,v}$ are Weil functions associated to Θ_i for $i = 1, 2, 3, 4$ ([35, p. 119]).

Theorem 3.1.8 ([22, Chapter 11, Theorem 1.1]). *For any divisor D on J, there exists a Weil function $\hat{\lambda}_{D,v}\colon J_D(\mathbb{Q}_v) \to \mathbb{R}$ for each $v \in M_{\mathbb{Q}}$ such that the following properties hold:*

(i) For two divisors D, D' on J, we have $\hat{\lambda}_{D+D',v} = \hat{\lambda}_{D,v} + \hat{\lambda}_{D',v} + \gamma_1(v)$ for all $v \in M_{\mathbb{Q}}$ wherever all of the functions are defined.

(ii) If $D = \operatorname{div}(f)$, then $\hat{\lambda}_{D,v}(P) = -\log|f(P)|_v + \gamma_2(v)$ for all $v \in M_{\mathbb{Q}}$ and all $P \in J_D(\mathbb{Q}_v)$.

(iii) For all $v \in M_{\mathbb{Q}}$ and $P \in J_{[2]^*D}(\mathbb{Q}_v)$, we have $\hat{\lambda}_{[2]^*D,v}(P) = \hat{\lambda}_{D,v}([2]P) + \gamma_3(v)$.

The γ_i are $M_{\mathbb{Q}}$-constants. With these properties the functions $\hat{\lambda}_{D,v}$ are defined uniquely up to an $M_{\mathbb{Q}}$-constant. We call these functions canonical local height functions on J associated with D. They furthermore have the following property:

(iv) Let $\varphi\colon A \to J$ be a homomorphism of abelian varieties defined over $\mathbb{Q}$. Then for all $v \in M_{\mathbb{Q}}$ and $P \in J_{\varphi^*D}(\mathbb{Q}_v)$, we have $\hat{\lambda}_{\varphi^*D,v}(P) = \hat{\lambda}_{D,v}(\varphi(P)) + \gamma_4(v)$, where γ_4 is an $M_{\mathbb{Q}}$-constant.

Proposition 3.1.9 ([22, Chapter 11, Proof of Theorem 1.1]). *Let D be a divisor on J satisfying $[2]^*D \sim 4D$. Let $\lambda_{D,v}\colon J_D(\mathbb{Q}_v) \to \mathbb{R}$ for $v \in M_{\mathbb{Q}}$ be a collection of Weil functions associated to D. Then the $\lambda_{D,v}$ are canonical local height functions associated to D if and only if they satisfy*

$$\lambda_{D,v}([2]P) = 4\lambda_{D,v}(P) - \log|\phi(P)|_v \tag{3.1}$$

for all $v \in M_{\mathbb{Q}}$ and all P such that $P, [2]P \in J_D(\mathbb{Q}_v)$, where ϕ is a rational function on J such that $[2]^*D = 4D + \operatorname{div}(\phi)$. Furthermore, each choice of such a function ϕ defines a unique collection of canonical local height functions satisfying (3.1).

In [35, Section 5], Uchida provides explicit canonical local heights on J associated to the divisors Θ_i for $i \in \{1, 2, 3, 4\}$. These can be obtained by adding an $M_{\mathbb{Q}}$-bounded continuous correction term to the naive height functions from Definition 3.1.4. For all $v \in M_{\mathbb{Q}}$ and $P \in J(\mathbb{Q}_v)$, we define

$$\Phi_v(P) := \frac{\max_j|\delta_j(x(P))|_v}{(\max_j|x_j(P)|_v)^4}.$$

Note that we define $\Phi_v(P)$ in terms of the normalization $x(P)$ of $\kappa(P)$, but because the δ_i are homogeneous polynomials of total degree 4, any other normalization gives the same result. When v is a prime q, we get

$$\Phi_q(P) = \max_j |\delta_j(x(P))|_q.$$

The collection of functions $\Phi_v(P)$ is $M_{\mathbb{Q}}$-bounded and continuous (see [35, Lemma 5.1]). Hence the following functions are well-defined Weil functions.

Definition 3.1.10. Let $v \in M_{\mathbb{Q}}$ and $i \in \{1,2,3,4\}$. We define the *canonical local real height* $\hat{\lambda}_{i,v}(P)\colon J_{\Theta_i}(\mathbb{Q}_v) \to \mathbb{R}$ by

$$\hat{\lambda}_{i,v}(P) = \lambda_{i,v}(P) + \sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \log \Phi_v([2^n]P).$$

Theorem 3.1.11 ([35, Theorem 5.3]). *Let $i \in \{1,2,3,4\}$, $v \in M_{\mathbb{Q}}$. For all $P \in J(\mathbb{Q}_v)$ such that $P, [2]P \notin \operatorname{supp}(\Theta_i)$, we have*

$$\hat{\lambda}_{i,v}([2]P) = 4\hat{\lambda}_{i,v}(P) - \log \left| \frac{\delta_i(x(P))}{x_i(P)^4} \right|_v.$$

In particular, $\hat{\lambda}_{i,v}$ is a canonical local height function associated with Θ_i.

Proof. The identity follows by simply working out the definition.

$$\begin{aligned}
&\hat{\lambda}_{i,v}([2]P) - 4\hat{\lambda}_{i,v}(P) \\
&\qquad = \lambda_{i,v}([2]P) + \sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \log \Phi_v([2^{n+1}]P) - 4\lambda_{i,v}(P) - \sum_{n=0}^{\infty} \frac{1}{4^n} \log \Phi_v([2^n]P) \\
&\qquad = \lambda_{i,v}([2]P) - 4\lambda_{i,v}(P) - \log \Phi_v(P) \\
&\qquad = \log \max_{1\le j\le 4} \left| \frac{x_j([2]P)}{x_i([2]P)} \right|_v - 4 \log \max_{1\le j\le 4} \left| \frac{x_j(P)}{x_i(P)} \right|_v - \log \frac{\max_{1\le j\le 4} |\delta_j(x(P))|_v}{\left(\max_{1\le j\le 4} |x_j(P)|_v\right)^4} \\
&\qquad = \log \max_{1\le j\le 4} \left| \frac{\delta_j(x(P))}{\delta_i(x(P))} \right|_v - \log \max_{1\le j\le 4} \left| \frac{\delta_j(x(P))}{x_i(P)^4} \right|_v \\
&\qquad = -\log \left| \frac{\delta_i(x(P))}{x_i(P)^4} \right|_v.
\end{aligned}$$

Because $\operatorname{div}\left(\frac{\delta_i(x(P))}{x_i(P)^4}\right) = [2]^*\Theta_i - 4\Theta_i$, Proposition 3.1.9 implies that $\hat{\lambda}_{i,v}$ is a canonical local height function associated with Θ_i. ∎

For any prime q, let us define the set

$$U_q(\mathbb{Q}_q) := \{P \in J(\mathbb{Q}_q) \mid \Phi_q(P) = 1\}.$$

Note that by definition of the normalization $x(P)$, we have $\max_i |x_i(P)|_q = 1$ for all primes q. Hence $P \in U_q(\mathbb{Q}_q)$ precisely when $\max_i |\delta_i(x(P))|_q = 1$.

Proposition 3.1.12 ([34, Theorem 4.1], [14, Lemma 1]). *Let q be a prime. Then*

(a) $U_q(\mathbb{Q}_q)$ is a subgroup of $J(\mathbb{Q}_q)$ of finite index, and $J_1(\mathbb{Q}_q) \subseteq U_q(\mathbb{Q}_q)$.

(b) If q is odd and $J/\mathbb{Q}$ has good reduction at q, then $U_q(\mathbb{Q}_q) = J(\mathbb{Q}_q)$.

Proposition 3.1.13. *Let $P \in U_q(\mathbb{Q}_q) \setminus \operatorname{supp}(\Theta_i)$ for some $i \in \{1,2,3,4\}$. Then*

$$\hat{\lambda}_{i,q}(P) = \lambda_{i,q}(P).$$

In particular, if q is odd and J has good reduction at q, this is true for all $P \in J_{\Theta_i}(\mathbb{Q}_q)$.

Proof. By Proposition 3.1.12(a), we know that $U_q(\mathbb{Q}_q)$ is a group. Hence if $P \in U_q(\mathbb{Q}_q)$, then also $[2^n]P \in U_q(\mathbb{Q}_q)$ for all $n \geq 0$. Hence $\Phi_q([2^n]P) = 1$ for all $n \geq 0$, so we conclude $\hat{\lambda}_{i,q}(P) = \lambda_{i,q}(P)$. The second claim follows directly from Proposition 3.1.12(b). ■

Recall that $\mathcal{C}$ has bad reduction at a prime q for only finitely many primes, and hence the same is true for its Jacobian J (Section 1.5.4). For each $P \in J_{\Theta_i}(\mathbb{Q}_q)$, we thus have $\hat{\lambda}_{i,q}(P) = \lambda_{i,q}(P)$ for all but finitely many primes, and hence $\hat{\lambda}_{i,q}(P) = 0$ for all but finitely many places.

Theorem 3.1.14 ([35, Theorem 5.7]). *Let $P \in J_{\Theta_i}(\mathbb{Q})$ for some $i \in \{1,2,3,4\}$. Then we have*

$$\hat{h}(P) = \sum_{v \in M_{\mathbb{Q}}} \hat{\lambda}_{i,v}(P).$$

We thus get a local decomposition of the canonical real height $\hat{h}$ this way. In [14, p. 341], Flynn and Smart define local height functions on all of $J(\mathbb{Q})$ as follows. For each point $P \in J(\mathbb{Q})$, let i be the smallest index such that $x_i(P) \neq 0$. They define the local height at P as $\hat{\lambda}_{i,v}(P)$ for that index i.

In [36, Section 7], Uchida notes that the division polynomial ϕ_2 defined in Section 1.5.5 satisfies $[2]^*\Theta = 4\Theta + \operatorname{div}(\phi_2)$. Hence there exists a canonical local height function $\hat{\lambda}_{\Theta,v}$ associated with Θ for each $v \in M_{\mathbb{Q}}$ that satisfies

$$\hat{\lambda}_{\Theta,v}([2]P) = 4\hat{\lambda}_{\Theta,v}(P) - \log|\phi_2(P)|_v.$$

We also have $[2]^*(\Theta_1) = 2\,[2]^*(\Theta) = 4\Theta_1 + \operatorname{div}(\phi_2^2)$, and hence $\hat{\lambda}_{\Theta_1,v} := 2\hat{\lambda}_{\Theta,v}$ is a canonical local height function associated with Θ_1. Because $\hat{\lambda}_{\Theta_1,v}$ and $\hat{\lambda}_{1,v}$ defined in Definition 3.1.10 are both canonical local height functions on J associated with Θ_1, they must differ by an $M_{\mathbb{Q}}$-constant $\gamma(v)$. In [18, Proposition 6.1], it is shown that we actually have

$$\hat{\lambda}_{\Theta_1,v} = \hat{\lambda}_{1,v} \tag{3.2}$$

on $J_{\Theta_1}(\mathbb{Q}_v)$ for each place v. In [36, Theorem 7.5], Uchida shows that these functions have the following properties on $J_{\Theta_1}(\mathbb{Q}_v)$:

Theorem 3.1.15 ([36, Theorem 7.5]). *Let v be a place of $\mathbb{Q}$ and $P, Q \in J_{\Theta_1}(\mathbb{Q}_v)$. Then*

(a) If $P+Q, P-Q \notin \operatorname{supp}(\Theta_1)$, we have

$$\begin{aligned}\hat{\lambda}_{\Theta_1,v}(P+Q) + \hat{\lambda}_{\Theta_1,v}(P-Q) &= 2\hat{\lambda}_{\Theta_1,v}(P) + 2\hat{\lambda}_{\Theta_1,v}(Q) \\ &\quad - 2\log|-\wp_{11}(P) + \wp_{11}(Q) - \wp_{12}(P)\wp_{22}(Q) + \wp_{22}(P)\wp_{12}(Q)|_v.\end{aligned}$$

(b) If $n \in \mathbb{Z} \setminus \{0\}$ and $[n]P \notin \operatorname{supp}(\Theta_1)$, we have

$$\hat{\lambda}_{\Theta_1,v}([n]P) = n^2\hat{\lambda}_{\Theta_1,v}(P) - 2\log|\phi_n(P)|_v,$$

where ϕ_n is the division polynomial defined in Section 1.5.5.

3.2 A p-adic height on the Jacobian of a genus 2 curve

Similarly to what we did for elliptic curves in Section 2.2, we can define a p-adic height function on a Jacobian by defining local heights at each place. Fix an odd prime p. We consider a smooth curve $\mathcal{C}$ of genus 2 over $\mathbb{Q}$ given by an equation of the form

$$\mathcal{C}\colon y^2 = f(x) = x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0 \tag{3.3}$$

with $f_i \in \mathbb{Z}$, such that $\mathcal{C}$ has good reduction at p. We introduce local height functions away from the divisor Θ at each place of $\mathbb{Q}$, as defined by Bianchi [4]. Again, the local p-adic height at ∞ is equal to 0. For the other places, we have to distinguish between p and primes away from p, as we did in Section 2.2.

3.2.1 Local p-adic heights at primes different from p

Let $q \neq p$ be a prime. Then we can define a local height at q by taking the height $\hat{\lambda}_{1,q}$ from the previous section, and replacing the real logarithm by the p-adic logarithm $\log_p$.

Definition 3.2.1. Let $q \neq p$ be a prime. Let $P \in U_q(\mathbb{Q}_q) \setminus \operatorname{supp}(\Theta)$. We define a local p-adic height $\hat{\lambda}_q\colon U_q(\mathbb{Q}_q) \setminus \operatorname{supp}(\Theta) \to \mathbb{Q}_p$ by

$$\hat{\lambda}_q(P) = -\log_p |x_1(P)|_q.$$

The local p-adic heights satisfy the following properties.

Theorem 3.2.2. *Let $q \neq p$ be a prime, and $P, Q \in U_q(\mathbb{Q}_q) \setminus \operatorname{supp}(\Theta)$. Then*

(a) If $P+Q, P-Q \notin \operatorname{supp}(\Theta)$, we have

$$\begin{aligned}\hat{\lambda}_q(P+Q) + \hat{\lambda}_q(P-Q) &= 2\hat{\lambda}_q(P) + 2\hat{\lambda}_q(Q) \\ &\quad - 2\log_p |-\wp_{11}(P) + \wp_{11}(Q) - \wp_{12}(P)\wp_{22}(Q) + \wp_{22}(P)\wp_{12}(Q)|_q.\end{aligned}$$

(b) If $n \in \mathbb{Z} \setminus \{0\}$ and $[n]P \notin \operatorname{supp}(\Theta)$, we have

$$\hat{\lambda}_q([n]P) = n^2\hat{\lambda}_q(P) - 2\log_p |\phi_n(P)|_q.$$

Proof. We note that $\hat{\lambda}_q$ looks very similar to the local real height $\hat{\lambda}_{1,q}$, because in Proposition 3.1.13 we saw that on $U_q(\mathbb{Q}_q) \setminus \operatorname{supp}(\Theta)$, we have $\hat{\lambda}_{1,q}(P) = \lambda_{1,q}(P) = -\log |x_1(P)|_q$. We also saw in (3.2) that $\hat{\lambda}_{\Theta_1,q} = \hat{\lambda}_{1,q}$. So we have $\hat{\lambda}_q(P) = \log_p(\exp(\hat{\lambda}_{\Theta_1,q}(P)))$ on $U_q(\mathbb{Q}_q) \setminus \operatorname{supp}(\Theta)$. We know that $\hat{\lambda}_{\Theta_1,q}$ satisfies the properties in Theorem 3.1.15, and by subsequently taking the exponential and p-adic logarithm on both sides of the equations there, we obtain the result. ■

3.2.2 Local p-adic height at p

To construct a local p-adic height at p we use a p-adic σ-function, as we did in Section 2.2.2 for elliptic curves. This function is defined in [5, Theorem 2.4]. It is based on the complex σ-function associated to the Jacobian of $\mathcal{C}$. The σ-function is an odd function in two variables that has a Taylor expansion around $(0,0)$ of the form $\sigma(z_1, z_2) \in z_1 + (z_1, z_2)^3\mathbb{Q}[[z_1, z_2]]$ (see [36, Proposition 2.1, Proposition 2.3]). We define

$$\sigma_p(\boldsymbol{T}) := \sigma(\mathcal{L}(\boldsymbol{T})),$$

where $\mathcal{L}$ is the strict formal logarithm on the formal group $\hat{J}$ corresponding to J as defined in Section 1.6.4. Because σ is odd and $\mathcal{L}$ is a formal group homomorphism from $\hat{J}$ to $\hat{\mathbb{G}}_a^2$, and we saw that the formal inverse on $\hat{J}$ is $\boldsymbol{\imath}_J(\boldsymbol{T}) = -\boldsymbol{T}$ (Section 1.6.3), we conclude that also σ_p is odd in the sense that it has only terms of total odd degree.

Theorem 3.2.3 ([5, Theorem 2.4]). *The series $\sigma_p(\boldsymbol{T})$ converges on $(p\mathbb{Z}_p)^2$.*

Recall that when $P \in J_1(\mathbb{Q}_p)$, we have $t_1(P), t_2(P) \in p\mathbb{Z}_p$, where $\boldsymbol{t}(P) = (t_1(P), t_2(P))$ is the image of P under the map ψ_J in (1.30) and the functions t_1 and t_2 are defined in Lemma 1.6.14. This implies that $\sigma_p(\boldsymbol{T})$ converges at $\boldsymbol{t}(P)$.

We have $\sigma_p(\boldsymbol{T}) \in T_1(1 + (T_1, T_2)\mathbb{Q}[[T]])$ (see [5, Appendix A]), so it vanishes for $(T_1, T_2) \in (p\mathbb{Z}_p)^2$ precisely when $T_1 = 0$.

Lemma 3.2.4. *Let $P \in J_1(\mathbb{Q}_p)$. Then $t_1(P) = 0$ if and only if $P \in \operatorname{supp}(\Theta)$.*

Proof. Recall from Lemma 1.6.14 that $t_1 = -X_{11}/X_{111}$. From the explicit description of the map (1.15) in [20, Remark 2], we see that $X_{11}(P)/X_{111}(P) = 0$ for all $P \in \operatorname{supp}(\Theta)$. When $P \notin \operatorname{supp}(\Theta)$, we have $t_1(P) = \wp_{11}(P)/\wp_{111}(P)$. Note that for $P \in J_1(\mathbb{Q}_p)$ we have $\widetilde{\kappa}(P) = [0 : 0 : 0 : 1]$, because the diagram (1.20) is commutative. In particular, because $\kappa(P) = [1 : \wp_{22}(P) : -\wp_{12}(P) : \wp_{11}(P)]$ (see (1.17)), this implies that $\wp_{11}(P) \neq 0$. Hence $t_1(P) \neq 0$. ∎

It follows that $\sigma_p(\boldsymbol{T})$ is nonzero on $J_1(\mathbb{Q}_p) \setminus \operatorname{supp}(\Theta)$. It has the following properties.

Proposition 3.2.5. *Let $P, Q \in J_1(\mathbb{Q}_p) \setminus \operatorname{supp}(\Theta)$. Then*

$$\frac{\sigma_p(\boldsymbol{t}(P+Q))\sigma_p(\boldsymbol{t}(P-Q))}{\sigma_p(\boldsymbol{t}(P))^2\sigma_p(\boldsymbol{t}(Q))^2} = -\wp_{11}(P) + \wp_{11}(Q) - \wp_{12}(P)\wp_{22}(Q) + \wp_{22}(P)\wp_{12}(Q),$$

and for all $n \neq 0$,

$$\frac{\sigma_p(\boldsymbol{t}([n]P))}{\sigma_p(\boldsymbol{t}(P))^{n^2}} = \phi_n(P). \tag{3.4}$$

Proof. This follows from [5, Theorem 2.4] using the facts that $\varphi_J(\phi_n)(\boldsymbol{t}(P)) = \phi_n(P)$ and $\wp_{ij}^T(\boldsymbol{t}(P)) = \wp_{ij}(P)$, which follows from (1.28). The second statement is only shown for $n > 0$, but for $n < 0$ we note that

$$\frac{\sigma_p(\boldsymbol{t}([n]P))}{\sigma_p(\boldsymbol{t}(P))^{n^2}} = \frac{-\sigma_p(\boldsymbol{t}([-n]P))}{\sigma_p(\boldsymbol{t}(P))^{(-n)^2}} = -\phi_{-n}(P) = \phi_n(P).$$

using (1.21) and the fact that σ_p is an odd function. ∎

We use σ_p to define a local p-adic height at p.

Definition 3.2.6. We define a local p-adic height $\hat{\lambda}_p \colon J_1(\mathbb{Q}_p) \setminus \operatorname{supp}(\Theta) \to \mathbb{Q}_p$ by

$$\hat{\lambda}_p(P) = -2\log_p(\sigma_p(\boldsymbol{t}(P))).$$

Proposition 3.2.7. *Let $\hat{\lambda}_p \colon J_1(\mathbb{Q}_p) \setminus \operatorname{supp}(\Theta) \to \mathbb{Q}_p$ be as defined in Definition 3.2.6.*

(a) For all $P \in J_1(\mathbb{Q}_p) \setminus \mathrm{supp}(\Theta)$ and for all $n \neq 0$ such that $[n]P \notin \mathrm{supp}(\Theta)$, we have

$$\hat{\lambda}_p([n]P) = n^2\hat{\lambda}_p(P) - 2\log_p(\phi_n(P)).$$

(b) For all $P, Q \in J_1(\mathbb{Q}_p) \setminus \mathrm{supp}(\Theta)$ such that also $P+Q, P-Q \notin \mathrm{supp}(\Theta)$, we have

$$\begin{aligned}\hat{\lambda}_p(P+Q) + \hat{\lambda}_p(P-Q) = 2\hat{\lambda}_p(P) + 2\hat{\lambda}_p(Q)\\ - 2\log_p(-\wp_{11}(P) + \wp_{11}(Q) - \wp_{12}(P)\wp_{22}(Q) + \wp_{22}(P)\wp_{12}(Q)).\end{aligned}$$

Proof. For (a), from Definition 3.2.6, we get

$$\begin{aligned}\hat{\lambda}_p([n]P) &= -2\log_p(\sigma_p(\boldsymbol{t}([n]P)))\\ &= -2\log_p(\sigma_p(\boldsymbol{t}(P))^{n^2}\phi_n(P)) && \text{(Proposition 3.2.5)}\\ &= -2n^2\log_p(\sigma_p(\boldsymbol{t}(P))) - 2\log_p(\phi_n(P))\\ &= n^2\hat{\lambda}_p(P) - 2\log_p(\phi_n(P)).\end{aligned}$$

For (b), we again use Proposition 3.2.5 to get

$$\begin{aligned}\hat{\lambda}_p(P+Q) + \hat{\lambda}_p(P-Q) &= -2\log_p(\sigma_p(\boldsymbol{t}(P+Q))\sigma_p(\boldsymbol{t}(P-Q)))\\ &= -2\log_p(\sigma_p(\boldsymbol{t}(P))^2\sigma_p(\boldsymbol{t}(Q))^2)\\ &\quad - 2\log_p(-\wp_{11}(P) + \wp_{11}(Q) - \wp_{12}(P)\wp_{22}(Q) + \wp_{22}(P)\wp_{12}(Q))\\ &= 2\hat{\lambda}_p(P) + 2\hat{\lambda}_p(Q)\\ &\quad - 2\log_p(-\wp_{11}(P) + \wp_{11}(Q) - \wp_{12}(P)\wp_{22}(Q) + \wp_{22}(P)\wp_{12}(Q)).\end{aligned}$$

■

3.2.3 A global p-adic height on J

Now we define a global p-adic height as the sum of the local contributions in Definition 3.2.1 and Definition 3.2.6. We first construct a suitable subgroup on which all local heights are defined. Let us define $U_q(\mathbb{Q}) := U_q(\mathbb{Q}_q) \cap J(\mathbb{Q})$. We furthermore write $J_U(\mathbb{Q}) := \cap_{q\,\mathrm{prime}} U_q(\mathbb{Q})$, and

$$J_p(\mathbb{Q}) := J_1^{(p)}(\mathbb{Q}) \cap J_U(\mathbb{Q}), \tag{3.5}$$

where $J_1^{(p)}(\mathbb{Q})$ is the kernel of reduction as defined in Section 1.5.4. These are all subgroups of $J(\mathbb{Q})$.

Lemma 3.2.8. *Let $P \in J_U(\mathbb{Q})$. Then $\hat{\lambda}_q(P) = 0$ for all but finitely many primes q.*

Proof. Because $x_1(P) \in \mathbb{Z} \setminus \{0\}$ we have that $|x_1(P)|_q = 1$ and hence $\hat{\lambda}_q(P) = 0$ for all but finitely many q. ■

Proposition 3.2.9. *$J_p(\mathbb{Q})$ is a subgroup of finite index of $J(\mathbb{Q})$.*

Proof. We know that $\mathcal{C}$ has bad reduction at only finitely many primes $q_1, \ldots, q_r$, and when $\mathcal{C}$ has good reduction at an odd prime q, then the same is true for J. So for odd $q \notin \{q_1, \ldots, q_r\}$, we have $U_q(\mathbb{Q}) = J(\mathbb{Q})$ by Proposition 3.1.12(b). Hence

$$J_p(\mathbb{Q}) = J_1^{(p)}(\mathbb{Q}) \cap U_2(\mathbb{Q}) \cap U_{q_1}(\mathbb{Q}) \cap \cdots \cap U_{q_r}(\mathbb{Q}).$$

From Proposition 3.1.12(a), we know that for each prime q, the subgroup $U_q(\mathbb{Q}_q)$ has finite index in $J(\mathbb{Q}_q)$. We also have that $J_1^{(p)}(\mathbb{Q})$ has finite index in $J(\mathbb{Q})$, because $J_1^{(p)}(\mathbb{Q})$ is the kernel of the reduction map $J(\mathbb{Q}) \to \widetilde{J}(\mathbb{F}_p)$ modulo p. We conclude that $J_p(\mathbb{Q})$ is a finite intersection of subgroups of finite index, which thus has finite index in $J(\mathbb{Q})$. ■

Lemma 3.2.10 ([18, Lemma 8.1]). *Let $P \in J(\mathbb{Q}) \setminus J_{\mathrm{tors}}$ be such that $P \in \mathrm{supp}(\Theta)$. Then one of $[2]P, [3]P, [4]P$ is in $J_\Theta(\mathbb{Q})$.*

Definition 3.2.11. We define a global height $\hat{h}_p \colon J(\mathbb{Q}) \to \mathbb{Q}_p$ as follows. For $P \notin J_{\mathrm{tors}}$, we set $\hat{h}_p(P) = 0$. For $P \in J(\mathbb{Q}) \setminus J_{\mathrm{tors}}$, let $m \in \mathbb{Z}_{>0}$ such that $[m]P \in J_p(\mathbb{Q}) \setminus \mathrm{supp}(\Theta)$ (which exists by Proposition 3.2.9 and Lemma 3.2.10). We define

$$\hat{h}_p(P) = \sum_{q \text{ prime}} \frac{1}{m^2} \hat{\lambda}_q([m]P), \tag{3.6}$$

with $\hat{\lambda}_q$ as defined in Definition 3.2.1 and Definition 3.2.6.

To see that this function is well-defined, first of all note that the sum in (3.6) is finite by Lemma 3.2.8. The following result shows that the definition is not dependent on the choice of m.

Proposition 3.2.12. *Let $P \in J(\mathbb{Q}) \setminus J_{\mathrm{tors}}$, and let m and n be positive integers such that $[m]P, [n]P \in J_p(\mathbb{Q}) \setminus \mathrm{supp}(\Theta)$. Then*

$$\sum_{q \text{ prime}} \frac{1}{m^2} \hat{\lambda}_q([m]P) = \sum_{q \text{ prime}} \frac{1}{n^2} \hat{\lambda}_q([n]P).$$

Proof. Let $l \in \mathbb{Z}_{>0}$ be such that $[mnl]P \in J_p(\mathbb{Q}) \setminus \mathrm{supp}(\Theta)$. For each prime $q \neq p$, Theorem 3.2.2 implies that

$$\begin{aligned} \hat{\lambda}_q([mnl]P) &= (nl)^2 \hat{\lambda}_q([m]P) - 2 \log_p |\phi_{nl}([m]P)|_q \\ &= (ml)^2 \hat{\lambda}_q([n]P) - 2 \log_p |\phi_{ml}([n]P)|_q. \end{aligned}$$

We use this to deduce

$$\frac{1}{m^2} \hat{\lambda}_q([m]P) - \frac{1}{n^2} \hat{\lambda}_q([n]P) = \frac{2}{(mnl)^2} \left(\log_p |\phi_{nl}([m]P)|_q - \log_p |\phi_{ml}([n]P)|_q \right)$$

At p, we get a similar equality from Proposition 3.2.7:

$$\begin{aligned} \hat{\lambda}_p([mnl]P) &= (nl)^2 \hat{\lambda}_p([m]P) - 2 \log_p(\phi_{nl}([m]P)) \\ &= (ml)^2 \hat{\lambda}_p([n]P) - 2 \log_p(\phi_{ml}([n]P)), \end{aligned}$$

which implies

$$\frac{1}{m^2} \hat{\lambda}_p([m]P) - \frac{1}{n^2} \hat{\lambda}_p([n]P) = \frac{2}{(mnl)^2} \left(\log_p(\phi_{ln}([m]P)) - \log_p(\phi_{lm}([n]P)) \right).$$

The product formula in Lemma 1.1.17 then implies that

$$\sum_{q \text{ prime}} \frac{1}{m^2} \hat{\lambda}_q([m]P) - \sum_{q \text{ prime}} \frac{1}{n^2} \hat{\lambda}_q([n]P) = 0.$$

■

We can give a more explicit description of $\hat{h}_p$ using the explicit descriptions of the local p-adic heights.

Proposition 3.2.13. *Let $P \in J(\mathbb{Q}) \setminus J_{\text{tors}}$ and let $m \in \mathbb{Z}_{>0}$ such that $[m]P \in J_p(\mathbb{Q}) \setminus \text{supp}(\Theta)$. Then*

$$\hat{h}_p(P) = -\frac{1}{m^2} \log_p \left(\frac{\sigma_p^2(\boldsymbol{t}([m]P))}{x_1([m]P)} \right).$$

Proof. We have

$$\begin{aligned}
\hat{h}_p(P) &= \sum_{q \text{ prime}} \frac{1}{m^2} \hat{\lambda}_q([m]P) \\
&= -\frac{1}{m^2} \left[2 \log_p(\sigma_p(\boldsymbol{t}([m]P))) + \sum_{q \neq p} \log_p |x_1([m]P)|_q \right] && \text{(Definition 3.2.6, 3.2.1)} \\
&= -\frac{1}{m^2} \log_p \left(\frac{\sigma_p^2(\boldsymbol{t}([m]P))}{x_1([m]P)} \right). && \text{(Lemma 1.1.17)}
\end{aligned}$$

■

Proposition 3.2.14. *The p-adic height $\hat{h}_p$ is a quadratic function, that is, for all $P \in J(\mathbb{Q})$ and $n \in \mathbb{Z}$, we have*

$$\hat{h}_p([n]P) = n^2 \hat{h}(P).$$

Proof. If P is a torsion point, the statement is clear for all $n \in \mathbb{Z}$. Now assume $P \notin J_{\text{tors}}$ and $n \in \mathbb{Z}$. For $n = 0$ the result is immediate. Let $n \neq 0$, and let $m \in \mathbb{Z}_{>0}$ be such that $[mn]P \in J_p(\mathbb{Q}) \setminus \text{supp}(\Theta)$. Then by definition of $\hat{h}_p$ we get

$$\hat{h}_p([n]P) = \sum_{q \text{ prime}} \frac{1}{m^2} \hat{\lambda}_q([mn]P) = n^2 \sum_{q \text{ prime}} \frac{1}{(mn)^2} \hat{\lambda}_q([mn]P) = n^2 \hat{h}_p(P).$$

■

The height $\hat{h}_p$ actually also satisfies the parallelogram law, and thus is a quadratic form. We do not show this here, but in the next section (Section 3.3), we define a height h_p in a different way and show that it is a quadratic form in Theorem 3.3.19. In Theorem 3.3.25 we show that $\hat{h}_p$ is equal to h_p, which then implies that $\hat{h}_p$ is a quadratic from.

3.3 A naive p-adic height on the Jacobian of a genus 2 curve

We consider the same setting as in the previous section, with an odd prime p and a smooth curve $\mathcal{C}$ of genus 2 over $\mathbb{Q}$ defined by (3.3) with integer coefficients and good reduction at p. In this section, our goal is to construct a quadratic p-adic height in a way that is different from the method we saw in Section 3.2, namely with a naive height and a construction analogous to the construction of Perrin-Riou in Section 2.3.

We start by considering points in the group $J_p(\mathbb{Q})$ as defined in (3.5). Note that when $P \in J_1^{(p)}(\mathbb{Q})$, we have $\widetilde{P} = \mathcal{O}$ modulo p, and then also $\widetilde{\kappa}(P) = [0:0:0:1]$ because the diagram (1.20) is commutative. In particular, we have that $x_4(P)$ is not divisible by p and that $x_4(P) \neq 0$. We define a naive p-adic height $H_p \colon J_p(\mathbb{Q}) \to \mathbb{Q}_p$ as follows:

$$H_p(P) = \log_p(x_4(P)).$$

Note the similarity between this function and the naive height function H_2 on elliptic curves in (2.18). For $P \in E_p(\mathbb{Q}) \setminus \{\mathcal{O}\}$, if we write $\kappa(P) = [x_1(P) : x_2(P)]$ with $x_1(P), x_2(P) \in \mathbb{Z}$ such that $\gcd(x_1(P), x_2(P)) = 1$ (with κ as in (1.6)), we have $H_2(P) = \log_p(x_1(P))$. Both H_2 and H_p are defined at $P \in E_p(\mathbb{Q}) \setminus \{\mathcal{O}\}$ and $P \in J_p(\mathbb{Q})$, respectively, as the p-adic logarithm of the coordinate of $\kappa(P)$ with the lowest p-adic valuation.

The goal of this section is to prove the following result, which is an analogue of Theorem 2.3.1:

Theorem 3.3.1. *Let $P \in J_p(\mathbb{Q})$. Then the following limit exists:*

$$h_p(P) = \lim_{n\to\infty} \frac{1}{p^{2n}} H_p([p^n]P). \tag{3.7}$$

We show the existence of the limit (3.7) in Section 3.3.1. In Section 3.3.2 we show that the resulting function h_p satisfies the parallelogram law. In Section 3.3.3 we show how the definition of h_p can be extended to obtain a quadratic form on all of $J(\mathbb{Q})$. Finally, in Section 3.3.4, we compare h_p to the height $\hat{h}_p$ from Section 3.2.3, and we show that they are actually the same.

3.3.1 Existence of the limit defining h_p

Let us start by proving that the limit (3.7) exists. We do this by showing that the sequence $\frac{1}{p^{2n}} H_p([p^n]P)$ is a Cauchy sequence in the complete metric space $\mathbb{Q}_p$. Using Lemma 1.1.6, we can instead show that as n approaches infinity, we have

$$\frac{1}{p^{2(n+1)}} H_p([p^{n+1}]P) - \frac{1}{p^{2n}} H_p([p^n]P) \xrightarrow{n\to\infty} 0. \tag{3.8}$$

Let us start by looking at the expression $H_p([p]P) - p^2 H_p(P)$ for $P \in J_p(\mathbb{Q})$. To evaluate H_p at the point $[p]P$, we need a description of its image on the Kummer surface. We use the multiplication formulas defined in Theorem 1.5.4. The functions μ_m evaluated at P give projective coordinates for $\kappa([m]P)$, but the theorem does not tell us which specific normalization for $\kappa([m]P)$ we obtain. Uchida has the following result about the normalization when $P = \mathcal{O}$.

Lemma 3.3.2 ([35, Lemma 3.9]). *We have $\mu_m(0,0,0,1) = (0,0,0,1)$ for all $m \geq 0$.*

We want to determine the normalization of $\kappa([m]P)$ we obtain from the functions $\mu_{m,i}$ also at other points P. Specifically, we show that for points P in the subgroup $J_p(\mathbb{Q})$, we have

$\gcd(\mu_{m,1}(x(P)), \mu_{m,2}(x(P)), \mu_{m,3}(x(P)), \mu_{m,4}(x(P))) = 1$. Note that for $m = 2$, this is true by definition of $J_p(\mathbb{Q})$. Namely, if $P \in J_p(\mathbb{Q})$, then $P \in U_q(\mathbb{Q})$ for all primes q. Hence $\Phi_q(P) = \max_j |\delta_j(x(P))|_q = 1$ for all q, which implies that $\gcd(\delta_1(x(P)), \ldots, \delta_4(x(P))) = 1$. To show that the same is satisfied for all other μ_m, we use some theory about real local height functions on the Jacobian, which we already saw in Section 3.1.1. Recall that we presented Uchida's naive and canonical local real height functions in Definition 3.1.4 and Definition 3.1.10, respectively. We make use of a property of these canonical local height functions that was proven by Uchida in [35, Theorem 5.3]. We reproduce the result here and fill in some details in Uchida's proof for the case $i = 4$. This case is of interest in the current setting because we consider points $P \in J_p(\mathbb{Q}) \subseteq J_1^{(p)}(\mathbb{Q})$, and for these points we have $\widetilde{\kappa}(P) = [0 : 0 : 0 : 1]$, which implies that $x_4(P) \neq 0$. We thus have $J_1^{(p)}(\mathbb{Q}) \subseteq J_{\Theta_4}(\mathbb{Q})$.

Theorem 3.3.3 ([35, Theorem 5.3]). *Let q be a prime. Let $\hat{\lambda}_{4,q}$ be the canonical local real height defined in Definition 3.1.10. For any $m \in \mathbb{Z}_{>0}$ and $P \in J(\mathbb{Q}_q)$ with $P, [m]P \notin \operatorname{supp}(\Theta_4)$, we have*

$$\hat{\lambda}_{4,q}([m]P) - m^2\hat{\lambda}_{4,q}(P) = -\log\left|\frac{\mu_{m,4}(x(P))}{x_4(P)^{m^2}}\right|_q.$$

Proof. For $m = 1$ the statement is trivial. For $m = 2$, we showed the statement in Theorem 3.1.11. In that theorem, we also saw that $\hat{\lambda}_{4,q}$ is a canonical local height function associated with the divisor Θ_4, and hence it satisfies the properties in Theorem 3.1.8. We note that

$$\operatorname{div}\left(\frac{\mu_{m,4}(x(P))}{x_4(P)^{m^2}}\right) = [m]^*\Theta_4 - m^2\Theta_4.$$

We can then use the properties in Theorem 3.1.8 to find

$$\begin{aligned}
\hat{\lambda}_{4,q}([m]P) - m^2\hat{\lambda}_{4,q}(P) &= \hat{\lambda}_{[m]^*\Theta_4,q}(P) - \hat{\lambda}_{m^2\Theta_4,q}(P) + \gamma_1 && \text{(property (iv), (i))} \\
&= \hat{\lambda}_{([m]^*\Theta_4 - m^2\Theta_4),q}(P) + \gamma_2 && \text{(property (i))} \\
&= -\log\left|\frac{\mu_{m,4}(x(P))}{x_4(P)^{m^2}}\right|_q + \gamma_3, && \text{(property (ii))} \qquad (3.9)
\end{aligned}$$

where the γ_i are constants. We thus need

$$\gamma_3 = \hat{\lambda}_{4,q}([m]P) - m^2\hat{\lambda}_{4,q}(P) + \log\left|\frac{\mu_{m,4}(x(P))}{x_4(P)^{m^2}}\right|_q \qquad (3.10)$$

for all P such that $P, [m]P \in J_{\Theta_4}(\mathbb{Q}_q)$, so in particular for $P = \mathcal{O}$ with $\kappa(\mathcal{O}) = [0 : 0 : 0 : 1]$. But we know that $\mu_m(0, 0, 0, 1) = (0, 0, 0, 1)$ by Lemma 3.3.2, and hence also $\Phi_q(\mathcal{O}) = 1$. This shows that $\hat{\lambda}_{4,q}(\mathcal{O}) = 0$, and thus that all terms on the right-hand side of (3.10) evaluate to 0 at $\mathcal{O}$, which implies $\gamma_3 = 0$ independently of P. Then (3.9) gives the desired result. ∎

Theorem 3.3.4. *Let $P \in J_p(\mathbb{Q})$. Then $x_i([m]P) = \pm\mu_{m,i}(x(P))$ for all $1 \leq i \leq 4$ and all $m \geq 1$.*

Proof. Consider any prime q and any $m \in \mathbb{Z}_{>0}$. Recall that $J_1^{(p)}(Q) \subseteq J_{\Theta_4}(\mathbb{Q})$, and thus $P, [m]P \in J_{\Theta_4}(\mathbb{Q})$. We apply Theorem 3.3.3 to obtain

$$\begin{aligned}
\hat{\lambda}_{4,q}([m]P) - m^2\hat{\lambda}_{4,q}(P) &= -\log\left|\frac{\mu_{m,4}(x(P))}{x_4(P)^{m^2}}\right|_q \\
&= -\log|\mu_{m,4}(x(P))|_q + m^2\log|x_4(P)|_q. \qquad (3.11)
\end{aligned}$$

On the other hand, because $P, [m]P \in J_U(\mathbb{Q})$, we have from Proposition 3.1.13 that

$$\begin{aligned}\hat{\lambda}_{4,q}([m]P) - m^2\hat{\lambda}_{4,q}(P) &= \lambda_{4,q}([m]P) - m^2\lambda_{4,q}(P) \\ &= -\log|x_4([m]P)|_q + m^2\log|x_4(P)|_q\,. \end{aligned} \tag{3.12}$$

Equating (3.11) and (3.12) then gives

$$-\log|x_4([m]P)|_q = -\log|\mu_{m,4}(x(P))|_q\,.$$

We thus know that $x_4([m]P), \mu_{m,4}(x(P)) \in \mathbb{Z}$ such that $|x_4([m]P)|_q = |\mu_{m,4}(x(P))|_q$ for all primes q. This implies that $x_4([m]P) = \pm\mu_{m,4}(x(P))$. Because

$$\begin{aligned}\kappa([m]P) &= [x_1([m]P) : x_2([m]P) : x_3([m]P) : x_4([m]P)] \\ &= [\mu_{m,1}(x(P)) : \mu_{m,2}(x(P)) : \mu_{m,3}(x(P)) : \mu_{m,4}(x(P))],\end{aligned}$$

this implies that $x_i([m]P) = \pm\mu_{m,i}(x(P))$ for all $1 \le i \le 4$. ■

In particular, we deduce that $\gcd(\mu_{m,1}(x(P)), \mu_{m,2}(x(P)), \mu_{m,3}(x(P)), \mu_{m,4}(x(P))) = 1$ for all $m \ge 0$.

Corollary 3.3.5. *Let $P \in J_p(\mathbb{Q})$ and $m \ge 1$. Then*

$$H_p([m]P) - m^2 H_p(P) = \log_p\left(\frac{\mu_{m,4}(x(P))}{x_4(P)^{m^2}}\right). \tag{3.13}$$

We now need to rewrite the argument of the logarithm in (3.13). If $P \in J_1^{(p)}(\mathbb{Q})$, we know that $x_4(P) \neq 0$. Note that we can view

$$\frac{\mu_{m,4}(x_1,x_2,x_3,x_4)}{x_4^{m^2}} = \mu_{m,4}\left(\frac{x_1}{x_4}, \frac{x_2}{x_4}, \frac{x_3}{x_4}, 1\right)$$

as a polynomial of total degree at most m^2 in $\mathbb{Z}\left[\frac{x_1}{x_4}, \frac{x_2}{x_4}, \frac{x_3}{x_4}\right]$. Because $x_4(P) \neq 0$, we get from (1.18) that

$$\frac{x_1(P)}{x_4(P)} = \frac{1}{\wp_{11}}(P),\ \frac{x_2(P)}{x_4(P)} = \frac{\wp_{22}}{\wp_{11}}(P) \text{ and } \frac{x_3(P)}{x_4(P)} = -\frac{\wp_{12}}{\wp_{11}}(P). \tag{3.14}$$

Hence we have

$$\frac{\mu_{m,4}(x(P))}{x_4(P)^{m^2}} = \mu_{m,4}\left(\frac{1}{\wp_{11}}(P), \frac{\wp_{22}}{\wp_{11}}(P), -\frac{\wp_{12}}{\wp_{11}}(P), 1\right). \tag{3.15}$$

We now use the 2-parameter formal group associated to J, which we defined in Section 1.6.3. Recall that in (1.29), we have expansions of the coordinate functions $\wp_{ij}$ defining the map to the Kummer surface in the parameters t_1 and t_2. Using these, we find

$$\begin{aligned}\frac{1}{\wp_{11}} &= t_1^2 + (\text{terms of total degree} \ge 3) \\ \frac{\wp_{22}}{\wp_{11}} &= 2t_1t_2 + (\text{terms of total degree} \ge 3) \\ -\frac{\wp_{12}}{\wp_{11}} &= t_2^2 + (\text{terms of total degree} \ge 3)\end{aligned} \tag{3.16}$$

which are all in $\mathbb{Z}[[t_1, t_2]]$. To find an expansion for $\mu_{m,4}\left(\frac{1}{\wp_{11}}, \frac{\wp_{22}}{\wp_{11}}, -\frac{\wp_{12}}{\wp_{11}}, 1\right)$ in t_1 and t_2, we first look more closely at the coefficients of the polynomial $\mu_{m,4}$. We prove a few properties, using the equations for δ given in [13, Appendix C] and the equations for the biquadratic formulas B_{ij} from [12]. We do not reproduce the equations here, but we highlight some properties.

Properties 3.3.6. *The polynomials $\delta_i(k_1, k_2, k_3, k_4)$ have the following property:*

(a) The coefficient of k_4^4 in δ_i is 0 for $i = 1, 2, 3$, and 1 for $i = 4$.

(b) The terms $k_4^3 k_1$, $k_4^3 k_2$, $k_4^3 k_3$ have coefficient 0 in δ_4.

The biquadratic polynomials $B_{ii}((k_1, k_2, k_3, k_4), (l_1, l_2, l_3, l_4))$ have the following properties:

(c) In B_{ii} for $i = 1, 2, 3$, the coefficients of the terms of the form $k_4^2 l_j l_4$ and $k_j k_4 l_4^2$ for $j = 1, 2, 3, 4$ are 0.

(d) In B_{44}, the coefficients of terms of the form $k_4^2 l_i l_j$ and $k_i k_j l_4^2$ for $i, j \in \{1, 2, 3, 4\}$, are 0, unless $i = j = 4$, in which case the coefficient is 1.

Lemma 3.3.7. *The coefficient of $k_4^{m^2}$ in the homogeneous polynomial $\mu_{m,i}(k_1, k_2, k_3, k_4)$ is equal to 0 for $i = 1, 2, 3$, and 1 for $i = 4$.*

Proof. Let us show this by induction on m using the inductive definition of μ_m in Theorem 1.5.4. It is clear from the definition that the statement is true for $\mu_0 = (0, 0, 0, 1)$ and $\mu_1 = (k_1, k_2, k_3, k_4)$.

We now show that if the statement is true for μ_l with $l \geq 1$, then it is also true for μ_{2l}. Namely, by definition $\mu_{2l,i}(k) = \delta_i(\mu_l(k))$. Because the coefficient of $k_4^{l^2}$ is 0 in $\mu_{l,1}$, $\mu_{l,2}$ and $\mu_{l,3}$ by the induction hypothesis, the only term in $\delta_i(\mu_l)$ that can contribute to the $k_4^{(2l)^2}$-term in $\delta_i(\mu_l(k))$ is the $\mu_{l,4}^4$-term. However, we see from Properties 3.3.6(a) that this term vanishes in $\delta_i(\mu_l)$ for $i = 1, 2, 3$. In $\delta_4(\mu_l)$, its coefficient is 1, and the coefficient of $k_4^{l^2}$ in $\mu_{l,4}$ is also 1 by the induction hypothesis. This shows the statement for $m = 2l$.

Now we show that if the statement is true for μ_l and μ_{l+1} with $l \geq 1$, then it is also true for μ_{2l+1}. Namely, by definition $\mu_{2l+1,i}(k)\, k_i = B_{ii}(\mu_{l+1}(k), \mu_l(k))$ for $i = 1, 2, 3, 4$. Hence the coefficient of $k_4^{(2l+1)^2}$ in $\mu_{2l+1,i}(k)$ corresponds to the coefficient of $k_i k_4^{(2l+1)^2}$ in $B_{ii}(\mu_{l+1}(k), \mu_l(k))$. By the induction hypothesis, we know that $\mu_{l+1,4}$ and $\mu_{l,4}$ are the only coordinates that have a nonzero coefficient of $k_4^{(l+1)^2}$ and $k_4^{l^2}$, respectively. Therefore, the only terms in $B_{ii}(\mu_{l+1}, \mu_l)$ that could contribute to the $k_i k_4^{(2l+1)^2}$-term in $B_{ii}(\mu_{l+1}(k), \mu_l(k))$ are terms of the form $\mu_{l+1,4}^2 \mu_{l,j} \mu_{l,4}$ and $\mu_{l+1,j} \mu_{l+1,4} \mu_{l,4}^2$ for some $j \in \{1, 2, 3, 4\}$. However, Properties 3.3.6(c) shows that for $i = 1, 2, 3$, all these terms have coefficient 0. For $i = 4$, Properties 3.3.6(d) tells us that the coefficient of $\mu_{l+1,4}^2 \mu_{l,4}^2$ in $B_{44}(\mu_{l+1}(k), \mu_l)$ is 1. By the induction hypothesis, the coefficient of $k_4^{(l+1)^2}$ in $\mu_{l+1,4}$ and the coefficient of $k_4^{l^2}$ in $\mu_{l,4}$ are 1. These facts show that the coefficient of $k_4^{(2l+1)^2}$ in $\mu_{2l+1,i}(k)$ is equal to 0 for $i = 1, 2, 3$ and equal to 1 for $i = 4$. ∎

Lemma 3.3.8. *Let $m \geq 1$. The coefficient of $k_4^{m^2-1} k_i$ in $\mu_{m,4}(k_1, k_2, k_3, k_4)$ is equal to 0 for $i = 1, 2, 3$.*

Proof. We again use induction on m. Note that the statement is true for $m = 1$ because $\mu_{1,4} = k_4$.

Let us assume the statement is true for $m = l$, and show it is true for $m = 2l$. Let us fix $i \in \{1, 2, 3\}$. From Lemma 3.3.7, we deduce that the only terms in $\delta_4(\mu_l)$ that can contribute to the $k_4^{m^2-1} k_i$-term in $\delta_4(\mu_l(k)) = \mu_{2l,4}(k)$ are of the form $\mu_{l,4}^3 \mu_{l,j}$ for some $j \in \{1, 2, 3, 4\}$.

Properties 3.3.6(b) tells us that for $j = 1, 2, 3$, these terms have coefficient 0. Hence they cannot contribute, and the only term left is $\mu_{l,4}^4$. However, the coefficient of $k_4^{l^2-1}k_i$ is equal to 0 in $\mu_{l,4}(k)$ by the induction hypothesis. Hence this term also cannot contribute. We conclude that the coefficient of $k_4^{(2l)^2-1}k_i$ in $\mu_{2l,4}(k)$ is 0.

Now we assume the statement is true for $m = l$ and $m = l+1$, and show it is true for $m = 2l+1$. Let us again fix $i \in \{1, 2, 3\}$. By definition, the coefficient of $k_4^{(2l+1)^2-1}k_i$ in $\mu_{2l+1,4}(k)$ corresponds to the coefficient of $k_4^{(2l+1)^2}k_i$ in $B_{44}(\mu_{l+1}(k), \mu_l(k))$. It follows from Lemma 3.3.7 that the only terms in $B_{44}(\mu_{l+1}, \mu_l)$ that can contribute to the $k_4^{(2l+1)^2}k_i$-term in $B_{44}(\mu_{l+1}(k), \mu_l(k))$ are the terms of the form $\mu_{l+1,4}^2\mu_{l,j}\mu_{l,4}$ and $\mu_{l+1,j}\mu_{l+1,4}\mu_{l,4}^2$. However, from Properties 3.3.6(d) it follows that for $j = 1, 2, 3$ these terms have coefficient 0. For $j = 4$ we get the term $\mu_{l+1,4}^2\mu_{l,4}^2$, but from the induction hypothesis we know that the coefficient of $k_4^{l^2-1}k_i$ in $\mu_{l,4}(k)$ and the coefficient of $k_4^{(l+1)^2-1}k_i$ in $\mu_{l+1,4}(k)$ are 0. Then this term can also not contribute to the $k_4^{(2l+1)^2}k_i$-term in $B_{44}(\mu_{l+1}(k), \mu_l(k))$, so the latter must have coefficient 0. This shows that the coefficient of $k_4^{(2l+1)^2-1}k_i$ in $\mu_{2l+1,4}(k)$ is 0. ■

We can use these facts about the polynomial $\mu_{m,4}$ to say something about the (t_1, t_2)-expansion of $\mu_{m,4}\left(\frac{1}{\wp_{11}}, \frac{\wp_{22}}{\wp_{11}}, -\frac{\wp_{12}}{\wp_{11}}, 1\right)$.

Proposition 3.3.9. *Let $m \geq 1$. Then $\mu_{m,4}\left(\frac{1}{\wp_{11}}, \frac{\wp_{22}}{\wp_{11}}, -\frac{\wp_{12}}{\wp_{11}}, 1\right)$ has an expansion in t_1 and t_2 of the form*

$$u_m(t_1, t_2) \in 1 + (t_1, t_2)^4\mathbb{Z}_p[[t_1, t_2]].$$

Proof. Recall that $\mu_{m,4}$ is a homogeneous polynomial of degree m^2. Let us write

$$\mu_{m,4}(k_1, k_2, k_3, k_4) = \sum_{i+j+l+w=m^2} a_{ijlw}k_1^i k_2^j k_3^l k_4^w.$$

Then Lemma 3.3.7 says that $a_{0,0,0,m^2} = 1$, and Lemma 3.3.8 says that $a_{1,0,0,m^2-1} = a_{0,1,0,m^2-1} = a_{0,0,1,m^2-1} = 0$. We thus get

$$\begin{aligned}\mu_{m,4}\left(\frac{1}{\wp_{11}}, \frac{\wp_{22}}{\wp_{11}}, -\frac{\wp_{12}}{\wp_{11}}, 1\right) &= \sum_{i+j+l+w=m^2} a_{ijlw}\left(\frac{1}{\wp_{11}}\right)^i\left(\frac{\wp_{22}}{\wp_{11}}\right)^j\left(-\frac{\wp_{12}}{\wp_{11}}\right)^l \\ &= 1 + \sum_{\substack{i+j+l+w=m^2 \\ i+j+l\geq 2}} a_{ijlw}\left(\frac{1}{\wp_{11}}\right)^i\left(\frac{\wp_{22}}{\wp_{11}}\right)^j\left(-\frac{\wp_{12}}{\wp_{11}}\right)^l. \qquad (3.17)\end{aligned}$$

From the expansions in (3.16) we note that $\frac{1}{\wp_{11}}, \frac{\wp_{22}}{\wp_{11}}, -\frac{\wp_{12}}{\wp_{11}} \in (t_1, t_2)^2\mathbb{Z}[[t_1, t_2]]$. In the last sum in (3.17), each term satisfies $i + j + l \geq 2$, and hence we conclude that this sum is contained in $(t_1, t_2)^4\mathbb{Z}[[t_1, t_2]]$. This implies the result. ■

For $P \in J_1^{(p)}(\mathbb{Q})$, we then get from (3.15) that

$$u_m(t_1(P), t_2(P)) = \frac{\mu_{m,4}(x(P))}{x_4(P)^{m^2}}. \qquad (3.18)$$

We have the following convergence results, which are very similar to Corollary 2.3.3 and Corollary 2.3.4 for elliptic curves.

Corollary 3.3.10. *Let $P \in J_1(\mathbb{Q}_p)$. Let $g(T_1, T_2) \in 1 + (T_1, T_2)^k \mathbb{Q}_p[[T_1, T_2]]$ for some integer $k > 0$, such that g converges on some neighborhood of $(0, 0)$. Then for large enough $n \in \mathbb{Z}_{\geq 0}$, $g(t_1([p^n]P), t_2([p^n]P))$ converges, and for $m \in \mathbb{Z}_{<k}$ we have*

$$\lim_{n\to\infty} \frac{1}{p^{mn}} \log_p(g(t_1([p^n]P), t_2([p^n]P))) = 0.$$

Proof. Because $P \in J_1(\mathbb{Q}_p)$, we have $\mathrm{ord}_p(t_1([p^n]P)), \mathrm{ord}_p(t_2([p^n]P)) \geq n$ for all $n \geq 0$ (Corollary 1.6.18). The result then follows from Lemma 2.3.2. ■

Corollary 3.3.11. *Let $P \in J_1(\mathbb{Q}_p)$. Let $g(T_1, T_2) \in 1 + (T_1, T_2)^3 \mathbb{Z}_p[[T_1, T_2]]$. Then*

$$\lim_{n\to\infty} \frac{1}{p^{2n}} \log_p(g(t_1([p^n]P), t_2([p^n]P))) = 0.$$

Proof. The series $g(T_1, T_2)$ converges for $T_1, T_2 \in p\mathbb{Z}_p$. The result follows from Corollary 3.3.10. ■

We use this to show the existence of the limit (3.7).

Proof of Theorem 3.3.1. Recall that we can prove the theorem by showing the limit in (3.8). Note that $[p^n]P \in J_p(\mathbb{Q})$ for all $n \geq 0$. We have

$$\begin{aligned}
&\lim_{n\to\infty} \left(\frac{1}{p^{2(n+1)}} H_p([p^{(n+1)}]P) - \frac{1}{p^{2n}} H_p([p^n]P) \right) \\
&\qquad = \lim_{n\to\infty} \frac{1}{p^{2(n+1)}} \left(H_p([p]([p^n]P)) - p^2 H_p([p^n]P) \right) \\
&\qquad = \frac{1}{p^2} \lim_{n\to\infty} \frac{1}{p^{2n}} \log_p \left(\frac{\mu_{p,4}(x([p^n]P))}{x_4([p^n]P)^{p^2}} \right) && \text{(Corollary 3.3.5)} \\
&\qquad = \frac{1}{p^2} \lim_{n\to\infty} \frac{1}{p^{2n}} \log_p \left(u_p(t_1([p^n]P), t_2([p^n]P)) \right) && \text{(using (3.18))} \\
&\qquad = 0. && \text{(Proposition 3.3.9, Corollary 3.3.11)}
\end{aligned}$$

■

3.3.2 Quadraticity of h_p

Next, our goal is to prove that the function h_p satisfies the parallelogram law on $J_p(\mathbb{Q})$. Explicitly we want to show the following theorem.

Theorem 3.3.12. *Let $P, Q \in J_p(\mathbb{Q})$. Then*

$$h_p(P + Q) + h_p(P - Q) = 2h_p(P) + 2h_p(Q).$$

We first note that by definition, for $P, Q \in J_p(\mathbb{Q})$ we have

$$H_p(P + Q) + H_p(P - Q) = \log_p(x_4(P + Q)x_4(P - Q)). \tag{3.19}$$

Our goal is to rewrite the right-hand side in such a way that it depends on the coordinates of P and Q instead. As in the previous section, we use theory on the canonical local real height

function by Uchida which were introduced in Section 3.1.1. Again, we only need to consider the local height away from Θ_4, because we know that $J_p(\mathbb{Q}) \subseteq J_{\Theta_4}(\mathbb{Q})$. We use the following result by Uchida. Uchida states this result for all Θ_i with $i = 1, 2, 3, 4$, but we only need the case $i = 4$ and we fill in some details in the proof for this case.

Lemma 3.3.13 ([35, Theorem 5.6]). *Let q be a prime, and let $\hat{\lambda}_{4,q}$ be the canonical local real height defined in Definition 3.1.10. Let $P, Q \in J(\mathbb{Q}_q)$ be such that $P, Q, P+Q, P-Q \notin \operatorname{supp}(\Theta_4)$. Then*

$$\hat{\lambda}_{4,q}(P+Q) + \hat{\lambda}_{4,q}(P-Q) - 2\hat{\lambda}_{4,q}(P) - 2\hat{\lambda}_{4,q}(Q) = -\log \left| \frac{B_{44}(x(P), x(Q))}{x_4(P)^2 x_4(Q)^2} \right|_q .$$

Proof. Recall from the proof of Theorem 3.1.11 that $\hat{\lambda}_{4,q}$ is a canonical local height corresponding to Θ_4. If we define the morphisms $\sigma, \epsilon, \pi_1, \pi_2 \colon J \times J \to J$ by $\sigma(P,Q) = P+Q$, $\epsilon(P,Q) = P-Q$, $\pi_1(P,Q) = P$ and $\pi_2(P,Q) = Q$, we have

$$\operatorname{div}\left(\frac{B_{44}(x(P), x(Q))}{x_4(P)^2 x_4(Q)^2} \right) = \sigma^*\Theta_4 + \epsilon^*\Theta_4 - 2\pi_1^*\Theta_4 - 2\pi_2^*\Theta_4.$$

We use the properties of canonical local height functions in Theorem 3.1.8 to conclude that

$$\begin{aligned}
&\hat{\lambda}_{4,q}(P+Q) + \hat{\lambda}_{4,q}(P-Q) - 2\hat{\lambda}_{4,q}(P) - 2\hat{\lambda}_{4,q}(Q) \\
&\quad = \hat{\lambda}_{\sigma^*\Theta_4,q}(P,Q) + \hat{\lambda}_{\epsilon^*\Theta_4,q}(P,Q) - 2\hat{\lambda}_{\pi_1^*\Theta_4,q}(P,Q) - 2\hat{\lambda}_{\pi_2^*\Theta_4,q}(P,Q) + \gamma_1 \quad \text{(property (iv))} \\
&\quad = \hat{\lambda}_{\sigma^*\Theta_4+\epsilon^*\Theta_4-2\pi_1^*\Theta_4-2\pi_2^*\Theta_4,q}(P,Q) + \gamma_2 \quad \text{(property (i))} \\
&\quad = -\log \left| \frac{B_{44}(x(P), x(Q))}{x_4(P)^2 x_4(Q)^2} \right|_q + \gamma_3, \quad \text{(property (ii))}
\end{aligned} \tag{3.20}$$

where the γ_i are constants. We rearrange this equation to get an expression for γ_3:

$$\gamma_3 = \hat{\lambda}_{4,q}(P+Q) + \hat{\lambda}_{4,q}(P-Q) - 2\hat{\lambda}_{4,q}(P) - 2\hat{\lambda}_{4,q}(Q) + \log \left| \frac{B_{44}(x(P), x(Q))}{x_4(P)^2 x_4(Q)^2} \right|_q .$$

This equality holds in particular for $P = Q = \mathcal{O}$ with $\kappa(\mathcal{O}) = [0:0:0:1]$. In that case we have $\hat{\lambda}_{4,q}(\mathcal{O}) = 0$, and we also conclude that $B_{44}(x(P), x(Q)) = 1$ from Properties 3.3.6(d). Hence all terms on the right-hand side evaluate to 0, so $\gamma_3 = 0$. But as this value is independent of P and Q, we conclude from (3.20) that the desired equation is satisfied. ∎

Proposition 3.3.14. *Let $P, Q \in J_p(\mathbb{Q})$. Then $B_{ii}(x(P), x(Q)) = \pm x_i(P+Q)x_i(P-Q)$ for $i = 1, 2, 3, 4$.*

Proof. Recall that $J_1^{(p)}(\mathbb{Q}) \subseteq J_{\Theta_4}(\mathbb{Q})$. Hence we can apply Lemma 3.3.13 for any prime q, which gives us

$$\begin{aligned}
\hat{\lambda}_{4,q}(P+Q) + \hat{\lambda}_{4,q}(P-Q) - 2\hat{\lambda}_{4,q}(P) - 2\hat{\lambda}_{4,q}(Q) &= -\log \left| \frac{B_{44}(x(P), x(Q))}{x_4(P)^2 x_4(Q)^2} \right|_q \\
&= -\log |B_{44}(x(P), x(Q))|_q \\
&\quad + 2\log |x_4(P)|_q + 2\log |x_4(Q)|_q.
\end{aligned} \tag{3.21}$$

On the other hand, because $P, Q \in J_U(\mathbb{Q})$, and hence $P+Q, P-Q \in J_U(\mathbb{Q})$, Proposition 3.1.13 implies

$$\begin{aligned}\hat{\lambda}_{4,q}(P+Q) + \hat{\lambda}_{4,q}(P-Q) - 2\hat{\lambda}_{4,q}(P) - 2\hat{\lambda}_{4,q}(Q) \\ = \lambda_{4,q}(P+Q) + \lambda_{4,q}(P-Q) - 2\lambda_{4,q}(P) - 2\lambda_{4,q}(Q) \\ = -\log|x_4(P+Q)|_q - \log|x_4(P-Q)|_q + 2\log|x_4(P)|_q + 2\log|x_4(Q)|_q. \quad (3.22)\end{aligned}$$

Equating (3.21) and (3.22) gives

$$-\log|B_{44}(x(P),x(Q))|_q = -\log|x_4(P+Q)x_4(P-Q)|_q.$$

We conclude that $\mathrm{ord}_q(B_{44}(x(P),x(Q))) = \mathrm{ord}_q(x_4(P+Q)x_4(P-Q))$ for every prime q. Because $x_4(P+Q)x_4(P-Q)$ is nonzero, this implies that

$$B_{44}(x(P),x(Q)) = \pm x_4(P+Q)x_4(P-Q).$$

From Theorem 1.5.2 we deduce that

$$\begin{aligned}&[B_{11}(x(P),x(Q)) : B_{22}(x(P),x(Q)) : B_{33}(x(P),x(Q)) : B_{44}(x(P),x(Q))] = \\ &[x_1(P+Q)x_1(P-Q) : x_2(P+Q)x_2(P-Q) : x_3(P+Q)x_3(P-Q) : x_4(P+Q)x_4(P-Q)]\end{aligned}$$

as projective points. Therefore $B_{ii}(x(P),x(Q)) = \pm x_i(P+Q)x_i(P-Q)$ for all $i = 1,2,3,4$. ■

Together, (3.19) and Proposition 3.3.14 give

$$H_p(P+Q) + H_p(P-Q) = \log_p(B_{44}(x(P),x(Q))). \quad (3.23)$$

We write $B_{44}(x(P),x(Q)) = x_4(P)^2x_4(Q)^2\lambda(P,Q)$, where by definition

$$\lambda(P,Q) := \frac{B_{44}(x(P),x(Q))}{x_4(P)^2x_4(Q)^2}.$$

Because $B_{44}(k,l)$ is a biquadratic form in the variables k_1,k_2,k_3,k_4 and l_1,l_2,l_3,l_4, we can view $\lambda(P,Q)$ as a polynomial

$$\lambda(P,Q) \in \mathbb{Z}\left[\frac{x_1(P)}{x_4(P)}, \frac{x_2(P)}{x_4(P)}, \frac{x_3(P)}{x_4(P)}, \frac{x_1(Q)}{x_4(Q)}, \frac{x_2(Q)}{x_4(Q)}, \frac{x_3(Q)}{x_4(Q)}\right].$$

From Properties 3.3.6(d), we conclude that the constant coefficient of λ is 1. It also says that $k_4^2l_4^2$ is the only term in $B_{44}(k,l)$ that involves k_4^2 or l_4^2, and therefore all nonconstant terms in the polynomial $\lambda(P,Q)$ contain at least one factor $\frac{x_i(P)}{x_4(P)}$ and one factor $\frac{x_j(Q)}{x_4(Q)}$ for some $i,j \in \{1,2,3\}$. Recall that because $P, Q \in J_1^{(p)}(\mathbb{Q})$, we have (3.14) for P and Q. Using (3.14) and (3.16), we then conclude that there is a series

$$\lambda^T(T_1,T_2,S_1,S_2) \in 1 + (T_1,T_2)^2(S_1,S_2)^2\mathbb{Z}[[T_1,T_2,S_1,S_2]] \quad (3.24)$$

such that $\lambda(P,Q) = \lambda^T(\boldsymbol{t}(P),\boldsymbol{t}(Q))$.

Lemma 3.3.15. *Let $P, Q \in J_1^{(p)}(\mathbb{Q}_p)$ and*

$$g(T_1,T_2,S_1,S_2) \in 1 + (T_1,T_2)^2(S_1,S_2)^2\mathbb{Z}_p[[T_1,T_2,S_1,S_2]].$$

Then

$$\lim_{n\to\infty} \frac{1}{p^{2n}} \log_p(g(\boldsymbol{t}([p^n]P),\boldsymbol{t}([p^n]Q))) = 0.$$

Proof. Recall from Corollary 1.6.18 that $\mathrm{ord}_p(t_i([p^n]P)), \mathrm{ord}_p(t_i([p^n]Q)) \geq n$ for $i = 1, 2$. Because g has coefficients in $\mathbb{Z}_p$, it converges when $\mathrm{ord}_p(t_i), \mathrm{ord}_p(s_i) > 0$ for $i = 1, 2$ by Lemma 1.1.7. Then the result follows from Lemma 2.3.2 with $r = 4$, $k = 4$ and $m = 2$. ∎

We rewrite (3.23) as

$$\begin{aligned} H_p(P+Q) + H_p(P-Q) &= \log_p\left(x_4(P)^2 x_4(Q)^2 \lambda(P,Q)\right) \\ &= 2\log_p(x_4(P)) + 2\log_p(x_4(Q)) + \log_p(\lambda(P,Q)) \\ &= 2H_p(P) + 2H_p(Q) + \log_p(\lambda^T(\boldsymbol{t}(P), \boldsymbol{t}(Q))). \end{aligned}$$

We use this to show that h_p satisfies the parallelogram law.

Proof of Theorem 3.3.12. For $P, Q \in J_p(\mathbb{Q})$, we obtain

$$\begin{aligned} h_p(P+Q) + h_p(P-Q) &= \lim_{n\to\infty} \frac{1}{p^{2n}} \left(H_p([p^n]P + [p^n]Q) + H_p([p^n]P - [p^n]Q)\right) \\ &= \lim_{n\to\infty} \frac{1}{p^{2n}} \left(2H_p([p^n]P) + 2H_p([p^n]Q) + \log_p(\lambda^T(\boldsymbol{t}([p^n]P), \boldsymbol{t}([p^n]Q)))\right) \\ &= 2h_p(P) + 2h_p(Q). \qquad \text{(using (3.24) and Lemma 3.3.15)} \end{aligned}$$

∎

Corollary 3.3.16. *Let $P \in J_p(\mathbb{Q})$ and let $n \in \mathbb{Z}$. Then*

$$h_p([n]P) = n^2 h_p(P).$$

Proof. Because $J_p(\mathbb{Q})$ is an abelian group, this follows from Proposition 2.1.5 and Theorem 3.3.12. Alternatively, this can be shown directly using Corollary 3.3.5 and an argument similar to the proof of Theorem 3.3.1. ∎

3.3.3 Extension of h_p to $J(\mathbb{Q})$

We defined h_p only on $J_p(\mathbb{Q})$. We now extend the definition to $J(\mathbb{Q})$ in such a way that the resulting function is a quadratic form on $J(\mathbb{Q})$. Recall that $J_p(\mathbb{Q})$ is a subgroup of finite index in $J(\mathbb{Q})$ (Proposition 3.2.9), and hence each point $P \in J(\mathbb{Q})$ has a multiple that lies in $J_p(\mathbb{Q})$.

Definition 3.3.17. Let $P \in J(\mathbb{Q})$. Let $m \in \mathbb{Z}_{>0}$ such that $[m]P \in J_p(\mathbb{Q})$. Then we define

$$h_p(P) = \frac{1}{m^2} h_p([m]P).$$

To show that this definition makes sense, we need the following property.

Lemma 3.3.18. *Let $P \in J(\mathbb{Q})$ and $m_1, m_2 \in \mathbb{Z}_{>0}$ such that $[m_1]P, [m_2]P \in J_p(\mathbb{Q})$. Then*

$$\frac{1}{m_1^2} h_p([m_1]P) = \frac{1}{m_2^2} h_p([m_2]P).$$

Proof. Because also $[m_1m_2]P \in J_p(\mathbb{Q})$, we can use Corollary 3.3.16 to conclude that

$$\begin{aligned}\frac{1}{m_1^2}h_p([m_1]P) &= \frac{1}{m_1^2m_2^2}h_p([m_1m_2]P)\\ &= \frac{1}{m_2^2}h_p([m_2]P).\end{aligned}$$

■

It is then also clear that Definition 3.3.17 does not conflict with the original definition of h_p on $J_p(\mathbb{Q})$, because we can take $m = 1$ when $P \in J_p(\mathbb{Q})$.

Theorem 3.3.19. *The function $h_p\colon J(\mathbb{Q}) \to \mathbb{Q}_p$ is a quadratic form. Explicitly, it has the following properties.*

(a) For all $P, Q \in J(\mathbb{Q})$, we have $h_p(P+Q) + h_p(P-Q) = 2h_p(P) + 2h_p(Q)$.

(b) For all $P \in J(\mathbb{Q})$ and $n \in \mathbb{Z}$, we have $h_p([n]P) = n^2h_p(P)$.

Proof. Let $m_1, m_2 \in \mathbb{Z}_{>0}$ be such that $[m_1]P, [m_2]Q \in J_p(\mathbb{Q})$. These exist by Proposition 3.2.9. Then also $[m_1m_2]P$, $[m_1m_2]Q$ and their sum and difference are all in $J_p(\mathbb{Q})$. Therefore, using Definition 3.3.17 we get

$$\begin{aligned}h_p(P+Q) + h_p(P-Q) &= \frac{1}{m_1^2m_2^2}\left(h_p([m_1m_2]P + [m_1m_2]Q) + h_p([m_1m_2]P - [m_1m_2]Q)\right)\\ &= \frac{1}{m_1^2m_2^2}\left(2h_p([m_1m_2]P) + 2h_p([m_1m_2]Q)\right) \qquad \text{(Theorem 3.3.12)}\\ &= 2h_p(P) + 2h_p(Q).\end{aligned}$$

This shows part (a). Part (b) follows from part (a) and Proposition 2.1.5. ■

3.3.4 Comparison of h_p and $\hat{h}_p$

Now that we have found a quadratic p-adic height h_p as a limit of the naive height H_p, we compare it with the p-adic height $\hat{h}_p$ from Section 3.2.3. In this section, we show that the two heights turn out to be identical. We first show this on the subset $J_p(\mathbb{Q}) \setminus \operatorname{supp}(\Theta)$, because there we have more straightforward descriptions of h_p and $\hat{h}_p$. We then use that result to show that the heights must be equal on all of $J(\mathbb{Q})$.

We take a similar approach as in Section 2.3.6 for elliptic curves. First we find an expression $g(P)$ such that $\hat{h}_p(P) = H_p(P) + g(P)$ for all $P \in J_p(\mathbb{Q}) \setminus \operatorname{supp}(\Theta)$. Then we want to take a limit over p-power multiples of P on both sides such that the term involving g vanishes, and we obtain $h_p(P)$ on the right-hand side. However, because we only have this expression for $P \in J_p(\mathbb{Q}) \setminus \operatorname{supp}(\Theta)$, we can only take the limit over multiples $[p^n]P$ of P that are also not in $\operatorname{supp}(\Theta)$. We thus first show that for any $P \in J_1(\mathbb{Q}) \setminus \{\mathcal{O}\}$, the set $S(P) = \{n \in \mathbb{Z}_{>0} \mid [p^n]P \notin \operatorname{supp}(\Theta)\}$ is infinite, so that we can take the limit over the multiples $[p^n]P$ with $n \in S(P)$ rather than over all $n \in \mathbb{Z}_{>0}$. To show that $S(P)$ is infinite, we first need some lemmas about the multiplication-by-p map on the formal group associated to J.

Lemma 3.3.20. *Let $m \geq 1$. Let $[m] = ([m]_1, [m]_2)$ be the multiplication-by-m homomorphism from Definition 1.6.4. The series $[m]_1(0, T_2) \in \mathbb{Z}_p[[T_2]]$ is of the form*

$$[m]_1(0, T_2) = \xi_m T_2^3 + (\textit{terms of degree} \geq 5),$$

where $\xi_m := -\sum_{i=1}^{m} i(i-1)$.

Proof. The formal group law $\boldsymbol{F}_J$ of $\hat{J}$ can be computed explicitly, and it is shown in [4] that $\boldsymbol{F}_J$ has an expansion of the form

$$\begin{aligned} F_{J,1}(X_1, X_2, Y_1, Y_2) &= X_1 + Y_1 - f_2 X_1^2 Y_1 - f_2 X_1 Y_1^2 - X_2^2 Y_2 - X_2 Y_2^2 \\ &\qquad + (\text{terms of total degree} \geq 5) \\ F_{J,2}(X_1, X_2, Y_1, Y_2) &= X_2 + Y_2 - f_1 X_1^2 Y_1 - f_1 X_1 Y_1^2 + 2 f_4 X_2^2 Y_2 + 2 f_4 X_2 Y_2^2 \\ &\qquad + (\text{terms of total degree} \geq 5). \end{aligned}$$

We noted in Section 1.6.3 that the series $F_{1,J}$, $F_{2,J}$ only have terms of total odd degree, and from the definition of $[m]$ we deduce that the same is then true for the $[m]_1$ and $[m]_2$.

For $m = 1$, we find that

$$[1]_1(0, T_2) = F_{J,1}(0, 0, 0, T_2) \in T_2^5 \mathbb{Z}_p[[T_2]]$$

and hence it has the desired form with $\xi_1 = 0$.

For induction, let $k \geq 1$ and let us assume that $[m]_1(0, T_2) = \xi_m T_2^3 + (\text{terms of degree} \geq 5)$ for all $m \leq k$. We note that $[k]_2(0, T_2) = kT_2 + (\text{terms of degree} \geq 3)$ by Proposition 1.6.5 and because $[k]_2$ is odd. We then get

$$\begin{aligned} [k+1]_1(0, T_2) &= F_{J,1}\left([k]_1(0, T_2),\, [k]_2(0, T_2),\, 0,\, T_2\right) \\ &= [k]_1(0, T_2) - T_2([k]_2(0, T_2))^2 - T_2^2 [k]_2(0, T_2) + (\text{terms of degree} \geq 5) \\ &= \xi_k T_2^3 - k^2 T_2^3 - k T_2^3 + (\text{terms of degree} \geq 5) \\ &= (\xi_k - k(k+1)) T_2^3 + (\text{terms of degree} \geq 5). \end{aligned}$$

Because $\xi_{k+1} = \xi_k - k(k+1)$, this implies the result. ∎

Lemma 3.3.21. *Let p be a prime. Then for ξ_p as defined in Lemma 3.3.20, we have* $\operatorname{ord}_3(\xi_3) = 0$, *and* $\operatorname{ord}_p(\xi_p) = 1$ *for $p \neq 3$.*

Proof. We note that

$$\xi_p = -\sum_{i=1}^{p} i(i-1) = -\frac{p(p+1)(2p+1)}{6} + \frac{p(p+1)}{2} = -\frac{p(p+1)(p-1)}{3}.$$

Because $\operatorname{ord}_p(p+1) = \operatorname{ord}_p(p-1) = 0$, we find $\operatorname{ord}_3(\xi_3) = 0$ and $\operatorname{ord}_p(\xi_p) = 1$ for $p \neq 3$. ∎

Theorem 3.3.22. *Let $P \in J_1(\mathbb{Q}_p) \cap \operatorname{supp}(\Theta)$ and $P \neq \mathcal{O}$. Then $[p]P \in J_\Theta(\mathbb{Q}_p)$.*

Proof. We know from Lemma 3.2.4 that $P \in \operatorname{supp}(\Theta)$ implies that $t_1(P) = 0$. If we assume that $[p]P \in \operatorname{supp}(\Theta)$, then we must have $t_1([p]P) = 0$. From Lemma 3.3.20 we know that

$$t_1([p]P) = [p]_1(0, t_2(P)) = t_2^2(P)\left(\xi_p + (\text{terms of degree} \geq 2 \text{ in } t_2(P))\right).$$

Because $\operatorname{ord}_p(\xi_p) \leq 1$ by Lemma 3.3.21, this can only be zero when $t_2(P) = 0$. But $\boldsymbol{t}(P) = (0,0)$ if and only if $P = \mathcal{O}$. This contradicts our assumption, and hence we must have $[p]P \notin \operatorname{supp}(\Theta)$. ■

Corollary 3.3.23. *Let $P \in J_1(\mathbb{Q}_p) \setminus \{\mathcal{O}\}$. Then the set $S(P) = \{n \in \mathbb{Z}_{>0} \mid [p^n]P \notin \operatorname{supp}(\Theta)\}$ is infinite.*

Proof. If $\mathbb{Z}_{>0} \setminus S(P)$ is finite, this is immediate. Now assume $\mathbb{Z}_{>0} \setminus S(P)$ is infinite. Corollary 1.6.26 implies that P is a nontorsion point, and hence for every $n \in \mathbb{Z}_{>0} \setminus S(P)$, we have $[p^n]P \in \operatorname{supp}(\Theta) \setminus \{\mathcal{O}\}$. Then Theorem 3.3.22 implies that $n+1 \in S(P)$. Hence $S(P)$ must also be infinite. ■

We now use this fact to show that h_p and $\hat{h}_p$ are equal.

Theorem 3.3.24. *Let $P \in J_p(\mathbb{Q}) \setminus \operatorname{supp}(\Theta)$. Then*

$$\hat{h}_p(P) = h_p(P).$$

Proof. Let us consider a point $Q \in J_p(\mathbb{Q}) \setminus \operatorname{supp}(\Theta)$. Note that Corollary 1.6.26 implies that $Q \notin J_{\text{tors}}$. Furthermore, because $Q \in J_1^{(p)}(\mathbb{Q})$, we have $x_4(P) \neq 0$. We get

$$\begin{aligned}
\hat{h}_p(Q) &= -\log_p\left(\frac{\sigma_p(\boldsymbol{t}(Q))^2}{x_1(Q)}\right) && \text{(Proposition 3.2.13)} \\
&= -\log_p\left(\sigma_p(\boldsymbol{t}(Q))^2 \frac{x_4(Q)}{x_1(Q)}\right) + \log_p(x_4(Q)) \\
&= -\log_p\left(\sigma_p(\boldsymbol{t}(Q))^2 \wp_{11}^T(\boldsymbol{t}(Q))\right) + H_p(Q). && (3.25)
\end{aligned}$$

In the last step we used that because $Q \notin \operatorname{supp}(\Theta)$, we know from (1.17) and (1.28) that $x_4(Q)/x_1(Q) = \wp_{11}(Q) = \wp_{11}^T(\boldsymbol{t}(Q))$, the expansion of which is given in (1.29). We see in [5, Appendix A] that $\sigma_p(\boldsymbol{T})$ has an expansion of the form

$$\sigma_p(\boldsymbol{T}) \in T_1\left(1 + \frac{f_2}{2}T_1^2 + (T_1, T_2)^4\mathbb{Q}[[T_1, T_2]]\right).$$

Using these expansions we deduce that

$$\sigma_p(\boldsymbol{T})^2 \wp_{11}^T(\boldsymbol{T}) \in 1 + (T_1, T_2)^4\mathbb{Q}_p[[T_1, T_2]]. \tag{3.26}$$

Recall that $\sigma_p(\boldsymbol{T})$ converges for $\boldsymbol{T} \in (p\mathbb{Z}_p)^2$ (Theorem 3.2.3). We also know that $\wp_{11}^T(\boldsymbol{T})$ with expansion (1.29) converges on $(p\mathbb{Z}_p)^2 \setminus \{(0,0)\}$, and $\sigma_p(\boldsymbol{T})^2\wp_{11}^T(\boldsymbol{T})$ evaluates to 1 at $(0,0)$. We conclude that the series $\sigma_p(\boldsymbol{T})^2\wp_{11}^T(\boldsymbol{T})$ converges on a neighborhood of $(0,0)$.

Recall from Corollary 3.3.23 that $S(P)$ is an infinite set, so we can take a limit over $n \in S(P)$. We get

$$\begin{aligned}
\hat{h}_p(P) &= \lim_{\substack{n\to\infty \\ n\in S(P)}} \frac{1}{p^{2n}} \hat{h}_p([p^n]P) && \text{(because } \hat{h}_p \text{ is quadratic)} \\
&= \lim_{\substack{n\to\infty \\ n\in S(P)}} \frac{1}{p^{2n}} H_p([p^n]P) - \lim_{\substack{n\to\infty \\ n\in S(P)}} \frac{1}{p^{2n}} \log_p \left(\sigma_p(\boldsymbol{t}([p^n]P))^2 \wp_{11}^T(\boldsymbol{t}([p^n]P))\right) && \text{(using (3.25))} \\
&= \lim_{n\to\infty} \frac{1}{p^{2n}} H_p([p^n]P) - \lim_{n\to\infty} \frac{1}{p^{2n}} \log_p \left(\sigma_p(\boldsymbol{t}([p^n]P))^2 \wp_{11}^T(\boldsymbol{t}([p^n]P))\right) \\
&= h_p(P). && \text{(using Theorem 3.3.1, (3.26) and Corollary 3.3.10)}
\end{aligned}$$

The equality between the second and third line is satisfied provided the limits exist, which is shown in the final step. ■

Finally, we show that $h_p = \hat{h}_p$ on all of $J(\mathbb{Q})$.

Theorem 3.3.25. *For all $P \in J(\mathbb{Q})$, we have $\hat{h}_p(P) = h_p(P)$.*

Proof. First of all, let us consider $P \in J_{\text{tors}}(\mathbb{Q})$ with $m \in \mathbb{Z}_{>0}$ such that $[m]P = \mathcal{O}$. We have $\hat{h}_p(P) = 0$ by Definition 3.2.11. On the other hand, $h_p(P) = \frac{1}{m^2} h_p(\mathcal{O})$, and we note that $H_p(\mathcal{O}) = 0$ which implies by definition that $h_p(\mathcal{O}) = 0$. Hence $\hat{h}_p(P) = h_p(P) = 0$.

For $P \in J(\mathbb{Q}) \setminus J_{\text{tors}}$, let us consider $m \in \mathbb{Z}_{>0}$ such that $[m]P \in J_p(\mathbb{Q}) \setminus \text{supp}(\Theta)$, which exists by Proposition 3.2.9 and Lemma 3.2.10. Then

$$\begin{aligned}
\hat{h}_p(P) &= \frac{1}{m^2} \hat{h}_p([m]P) && \text{(Proposition 3.2.14)} \\
&= \frac{1}{m^2} h_p([m]P) && \text{(Theorem 3.3.24)} \\
&= h_p([m]P). && \text{(Theorem 3.3.19)}
\end{aligned}$$

■

In particular, because we showed that h_p is a quadratic form on $J(\mathbb{Q})$, the same is true for $\hat{h}_p$. This way we indirectly showed that the global height defined in Section 3.2.3 satisfies the parallelogram law.

In conclusion, we indeed succeeded in providing an alternate construction of a quadratic p-adic height on the Jacobian of a genus 2 curve, by defining a naive height and using a limit process.

Appendix

Consider a smooth projective curve $\mathcal{C}$ of genus 2 over a perfect field K with $\mathrm{char}(K) \neq 2$, defined by the affine equation

$$\mathcal{C}\colon y^2 = x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0$$

with $f_i \in K$. The corresponding Jacobian J can be defined as the zero set of the following 13 polynomials in $\mathbb{P}^8$, as shown in [16, Section 2].

$$\begin{aligned}
F_2 &= 2X_0X - X_{11}X_{22} + X_{12}^2 - f_3X_0X_{12} + f_1X_0^2,\\
F_3 &= X_0X_{112} - X_{222}X_{12} + X_{122}X_{22},\\
F_4 &= X_0X_{111} + X_{222}X_{11} + X_{122}X_{12} - 2X_{112}X_{22} - 2f_4X_0X_{112} + f_3X_0X_{122},\\
F_5 &= X_0X_{122}^2 - X_{11}X_{22}^2 + 2X_0XX_{22} + X_0X_{11}X_{12} - f_4X_0X_{11}X_{22} - f_3X_0X_{12}X_{22} + 2f_4X_0^2X\\
&\quad - f_4f_3X_0^2X_{12} + f_1X_0^2X_{22} + (f_4f_1 - f_0)X_0^3,\\
F_6 &= X_0X_{222}^2 - X_{22}^3 - X_0X_{12}X_{22} - f_4X_0X_{22}^2 - X_0^2X_{11} - f_3X_0^2X_{22} - f_2X_0^3,\\
F_7 &= X_0X_{122}X_{222} - X_{12}X_{22}^2 + X_0^2X - f_3X_0^2X_{12} - f_4X_0X_{12}X_{22},\\
F_8 &= X_0X_{111}^2 - X_{11}^3 - f_2X_0X_{11}^2 - f_1X_0X_{11}X_{12} + 3f_0X_0X_{11}X_{22} + 2f_0X_0^2X\\
&\quad + (4f_4f_0 - f_3f_1)X_0^2X_{11} - 3f_3f_0X_0^2X_{12} + (3f_2f_0 - f_1^2)X_0^2X_{22}\\
&\quad + (4f_4f_2f_0 + f_1f_0 - f_4f_1^2 - f_3^2f_0)X_0^3,\\
F_9 &= -X_{111}X_{112} + f_4X_{111}X_{122} - f_3X_{112}X_{122} + f_2X_{112}X_{222} - f_1X_{122}X_{222} + f_0X_{222}^2 - X^2\\
&\quad - f_4XX_{11} + f_3XX_{12} - f_2XX_{22} - f_2X_{11}X_{12} + f_4f_2X_{11}X_{22} - (f_0 + f_4f_1)X_{12}X_{22}\\
&\quad + 2f_4f_0X_{22}^2 - 2(f_4f_2 + f_1)X_0X - 2f_0X_0X_{11}\\
&\quad + (2f_3f_1 + f_4f_3f_2 + f_4f_0 - f_2^2 - f_4^2f_1)X_0X_{12} + 2f_0(f_4^2 - f_3)X_0X_{22}\\
&\quad + (f_4f_3f_0 - f_4f_2f_1 - 2f_2f_0)X_0^2,\\
F_{10} &= X_{112}^2 - X_{111}X_{122} + X_{11}X - f_2X_{11}X_{22} + 2f_1X_{12}X_{22} - 3f_0X_{22}^2 + 2f_2X_0X\\
&\quad + (f_4f_1 - f_2f_3 - f_0)X_0X_{12} - 2f_4f_0X_0X_{22} + (f_2f_1 - f_3f_0)X_0^2,\\
F_{11} &= X_{111}X_{222} - X_{112}X_{122} - 2XX_{12} + X_{11}^2 - 2f_4X_{11}X_{12} + 3f_3X_{11}X_{22} - 2f_2X_{12}X_{22} + f_1X_{22}^2\\
&\quad - 5f_3X_0X + f_2X_0X_{11} + (3f_3^2 - 2f_4f_2)X_0X_{12} + (f_4f_1 - f_0)X_0X_{22} - 2f_3f_1X_0^2,\\
F_{12} &= X_{122}^2 - X_{112}X_{222} + X_{22}X + 2X_{11}X_{12} - f_4X_{11}X_{22} + 2f_4X_0X + (f_2 - f_4f_3)X_0X_{12}\\
&\quad + (f_4f_1 - f_0)X_0^2,\\
F_{13} &= X_{111}X_{12} - X_{112}X_{11} - f_1X_0X_{122} + 2f_0X_0X_{222},\\
F_{14} &= 2X_{122}X_{11} - X_{112}X_{12} - X_{111}X_{22} - f_3X_{112} + 2f_2X_0X_{122} - f_1X_0X_{222}.
\end{aligned}$$

Bibliography

[1] J. S. Balakrishnan and N. Dogra. "Quadratic Chabauty and rational points, I: p-adic heights". In: *Duke Mathematical Journal* 167.11 (2018), pp. 1981–2038.

[2] J. S. Balakrishnan, J. S. Müller, and W. A. Stein. "A p-adic analogue of the conjecture of Birch and Swinnerton-Dyer for modular abelian varieties". In: *Mathematics of Computation* 85.298 (2016), pp. 983–1016.

[3] D. Bernardi. "Hauteur p-adique sur les courbes elliptiques". In: *Seminar on Number Theory, Paris 1979–80*. Vol. 12. Progress in Mathematics. Birkhäuser, 1981, pp. 1–14.

[4] F. Bianchi. *p-adic sigma functions and heights on Jacobians of genus 2 curves*. In preparation.

[5] F. Bianchi. *Bernardi-like p-adic sigma function in genus 2*. `https://sites.google.com/view/francescabianchi/mt_ns_note`. 2022.

[6] F. Bianchi. "Topics in the theory of p-adic heights on elliptic curves". PhD thesis. University of Oxford, 2019.

[7] C. Birkenhake and H. Lange. *Complex abelian varieties*. Second Edition. Vol. 302. Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, 2004.

[8] C. Blakestad. "On Generalizations of p-Adic Weierstrass Sigma and Zeta Functions". PhD thesis. University of Colorado, 2018.

[9] J. W. S. Cassels. *Lectures on elliptic curves*. Vol. 24. London Mathematical Society Student Texts. Cambridge University Press, 1991.

[10] J. W. S. Cassels and E. V. Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus 2*. Vol. 230. London Mathematical Society Lecture Note Series. Cambridge University Press, 1996.

[11] J. W. S. Cassels and A. Fröhlich. *Algebraic number theory*. Academic Press Limited, 1967.

[12] E. V. Flynn. *Biquadratic Forms*. `https://people.maths.ox.ac.uk/flynn/genus2/kummer/biquadratic.forms`. Accessed: 12 November 2021.

[13] E. V. Flynn. "The group law on the Jacobian of a curve of genus 2". In: *Journal für die reine und angewandte Mathematik* 439 (1993), pp. 45–69.

[14] E. V. Flynn and N. P. Smart. "Canonical heights on the Jacobians of curves of genus 2 and the infinite descent". In: *Acta Arithmetica* 79.4 (1997), pp. 333–352.

[15] F. Q. Gouvêa. *p-adic Numbers*. Third Edition. Universitext. Springer, 2020.

[16] D. Grant. "Formal groups in genus two". In: *Journal für die Reine und Angewandte Mathematik* 411 (1990), pp. 96–121.

[17] R. Hartshorne. *Algebraic geometry*. Vol. 52. Graduate Texts in Mathematics. Springer-Verlag, 1977.

[18] R. de Jong and J. S. Müller. "Canonical heights and division polynomials". In: *Mathematical Proceedings of the Cambridge Philosophical Society* 157.2 (2014), pp. 357–373.

[19] N. Kanayama. "Corrections to "Division polynomials and multiplication formulae in dimension 2"". In: *Mathematical Proceedings of the Cambridge Philosophical Society* 149.1 (2010), pp. 189–192.
[20] N. Kanayama. "Division polynomials and multiplication formulae of Jacobian varieties of dimension 2". In: *Mathematical Proceedings of the Cambridge Philosophical Society* 139.3 (2005), pp. 399–409.
[21] N. Koblitz. *p-adic numbers, p-adic analysis, and zeta-functions*. Second Edition. Vol. 58. Graduate Texts in Mathematics. Springer-Verlag, 1984.
[22] S. Lang. *Fundamentals of Diophantine geometry*. Springer-Verlag, 1983.
[23] H. Matsumura. *Commutative Algebra*. Second Edition. Vol. 56. Mathematics Lecture Note Series. The Benjamin/Cummings Publishing Company, Inc., 1980.
[24] B. Mazur and J. Tate. "The p-adic sigma function". In: *Duke Mathematical Journal* 62.3 (1991), pp. 663–688.
[25] B. Mazur, J. Tate, and J. Teitelbaum. "On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer". In: *Inventiones Mathematicae* 84.1 (1986), pp. 1–48.
[26] A. Néron. "Fonctions thêta p-adiques et hauteurs p-adiques". In: vol. 22. Progress in Mathematics. Birkhäuser, 1982, pp. 149–174.
[27] A. Néron. "Quasi-fonctions et hauteurs sur les variétés abéliennes". In: *Annals of Mathematics. Second Series* 82 (1965), pp. 249–331.
[28] B. Perrin-Riou. "Hauteurs p-adiques". In: *Seminar on number theory, Paris 1982–83* 51 (1984), pp. 233–257.
[29] B. Perrin-Riou. "Sur les hauteurs p-adiques". In: *Comptes Rendus des Séances de l'Académie des Sciences. Série I. Mathématique* 296 (1983), pp. 291–294.
[30] G. Shimura. *Elementary Dirichlet series and modular forms*. Springer Monographs in Mathematics. Springer, New York, 2007.
[31] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*. Vol. 151. Graduate Texts in Mathematics. Springer-Verlag, 1994.
[32] J. H. Silverman. *The arithmetic of elliptic curves*. Second Edition. Vol. 106. Graduate Texts in Mathematics. Springer, 2009.
[33] M. Stoll. *Arithmetic of hyperelliptic curves*. `https://www.mathe2.uni-bayreuth.de/stoll/teaching/ArithHypKurven-SS2019/Skript-ArithHypCurves-pub-screen.pdf`. Accessed: April 2022. 2019.
[34] M. Stoll. "On the height constant for curves of genus two. II". In: *Acta Arithmetica* 104.2 (2002), pp. 165–182.
[35] Y. Uchida. "Canonical local heights and multiplication formulas for the Jacobians of curves of genus 2". In: *Acta Arithmetica* 149.2 (2011), pp. 111–130.
[36] Y. Uchida. "Division polynomials and canonical local heights on hyperelliptic Jacobians". In: *Manuscripta Mathematica* 134.3-4 (2011), pp. 273–308.
[37] L. C. Washington. *Elliptic curves*. Second Edition. Discrete Mathematics and its Applications. Chapman & Hall/CRC, 2008.
[38] T. Zink. *Cartiertheorie kommutativer formaler Gruppen*. Vol. 68. Teubner-Texte zur Mathematik. BSB B. G. Teubner Verlagsgesellschaft, 1984.