

# *Algebra & Number Theory*

Volume 10

2016

No. 10

**Canonical heights on genus-2 Jacobians**

Jan Steffen Müller and Michael Stoll



# Canonical heights on genus-2 Jacobians

Jan Steffen Müller and Michael Stoll

*Scale New Heights!*

Motto of International (now Jacobs) University Bremen,  
where the first author started his Ph.D. under the supervision of the second.

Let  $K$  be a number field and let  $C/K$  be a curve of genus 2 with Jacobian variety  $J$ . We study the canonical height  $\hat{h}: J(K) \rightarrow \mathbb{R}$ . More specifically, we consider the following two problems, which are important in applications:

- (1) for a given  $P \in J(K)$ , compute  $\hat{h}(P)$  efficiently;
- (2) for a given bound  $B > 0$ , find all  $P \in J(K)$  with  $\hat{h}(P) \leq B$ .

We develop an algorithm running in polynomial time (and fast in practice) to deal with the first problem. For the second problem, we show how to tweak the naive height  $h$  to obtain significantly improved bounds for the difference  $h - \hat{h}$ , which allows a much faster enumeration of the desired set of points.

Our approach is to use the standard decomposition of  $h(P) - \hat{h}(P)$  as a sum of local “height correction functions”. We study these functions carefully, which leads to efficient ways of computing them and to essentially optimal bounds. To get our polynomial-time algorithm, we have to avoid the factorization step needed to find the finite set of places where the correction might be nonzero. The main innovation is to replace factorization into primes by factorization into coprimes.

Most of our results are valid for more general fields with a set of absolute values satisfying the product formula.

*An errata was submitted on 30 Dec 2022 and posted [online](#) on 16 Feb 2023.*

1. Introduction	2154
<b>Part I. Generalities on heights and genus-2 Jacobians</b>	2159
2. Generalized naive heights	2159
3. Local height correction functions for genus-2 Jacobians	2162
4. Canonical local heights on Kummer coordinates	2169
5. Stably minimal Weierstrass models	2172
6. Igusa invariants	2175

*MSC2010:* primary 11G50; secondary 11G30, 11G10, 14G40, 14Q05, 14G05.

*Keywords:* canonical height, hyperelliptic curve, curve of genus 2, Jacobian surface, Kummer surface.

<b>Part II. Study of local height correction functions</b>	2177
7. The “kernel” of $\mu$	2177
8. Néron functions and reduction graphs	2182
9. Formulas and bounds for $\mu(P)$ in the nodal reduction case	2186
10. Formulas and bounds for $\mu(P)$ in the cuspidal reduction case	2192
11. General upper and lower bounds for $\bar{\beta}$	2202
<b>Part III. Efficient computation of canonical heights</b>	2205
12. Computing $\mu$ at nonarchimedean places	2206
13. Computing $\mu$ at archimedean places	2210
14. Computing the canonical height of rational points	2212
15. Examples	2218
<b>Part IV. Efficient search for points with bounded canonical height</b>	2221
16. Bounding the height difference at archimedean places	2221
17. Optimizing the naive height	2224
18. Efficient enumeration of points of bounded canonical height	2227
19. Example	2229
Acknowledgments	2232
References	2232

## 1. Introduction

Let  $K$  be a global field and let  $C/K$  be a curve of genus 2 with Jacobian variety  $J$ . There is a map  $\kappa : J \rightarrow \mathbb{P}^3$  that corresponds to the class of twice the theta divisor on  $J$ ; it identifies a point on  $J$  with its negative, and its image is the Kummer surface  $\text{KS}$  of  $J$ . Explicit versions of  $\kappa$  can be found in the book [Cassels and Flynn 1996] for  $C$  given in the form  $y^2 = f(x)$  and in the paper [Müller 2010] by the first author for general  $C$  (also in characteristic 2). Thus  $\kappa$  gives rise to a height function  $h : J(K) \rightarrow \mathbb{R}$ , which we call the *naive height* on  $J$ . It is defined by

$$h(P) = \sum_{v \in M_K} \log \max\{|\kappa_1(P)|_v, |\kappa_2(P)|_v, |\kappa_3(P)|_v, |\kappa_4(P)|_v\},$$

where  $\kappa(P) = (\kappa_1(P) : \kappa_2(P) : \kappa_3(P) : \kappa_4(P))$ ,  $M_K$  is the set of places of  $K$ , and  $|\cdot|_v$  is the  $v$ -adic absolute value, normalized so that the product formula holds:

$$\prod_{v \in M_K} |x|_v = 1 \quad \text{for all } x \in K^\times.$$

By general theory [Hindry and Silverman 2000, Chapter B] the limit

$$\hat{h}(P) = \lim_{n \rightarrow \infty} \frac{h(nP)}{n^2}$$

exists; it is called the *canonical height* (or *Néron–Tate height*) of  $P \in J(K)$ . The difference  $h - \hat{h}$  is bounded. The canonical height induces a positive definite quadratic form on  $J(K)/J(K)_{\text{tors}}$  (and on the  $\mathbb{R}$ -vector space  $J(K) \otimes_{\mathbb{Z}} \mathbb{R}$ ).

In this paper, we tackle the following two problems:

**Problem 1.1.** Find an efficient algorithm for the computation of  $\hat{h}(P)$  for a given point  $P \in J(K)$ .

**Problem 1.2.** Find an efficient algorithm for the enumeration of all  $P \in J(K)$  which satisfy  $\hat{h}(P) \leq B$ , where  $B$  is a given real number.

These problems are important because such algorithms are needed if we want to saturate a given finite-index subgroup of  $J(K)$  (see the discussion at the end of [Section 18](#)). This, in turn, is necessary for the computation of generators of  $J(K)$ . Such generators are required, for instance, to carry out the method described in [\[Bugeaud et al. 2008\]](#) for the computation of all integral points on a hyperelliptic curve over  $\mathbb{Q}$ . Furthermore, the regulator of  $J(K)$  appearing in the conjecture of Birch and Swinnerton-Dyer is the Gram determinant of a set of generators of  $J(K)/J(K)_{\text{tors}}$  with respect to the canonical height. So [Problems 1.1](#) and [1.2](#) are also important in the context of gathering numerical evidence for this conjecture as in [\[Flynn et al. 2001\]](#).

It is a classical fact, going back to work by Néron [\[1965\]](#), that  $\hat{h}(P)$  and the difference  $h(P) - \hat{h}(P)$  can be decomposed into a finite sum of local terms. In our situation, this can be done explicitly as follows. The duplication map  $P \mapsto 2P$  on  $J$  induces a morphism  $\delta: \text{KS} \rightarrow \text{KS}$ , given by homogeneous polynomials  $(\delta_1, \delta_2, \delta_3, \delta_4)$  of degree 4; explicit equations can again be found in [\[Cassels and Flynn 1996\]](#) and [\[Müller 2010\]](#). For a point  $Q \in J(K_v)$ , where  $K_v$  is the completion of  $K$  at a place  $v \in M_K$ , such that  $\kappa(Q) = (x_1 : x_2 : x_3 : x_4) \in \text{KS}(K_v)$ , we set

$$\tilde{\varepsilon}_v(Q) = -\log \max\{|\delta_j(x_1, x_2, x_3, x_4)|_v : 1 \leq j \leq 4\} + 4 \log \max\{|x_j|_v : 1 \leq j \leq 4\}.$$

Note that this does not depend on the scaling of the coordinates. We can then write  $\hat{h}(P)$  in the following form (compare [Lemma 2.4](#)):

$$\hat{h}(P) = h(P) - \sum_{v \in M_K} \sum_{n=0}^{\infty} 4^{-(n+1)} \tilde{\varepsilon}_v(2^n P).$$

We set, for  $Q \in J(K_v)$  as above,

$$\tilde{\mu}_v(Q) = \sum_{n=0}^{\infty} 4^{-(n+1)} \tilde{\varepsilon}_v(2^n Q), \tag{1-1}$$

and we deduce the decomposition

$$h(P) - \hat{h}(P) = \sum_{v \in M_K} \tilde{\mu}_v(P), \tag{1-2}$$

which is valid for all points  $P \in J(K)$ . In addition,  $\tilde{\varepsilon}_v = \tilde{\mu}_v = 0$  for all but finitely many  $v$  (the exceptions are among the places of bad reduction, the places where the given equation of  $C$  is not integral and the archimedean places). The maps  $\tilde{\varepsilon}_v : J(K_v) \rightarrow \mathbb{R}$  are continuous maps (with respect to the  $v$ -adic topology) with compact domains, so they are bounded. Therefore  $\tilde{\mu}_v$  is also bounded.

Let us first discuss [Problem 1.1](#). Because of (1-2), it suffices to compute  $h(P)$  (which is easy) and  $\sum_{v \in M_K} \tilde{\mu}_v(P)$  in order to compute  $\hat{h}(P)$  for a point  $P \in J(K)$ . Building on earlier work of Flynn and Smart [1997], the second author introduced an algorithm for the computation of  $\tilde{\mu}_v(P)$  in [Stoll 2002]. One of the main problems with this approach is that we need integer factorization to compute the sum  $\tilde{\mu}^f(P) := \sum_v \tilde{\mu}_v(P)$ , where  $v$  runs through the finite primes  $v$  such that  $\tilde{\mu}_v(P) \neq 0$ , because we need to find these primes, or at least a finite set of primes containing them.

We use an idea which was already exploited in [Müller and Stoll 2016] to obtain a polynomial-time algorithm for the computation of the canonical height of a point on an elliptic curve (in fact, we first used this technique in genus 2 and only later realized that it also works, and is actually easier to implement, for elliptic curves). When  $v$  is nonarchimedean, there is a constant  $c_v > 0$  such that the function

$$\mu_v := \tilde{\mu}_v / c_v$$

maps  $J(K_v)$  to  $\mathbb{Q}$ . More precisely,  $\tilde{\mu}^f(P)$  is a sum of rational multiples of logarithms of positive integers. As in [Müller and Stoll 2016], we find a bound on the denominator of  $\mu_v$  that depends only on the valuation of the discriminant; this allows us to devise an algorithm that computes  $\tilde{\mu}^f(P)$  in quasilinear time. We can compute  $\tilde{\mu}_v(P)$  for archimedean  $v$  essentially from the definition of  $\tilde{\mu}_v$ . This leads to a factorization-free algorithm that computes  $\hat{h}(P)$  in polynomial time:

**Theorem 1.3.** *Let  $J$  be the Jacobian of a curve of genus 2 defined over  $\mathbb{Q}$ , and let  $P \in J(\mathbb{Q})$ . There is an algorithm that computes  $\hat{h}(P)$  in time quasilinear in the size of the coordinates of  $P$  and the coefficients of the given equation of  $C$ , and quasiquadratic in the desired number of digits of precision.*

See [Theorem 14.5](#) for a precise statement. We expect a similar result to be true for any number field  $K$  in place of  $\mathbb{Q}$ .

We now move on to [Problem 1.2](#). If we have an upper bound  $\beta$  for  $h - \hat{h}$ , then the set of all points  $P \in J(K)$  such that  $h(P) \leq B + \beta$  contains the set  $\{P \in J(K) : \hat{h}(P) \leq B\}$ . Since the naive height  $h$  is a logarithmic height,  $\beta$  contributes exponentially to the size of the box we need to search for the enumeration. Therefore it is crucial to keep  $\beta$  as small as possible.

We write  $\tilde{\beta}_v = \max\{\tilde{\mu}_v(Q) : Q \in J(K_v)\}$ , and we obtain the bound

$$h(P) - \hat{h}(P) \leq \sum_{v \in M_K} \tilde{\beta}_v$$

from (1-2). If we write

$$\tilde{\gamma}_v = \max\{\tilde{\epsilon}_v(Q) : Q \in J(K_v)\},$$

then clearly  $\frac{1}{4}\tilde{\gamma}_v \leq \tilde{\beta}_v \leq \frac{1}{3}\tilde{\gamma}_v$ . In [Stoll 1999], it is shown that for curves given in the form  $y^2 = f(x)$ , where  $f$  has  $v$ -adically integral coefficients, we have

$$\tilde{\gamma}_v \leq -\log |2^4 \text{disc}(f)|_v = -\log |2^{-4} \Delta|_v,$$

with  $\text{disc}(f)$  denoting the discriminant of  $f$  considered as a polynomial of degree 6 and  $\Delta$  denoting the discriminant of the given equation of  $C$ . When  $v$  is nonarchimedean and the normalized additive valuation of  $\Delta$  is 1, we can take  $\tilde{\gamma}_v = \tilde{\beta}_v = 0$  [Stoll 2002].

The results of the present paper improve on this; they are based on a careful study of the functions  $\tilde{\mu}_v$ . It turns out that when  $v$  is nonarchimedean, the set of points where  $\mu_v$  (or equivalently,  $\tilde{\mu}_v$ ) vanishes forms a group. Moreover, the function  $\mu_v$  factors through the component group of the Néron model of  $J$  when the given model of  $C/K_v$ , which we assume to have  $v$ -integral coefficients in the following, has rational singularities; see Theorem 7.4. If the minimal proper regular model of  $C$  is semistable, then we can use results of Zhang [1993] and Heinz [2004] to give explicit formulas for  $\mu_v$  in terms of the resistance function on the reduction graph of  $C$  (which is essentially the dual graph of the special fiber of the minimal proper regular model, suitably metrized). We use this to find simple explicit formulas for  $\mu_v$  that apply in the most frequent cases of bad reduction, namely nodal or cuspidal reduction. These explicit formulas give us the optimal bounds for  $\tilde{\mu}_v$  in these cases. By reducing to the semistable case and tracking how  $\mu_v$  changes as we change the Weierstrass equation of  $C$ , we deduce the general upper bound

$$\tilde{\beta}_v \leq -\frac{1}{4} \log |\Delta|_v \tag{1-3}$$

for nonarchimedean  $v$ ; see Theorem 11.3.

When  $v$  is archimedean, we also get a new bound for  $\tilde{\mu}_v$  by iterating the bound obtained in [Stoll 1999], leading to vast improvements for  $\tilde{\beta}_v$ . Combining the archimedean and nonarchimedean bounds, we find a nearly optimal bound  $\beta$  for  $h - \hat{h}$ .

To get even smaller search spaces for the enumeration, we make use of the observation that we can replace the naive height  $h$  by any function  $h'$  such that  $|h' - h|$  is bounded. Using the results on nearly optimal bounds for  $\mu_v$  and such a modified naive height  $h'$  (which is also better suited than  $h$  for the enumeration process itself) we get a much smaller bound on the difference  $h' - \hat{h}$  than what was previously possible. This makes the enumeration feasible in many cases that were completely out of reach so far.

As an example, we compute explicit generators for the Mordell–Weil group of the Jacobian of the curve

$$C: y^2 = 82342800x^6 - 470135160x^5 + 52485681x^4 + 2396040466x^3 + 567207969x^2 - 985905640x + 247747600 \quad (1-4)$$

over  $\mathbb{Q}$ , conditional on the generalized Riemann hypothesis (which is needed to show that the rank is 22). See [Proposition 19.1](#). This curve has at least 642 rational points, which is the current record for the largest number of known rational points on a curve of genus 2; see [\[Stoll 2008\]](#).

The paper is divided into four parts. In [Part I](#), we first generalize the usual notion of the naive height on projective space and clarify the relation between these generalized naive heights and suitable canonical heights, all in [Section 2](#). We then introduce local height correction functions  $\varepsilon$  and  $\mu$  ( $= \mu_v$  in the notation introduced above) on the Jacobian of a genus-2 curve over a nonarchimedean local field in [Section 3](#). This is followed in [Section 4](#) by a study of certain canonical local heights constructed in terms of  $\mu$ . We close [Part I](#) by introducing and investigating the notion of stably minimal Weierstrass models of curves of genus 2 in [Section 5](#) and recalling some well-known results on Igusa invariants in [Section 6](#).

[Part II](#) is in some sense the central part of the present paper. Here we study the local height correction function  $\mu$  over a nonarchimedean local field. Using Picard functors, we show in [Section 7](#) that  $\mu$  factors through the component group of the Néron model of the Jacobian when the given model of the curve has rational singularities. We then relate  $\mu$  to the reduction graph of  $C$  in [Section 8](#). Building on this, the following sections contain simple explicit formulas for  $\mu$  when the reduction of the curve is nodal ([Section 9](#)), respectively cuspidal ([Section 10](#)). A simple argument then gives the improved general upper bound (1-3) for  $\mu$ ; see [Section 11](#).

In [Part III](#) we describe our factorization-free algorithm for the computation of  $\hat{h}(P)$  for  $P \in J(K)$ , where  $K$  is a global field. We start in [Section 12](#) by showing how to compute  $\mu_v(P)$  for nonarchimedean  $v$ , using a bound on its denominator. The following section deals with archimedean places, before we finally combine these results in [Section 14](#) into an algorithm for the computation of  $\hat{h}(P)$  that runs in polynomial time; this proves [Theorem 1.3](#). Some examples are discussed in [Section 15](#).

In [Part IV](#) we turn to [Problem 1.2](#). [Section 16](#) contains two methods for bounding  $\tilde{\mu}_v$  for archimedean  $v$ . In [Section 17](#) we describe a modified naive height  $h'$  such that the bound on the difference  $h' - \hat{h}$  becomes small. We use this, the results of [Section 16](#), and our nearly optimal bounds for the nonarchimedean height correction functions from [Part II](#) to give an efficient algorithm for the enumeration of the set of rational points with bounded canonical height in [Section 18](#). In [Section 19](#) we compute generators of the Mordell–Weil group of the record curve (1-4).

## Part I. Generalities on heights and genus-2 Jacobians

### 2. Generalized naive heights

Let  $K$  be a field with a set  $M_K$  of places  $v$  and associated absolute values  $|\cdot|_v$  satisfying the product formula

$$\prod_{v \in M_K} |x|_v = 1 \quad \text{for all } x \in K^\times.$$

We write  $K_v$  for the completion of  $K$  at  $v$ . For a tuple  $x = (x_1, \dots, x_m) \in K_v^m$  we set  $\|x\|_v = \max\{|x_1|_v, \dots, |x_m|_v\}$ .

In the following we will introduce some flexibility into our notion of height on projective spaces. (This is similar to the framework of “admissible families” in [Zarkhin 1995].)

**Definition 2.1.** (1) Let  $v \in M_K$ . A *local height function* on  $\mathbb{P}^m$  at  $v$  is a map  $h_v: K_v^{m+1} \setminus \{0\} \rightarrow \mathbb{R}$  such that

- (i)  $h_v(\lambda x) = \log |\lambda|_v + h_v(x)$  for all  $x \in K_v^{m+1} \setminus \{0\}$  and all  $\lambda \in K_v^\times$ , and
- (ii)  $|h_v(x) - \log \|x\|_v|$  is bounded.

(2) A function  $h: \mathbb{P}^m(K) \rightarrow \mathbb{R}$  is a *height* on  $\mathbb{P}^m$  over  $K$  if there are local height functions  $h_v$  such that for all  $x \in \mathbb{P}^m(K)$  we have

$$h((x_1 : x_2 : \dots : x_{m+1})) = \sum_{v \in M_K} h_v(x_1, x_2, \dots, x_{m+1})$$

and  $h_v(x) = \log \|x\|_v$  for all but finitely many places  $v$ .

Note that property (i) of local height functions together with the product formula imply that  $h$  is invariant under scaling of the coordinates and hence is well-defined.

One example of such a height is the standard height  $h_{\text{std}}$ , which we obtain by setting  $h_v(x) = \log \|x\|_v$  for all  $v$ . We then have the following simple fact.

**Lemma 2.2.** *Let  $h$  be any height on  $\mathbb{P}^m$  over  $K$  and let  $h_{\text{std}}$  be the standard height. Then there is a constant  $c = c(h)$  such that*

$$|h(P) - h_{\text{std}}(P)| \leq c \quad \text{for all } P \in \mathbb{P}^m(K).$$

*Proof.* This follows from property (ii) of local height functions and the requirement that  $h_v(x) = \log \|x\|_v$  for all but finitely many  $v$ . □

**Example 2.3.** Other examples of heights can be obtained in the following way. For each place  $v$ , fix a linear form  $l_v(x_1, \dots, x_{m+1}) = a_{v,1}x_1 + \dots + a_{v,m+1}x_{m+1}$ , with



$a_{v,1}, \dots, a_{v,m+1} \in K_v$  and  $a_{v,m+1} \neq 0$ , such that  $l_v(x) = x_{m+1}$  for all but finitely many  $v$ . Then

$$h((x_1 : \dots : x_m : x_{m+1})) = \sum_{v \in M_K} \log \max\{|x_1|_v, \dots, |x_m|_v, |l_v(x_1, \dots, x_{m+1})|_v\}$$

is a height on  $\mathbb{P}^m$ .

More generally, we could consider a family of automorphisms  $A_v$  of  $K_v^{m+1}$  with  $A_v$  equal to the identity for all but finitely many  $v$ , and take

$$h(x) = \sum_{v \in M_K} \log \max \|A_v(x)\|_v.$$

Now consider a projective variety  $V \subset \mathbb{P}_K^m$  and an endomorphism  $\varphi: V \rightarrow V$  of degree  $d$  (i.e., given by homogeneous polynomials of degree  $d$ ). Then by general theory (see, e.g., [Hindry and Silverman 2000, Theorem B.2.5])  $|h_{\text{std}}(\varphi(P)) - dh_{\text{std}}(P)|$  is bounded on  $V(K)$ . We write  $\varphi^{on}$  for the  $n$ -fold iteration of  $\varphi$ . Then the *canonical height*

$$\hat{h}(P) = \lim_{n \rightarrow \infty} d^{-n} h_{\text{std}}(\varphi^{on}(P))$$

exists (and satisfies  $\hat{h}(\varphi(P)) = d\hat{h}(P)$ ) [Hindry and Silverman 2000, Theorem B.4.1]. Let  $h$  be any height on  $\mathbb{P}^m$ . Since  $|h - h_{\text{std}}|$  is bounded, we can replace  $h_{\text{std}}$  by  $h$  in the definition of  $\hat{h}$  without changing the result. We can then play the usual telescoping series trick in our more general setting.

**Lemma 2.4.** *Let*

$$\varphi((x_1 : \dots : x_{m+1})) = (\varphi_1(x) : \dots : \varphi_{m+1}(x))$$

*with homogeneous polynomials  $\varphi_j \in K[x_1, \dots, x_{m+1}]$  of degree  $d$ . We have*

$$\hat{h}(P) = h(P) - \sum_{v \in M_K} \tilde{\mu}_v(P),$$

*where*

$$\tilde{\mu}_v(P) = \sum_{n=0}^{\infty} d^{-(n+1)} \tilde{\varepsilon}_v(\varphi^{on}(P))$$

*and, when  $P = (x_1 : \dots : x_{m+1})$  and  $x = (x_1, \dots, x_{m+1})$ ,*

$$\tilde{\varepsilon}_v(P) = dh_v(x) - h_v(\varphi_1(x), \dots, \varphi_{m+1}(x)).$$

*Proof.* Note that  $\tilde{\varepsilon}_v$  is well-defined: scaling  $x$  by  $\lambda$  adds  $|\lambda|_v$  to  $h_v(x)$  and  $d|\lambda|_v$  to  $h_v(\varphi_1(x), \dots, \varphi_{m+1}(x))$ . Let  $x$  be projective coordinates for  $P$  and write  $x^{(n)}$  for

the result of applying  $(\varphi_1, \dots, \varphi_{m+1})$   $n$  times to  $x = x^{(0)}$ . Then

$$\begin{aligned} \hat{h}(P) &= \lim_{n \rightarrow \infty} d^{-n} h(\varphi^{\circ n}(P)) \\ &= h(P) + \sum_{n=0}^{\infty} d^{-(n+1)} (h(\varphi^{\circ(n+1)}(P)) - dh(\varphi^{\circ n}(P))) \\ &= h(P) + \sum_{n=0}^{\infty} d^{-(n+1)} \sum_{v \in M_K} (h_v(x^{(n+1)}) - dh_v(x^{(n)})) \\ &= h(P) - \sum_{v \in M_K} \sum_{n=0}^{\infty} d^{-(n+1)} \tilde{\varepsilon}_v(\varphi^{\circ n}(P)) \\ &= h(P) - \sum_{v \in M_K} \tilde{\mu}_v(P). \end{aligned} \quad \square$$

We call the functions  $\tilde{\mu}_v : \mathbb{P}^m(K_v) \rightarrow \mathbb{R}$  *local height correction functions*.

Note that when  $K_v$  is a discretely valued field such that  $|x|_v = \exp(-c_v v(x))$  for  $x \in K^\times$  with a constant  $c_v > 0$  (and where we abuse notation and write  $v : K_v^\times \rightarrow \mathbb{Z}$  also for the normalized additive valuation associated to the place  $v$ ) and  $h = h_{\text{std}}$ , then we have

$$\tilde{\mu}_v(P) = c_v \mu_v(P) \quad \text{and} \quad \tilde{\varepsilon}_v(P) = c_v \varepsilon_v(P),$$

where

$$\mu_v(P) = \sum_{n=0}^{\infty} d^{-(n+1)} \varepsilon_v(P)$$

and

$$\varepsilon_v(P) = \min\{v(\varphi_1(x)), \dots, v(\varphi_{m+1}(x))\} - d \min\{v(x_1), \dots, v(x_{m+1})\},$$

if  $x = (x_1, \dots, x_{m+1})$  are homogeneous coordinates for  $P$ . This is the situation that we will study in some detail in [Part II](#) of this paper, for the special case when  $V \subset \mathbb{P}^3$  is the Kummer surface associated to a curve of genus 2 and its Jacobian  $J$  and  $\varphi$  is the duplication map (then  $d = 4$ ).

To deal with [Problem 1.1](#), we work with the standard height  $h_{\text{std}}$ . We use our detailed results on the local height correction functions to deduce a bound on the denominator of  $\mu_v$  (its values are rational) in terms of the valuation of the discriminant of the curve. This is the key ingredient that leads to our new factorization-free and fast algorithm for computing  $\hat{h}$ ; see [Part III](#).

To deal with [Problem 1.2](#), we use the flexibility in choosing the (naive) height  $h$  and modify the standard height in such a way that the sum  $\sum_{v \in M_K} \sup \tilde{\mu}_v(J(K_v))$  that bounds the difference  $h - \hat{h}$  is as small as we can make it. The local height functions we use are as in [Example 2.3](#) above, with  $l_v(x_1, x_2, x_3, x_4) = x_4/s_v$  for

certain  $s_v \in K_v^\times$  in most cases. Every height function of this type has the property that for any point  $P = (x_1 : x_2 : x_3 : x_4) \in \mathbb{P}^3(K)$  different from  $(0 : 0 : 0 : 1)$  we have

$$0 \leq h_{\text{std}}((x_1 : x_2 : x_3)) \leq h(P).$$

This is relevant, since we can fairly easily enumerate all points  $P$  as above that are on the Kummer surface and satisfy  $h_{\text{std}}((x_1 : x_2 : x_3)) \leq B$ ; see [Part IV](#). Refinements of the standard height constructed using Arakelov theory were also used by Holmes [\[2014\]](#) to give an “in principle” algorithm for the enumeration of points of bounded canonical height on Jacobians of hyperelliptic curves over global fields.

### 3. Local height correction functions for genus-2 Jacobians

Until further notice, we let  $k$  be a nonarchimedean local field with additive valuation  $v$ , normalized to be surjective onto  $\mathbb{Z}$ . Let  $\mathcal{O}$  denote the valuation ring of  $k$  with residue class field  $\mathfrak{k}$  and let  $\pi$  be a uniformizing element of  $\mathcal{O}$ . We consider a smooth projective curve  $C$  of genus 2 over  $k$ , given by a Weierstrass equation

$$Y^2 + H(X, Z)Y = F(X, Z) \tag{3-1}$$

in weighted projective space  $\mathbb{P}_k(1, 3, 1)$ , with weights 1, 3 and 1 assigned to the variables  $X$ ,  $Y$  and  $Z$ , respectively. Here

$$F(X, Z) = f_0Z^6 + f_1XZ^5 + f_2X^2Z^4 + f_3X^3Z^3 + f_4X^4Z^2 + f_5X^5Z + f_6X^6$$

and

$$H(X, Z) = h_0Z^3 + h_1XZ^2 + h_2X^2Z + h_3X^3$$

are binary forms of degrees 6 and 3, respectively, such that the discriminant  $\Delta(F, H)$  of the Weierstrass equation [\(3-1\)](#) is nonzero. In characteristic different from 2, this discriminant is defined as

$$\Delta(F, H) = 2^{-12} \text{disc}(4F + H^2) \in \mathbb{Z}[h_0, \dots, h_3, f_0, \dots, f_6],$$

and in general, we define it by the generic polynomial given by this formula. The curve defined by the equation is smooth if and only if  $\Delta(F, H) \neq 0$ .

For the remainder of this section we assume that  $F, H \in \mathcal{O}[X, Z]$ , so that [\(3-1\)](#) defines an *integral Weierstrass model*  $\mathcal{C}$  of the curve in the terminology of [Section 5](#) below. The discriminant of this model is then defined to be  $\Delta(\mathcal{C}) := \Delta(F, H)$ . We may assume that  $C$  is given by such an integral equation if  $k$  is the completion at a nonarchimedean place of a number field  $K$  and  $C$  is obtained by base change from  $K$ , since we can choose a globally integral Weierstrass equation for the curve. But also in general, we can always assume that  $C$  is given by an integral equation after applying a transformation defined over  $k$ , since we know from [Corollary 4.6](#) in

the next section how the local height correction function  $\mu$  defined in [Definition 3.1](#) below behaves under such transformations.

We now generalize the definition of  $\varepsilon$  given in [\[Stoll 2002\]](#) (where the author works with Weierstrass equations that have  $H = 0$ ) to our more general setting. As in the [Introduction](#), let  $J$  denote the Jacobian of  $C$  and let KS be its Kummer surface, constructed explicitly together with an explicit embedding into  $\mathbb{P}^3$  in [\[Cassels and Flynn 1996\]](#) in the case  $H = 0$  and in [\[Müller 2010\]](#) in the general case. Also let  $\kappa : J \rightarrow \mathbb{P}^3$  denote the composition of the quotient map from  $J$  to KS with this embedding; it maps the origin  $O \in J(k)$  to the point  $(0 : 0 : 0 : 1)$ . A quadruple  $x = (x_1, x_2, x_3, x_4) \in k^4$  is called a set of *Kummer coordinates* on KS if  $x$  is a set of projective coordinates for a point in  $\text{KS}(k)$ ; we denote the set of sets of Kummer coordinates on KS by  $\text{KS}_{\mathbb{A}}$  (this is the set of  $k$ -rational points on the pointed affine cone over KS). For  $x \in \text{KS}_{\mathbb{A}}$  we write  $v(x) = \min\{v(x_1), \dots, v(x_4)\}$ , and we say that  $x$  is *normalized* if  $v(x) = 0$ . If  $P \in J(k)$ , we say that  $x \in \text{KS}_{\mathbb{A}}$  is a set of *Kummer coordinates for P* if  $\kappa(P) = (x_1 : x_2 : x_3 : x_4)$ .

We let  $\delta$  denote the duplication map on KS, which is given by homogeneous polynomials  $\delta_1, \dots, \delta_4 \in \mathcal{O}[x_1, \dots, x_4]$  of degree 4 such that  $\delta(0, 0, 0, 1) = (0, 0, 0, 1)$ . We recall that there is a symmetric matrix  $B = (B_{ij})_{1 \leq i, j \leq 4}$  of polynomials that are bihomogeneous of degree 2 in  $x_1, \dots, x_4$  and also in  $y_1, \dots, y_4$  and have coefficients in  $\mathcal{O}$ . They have the following properties; see Chapter 3 of [\[Cassels and Flynn 1996\]](#) and [\[Müller 2010\]](#).

- (i) Let  $x, y \in \text{KS}_{\mathbb{A}}$  be Kummer coordinates for  $P, Q \in J(k)$ . Then there are Kummer coordinates  $w, z \in \text{KS}_{\mathbb{A}}$  for  $P + Q$  and  $P - Q$ , respectively, such that

$$w * z := (w_i z_j + n_{ij} w_j z_i)_{1 \leq i, j \leq 4} = B(x, y)$$

and hence  $v(w) + v(z) = v(B(x, y))$ ; here  $n_{ij} = 1$  if  $i \neq j$  and  $n_{ij} = 0$  if  $i = j$ .

- (ii) If  $x \in \text{KS}_{\mathbb{A}}$ , then  $B(x, x) = \delta(x) * (0, 0, 0, 1)$ .

We specialize the notions introduced in [Section 2](#) to our situation: we consider the Kummer surface  $\text{KS} \subset \mathbb{P}^3$  with the duplication map  $\delta$  of degree  $d = 4$ . We use the standard local height on  $\mathbb{P}^3$ .

**Definition 3.1.** Let  $x \in \text{KS}_{\mathbb{A}}$  be a set of Kummer coordinates on KS. Then we set

$$\varepsilon(x) = v(\delta(x)) - 4v(x) \in \mathbb{Z} \quad \text{and} \quad \mu(x) = \sum_{n=0}^{\infty} \frac{1}{4^{n+1}} \varepsilon(\delta^{on}(x)),$$

where  $\delta^{on}$  denotes the  $n$ -fold composition  $\delta \circ \dots \circ \delta$ .

Because  $\delta$  is given by homogeneous polynomials of degree 4,  $\varepsilon(x)$  does not depend on the scaling of  $x$ , so it makes sense to define  $\varepsilon(P) = \varepsilon(x)$  for points  $P \in \text{KS}(k)$ , where  $x \in \text{KS}_{\mathbb{A}}$  is any set of Kummer coordinates for  $P$ , and to define

$\varepsilon(P) = \varepsilon(\kappa(P))$  for points  $P \in J(k)$ . We likewise extend the definition of  $\mu$ . Then we have

$$\mu(2P) - 4\mu(P) = -\varepsilon(P) \quad \text{for all } P \in J(k).$$

Note that our assumption  $F, H \in \mathcal{O}[X, Z]$  implies that  $\varepsilon \geq 0$ . If  $k$  is a local field (as we assume here), then  $\text{KS}(k)$  is compact in the  $v$ -adic topology, and  $\varepsilon$  is continuous, so  $\varepsilon$  is bounded.

**Remark 3.2.** More generally, if  $k$  is a field with a discrete valuation and not of characteristic 2, then the arguments in [Stoll 1999] show that when  $H = 0$ ,  $\varepsilon \leq v(2^4 \text{disc}(F))$ , so  $\varepsilon$  is bounded also for these more general fields.

If  $k$  is any field with a discrete valuation, then one can still conclude that  $\varepsilon$  is bounded, by making use of the fact that the duplication map is well-defined on  $\text{KS}$ , which implies that the ideal generated by the  $\delta_j$  and the polynomial  $\delta_0$  defining  $\text{KS}$  contains a power of the irrelevant ideal. So for some  $N > 0$ , one can express every  $x_j^N$  as a linear combination of  $\delta_0(x), \dots, \delta_4(x)$  with coefficients that are homogeneous polynomials of degree  $N - 4$  with coefficients in  $k$ . The negative of the minimum of the valuations of these coefficients then gives a bound for  $\varepsilon$ .

**Remark 3.3.** If  $k$  is the completion of a global field at a place  $v$ , then for  $\alpha \in k^\times$ ,  $v(\alpha)/\log \|\alpha\|_v = -c_v$  is a negative constant. So for  $P \in J(k)$  we have  $\varepsilon(P) = c_v \tilde{\varepsilon}_v(P)$  and  $\mu(P) = c_v \tilde{\mu}_v(P)$ , where  $\tilde{\varepsilon}_v$  and  $\tilde{\mu}_v$  are as defined in the introduction.

We will also have occasion to use the following function. Let  $x, y \in \text{KS}_{\mathbb{A}}$  and define

$$\varepsilon(x, y) = v(B(x, y)) - 2v(x) - 2v(y). \tag{3-2}$$

In the same way as for  $\varepsilon(x)$  above, we can extend this to points in  $\text{KS}(k)$  and  $J(k)$ .

**Lemma 3.4.** *Let  $x, y, w, z \in \text{KS}_{\mathbb{A}}$  be Kummer coordinates satisfying  $w * z = B(x, y)$ . Then we have*

$$\delta(w) * \delta(z) = B(\delta(x), \delta(y)).$$

*Proof.* The proof carries over verbatim from the proof of [Stoll 2002, Lemma 3.2]. □

We deduce the following:

**Lemma 3.5.** *Let  $x, y, w, z \in \text{KS}_{\mathbb{A}}$  be Kummer coordinates satisfying  $w * z = B(x, y)$ . Then we have*

$$\varepsilon(\delta(x), \delta(y)) + 2\varepsilon(x) + 2\varepsilon(y) = \varepsilon(w) + \varepsilon(z) + 4\varepsilon(x, y).$$

*Proof.* Using Lemma 3.4, relation (3-2), and property (i) above for  $\delta(w), \delta(z), \delta(x)$  and  $\delta(y)$ , we obtain

$$v(\delta(w)) + v(\delta(z)) = v(B(\delta(x), \delta(y))) = \varepsilon(\delta(x), \delta(y)) + 2v(\delta(x)) + 2v(\delta(y)).$$

Subtracting four times the corresponding relation for  $w, z, x$  and  $y$ , we get

$$\varepsilon(w) + \varepsilon(z) = \varepsilon(\delta(x), \delta(y)) - 4\varepsilon(x, y) + 2\varepsilon(x) + 2\varepsilon(y),$$

which is the claim. □

We state a few general facts on the functions  $\varepsilon$  and  $\mu$ .

**Lemma 3.6.** *For points  $P, Q \in J(k)$ , we have the relation*

$$\mu(P + Q) + \mu(P - Q) - 2\mu(P) - 2\mu(Q) = -\varepsilon(P, Q).$$

*Proof.* Let  $x$  and  $y$  be Kummer coordinates for  $P$  and  $Q$ , respectively; then  $w$  and  $z$  as in Lemma 3.5 are Kummer coordinates for  $P + Q$  and  $P - Q$  (in some order). The claim now follows from the formula in Lemma 3.5:

$$\begin{aligned} &\mu(P + Q) + \mu(P - Q) - 2\mu(P) - 2\mu(Q) \\ &= \sum_{n=0}^{\infty} 4^{-n-1} (\varepsilon(2^n P + 2^n Q) + \varepsilon(2^n P - 2^n Q) - 2\varepsilon(2^n P) - 2\varepsilon(2^n Q)) \\ &= \sum_{n=0}^{\infty} 4^{-n-1} (\varepsilon(\delta^{on}(w)) + \varepsilon(\delta^{on}(z)) - 2\varepsilon(\delta^{on}(x)) - 2\varepsilon(\delta^{on}(y))) \\ &= \sum_{n=0}^{\infty} 4^{-n-1} (\varepsilon(\delta^{\circ(n+1)}(x), \delta^{\circ(n+1)}(y)) - 4\varepsilon(\delta^{on}(x), \delta^{on}(y))) \\ &= -\varepsilon(x, y) = -\varepsilon(P, Q). \end{aligned} \quad \square$$

**Lemma 3.7.** *If  $P \in J(k)$  satisfies  $\mu(P) = 0$ , then  $\mu(P + Q) = \mu(Q)$  for all  $Q \in J(k)$ .*

*Proof.* We apply Lemma 3.6 with  $P$  and  $Q$  replaced by  $Q + nP$  and  $P$ , respectively, where  $n \in \mathbb{Z}$ . Taking into account that  $\mu(P) = 0$  and writing  $a_n$  for  $\mu(Q + nP)$ , this gives

$$a_{n+1} - 2a_n + a_{n-1} = -\varepsilon(P, Q + nP).$$

As  $k$  is a nonarchimedean local field, the multiples of  $P$  accumulate at the origin  $O$  in  $J(k)$ . Recall that  $\varepsilon$  is locally constant. This implies that every value  $\varepsilon(P, Q + nP)$  occurs for infinitely many  $n \in \mathbb{Z}$ , since  $Q + (n + N)P$  will be close to  $Q + nP$  for suitably chosen  $N$ . We have for any  $m > 0$

$$a_{m+1} - a_m - a_{-m} + a_{-m-1} = \sum_{n=-m}^m (a_{n+1} - 2a_n + a_{n-1}) = -\sum_{n=-m}^m \varepsilon(P, Q + nP).$$

Since  $\mu$  is bounded, the left-hand side is bounded independently of  $m$ . We also know that  $\varepsilon(P, Q + nP) \geq 0$ . But if  $\varepsilon(P, Q + nP)$  were nonzero for some  $n$ , then by the discussion above, the right-hand side would be unbounded as  $m \rightarrow \infty$ .

Therefore it follows that  $\varepsilon(P, Q + nP) = 0$  for all  $n \in \mathbb{Z}$ . This in turn implies  $a_{n+1} - 2a_n + a_{n-1} = 0$  for all  $n \in \mathbb{Z}$ . The only bounded solutions of this recurrence are constant sequences. In particular, we have

$$\mu(P + Q) = a_1 = a_0 = \mu(Q). \quad \square$$

**Proposition 3.8.** *The subset  $U = \{P \in J(k) : \mu(P) = 0\}$  is a subgroup of finite index in  $J(k)$ . The functions  $\varepsilon$  and  $\mu$  factor through the quotient  $J(k)/U$ .*

*Proof.* Lemma 3.7 shows that  $U$  is a subgroup. We have  $\varepsilon(P) = 0$  for  $P \in J(k)$  sufficiently close to the origin. So taking a sufficiently small subgroup neighborhood  $U'$  of the origin in  $J(k)$ , we see that  $\varepsilon(2^n P) = 0$  for all  $P \in U'$  and all  $n \geq 0$ . This implies that  $\mu = 0$  on  $U'$ , so  $U \supset U'$ . Because  $k$  is a local field,  $U'$  and therefore also  $U$  have finite index in  $J(k)$ . By Lemma 3.7 again,  $\mu$  factors through  $J(k)/U$ , and since  $\varepsilon(P) = 4\mu(P) - \mu(2P)$ , the same is true for  $\varepsilon$ .  $\square$

We will now show that we actually have

$$U = \{P \in J(k) : \varepsilon(P) = 0\}$$

(the inclusion “ $\subset$ ” is clear from the definition and Proposition 3.8). This is equivalent to the implication  $\varepsilon(x) = 0 \Rightarrow \varepsilon(\delta(x)) = 0$  and generalizes [Stoll 2002, Theorem 4.1]. For this we first provide a characteristic-2 analogue of Proposition 3.1(1) of the same paper.

We temporarily let  $k$  denote an arbitrary field. Let  $C_{F,H}$  be a (not necessarily smooth) curve in the weighted projective plane with respective weights 1, 3, 1 assigned to the variables  $X, Y, Z$  that is given by an equation

$$Y^2 + H(X, Z)Y = F(X, Z), \tag{3-3}$$

where  $F, H \in k[X, Z]$  are binary forms of respective degrees 6 and 3. Let  $\text{KS}_{F,H}$  denote the subscheme of  $\mathbb{P}^3$  given by the vanishing of the equation defining the Kummer surface of  $C_{F,H}$  if  $C_{F,H}$  is nonsingular. Then the construction of  $\delta = (\delta_1, \delta_2, \delta_3, \delta_4)$  still makes sense in this context, but we may now have  $\delta_i(x) = 0$  for all  $1 \leq i \leq 4$  (which we abbreviate by  $\delta(x) = 0$ ) for a set  $x$  of Kummer coordinates on  $\text{KS}_{F,H}$ . We generalize Proposition 3.1 in [Stoll 2002] (which assumes  $H = 0$ ) to the case considered here.

Note that two equations (3-3) for  $C_{F,H}$  are related by a transformation  $\tau$  acting on an affine point  $(\xi, \eta)$  by

$$\tau(\xi, \eta) = \left( \frac{a\xi + b}{c\xi + d}, \frac{e\eta + U(\xi, 1)}{(c\xi + d)^3} \right), \tag{3-4}$$

type	$H$	$F$	conditions
1	0	0	
2	$Z^3$	0	
3	$Z^3$	$aXZ^5$	$a \neq 0$
4	$XZ^2$	$aXZ^5$	$a \neq 0$
5	$XZ^2$	$bX^3Z^3$	$b \neq 0$
6	$Z^3$	$aXZ^5 + bX^3Z^3$	$ab \neq 0$
7	$XZ^2$	0	
8	$XZ(X + Z)$	0	
9	$XZ(X + Z)$	$bX^3Z^3$	$b(b + 1) \neq 0$
10	$XZ(X + Z)$	$aXZ^5 + bX^3Z^3$	$a(a + b)(a + b + 1) \neq 0$
11	$XZ^2$	$aXZ^5 + bX^3Z^3$	$ab \neq 0$
12	0	$XZ^5$	
13	0	$X^3Z^3$	

**Table 1.** Representatives in characteristic 2.

where  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(k)$ ,  $e \in k^\times$  and  $U \in k[X, Z]$  is homogeneous of degree 3. The transformation  $\tau$  also acts on the forms  $F$  and  $H$  by

$$\begin{aligned} \tau^*F(X, Z) &= (ad - bc)^{-6}(e^2F^A + (eH^A - U^A)U^A), \\ \tau^*H(X, Z) &= (ad - bc)^{-3}(eH^A - 2U^A), \end{aligned}$$

where we write

$$S^A = S(dX - bZ, -cX + aZ)$$

for a binary form  $S \in k[X, Z]$ .

**Lemma 3.9.** *Let  $x \in \text{KS}_{F,H}(k)$ . If  $\delta(\delta(x)) = 0$ , then we already have  $\delta(x) = 0$ .*

*Proof.* If  $k$  has characteristic different from 2, we can apply a transformation so that the new Weierstrass equation will have  $H = 0$ ; the statement is then [Stoll 2002, Proposition 3.1(1)]. So from now on,  $k$  has characteristic 2. We may assume without loss of generality that  $k$  is algebraically closed. If the given curve is smooth, then the result is obvious, because the situation described in the statement can never occur. If it is not smooth, we can act on  $F$  and  $H$  using transformations of the form (3-4), so it is enough to consider only one representative of each orbit under such transformations. This is analogous to the strategy in the proof of [Stoll 2002, Proposition 3.1]. We can, for example, pick the representatives listed in Table 1.

For these representatives, elementary methods as in that proof can be used to check that  $\delta(x) = 0$  indeed follows from  $\delta(\delta(x)) = 0$ . □

We can use the above to analyze the group  $U$ .



**Theorem 3.10.** *Suppose that  $k$  is a nonarchimedean local field and that  $J$  is the Jacobian of a smooth projective curve of genus 2, given by a Weierstrass equation (3-1) with integral coefficients. Then the set  $\{P \in J(k) : \varepsilon(P) = 0\}$  equals the subgroup  $U$  in Proposition 3.8. In particular,  $U$  is a subgroup of finite index in  $J(k)$  and  $\varepsilon$  and  $\mu$  factor through the quotient  $J(k)/U$ . Moreover we have that  $\varepsilon(-P) = \varepsilon(P)$  and  $U$  contains the kernel of reduction  $J(k)^1$  with respect to the given model of  $J$ , i.e., the subgroup of points whose image in  $\text{KS}(\mathfrak{k})$  equals that of  $O$ .*

*Proof.* The statement in Lemma 3.9 implies  $\varepsilon(P) = 0 \Rightarrow \varepsilon(2P) = 0$  for points  $P \in J(k)$ , since  $\varepsilon(P) = 0$  is equivalent to  $\delta(\tilde{x}) \neq 0$  if  $x$  are normalized Kummer coordinates for  $P$ , with reduction  $\tilde{x}$ . This shows that  $\varepsilon(P) = 0$  implies  $\mu(P) = 0$  (and conversely), so  $\{P \in J(k) : \varepsilon(P) = 0\} = \{P \in J(k) : \mu(P) = 0\} = U$ . The remaining statements now are immediate from Proposition 3.8, taking into account that, for  $P$  in the kernel of reduction, we trivially have  $\varepsilon(P) = 0$ . □

An algorithm for the computation of  $\mu(P)$  which is based on Theorem 3.10 (for  $H = 0$ ) is given in [Stoll 2002, §6]. Using the relation in Lemma 3.6, we obtain the following alternative procedure for computing  $\mu(P)$ .

1. Let  $x$  be normalized Kummer coordinates for  $P$ . Set  $y_0 = (0, 0, 0, 1)$  and  $y_1 = x$ .
2. For  $n = 1, 2, \dots$ , do the following.
  - a. Using pseudoaddition (see [Flynn and Smart 1997, §4]), compute normalized Kummer coordinates  $y_{n+1}$  for  $nP$  from  $x, y_{n-1}$  and  $y_n$ ; record  $\varepsilon(P, nP)$ , which is the shift in valuation occurring when normalizing  $y_{n+1}$ .
  - b. If  $\varepsilon(P, nP) = 0$ , check whether  $v(\delta(y_n)) = 0$  (by Theorem 3.10, this is equivalent to  $nP \in U$ ). If yes, let  $N = n$  and exit the loop.
3. Return

$$\mu(P) = \frac{1}{2N} \sum_{n=1}^{N-1} \varepsilon(P, nP).$$

To see that this works, note that by Lemma 3.6 we have

$$\mu((n + 1)P) - 2\mu(nP) + \mu((n - 1)P) = 2\mu(P) - \varepsilon(P, nP).$$

The sequence  $(\mu(nP))_{n \in \mathbb{Z}}$  is periodic with period  $N$ , where  $N$  is the smallest positive integer  $n$  such that  $nP \in U$  (which exists according to Theorem 3.10). Taking the sum over one period gives

$$2N\mu(P) = \sum_{n=0}^{N-1} \varepsilon(P, nP) = \sum_{n=1}^{N-1} \varepsilon(P, nP).$$

From the periodicity we can also deduce the possible denominators of  $\mu(P)$ . As  $\varepsilon$  has integral values, we see that  $\mu(P) \in \frac{1}{2N}\mathbb{Z}$  if  $N$  is a period of  $(\mu(nP))_{n \in \mathbb{Z}}$ . In fact, we can show a little bit more.

**Corollary 3.11.** *Let  $P \in J(k)$  and  $N = \min\{n \in \mathbb{Z}_{>0} : \mu(nP) = 0\}$ . Then*

$$\mu(P) \in \begin{cases} \frac{1}{N}\mathbb{Z} & \text{if } N \text{ is odd,} \\ \frac{1}{2N}\mathbb{Z} & \text{if } N \text{ is even.} \end{cases}$$

*Proof.* The sequence  $(\varepsilon(P, nP))_{n \in \mathbb{Z}}$  has period  $N$  and is symmetric. So if  $N$  is odd, we actually have

$$\mu(P) = \frac{1}{2N} \sum_{n=1}^{N-1} \varepsilon(P, nP) = \frac{1}{N} \sum_{n=1}^{\frac{1}{2}(N-1)} \varepsilon(P, nP) \in \frac{1}{N}\mathbb{Z}. \quad \square$$

Analyzing the possible denominators of  $\mu(P)$  will play a key role in [Section 12](#), where we discuss another algorithm for the computation of  $\mu(P)$ .

#### 4. Canonical local heights on Kummer coordinates

We now define a notion of canonical local height for Kummer coordinates. We keep the notation of the previous section.

**Definition 4.1.** Let  $x \in \text{KS}_{\mathbb{A}}$  be a set of Kummer coordinates on KS. The *canonical local height* of  $x$  is given by

$$\hat{\lambda}(x) = -v(x) - \mu(x).$$

**Remark 4.2.** We can also define the canonical local height on an archimedean local field in an analogous way. Then, if  $K$  is a global field and  $x$  is a set of Kummer coordinates for a point  $J(K)$ , we have

$$\hat{h}(P) = \sum_{v \in M_K} \frac{1}{c_v} \hat{\lambda}_v(x),$$

where  $c_v$  is the constant introduced in [Remark 3.3](#) for a nonarchimedean place  $v$  and  $c_v = [K_v : \mathbb{R}]^{-1}$  if  $v$  is archimedean.

The canonical local height  $\hat{\lambda}$  on Kummer coordinates has somewhat nicer properties than the canonical local height defined (for instance, in [\[Flynn and Smart 1997\]](#) or, more generally, in [\[Hindry and Silverman 2000, §B.9\]](#)) with respect to a divisor on  $J$ .

**Proposition 4.3.** *Let  $x, y, z, w \in \text{KS}_{\mathbb{A}}$ . Then the following hold:*

- (i)  $\hat{\lambda}(\delta(x)) = 4\hat{\lambda}(x)$ .

- (ii) If  $w * z = B(x, y)$ , then  $\hat{\lambda}(z) + \hat{\lambda}(w) = 2\hat{\lambda}(x) + 2\hat{\lambda}(y)$ .
- (iii)  $\hat{\lambda}(x) = -\lim_{n \rightarrow \infty} 4^{-n} v(\delta^{on}(x))$ .
- (iv) If  $k'/k$  is a finite extension of ramification index  $e$  and  $\hat{\lambda}'$  is the canonical local height over  $k'$ , then we have  $\hat{\lambda}'(x) = e \cdot \hat{\lambda}(x)$ .

*Proof.* (i) This follows easily from the two relations

$$v(\delta(x)) = 4v(x) + \varepsilon(x) \quad \text{and} \quad \mu(\delta(x)) = 4\mu(x) - \varepsilon(x).$$

(ii) This is similar, using [Lemma 3.6](#) and  $\varepsilon(x, y) = v(w) + v(z) - 2v(x) - 2v(y)$ .

(iii) This follows from (i) and the fact that  $\mu(x)$  is a bounded function, implying

$$\hat{\lambda}(x) = 4^{-n} \hat{\lambda}(\delta^{on}(x)) = -4^{-n} v(\delta^{on}(x)) + O(4^{-n}).$$

(iv) This is obvious from the definition of  $\hat{\lambda}$ . □

The canonical local height on Kummer coordinates also behaves well under isogenies.

**Proposition 4.4.** *Let  $C$  and  $C'$  be two curves of genus 2 over  $k$  given by Weierstrass equations, with associated Jacobians  $J$  and  $J'$ , Kummer surfaces  $\text{KS}$  and  $\text{KS}'$  and sets of sets of Kummer coordinates  $\text{KS}_{\mathbb{A}}$  and  $\text{KS}'_{\mathbb{A}}$ , respectively. Let  $\alpha: J \rightarrow J'$  be an isogeny defined over  $k$ . Then  $\alpha$  induces a map  $\alpha: \text{KS} \rightarrow \text{KS}'$ ; let  $d$  denote its degree. We also get a well-defined induced map  $\alpha: \text{KS}_{\mathbb{A}} \rightarrow \text{KS}'_{\mathbb{A}}$  if we fix  $a \in k^\times$  and require  $\alpha(0, 0, 0, 1) = (0, 0, 0, a)$ . Then we have*

$$\hat{\lambda}(\alpha(x)) = d\hat{\lambda}(x) - v(a) \quad \text{for all } x \in \text{KS}_{\mathbb{A}}.$$

*Proof.* All assertions except for the last one are obvious. By the definition of  $\hat{\lambda}$ , we can reduce to the case  $a = 1$ . Using part (iii) of [Proposition 4.3](#) it is then enough to show that

$$v(\delta^{on}(\alpha(x))) = dv(\delta^{on}(x)) + O(1).$$

However, we have  $v(\alpha(x)) - dv(x) = O(1)$  by assumption, so it suffices to show that

$$v(\delta^{on}(\alpha(x))) = v(\alpha(\delta^{on}(x))). \tag{4-1}$$

But since  $\alpha: J \rightarrow J'$  is an isogeny,  $\delta^{on}(\alpha(x))$  and  $\alpha(\delta^{on}(x))$  represent the same point on  $\text{KS}'$ , hence they are projectively equal. Because they also have the same degree, the factor of proportionality is independent of  $x$ . It therefore suffices to check (4-1) for a single  $x$ ; we take  $x = (0, 0, 0, 1) \in \text{KS}_{\mathbb{A}}$ . Because we have  $\delta(x) = x$  and, by assumption,  $\alpha(x) = x'$ , where  $x' = (0, 0, 0, 1) \in \text{KS}'_{\mathbb{A}}(k)$ , we find

$$\delta^{on}(\alpha(x)) = x' \quad \text{and} \quad \alpha(\delta^{on}(x)) = x',$$

thereby proving (4-1) and hence the proposition. □

**Remark 4.5.** Canonical local heights with similar functorial properties were constructed by Zarhin [1995] on total spaces of line bundles (without the zero section). See also [Bombieri and Gubler 2006] for an approach to canonical local heights using rigidified metrized line bundles.

The preceding proposition is particularly useful for analyzing the behavior of the canonical local height under a change of Weierstrass equation of the curve.

Recall that two Weierstrass equations for  $C$  are related by a transformation  $\tau$  as in (3-4), specified by a triple  $(A, e, U)$ , where  $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{GL}_2(k)$ ,  $e \in k^\times$  and

$$U = u_0Z^3 + u_1XZ^2 + u_2X^2Z + u_3X^3 \in k[X, Z]$$

is homogeneous of degree 3. Such a transformation induces a map on  $\text{KS}_\mathbb{A}$  as follows: Let  $x = (x_1, x_2, x_3, x_4) \in \text{KS}_\mathbb{A}$ . Then  $\tau(x)$  is given by the quadruple

$$(ad - bc)^{-1}(d^2x_1 + cdx_2 + c^2x_3, 2bdx_1 + (ad + bc)x_2 + 2acx_3, b^2x_1 + abx_2 + a^2x_3, (ad - bc)^{-2}(e^2x_4 + l_1x_1 + l_2x_2 + l_3x_3)),$$

where  $l_1, l_2, l_3$  do not depend on  $x$ . More precisely, we can write

$$l_i = l_{i,1} + l_{i,2} + l_{i,3},$$

where

$$l_{i,1} = \frac{e^2}{(ad - bc)^4} l'_{i,1} \quad \text{with } l'_{i,1} \in \mathbb{Z}[f_0, \dots, f_6, a, b, c, d],$$

$$l_{i,2} = \frac{e}{(ad - bc)^4} l'_{i,2} \quad \text{with } l'_{i,2} \in \mathbb{Z}[h_0, \dots, h_3, u_0, \dots, u_3, a, b, c, d],$$

$$l_{i,3} = \frac{1}{(ad - bc)^4} l'_{i,3} \quad \text{with } l'_{i,3} \in \mathbb{Z}[u_0, \dots, u_3, a, b, c, d]$$

for  $i = 1, 2, 3$ . All of the  $l'_{i,j}$  are homogeneous of degree 8 in  $a, b, c, d$  and homogeneous in the other variables.

So we see that  $\tau$  acts on  $k^4$  as a linear map  $\tau'$  whose determinant has valuation

$$v(\tau) := v(\det(\tau')) = 2v(e) - 3v(ad - bc).$$

In this situation, Proposition 4.4 implies:

**Corollary 4.6.** *Let  $\tau = ([a, b, c, d], e, U)$  be a transformation (3-4) between two Weierstrass equations  $W$  and  $W'$  of a smooth projective curve  $C/k$  of genus 2 and let  $\text{KS}$  be the model of the Kummer surface associated to  $W$ . Then we have*

$$\hat{\lambda}(\tau(x)) = \hat{\lambda}(x) - v(\tau) \quad \text{for all } x \in \text{KS}_\mathbb{A}.$$

In particular,

$$\mu(x) = \mu(\tau(x)) + v(\tau(x)) - v(x) - v(\tau).$$

This can be used to construct a canonical local height which does not depend on the choice of Weierstrass equation.

**Definition 4.7.** Let  $C/k$  be a smooth projective curve of genus 2 given by a Weierstrass equation (3-1) with discriminant  $\Delta$  and let  $\text{KS}$  be the associated Kummer surface. We call the function

$$\tilde{\lambda}: \text{KS}_{\mathbb{A}} \rightarrow \mathbb{R}, \quad x \mapsto \hat{\lambda}(x) + \frac{1}{10}v(\Delta),$$

the *normalized canonical local height on  $\text{KS}_{\mathbb{A}}$* .

**Corollary 4.8.** *The normalized canonical local height is independent of the given Weierstrass equation of  $C$ , in the following sense: if  $W$  and  $W'$  are two Weierstrass equations for  $C$ , with associated sets of sets of Kummer coordinates  $\text{KS}_{\mathbb{A}}$  and  $\text{KS}'_{\mathbb{A}}$  and canonical local heights  $\tilde{\lambda}$  and  $\tilde{\lambda}'$ , respectively, and  $\tau$  is a transformation (3-4) between them, then for all  $x \in \text{KS}_{\mathbb{A}}$  we have  $\tilde{\lambda}'(\tau(x)) = \tilde{\lambda}(x)$ .*

*Proof.* Let  $\Delta$  and  $\Delta'$  be the respective discriminants of  $W$  and  $W'$ . By [Liu 1996, §2], we have

$$v(\Delta') = v(\Delta) + 10v(\tau), \tag{4-2}$$

so, using Corollary 4.6,

$$\begin{aligned} \tilde{\lambda}'(\tau(x)) &= \hat{\lambda}'(\tau(x)) + \frac{1}{10}v(\Delta') \\ &= \hat{\lambda}(x) - v(\tau) + \frac{1}{10}v(\Delta') \\ &= \hat{\lambda}(x) + \frac{1}{10}v(\Delta) = \tilde{\lambda}(x). \end{aligned} \quad \square$$

We will not need the normalized canonical local height in the remainder of this paper.

### 5. Stably minimal Weierstrass models

In this section,  $k$  continues to denote a nonarchimedean local field with valuation ring  $\mathcal{O}$  and residue field  $\mathfrak{k}$ . We build on results established by Liu [1996] in the more general context of hyperelliptic curves of arbitrary genus.

Recall that an equation of the form (3-1) defining a curve  $C$  over  $k$  of genus 2 is an *integral Weierstrass model* of  $C$  if the polynomials  $F$  and  $H$  have coefficients in  $\mathcal{O}$ . (Note that this is slightly different from the notion of an “integral equation” as defined in [Liu 1996, Définition 2], but the difference is irrelevant for our purposes, since any minimal Weierstrass model is actually given by an integral equation; see [Liu 1996, Remarque 4].) It is a *minimal Weierstrass model* of  $C$  if it is integral and the valuation of its discriminant is minimal among all integral Weierstrass models of  $C$  [Liu 1996, Définition 3]. We introduce the following variant of this notion.

**Definition 5.1.** An integral Weierstrass model of a smooth projective curve  $C$  over  $k$

of genus 2 is *stably minimal* if it is a minimal Weierstrass model for  $C$  over  $k'$  for every finite field extension  $k'$  of  $k$ .

Stably minimal Weierstrass models can be characterized in terms of the multiplicities of the points on the special fiber.

**Definition 5.2.** Only for this definition let  $k$  be an arbitrary field, and let  $C_{F,H}$  be a curve in  $\mathbb{P}_k(1, 3, 1)$  given by an equation of the form (3-1) over  $k$ ; we assume that  $C_{F,H}$  is reduced. The *multiplicity*  $m(P, C_{F,H})$  of a geometric point  $P \in C_{F,H}(\bar{k})$  is defined as follows:

- If  $P$  is a singular point of type  $A_n$  (relative to the embedding of  $C_{F,H}$  into  $\mathbb{P}_k(1, 3, 1)$ ), then  $m(P, C_{F,H}) = n + 1$ .
- If  $P$  is fixed by the involution  $\iota(X : Y : Z) = (X : -Y - H(X, Z) : Z)$  and is nonsingular, then  $m(P, C_{F,H}) = 1$ .
- Otherwise  $m(P, C_{F,H}) = 0$ .

Singularities of type  $A_n$  were defined by Arnold over the complex numbers, and hence for arbitrary fields of characteristic zero; see for instance [Barth et al. 1984, §II.8]. For the case of positive characteristic, see [Greuel and Kröning 1990]. Note that if the characteristic of  $k$  is not 2, then  $\pi(P)$  is a root of multiplicity  $m(P, C_{F,H})$  of  $F^2 + 4H$ , where  $\pi : C_{F,H} \rightarrow \mathbb{P}^1$  sends  $(X : Y : Z)$  to  $(X : Z)$ .

We will use this notion in the context of points on the special fiber of a Weierstrass model of a curve of genus 2 over a complete local field. In this context, Definition 5.2 is equivalent to [Liu 1996, Définition 9] when the curve is reduced; see [Liu 1996, Remarque 8].

An algorithm that computes the multiplicity was given by Liu [1996, §6.1]. Liu defines [1996, Définition 10] further multiplicities  $\lambda_r(P)$  for points on the special fiber of an integral Weierstrass model (and  $r \geq 1$ ) that allow us to characterize when such a model is minimal. We note here that  $\lambda_r(P)$  gives the value of  $\lambda(P) = \lambda_1(P)$  after making a field extension of ramification index  $r$ . Also, Lemme 7(e) of [Liu 1996] states for  $r$  sufficiently large that  $\lambda_r(P) = m(P)$  if the special fiber is reduced and implies that  $\lambda_r(P) \geq r$  if the special fiber is nonreduced. In the reduced case, we also have  $\lambda(P) \leq m(P)$ .

Setting  $\lambda = \lambda_1$ , Corollaire 2 in [Liu 1996] states (for  $g = 2$ ) that the model is minimal if and only if  $\lambda(P) \leq 3$  and  $\lambda'(P) \leq 4$  (and is the unique minimal Weierstrass model up to  $\mathcal{O}$ -isomorphism, if and only if in addition  $\lambda'(P) \leq 3$ ) for all  $\mathfrak{k}$ -points  $P$  on the special fiber, where  $\lambda'(P)$  is a number satisfying  $\lambda'(P) \leq 2\lceil \lambda(P)/2 \rceil$ ; see [Liu 1996, Lemme 9(c)].

**Lemma 5.3.** *An integral Weierstrass model of a smooth projective curve  $C$  over  $k$  of genus 2 is stably minimal if and only if its special fiber is reduced and the multiplicity of every geometric point on the special fiber is at most 3.*

*If the special fiber is reduced and all multiplicities are at most 2, then the model is the unique minimal Weierstrass model of  $C$  over any finite extension  $k'$  of  $k$ , up to isomorphism over the valuation ring of  $k'$ .*

*Proof.* First note that the multiplicity of a point is a geometric property; it does not change when we replace  $k$  by a finite extension. If the special fiber of an integral Weierstrass model has the given properties, then it follows from Liu's results mentioned above that  $\lambda(P) \leq m(P) \leq 3$  and therefore  $\lambda'(P) \leq 4$  for all points  $P$  on the special fiber, even after replacing  $k$  by a finite extension. It follows that the model is stably minimal.

If  $m(P) \leq 2$  for all  $P$ , then  $\lambda(P) \leq 2$  and  $\lambda'(P) \leq 2$ , so by Liu's results, the model is the unique minimal Weierstrass model of  $C$  over  $k'$ .

Conversely, assume that the special fiber does not have the given properties. Then either the special fiber is nonreduced, or else there is a point  $P$  on the special fiber of multiplicity  $m(P) \geq 4$ . If the special fiber is nonreduced, then after replacing  $k$  by a sufficiently ramified extension  $k'$ , there is a point  $P$  on the special fiber such that  $\lambda(P) > 3$  over  $k'$  (ramification index 4 is sufficient). If the special fiber is reduced and there is a (geometric) point  $P$  on the special fiber with  $m(P) > 3$ , then again after replacing  $k$  by a sufficiently large finite extension  $k'$  (such that  $P$  is defined over the residue field and the ramification index is at least  $m(P)$ ), we have  $\lambda(P) = m(P) > 3$  over  $k'$ . Liu's results then show that the model is not minimal over  $k'$ .  $\square$

**Lemma 5.4.** *If  $C$  is a smooth projective curve over  $k$  of genus 2, then there is a finite extension  $k'$  of  $k$  such that*

- (i) *the minimal proper regular model of  $C$  over the valuation ring of  $k'$  has semistable reduction, and*
- (ii) *each minimal Weierstrass model of  $C$  over  $k'$  is already stably minimal.*

*Proof.* That there is a finite extension with the first property is a special case of the semistable reduction theorem [Deligne and Mumford 1969]. After a further unramified extension, we can assume that all geometric components of the special fiber of the minimal proper regular model (which all have multiplicity 1) are defined over the residue field and that at least one component has a smooth point defined over the residue field. This implies by Hensel's lemma that  $C(k') \neq \emptyset$ . It then follows from [Liu 1996, Corollaire 5] that every minimal Weierstrass model of  $C$  over  $k'$  is dominated by the minimal proper regular model. Since the latter has reduced special fiber, the same is true for each minimal Weierstrass model.

Now assume that there exists a stably minimal Weierstrass model of  $C$  over  $k'$ . Then every minimal Weierstrass model of  $C$  over  $k'$  must already be stably minimal, since both models must have the same valuation of the discriminant, and the discriminant of the stably minimal model remains minimal over any finite field extension of  $k'$ . So it is enough to show that a stably minimal model exists.

We now consider the various possibilities for the special fiber of the minimal proper regular model. The possible configurations are shown in Figures 1, 2, 3 and 5 (on pages 2187, 2188, 2189 and 2196). If the reduction type is  $[I_{m_1-m_2-m_3}]$  in the notation of [Namikawa and Ueno 1973], then the Weierstrass model whose special fiber contains the component(s) that are not  $(-2)$ -curves has the property that all points on the special fiber have multiplicity at most 2; this is then the unique minimal Weierstrass model, and it is stably minimal by Lemma 5.3. It remains to consider reduction type  $[I_{m_1} - I_{m_2} - l]$ . We see that the Weierstrass models that correspond to components in the chain linking the two polygons and also those coming from the component of one of the polygons that is connected to the chain satisfy the conditions of Lemma 5.3 and are thus stably minimal. On the other hand, Weierstrass models whose special fiber does not correspond to a component in the chain or to one of its neighbors have a point in the special fiber whose multiplicity is at least 4 and so cannot be stably minimal.  $\square$

### 6. Igusa invariants

In this section we describe how we can easily distinguish between different types of reduction using certain invariants of genus-2 curves introduced by Igusa [1960]. The results of this section are essentially due to Liu [1993]; see also [Mestre 1991].

Let  $k$  be an arbitrary field of characteristic not equal to 2 and consider the invariants  $J_2, J_4, J_6, J_8, J_{10}$  defined in [Igusa 1960], commonly called *Igusa invariants*. Then  $J_{2i}(F)$  is an invariant of degree  $2i$  of binary sextics, and if

$$F(X, Z) = f_0Z^6 + f_1XZ^5 + f_2X^2Z^4 + f_3X^3Z^3 + f_4X^4Z^2 + f_5X^5Z + f_6X^6$$

is a binary sextic, then

$$J_{2i}(F) \in \mathbb{Z}\left[\frac{1}{2}, f_0, \dots, f_6\right].$$

For example,  $J_{10}(F) = 2^{-12} \text{disc}(F)$ . It is shown in [Igusa 1960] that the invariants  $J_2, J_4, J_6, J_{10}$  generate the even-degree part of the ring of invariants of binary sextics.

Now let  $F$  and  $H$  be the generic binary forms over  $\mathbb{Z}$  of degrees 6 and 3, respectively, with coefficients  $f_0, \dots, f_6$  and  $h_0, \dots, h_3$  as before. It turns out that  $J_{2i}(4F + H^2)$  is an element of  $\mathbb{Z}[f_0, \dots, f_6, h_0, \dots, h_3]$ .

**Definition 6.1.** Let  $k$  be an arbitrary field and let  $H, F \in k[X, Z]$  be binary forms of respective degrees 3 and 6 over  $k$ . Let  $C_{F,H}$  be the curve given by the equation  $Y^2 + H(X, Z)Y = F(X, Z)$  in the weighted projective plane  $\mathbb{P}_k(1, 3, 1)$ . For  $1 \leq i \leq 5$  we define the *Igusa invariant*  $J_{2i}(C_{F,H})$  of  $C_{F,H}$  as

$$J_{2i}(C_{F,H}) = J_{2i}(4F + H^2).$$



Following [Liu 1993], we also define two additional invariants, namely

$$I_4(C_{F,H}) = J_2(C_{F,H})^2 - 24J_4(C_{F,H})$$

and

$$I_{12}(C_{F,H}) = -8J_4(C_{F,H})^3 + 9J_2(C_{F,H})J_4(C_{F,H})J_6(C_{F,H}) - 27J_6(C_{F,H})^2 - J_2(C_{F,H})^2J_8(C_{F,H}).$$

The following is a consequence of [Liu 1993, Théorème 1].

**Proposition 6.2.** *Let  $k$  be a field and let  $C_{F,H}/k$  be the curve given by the equation*

$$Y^2 + H(X, Z)Y = F(X, Z)$$

*in  $\mathbb{P}_k(1, 3, 1)$ , where  $H, F \in k[X, Z]$  are binary forms of degree 3 and 6, respectively. For  $1 \leq i \leq 5$  and  $j \in \{4, 12\}$  we set  $J_{2i} = J_{2i}(C_{F,H})$  and  $I_j = I_j(C_{F,H})$ .*

- (i)  $C_{F,H}$  is smooth  $\iff J_{10} \neq 0$ .
- (ii)  $C_{F,H}$  has a unique node and no point of higher multiplicity  $\iff J_{10} = 0$  and  $I_{12} \neq 0$ .
- (iii)  $C_{F,H}$  has exactly two nodes  $\iff J_{10} = I_{12} = 0$ ,  $I_4 \neq 0$ , and  $J_4 \neq 0$  or  $J_6 \neq 0$ .
- (iv)  $C_{F,H}$  has three nodes  $\iff J_{10} = I_{12} = J_4 = J_6 = 0$  and  $I_4 \neq 0$ .
- (v)  $C_{F,H}$  has a cusp  $\iff J_{10} = I_{12} = I_4 = 0$  and  $J_{2i} \neq 0$  for some  $i \leq 4$ .
- (vi)  $C_{F,H}$  is nonreduced or has a point of multiplicity at least 4  $\iff J_{2i} = 0$  for all  $i$ .

When  $C$  is a curve of genus 2 over a nonarchimedean local field, then Igusa invariants can also be used to obtain information on the reduction type of  $C$ ; see [Liu 1993, Théorème 1, Proposition 2].

**Proposition 6.3.** *Let  $k$  be a nonarchimedean local field with normalized additive valuation  $v: k^\times \rightarrow \mathbb{Z}$  and valuation ring  $\mathcal{O}$ , and let  $C/k$  be a smooth projective genus-2 curve, given by a minimal Weierstrass model with reduced special fiber. Suppose that the minimal proper regular model  $\mathcal{C}^{\min}$  of  $C$  over  $\text{Spec } \mathcal{O}$  is semistable and has reduction type  $\mathcal{K}$  in the notation of [Namikawa and Ueno 1973]. We set  $J_{2i} = J_{2i}(C)$  for  $i \in \{1, \dots, 5\}$  and  $I_4 = I_4(C)$ ,  $I_{12} = I_{12}(C)$ .*

- (i) If  $\mathcal{K} = [I_{m-0-0}]$ , where  $m > 0$ , then  $m = v(J_{10})$ .
- (ii) If  $\mathcal{K} = [I_{m_1-m_2-0}]$ , where  $0 < m_1 \leq m_2$ , then

$$m_1 = \min\left\{v(I_{12}), \frac{1}{2}v(J_{10})\right\} \quad \text{and} \quad m_2 = v(J_{10}) - m_1.$$

(iii) If  $\mathcal{K} = [I_{m_1 - m_2 - m_3}]$ , where  $0 < m_1 \leq m_2 \leq m_3$ , then

$$\begin{aligned} m_1 &= \min\left\{v(J_4), \frac{1}{3}v(J_{10}), \frac{1}{2}v(I_{12})\right\}, \\ m_2 &= \min\left\{v(I_{12}) - m_1, \frac{1}{2}(v(J_{10}) - m_1)\right\}, \text{ and} \\ m_3 &= v(J_{10}) - m_1 - m_2. \end{aligned}$$

(iv) If  $\mathcal{K} = [I_0 - I_0 - l]$ , then  $l = \frac{1}{12}v(J_{10})$ .

(v) If  $\mathcal{K} = [I_{m_1} - I_0 - l]$ , where  $m_1 > 0$ , then

$$l = \frac{1}{12}v(I_{12}) \quad \text{and} \quad m_1 = v(J_{10}) - v(I_{12}).$$

(vi) If  $\mathcal{K} = [I_{m_1} - I_{m_2} - l]$ , where  $m_2 \geq m_1 > 0$  and  $l > 0$ , then

$$\begin{aligned} l &= \frac{1}{4}v(I_4), \\ m_1 &= \min\left\{v(I_{12}) - 3v(I_4), \frac{1}{2}(v(J_{10}) - 3v(I_4))\right\}, \text{ and} \\ m_2 &= v(J_{10}) - 3v(I_4) - m_1. \end{aligned}$$

## Part II. Study of local height correction functions

In Part II of the paper,  $k$  will always denote a nonarchimedean local field with residue field  $\mathfrak{k}$ , valuation ring  $\mathcal{O}$  and normalized additive valuation  $v: k^\times \rightarrow \mathbb{Z}$ . We let  $C$  be a curve of genus 2 over  $k$ , given by an integral Weierstrass model  $\mathcal{C}$ , which we consider as a subscheme of the weighted projective plane  $\mathbb{P}_S(1, 3, 1)$ , where  $S = \text{Spec}(\mathcal{O})$ . In the following five sections we find explicit formulas and bounds for the local height correction function  $\mu$  for the most frequent cases of bad reduction and use these to deduce a general bound on  $\mu$ . We denote the minimal proper regular model of  $C$  over  $S$  by  $\mathcal{C}^{\min}$ . Let  $J$  be the Jacobian of  $C$ ; we denote its Néron model over  $S$  by  $\mathcal{J}$ . We write  $\mathcal{C}_v$ ,  $\mathcal{C}_v^{\min}$  and  $\mathcal{J}_v$  for the respective special fibers of  $\mathcal{C}$ ,  $\mathcal{C}^{\min}$  and  $\mathcal{J}$ .

### 7. The “kernel” of $\mu$

By Theorem 3.10, the set

$$U = \{P \in J(k) : \varepsilon(P) = 0\}$$

is a group and the local height correction function  $\mu$  factors through the quotient  $J(k)/U$ . In this section we relate  $U$  to the Néron model of  $J$  when  $\mathcal{C}$  has rational singularities. See [Artin 1986] for a brief account of the theory of rational singularities on arithmetic surfaces.

For the remainder of this section we assume that  $\mathcal{C}/S$  is normal and reduced. We let  $\mathcal{J}^0$  denote the fiberwise-connected component of the identity of  $\mathcal{J}$ . Then  $\mathcal{J}^0$  has generic fiber  $\mathcal{J}_k \cong J$  and special fiber  $\mathcal{J}_v^0$ , the connected component of the

identity of  $\mathcal{J}_v$ . If  $\mathcal{C}' \rightarrow \mathcal{C}$  is a desingularization of  $\mathcal{C}$ , then the identity components  $\text{Pic}_{\mathcal{C}'/S}^0$  and  $\text{Pic}_{\mathcal{C}/S}^0$  of the respective relative Picard functors of  $\mathcal{C}'$  and  $\mathcal{C}$  can both be represented by separated schemes; see [Bosch et al. 1990, Theorem 9.7.1]. There are canonical  $S$ -group scheme morphisms

$$\text{Pic}_{\mathcal{C}/S}^0 \rightarrow \text{Pic}_{\mathcal{C}'/S}^0 \xrightarrow{\sim} \mathcal{J}^0; \tag{7-1}$$

the latter map is an isomorphism by [Bosch et al. 1990, Theorem 9.4.2]. Let  $\alpha: \text{Pic}_{\mathcal{C}/S}^0 \rightarrow \mathcal{J}^0$  denote the composition of the morphisms from (7-1); note that  $\alpha$  does not depend on the choice of the desingularization  $\mathcal{C}'$ . We will show that if  $P \in J(k)$  has reduction on  $\mathcal{J}$  in the image of  $\alpha$ , then  $\varepsilon(P) = \mu(P) = 0$ . The idea is to first show that this is true for points in the image of a certain open subscheme; we then prove that this suffices for the general case.

Let  $\mathcal{C}_{\text{sm}}$  be the smooth locus of  $\mathcal{C}$ . Following [Bosch et al. 1990, §9.3], we define an  $S$ -subscheme  $W$  of the symmetric square  $\mathcal{C}_{\text{sm}}^{(2)}$  of  $\mathcal{C}_{\text{sm}}$  consisting of the points  $w \in \mathcal{C}_{\text{sm}}^{(2)}$  that satisfy the following conditions:

- $H^1(\mathcal{C}, \mathcal{O}_{\mathcal{C}}(D_w)) = 0$ , where  $D$  is the universal Cartier divisor  $D \subset \mathcal{C} \times_S \mathcal{C}_{\text{sm}}^{(2)}$  induced by the canonical map  $\mathcal{C}_{\text{sm}}^{(2)} \rightarrow \text{Div}_{\mathcal{C}/S}^2$ .
- If  $w = \{w_1, w_2\}$  with  $w_1, w_2$  geometric points on the special fiber of  $\mathcal{C}$ , then the hyperelliptic involution  $\iota$  maps the component containing  $w_1$  to the component containing  $w_2$ .

Then  $W$  has the following properties:

- (i)  $W$  is an open subscheme of  $\mathcal{C}_{\text{sm}}^{(2)}$ .
- (ii) There is a strict  $S$ -birational group law on  $W$ , induced by the group law on  $\text{Pic}_{\mathcal{C}/S}$ .
- (iii)  $\text{Pic}_{\mathcal{C}/S}^0$  is the  $S$ -group scheme associated with this strict  $S$ -birational group law.

For (ii) and (iii) see the discussion preceding [Bosch et al. 1990, Theorem 9.3.7].

Let  $\text{Pic}_{\mathcal{C}/S}^{[2]}$  be the open subfunctor of  $\text{Pic}_{\mathcal{C}/S}$  whose elements have total degree 2. Let  $\rho: W \rightarrow \text{Pic}_{\mathcal{C}/S}^{[2]}$  be the canonical map induced by  $D$ ; by [Bosch et al. 1990, Lemma 9.3.5] it is an open immersion. Replacing  $S$  by the spectrum of the valuation ring of a finite unramified extension of  $k$ , if necessary, we can find a section  $x_0 \in \mathbb{P}_S^1(S)$  such that its pullback  $D_0$  under the covering map  $\mathcal{C} \rightarrow \mathbb{P}_S^1$  is horizontal and does not intersect the singular locus of  $\mathcal{C}$ . We denote by  $c_0$  the class of  $D_0$  in  $\text{Pic}_{\mathcal{C}/S}^{[2]}$ . Let  $w = \{P_1, P_2\} \in W$ ; using the condition on the action of  $\iota$  on the components  $P_1$  and  $P_2$  lie on, we find that

$$\rho_0(w) := \rho(w) - c_0 \in \text{Pic}_{\mathcal{C}/S}^0.$$

In fact,  $\rho_0$  defines an open immersion  $\rho_0: W \rightarrow \text{Pic}_{\mathcal{C}/S}^0$ ; see [Bosch et al. 1990, Lemma 9.3.6].

**Lemma 7.1.** *Suppose that the residue characteristic of  $k$  is not 2. Let  $P \in J(k)$  such that the reduction of  $P$  on  $\mathcal{J}_v$  is in  $\alpha(\rho_0(W))$ . Then  $\varepsilon(P) = 0$ .*

*Proof.* We may assume that  $\mathcal{C}: Y^2 = F(X, Z)$ . Let  $J_F$  denote the model of  $J$  in  $\mathbb{P}^{15}$  constructed in [Cassels and Flynn 1996, Chapter 2] and let  $\mathcal{J}_F/S$  denote the model it defines over  $S$ . Following [Bruin and Stoll 2010, §5], we denote by  $\mathcal{J}_F^0$  the fiberwise-connected component of the identity of the smooth locus of  $\mathcal{J}_F$ , so that the generic fiber is  $\mathcal{J}_F$  and the special fiber  $\mathcal{J}_{F,v}^0$  is the connected component of the identity of the smooth locus of the special fiber  $\mathcal{J}_{F,v}$ . We have a morphism  $\psi: \mathcal{C}_{\text{sm}}^{(2)} \rightarrow \mathcal{J}_F^0$ , defined using the expressions for the coordinates on  $J_F$  in [Cassels and Flynn 1996, Chapter 2]; see the proof of [Bruin and Stoll 2010, Lemma 5.7]. We also denote the restriction of this morphism to  $W$  by  $\psi$ .

The Néron mapping property yields a natural map  $\varphi: \mathcal{J}_F^0 \rightarrow \mathcal{J}$ . In general, its image can be a proper subset of  $\mathcal{J}^0$ . Nevertheless, the following diagram of  $S$ -scheme morphisms is commutative by [Liu 2002, Proposition 3.3.11], since  $W$  is reduced,  $\mathcal{J}^0$  is separated and the diagram is commutative when restricted to generic fibers:

$$\begin{array}{ccc}
 W & \xrightarrow{\psi} & \mathcal{J}_F^0 \\
 \rho_0 \downarrow & & \downarrow \varphi \\
 \text{Pic}_{\mathcal{C}/S}^0 & \xrightarrow{\alpha} & \mathcal{J}^0
 \end{array} \tag{7-2}$$

It follows from [Bruin and Stoll 2010, Proposition 5.10] that a point  $P \in J(k)$  satisfies  $\varepsilon(P) = 0$  if and only if  $P$  reduces to  $\mathcal{J}_{F,v}^0(\mathfrak{k})$ . So if  $P$  has reduction in  $\alpha(\rho_0(W))$ , then the commutativity of the diagram (7-2) shows that  $\varepsilon(P) = 0$ .  $\square$

If the residue characteristic is 2, then no explicit analogue of the group scheme  $\mathcal{J}_F$  is known. Instead, we have to work with explicit expressions to prove a result analogous to Lemma 7.1.

Let  $\tilde{F}$  and  $\tilde{H}$  be the reductions of  $F$  and  $H$ , respectively. In analogy with [Bruin and Stoll 2010, Definition 5.1], we define the subscheme  $\tilde{\mathcal{D}}$  of  $\mathbb{A}_{\mathfrak{k}}^3 \times \mathbb{A}_{\mathfrak{k}}^4 \times \mathbb{A}_{\mathfrak{k}}^5$  consisting of all triples

$$(A, B, C) = ((a_0, a_1, a_2), (b_0, b_1, b_2, b_3), (c_0, c_1, c_2, c_3, c_4)) \in \mathbb{A}_{\mathfrak{k}}^3 \times \mathbb{A}_{\mathfrak{k}}^4 \times \mathbb{A}_{\mathfrak{k}}^5$$

such that

$$AC = \tilde{F} - B^2 - B\tilde{H},$$

where

$$\begin{aligned}
 A &= a_0Z^2 + a_1XZ + a_2X^2, \\
 B &= b_0Z^3 + b_1XZ^2 + b_2X^2Z + b_3X^3, \\
 C &= c_0Z^4 + c_1XZ^2 + c_2X^2Z^2 + c_3X^3Z + c_4X^4.
 \end{aligned}$$

Moreover, we set  $\mathcal{D} := (\pi_2 \times \text{id})(\text{pr}_{12}(\tilde{\mathcal{D}}))$ , where  $\text{pr}_{12}$  is the projection onto the first two factors and  $\pi_2$  is the canonical map  $\mathbb{A}_{\mathbb{F}}^3 \setminus \{(0, 0, 0)\} \rightarrow \mathbb{P}_{\mathbb{F}}^2$ .

Note that if the curve  $\mathcal{C}_v$  defined by  $Y^2 + \tilde{H}(X, Z)Y = \tilde{F}(X, Z)$  in  $\mathbb{P}_{\mathbb{F}}(1, 3, 1)$  is nonsingular, then  $\mathcal{D}(\mathbb{F})$  is in bijective correspondence with the possible Mumford representations of effective divisors of degree 2 on  $\mathcal{C}_v$ .

In general, this correspondence still holds for the subset  $\mathcal{D}'$  of all  $(A, B) \in \mathcal{D}$  such that  $A$  does not vanish at the image in  $\mathbb{P}^1$  of a singular point of  $\mathcal{C}_v$ , and those effective divisors with support in the smooth locus of  $\mathcal{C}_v$ . More precisely, we get a map  $\zeta : \mathcal{D}' \rightarrow \mathcal{C}_v^{(2)}$  such that if  $\zeta((A, B)) = \{\tilde{P}_1, \tilde{P}_2\}$ , then there are representatives  $(X_i, Y_i, Z_i)$  of  $\tilde{P}_i$  ( $i = 1, 2$ ) satisfying

- (i)  $A(X, Z) = (Z_1X - X_1Z)(Z_2X - X_2Z)$ ,
- (ii)  $Y_i = B(X_i, Z_i)$  for  $i = 1, 2$ .

If  $\mathcal{C}_v$  is nonsingular, and  $(A, B) \in \mathcal{D}$ , then we can compose the natural surjection  $\mathcal{D} \rightarrow \text{Jac}(\mathcal{C}_v) \setminus \{O\}$  with the quotient map  $\text{Jac}(\mathcal{C}_v) \rightarrow \text{KS}_{\tilde{F}, \tilde{H}}$ . In the general case one can also define a surjection  $\omega : \mathcal{D} \rightarrow \text{KS}_{\tilde{F}, \tilde{H}} \setminus \{(0 : 0 : 0 : 1)\}$  with the following property: if  $P = [(P_1) - (P_2)] \in J(k)$  is such that the reductions  $\tilde{P}_1$  and  $\tilde{P}_2$  are both smooth points on  $\mathcal{C}_v$ , and if  $(A, B) \in \mathcal{D}'$  is such that  $\zeta((A, B)) = \{\tilde{P}_1, \iota(\tilde{P}_2)\}$ , then the reduction of  $\kappa(P)$  on  $\text{KS}_{\tilde{F}, \tilde{H}}$  is  $\omega((A, B))$ . The image of a pair  $(A, B) \in \mathcal{D}$  under  $\omega$  is of the form  $(a_0 : -a_1 : a_2 : x_4)$ .

**Lemma 7.2.** *Suppose that the residue characteristic of  $k$  is 2. Let  $P \in J(k)$  such that the reduction of  $P$  on  $\mathcal{J}$  is in  $\alpha(\rho_0(W))$ . Then  $\varepsilon(P) = 0$ .*

*Proof.* Let  $(A, B) \in \mathcal{D}'_{\tilde{F}, \tilde{H}}$  such that  $\zeta((A, B)) = \{\tilde{P}_1, \tilde{P}_2\} \in W$ . By the discussion preceding the lemma, it suffices to show that we have  $\delta(x) \neq 0$  for  $x = \omega((A, B))$ .

Changing the given model, if necessary, we can assume that  $\tilde{H}$  and  $\tilde{F}$  are as in the list of representatives 1–13 in Table 1. Table 2 contains conditions on  $x$  which are equivalent to the vanishing of  $\delta(x)$  for each representative and additional conditions which a point  $x = (x_1 : x_2 : x_3 : x_4) \in \mathbb{P}^3$  satisfying  $\delta(x) = 0$  must satisfy in order to lie on  $\text{KS}_{\tilde{F}, \tilde{H}}$ . Finally, we have listed the multiplicities  $m(\infty)$ ,  $m(0)$ ,  $m(1)$  that  $\mathcal{C}_v$  has at the points with  $(X : Z) = (1 : 0)$ ,  $(X : Z) = (0 : 1)$  and  $(X : Z) = (1 : 1)$ , respectively, in case the multiplicities there are greater than 1. Note that we do not have to treat type 1, as  $\mathcal{C}_v$  is assumed to be reduced.

Since  $A(X, Z)$  does not vanish at the image in  $\mathbb{P}^1$  of a singular point, we get  $x_1 \neq 0$  and, if  $(0, 0)$  is a singular point, also  $x_3 \neq 0$ . Using Table 2, this already implies that  $\delta(x) \neq 0$  whenever  $\mathcal{C}_v$  is irreducible. In the reducible cases 2, 7 and 8,  $\mathcal{C}_v$  has two irreducible components, and one checks easily that  $x_4$  does not vanish because, by definition of  $W$ ,  $\iota$  maps the component containing  $\tilde{P}_1$  to the component containing  $\tilde{P}_2$ . Hence  $\delta(x) \neq 0$  by Table 2. □

The next proposition follows from Lemmas 7.1 and 7.2.

type	condition	additional	$m(\infty)$	$m(0)$	$m(1)$
1	$x_4 = 0$				
2	$x_4 = 0$		6		
3	$x_4 = 0$	$x_1 = 0$	5		
4	$x_4 = 0$	$x_1 = 0$	4		
5	$x_1x_3 = x_4 = 0$		3	2	
6	$x_1 = x_4 = 0$		3		
7	$x_4 = 0$		4	2	
8	$x_4 = 0$		2	2	2
9	$x_1x_3 = x_4 = 0$		2	2	
10	$x_1 = x_4 = 0$		2		
11	$x_1 = x_4 = 0$		3		
12	$x_4 = 0$	$x_1 = 0$	5		
13	$x_4 = 0$	$x_1x_3 = 0$	3	3	

**Table 2.** Conditions for the vanishing of  $\delta(x)$ .

**Proposition 7.3.** *Let  $\alpha : \text{Pic}_{\mathcal{C}/S}^0 \rightarrow \mathcal{J}^0$  be the canonical homomorphism. If the reduction of  $P \in J(k)$  on  $\mathcal{J}_v$  is in the image of  $\alpha$ , then  $\varepsilon(P) = \mu(P) = 0$ .*

*Proof.* If  $T$  is an  $S$ -scheme and  $x \in \text{Pic}_{\mathcal{C}/S}^0(T)$ , then by properties (ii) and (iii) of  $W$ , there is an étale cover  $T'/T$  and  $w_1, \dots, w_n \in W(T')$  such that

$$x = \rho_0(w_1) + \dots + \rho_0(w_n),$$

where the sum is taken with respect to the group law on  $\text{Pic}_{\mathcal{C}/S}^0$ . In fact we can take  $n = 2$ ; this follows from [Bosch et al. 1990, Lemma 5.1.4] and the discussion following Lemma 5.2.4 of the same paper. Using this and Theorem 3.10, it suffices to show that  $\varepsilon(P) = 0$  when the reduction of  $P$  on  $\mathcal{J}_v$  is in  $\alpha(\rho_0(W))$ . Hence the result follows from Lemmas 7.1 and 7.2. □

Let  $J_0(k)$  denote the subgroup of  $J(k)$  consisting of points whose image on the special fiber of  $\mathcal{J}$  is in  $\mathcal{J}^0(\mathfrak{k})$ . By [Bosch and Liu 1999, Lemma 2.1] the group  $\Phi(\mathfrak{k})$  of  $\mathfrak{k}$ -rational points in the component group  $\Phi$  of  $J$  satisfies

$$\Phi(\mathfrak{k}) \cong J(k)/J_0(k).$$

We can now give a criterion for when  $\varepsilon$  and  $\mu$  factor through  $\Phi(\mathfrak{k})$ .

**Theorem 7.4.** *Let  $\mathcal{C}$  be a smooth projective curve of genus 2 defined over a nonarchimedean local field  $k$ , given by an integral Weierstrass model  $\mathcal{C}$  with rational singularities. Then  $\varepsilon$  and  $\mu$  factor through  $\Phi(\mathfrak{k})$ .*

*Proof.* First note that if  $\mathcal{C}$  has rational singularities, then  $\mathcal{C}$  is normal and reduced. Moreover, according to [Bosch et al. 1990, Theorem 9.7.1], the homomorphism  $\alpha$  is an isomorphism if and only if  $\mathcal{C}$  has rational singularities. This implies that the

image of  $\alpha$ , restricted to the generic fiber, is  $J_0(k)$ . By [Proposition 7.3](#), we have  $\varepsilon(P) = \mu(P) = 0$  for  $P$  in the image of  $\alpha$ . [Theorem 3.10](#) implies that  $\mu$  and  $\varepsilon$  factor through  $\Phi(\mathfrak{k})$ .  $\square$

**Remark 7.5.** A nonminimal Weierstrass model cannot have rational singularities. Moreover, there are minimal (even stably minimal) Weierstrass models of curves of genus 2 that have nonrational singularities. See [Example 10.4](#) for a stably minimal Weierstrass model having  $\mu(P) \neq 0$  for some points  $P \in J_0(k)$ .

This behavior cannot occur for elliptic curves; here  $\mu$  always factors through  $\Phi(\mathfrak{k})$ , provided the given Weierstrass model is minimal; see [[Silverman 1988](#)]. This is crucial for the usual algorithms to compute canonical heights on elliptic curves. Note that a Weierstrass model of an elliptic curve is minimal if and only if it has rational singularities by [[Conrad 2005](#), Corollary 8.4].

## 8. Néron functions and reduction graphs

Our next goal is to derive a formula for  $\mu(P)$  in the case when the minimal proper regular model of  $C$  is semistable and  $\mu$  factors through  $\Phi(\mathfrak{k})$ . To this end, we need the notion of Néron functions. The following result is due to Néron; see [[Lang 1983](#), §11.1].

**Proposition 8.1.** *Let  $A$  be an abelian variety defined over a local field  $k$ . Then we can associate to any divisor  $D \in \text{Div}_A(\bar{k})$  a function  $\lambda_D: A(\bar{k}) \setminus \text{supp}(D) \rightarrow \mathbb{R}$  such that the following conditions are satisfied, where we write  $\lambda \equiv \lambda' \pmod{\text{const}}$  to indicate that the functions  $\lambda$  and  $\lambda'$  differ by a constant.*

- (1) *If  $D, E \in \text{Div}_A(\bar{k})$ , then  $\lambda_{D+E} \equiv \lambda_D + \lambda_E \pmod{\text{const}}$ .*
- (2) *If  $D = \text{div}(f) \in \text{Div}_A(\bar{k})$  is principal, then  $\lambda_D \equiv \bar{v} \circ f \pmod{\text{const}}$ , where  $\bar{v}$  is the extension of  $v$  to  $\bar{k}$ .*
- (3) *If  $D \in \text{Div}_A(\bar{k})$  and  $T_P: A \rightarrow A$  is the translation map by a point  $P \in A(\bar{k})$ , then we have  $\lambda_{T_P^*D} \equiv \lambda_D \circ T_P \pmod{\text{const}}$ .*

Also,  $\lambda_D$  is uniquely determined up to adding a constant.

We call a function  $\lambda_D$  as in [Proposition 8.1](#) a *Néron function associated with  $D$* .

We can use local heights on Kummer coordinates to construct Néron functions on the Jacobian  $J$  of our genus-2 curve  $C$ . If  $P_0 \in C(\bar{k})$ , then we have an embedding  $C_{\bar{k}} \rightarrow J_{\bar{k}}$  (defined over  $\bar{k}$ ) that maps  $P \in C(\bar{k})$  to the divisor class  $[(P) - (P_0)] \in \text{Pic}_C^0(\bar{k}) = J(\bar{k})$ . Its image is the theta divisor  $\Theta_{P_0}$ . We set  $\Theta_{P_0}^{\pm} = \Theta_{P_0} + \Theta_{\iota(P_0)}$ ; then  $\Theta_{P_0}^{\pm}$  is symmetric and in the linear equivalence class of  $2\Theta$  (where  $\Theta$  is a theta divisor coming from taking a Weierstrass point as base-point). For the following, fix a point  $\infty \in C(\bar{k})$  at infinity. For  $i \in \{1, \dots, 4\}$ , we set

$$D_i = \Theta_{\infty}^{\pm} + \text{div}\left(\frac{\kappa_i}{\kappa_1}\right)$$

and we define a function  $\hat{\lambda}_i: J(k) \setminus \text{supp}(D_i) \rightarrow \mathbb{R}$  by

$$\hat{\lambda}_i(P) = \hat{\lambda} \left( \frac{\kappa(P)}{\kappa_i(P)} \right).$$

**Lemma 8.2.** *Let  $\infty \in C(\bar{k})$  be a point at infinity as above and let  $i \in \{1, \dots, 4\}$ . Then  $D_i$  is defined over  $k$  and the function  $\hat{\lambda}_i$  is a Néron function associated with  $D_i$ .*

*Proof.* If  $\infty \notin C(k)$ , then we have  $\infty \in C(k')$  for some quadratic extension  $k'$  of  $k$  and the nontrivial element of the Galois group  $\text{Gal}(k'/k)$  maps  $\infty$  to  $\iota(\infty)$ , proving the first assertion. For a proof of the second assertion, see [Uchida 2011, Theorem 5.3]. □

**Definition 8.3.** Assume that  $C$  has semistable reduction over  $k$ . Let  $C' = \mathcal{C}_{v, \mathfrak{k}}^{\min}$  denote the special fiber of the minimal proper regular model  $\mathcal{C}^{\min}$  of  $C$ , considered over the algebraic closure of the residue field  $\mathfrak{k}$ . The *reduction graph*  $R(C)$  of  $C$  is a graph with vertex set the set of irreducible components of  $C'$ ; two vertices  $\Gamma_1$  and  $\Gamma_2$  are connected by  $n$  edges, where  $n$  is the number of intersection points of  $\Gamma_1$  and  $\Gamma_2$  if  $\Gamma_1 \neq \Gamma_2$ , and  $n$  is the number of nodes of  $\Gamma_1$  if  $\Gamma_1 = \Gamma_2$ . The Galois group of  $\mathfrak{k}$  acts on  $R(C)$  in a natural way.

We consider  $R(C)$  as a metric graph by giving each edge length 1. For two vertices  $\Gamma_1$  and  $\Gamma_2$ , we define  $r(\Gamma_1, \Gamma_2)$  as the resistance between the vertices, when  $R(C)$  is considered as an electric network with unit resistance along every edge.

**Remark 8.4.** We can compute  $r(\Gamma_1, \Gamma_2)$  as follows. Order the vertices of  $R(C)$  in some way and let  $M$  be the intersection matrix with respect to this ordering. Since all components of the special fiber have multiplicity one, the kernel of  $M$  is spanned by the “all-ones” vector and the image of  $M$  consists of the vectors whose entries sum to zero. Let  $v$  be the vector with entries zero except that the entry corresponding to  $\Gamma_1$  is 1 and the entry corresponding to  $\Gamma_2$  is  $-1$ . Then there is a vector  $g$  with rational entries such that  $Mg = v$ , and

$$r(\Gamma_1, \Gamma_2) = -g \cdot v$$

is, up to sign, the standard inner product of the two vectors. (Note that  $g$  is not unique, but adding a vector in the kernel of  $M$  to it will not change the result.) See for instance [Cinkir 2011, Lemma 6.1].

Note that the linear map given by  $M$  on the space of functions on the vertices can be interpreted as the discrete Laplace operator on the graph  $R(C)$ . It is then easy to see that  $g$ , viewed as a function on the vertices, is piecewise linear along sequences of edges not containing  $\Gamma_1$ ,  $\Gamma_2$  or a vertex of degree at least 3. This makes it quite easy to find  $g$  and to compute  $r(\Gamma_1, \Gamma_2)$ .

The reduction graph is unchanged when we replace  $k$  by an unramified extension. If we base-change to a ramified extension  $k'$  of  $k$  with ramification index  $e$ , then



the new reduction graph is obtained by subdividing the edges of  $R(C)$  into  $e$  new edges. We can give these new edges length  $1/e$ ; then the underlying metric space remains the same. In particular,  $r(\Gamma_1, \Gamma_2)$  does not depend on  $k'$ . This allows us to replace  $k$  by a finite extension if necessary. The scaling of the length corresponds to extending the valuation  $v: k^\times \rightarrow \mathbb{Z}$  to  $\bar{k}^\times \rightarrow \mathbb{Q}$  instead of considering the normalized valuation on  $k'$ . All notions defined in terms of the valuation (for example, intersection numbers) are then scaled accordingly.

**Proposition 8.5.** *We assume that  $C^{\min}$  is semistable. Let  $P = [(P_1) - (P_2)] \in J(k)$ , with  $P_1, P_2 \in C(k)$  mapping to components  $\Gamma_1$  and  $\Gamma_2$ , respectively, of the special fiber of  $C^{\min}$ . We make the following further assumptions.*

- (i) *If  $Q_1, Q_2 \in C(k)$  map to  $\Gamma_1$  and  $\Gamma_2$ , respectively, then  $\mu(P) = \mu([(Q_1) - (Q_2)])$ .*
- (ii) *There is a constant  $\mu_1 \in \mathbb{Q}$  such that  $\mu([(Q_1) - (Q'_1)]) = \mu_1$  for all  $Q_1, Q'_1 \in C(k)$  mapping to  $\Gamma_1$  such that the images of  $Q_1$  and  $Q'_1$  on the special fiber of  $C^{\min}$  are distinct.*
- (iii) *There is a constant  $\mu_2 \in \mathbb{Q}$  such that  $\mu([(Q_2) - (Q'_2)]) = \mu_2$  for all  $Q_2, Q'_2 \in C(k)$  mapping to  $\Gamma_2$  such that the images of  $Q_2$  and  $Q'_2$  on the special fiber of  $C^{\min}$  are distinct.*

Then we have

$$\mu(P) = r(\Gamma_1, \Gamma_2) + \frac{1}{2}(\mu_1 + \mu_2).$$

*Proof.* By the discussion preceding the statement of the theorem, we can assume that  $k$  is sufficiently large for  $C(k)$  to contain all points we might be interested in.

Let  $P_0 \in C(k)$ . The embedding with respect to  $P_0$  is obtained from the “difference map”  $\psi: C \times C \rightarrow J$  that sends a pair of points  $(P_1, P_2)$  to  $[(P_1) - (P_2)]$  by specializing the second argument to  $P_0$ . One easily checks that

$$\psi^* \Theta_{P_0} = \Delta_C + (\iota(P_0) \times C) + (C \times \{P_0\}),$$

where  $\Delta_C$  denotes the diagonal and  $\iota$  is the hyperelliptic involution on  $C$ . We then have

$$\psi^* \Theta_{P_0}^\pm = 2\Delta_C + \text{pr}_1^* D_0 + \text{pr}_2^* D_0,$$

where  $D_0 = (P_0) + (\iota(P_0))$ . By the results in [Heinz 2004] this implies that, taking  $\lambda_0$  to be a Néron function associated to  $\Theta_{P_0}^\pm$ ,

$$\lambda_0([(P_1) - (P_2)]) = 2\langle P_1, P_2 \rangle + \langle P_1 + P_2, P_0 + \iota(P_0) \rangle + c$$

for all points  $P_1, P_2 \in C(k^{\text{nr}})$  with  $P_1 \neq P_2$  and  $\{P_1, P_2\} \cap \{P_0, \iota(P_0)\} = \emptyset$ , where  $\langle \cdot, \cdot \rangle$  is the pairing in [Heinz 2004, Theorem 4.4] and  $c \in \mathbb{R}$  is a constant.

If  $C^{\min}$  has semistable reduction, then, by [Heinz 2004, Remark 4.6], the pairing  $\langle \cdot, \cdot \rangle$  coincides with Zhang’s admissible pairing  $(\cdot, \cdot)_a$  [1993] in terms of harmonic

analysis on the reduction graph  $R(C)$ . In these terms, we have, for  $Q, Q' \in C(k^{\text{nr}})$ ,

$$\langle Q, Q' \rangle = (Q, Q')_a = i(\bar{Q}, \bar{Q}') + g_\nu(\Gamma, \Gamma'),$$

where  $i(\bar{Q}, \bar{Q}')$  is the intersection multiplicity of the sections  $\bar{Q}, \bar{Q}' \in C^{\text{min}}(\mathcal{O}^{\text{nr}})$  induced by  $Q$  and  $Q'$ , respectively, and  $g_\nu(\Gamma, \Gamma')$  is the Green's function associated to a certain measure  $\nu$  on  $R(C)$ , with  $\Gamma$  and  $\Gamma'$  being the respective components of the special fiber of  $C^{\text{min}}$  that  $Q$  and  $Q'$  reduce to. See [Zhang 1993, §4]. We extend  $g_\nu$  to a bilinear map on the free abelian group generated by the vertices of  $R(C)$ .

**Lemma 8.2** gives, for  $P_0 = \infty$  and  $P = [(P_1) - (P_2)]$  with normalized Kummer coordinates  $x(P) = (x_1(P), \dots, x_4(P))$ ,

$$\begin{aligned} \mu(P) &= v(x_1(P)) - \hat{\lambda}_1(P) \\ &= v(x_1(P)) - 2i(\bar{P}_1, \bar{P}_2) - i(\bar{P}_1 + \bar{P}_2, \bar{P}_0 + \iota(\bar{P}_0)) \\ &\quad - 2g_\nu(\Gamma_1, \Gamma_2) - g_\nu(\Gamma_1 + \Gamma_2, \Gamma_0 + \Gamma'_0) - c, \end{aligned}$$

where  $\Gamma_1$  and  $\Gamma_2$  are the respective components that  $P_1$  and  $P_2$  reduce to, and  $\Gamma_0$  and  $\Gamma'_0$  are the respective components that  $P_0$  and  $\iota(P_0)$  reduce to. We assume for a moment that the images of  $P_1$  and  $P_2$  on the special fiber of the original model  $\mathcal{C}$  are distinct from the images of the points at infinity. By assumption (i),  $\mu(P)$  is unchanged when we replace the points  $P_1$  and  $P_2$  by other points still mapping to  $\Gamma_1$  and  $\Gamma_2$ , respectively. We can therefore assume that the images of  $P_1$  and  $P_2$  on the special fiber of  $C^{\text{min}}$  are distinct from each other and also from the images of  $P_0$  and  $\iota(P_0)$ . This implies that  $v(x_1(P)) = 0$  and that the intersection numbers in the formula above are zero. We can choose further points  $Q_1$  and  $Q_2$  that also reduce to  $\Gamma_1$  and  $\Gamma_2$  with reductions on the special fiber of  $\mathcal{C}$  distinct from those of  $P_0$  and  $\iota(P_0)$  and such that  $P_1, P_2, Q_1$  and  $Q_2$  all reduce to distinct points on the special fiber of  $C^{\text{min}}$ . Using assumptions (ii) and (iii), we obtain the relations

$$\begin{aligned} -\frac{1}{2}\mu_1 &= -\frac{1}{2}\mu([(P_1) - (Q_1)]) = g_\nu(\Gamma_1, \Gamma_1) + g_\nu(\Gamma_1, \Gamma_0 + \Gamma'_0) + \frac{1}{2}c, \\ \mu(P) &= \mu([(P_1) - (P_2)]) = -2g_\nu(\Gamma_1, \Gamma_2) - g_\nu(\Gamma_1 + \Gamma_2, \Gamma_0 + \Gamma'_0) - c, \\ -\frac{1}{2}\mu_2 &= -\frac{1}{2}\mu([(P_2) - (Q_2)]) = g_\nu(\Gamma_2, \Gamma_2) + g_\nu(\Gamma_2, \Gamma_0 + \Gamma'_0) + \frac{1}{2}c. \end{aligned}$$

Adding them together gives

$$\mu(P) - \frac{1}{2}(\mu_1 + \mu_2) = g_\nu(\Gamma_1 - \Gamma_2, \Gamma_1 - \Gamma_2) = r(\Gamma_1, \Gamma_2),$$

as desired. See [Zhang 1993, §3] for the last equality.

If our assumption that the images of  $P_1$  and  $P_2$  on the special fiber of the original model  $\mathcal{C}$  are distinct from the images of the points at infinity is not satisfied, then we choose another point  $P_0$  for which the assumption is satisfied. We can then perform a change of coordinates  $\tau$  over  $\mathcal{O}$  that moves  $P_0$  to infinity and apply the

result above. By [Corollary 4.6](#) (note that  $v(\tau) = 0$  in this case) and the fact that  $v(\tau(x)) = v(x)$ ,  $\mu(P)$  is unchanged by  $\tau$ .  $\square$

**Remark 8.6.** We see from the proof that for two points  $Q, Q'$  both having image on a component  $\Gamma$ , but with distinct reductions that are also distinct from those of  $P_0$  and  $\iota(P_0)$ , we always have

$$\mu([\Gamma(Q) - (Q')]) = -2g_v(\Gamma, \Gamma) - 2g_v(\Gamma, \Gamma_0 + \Gamma'_0) - c.$$

So the assumption that this value does not depend on the choice of  $Q$  and  $Q'$  is not really necessary.

**Theorem 8.7.** *Let  $C$  be a smooth projective curve of genus 2 defined over a nonarchimedean local field  $k$ , given by an integral Weierstrass model. Let  $J$  be the Jacobian of  $C$  and  $\mathcal{J}$  its Néron model over  $S = \text{Spec } \mathcal{O}$ . Assume that the minimal proper regular model  $C^{\min}$  of  $C$  over  $S$  is semistable and that  $\mu$  factors through the component group  $\Phi(\mathfrak{k})$  of  $\mathcal{J}$ . Let  $P \in J(k)$  be such that its image in  $\Phi(\mathfrak{k})$  is  $[\Gamma_1 - \Gamma_2]$ , where  $\Gamma_1$  and  $\Gamma_2$  are components of the special fiber of  $C^{\min}$ . Then we have*

$$\mu(P) = r(\Gamma_1, \Gamma_2).$$

*Proof.* Since  $\mu$  factors through  $\Phi(\mathfrak{k})$ , it follows that  $\mu([\Gamma(P_1) - (P_2)])$  vanishes when  $P_1$  and  $P_2$  map to the same component on the special fiber of  $C^{\min}$  and in general depends only on the components  $P_1$  and  $P_2$  map to. This shows that assumptions (i)–(iii) in [Proposition 8.5](#) are satisfied with  $\mu_1 = \mu_2 = 0$ . The claim follows.  $\square$

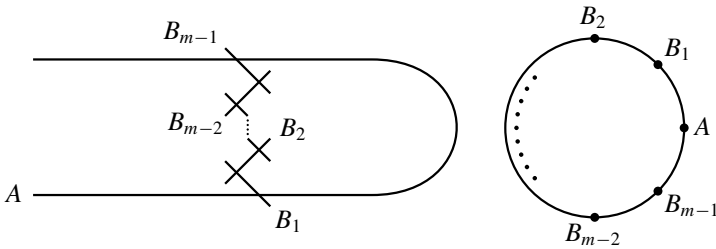
### 9. Formulas and bounds for $\mu(P)$ in the nodal reduction case

In this section and the next, we will deduce explicit formulas for  $\mu(P)$  when we have a stably minimal Weierstrass model  $\mathcal{C}$ . Recall that  $C^{\min}$  denotes the minimal proper regular model of  $\mathcal{C}$ . In the following, when we speak of components, points, and so on, of the special fiber of  $\mathcal{C}$  or  $C^{\min}$ , we always mean *geometric* components, points, and so on.

In this section we shall use [Theorem 8.7](#) and [Remark 8.4](#) to find explicit formulas for  $\mu(P)$  whenever  $C/k$  has nodal reduction, i.e., the special fiber  $\mathcal{C}_v$  of  $\mathcal{C}$  is reduced and all multiplicities are at most 2. In this case  $\mathcal{C}$  is semistable and therefore it has rational singularities. Let  $\Delta = \Delta(\mathcal{C})$  denote the discriminant of  $\mathcal{C}$ ; we assume that there is at least one node, so that  $v(\Delta) > 0$ .

Since there are at most three nodes in the special fiber of  $\mathcal{C}$ , we have to consider three different cases.

First suppose that there is a unique node in the special fiber of  $\mathcal{C}$  and set  $m = v(\Delta)$ . In the notation of [\[Namikawa and Ueno 1973\]](#) this is reduction type  $[I_{m-0-0}]$ . If  $m = 1$ , then  $\mathcal{C}$  is regular over  $S$ . In general, there is a unique component, which we denote by  $A$ , of genus 1 in the special fiber of  $C^{\min}$ . As in the case of multiplicative



**Figure 1.** The special fiber of reduction type  $[I_{m-0-0}]$  and its reduction graph.

reduction of elliptic curves (see, for example, [Silverman 1994]), the singular point on the special fiber is replaced by a string of  $m - 1$  components of  $\mathcal{C}^{\min}$ , all of genus 0 and multiplicity 1. We choose one of the two components intersecting  $A$  and call it  $B_1$  and number the other components  $B_2, \dots, B_{m-1}$  consecutively as in Figure 1.

Using [Bosch et al. 1990, Theorem 9.6.1], it is easy to see that the geometric component group  $\Phi(\bar{\mathfrak{k}})$  of the Néron model is generated by  $[B_1 - A]$  and is isomorphic to  $\mathbb{Z}/m\mathbb{Z}$ . We have  $[B_j - A] = j \cdot [B_1 - A]$  in  $\Phi(\bar{\mathfrak{k}})$ .

We set  $B_0 := B_m := A$ . Then we have the following result.

**Proposition 9.1.** *Suppose that there is a unique node in the special fiber of  $\mathcal{C}$ ; let  $m$  and the notation for the components of the special fiber of  $\mathcal{C}^{\min}$  be as above. If  $P \in J(k)$  maps to  $[B_i - A]$  in the component group, then we have*

$$\mu(P) = \frac{i(m - i)}{m}.$$

*Proof.* Since the given model is semistable, we can use Theorem 8.7 and Remark 8.4. One choice of  $g$  as in Remark 8.4 is given by

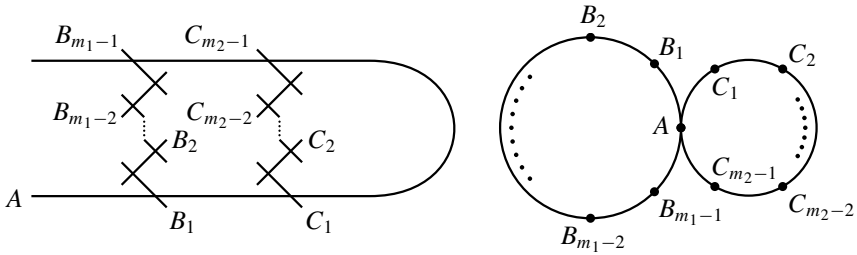
$$g(B_j) = \begin{cases} -\frac{j(m - i)}{m} & \text{if } 0 \leq j \leq i, \\ -\frac{i(m - j)}{m} & \text{if } i \leq j \leq m. \end{cases}$$

Then

$$\mu(P) = r(B_i, A) = -(g(B_i) - g(A)) = \frac{i(m - i)}{m}. \quad \square$$

**Remark 9.2.** Proposition 9.1 resembles the formula for the canonical local height on an elliptic curve with split multiplicative reduction given, for instance, in [Silverman 1988].

Now suppose that there are precisely two nodes in the special fiber of  $\mathcal{C}$ . The reduction type is  $[I_{m_1-m_2-0}]$  in the notation of [Namikawa and Ueno 1973], where  $m_1, m_2 \geq 1$  and  $m_1 + m_2 = v(\Delta)$ . The special fiber of  $\mathcal{C}^{\min}$  is obtained by blowing



**Figure 2.** The special fiber of reduction type  $[I_{m_1-m_2-0}]$  and its reduction graph.

up the two singular points of the special fiber of  $\mathcal{C}$  repeatedly and replacing them with a chain of  $m_1 - 1$  and  $m_2 - 1$  curves of genus 0, respectively. We call these components  $B_1, \dots, B_{m_1-1}, C_1, \dots, C_{m_2-1}$ , numbered as in Figure 2, where  $A$  contains all images of points reducing to a nonsingular point and we pick components  $B_1$  and  $C_1$  intersecting  $A$  as in the case of a unique node. The component group  $\Phi(\mathfrak{k})$  is isomorphic to  $\mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$  and is generated by  $[B_1 - A]$  and  $[C_1 - A]$ ; this follows again using [Bosch et al. 1990, Theorem 9.6.1]. If we have  $m_1 = 1$  or  $m_2 = 1$ , then the corresponding singular point on the special fiber of  $\mathcal{C}$  is regular and is therefore not blown up.

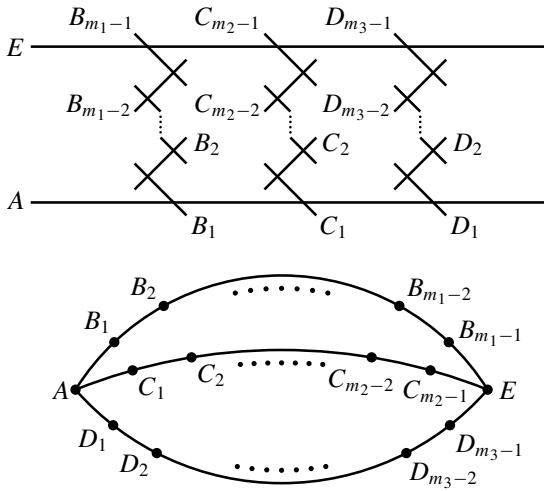
We set  $B_0 := B_{m_1} := C_0 := C_{m_2} := A$ . Then every element of the component group has a representative of the form  $[B_i - C_j]$  with  $0 \leq i \leq m_1$  and  $0 \leq j \leq m_2$ . The following result expresses  $\mu(P)$  in terms of this representative.

**Proposition 9.3.** *Suppose that there are exactly two nodes in the special fiber of  $\mathcal{C}$ ; let  $m_1$  and  $m_2$  and the notation for the components of the special fiber of  $\mathcal{C}^{\min}$  be as above. If  $P \in J(k)$  maps to  $[B_i - C_j]$  in the component group, then we have*

$$\mu(P) = \frac{i(m_1 - i)}{m_1} + \frac{j(m_2 - j)}{m_2}.$$

*Proof.* This is an easy computation along the same lines as in the proof of Proposition 9.1. □

The final case that we have to consider is the case of three nodes in the special fiber of  $\mathcal{C}$ , which then has two components. We call these components  $A$  and  $E$ . The special fiber of the minimal proper regular model is obtained using a sequence of blowups of the singular points; they are replaced by a chain of  $m_i - 1$  curves of genus 0 and multiplicity 1, respectively, where  $v(\Delta) = m_1 + m_2 + m_3$ . Hence the special fiber of  $\mathcal{C}^{\min}$  contains the two components  $A$  and  $E$ , connected by three chains of curves of genus 0 that we call  $B_1, \dots, B_{m_1-1}, C_1, \dots, C_{m_2-1}$  and  $D_1, \dots, D_{m_3-1}$ , respectively, where  $B_1, C_1$  and  $D_1$  intersect  $A$ , as shown in Figure 3. The reduction type is  $[I_{m_1-m_2-m_3}]$ .



**Figure 3.** The special fiber of reduction type  $[I_{m_1-m_2-m_3}]$  and its reduction graph.

By [Bosch et al. 1990, Proposition 9.6.10], the group  $\Phi(\bar{\mathfrak{E}})$  is isomorphic to  $\mathbb{Z}/d\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ , where

$$d = \gcd(m_1, m_2, m_3) \quad \text{and} \quad n = \frac{m_1 m_2 + m_1 m_3 + m_2 m_3}{d}.$$

We set  $B_0 := C_0 := D_0 := A$  and  $B_{m_1} := C_{m_2} := D_{m_3} := E$ . Then it is not hard to see that each element of  $\Phi(\bar{\mathfrak{E}})$  can be written in one of the forms

$$[B_i - C_j], \quad [C_j - D_l] \quad \text{or} \quad [D_l - B_i]$$

with  $0 \leq i \leq m_1$ ,  $0 \leq j \leq m_2$ ,  $0 \leq l \leq m_3$ . The following result allows us to express  $\mu(P)$  for any  $P \in J(k)$  in terms of the component  $P$  maps to.

**Proposition 9.4.** *Suppose that there are three nodes in the special fiber of  $\mathcal{C}$ ; let  $m_1, m_2, m_3$  and the notation for the components of the special fiber of  $\mathcal{C}^{\min}$  be as above. If  $P$  maps to  $[B_i - C_j]$  in the component group for some  $0 \leq i \leq m_1$  and  $0 \leq j \leq m_2$ , then we have*

$$\mu(P) = \frac{m_2 i(m_1 - i) + m_3(i + j)(m_1 - i + m_2 - j) + m_1 j(m_2 - j)}{m_1 m_2 + m_1 m_3 + m_2 m_3}.$$

The formulas for  $[C_j - D_l]$  and  $[D_l - B_i]$  are analogous.

*Proof.* The proof is analogous to those of Propositions 9.1 and 9.3. To find  $g$ , use that it is piecewise linear on the segments  $AB_1 \cdots B_i$ ,  $B_i \cdots B_{m_1-1}E$ ,  $AC_1 \cdots C_j$ ,  $C_j \cdots C_{m_2-1}E$ ,  $AD_1 \cdots D_{m_3-1}E$  and the relations at the vertices  $A, E, B_i, C_j$ .  $\square$

**Remark 9.5.** Using the relation  $\varepsilon(P) = 4\mu(P) - \mu(2P)$ , one can show by a somewhat tedious computation involving a number of different cases that if the image of  $P$  in  $\Phi(\mathfrak{k})$  is  $[\Gamma_1 - \Gamma_2]$ , where  $\Gamma_1$  and  $\Gamma_2$  are components of the special fiber of  $\mathcal{C}^{\min}$ , then  $\varepsilon(P)$  is the “distance” between  $\Gamma_1$  and  $\Gamma_2$  in the reduction graph, where the “length” of the path between  $B_i$  and  $B_j$  (say, analogously for  $C_i, C_j$  and  $D_i, D_j$ ) is  $\min\{2|i - j|, m_1\}$ , and otherwise “lengths” are additive. In particular, if  $\Phi(\mathfrak{k}) = \Phi(\bar{\mathfrak{k}})$ , then

$$\gamma = \max\{\varepsilon(P) : P \in J(k)\} = \max\{m_i + m_j - \delta_{ij} : 1 \leq i < j \leq 3\},$$

where  $\delta_{ij} = 0$  if both  $m_i$  and  $m_j$  are even, and  $\delta_{ij} = 1$  otherwise.

**Remark 9.6.** In order to use the results of this section to actually compute  $\mu(P)$  for a given point  $P \in J(k)$ , we need to be able to find the component of  $\mathcal{J}_v$  that  $P$  reduces to. One approach is to find  $P_1, P_2 \in C$  such that  $P = [(P_1) - (P_2)]$  and find the reductions of  $P_1$  and  $P_2$  to  $\mathcal{C}_v^{\min}$ . Another approach is to use a transformation (possibly defined over an unramified extension of  $k$ ) to move the singular points to  $\infty, (0, 0)$  and  $(1, 0)$ , respectively. Then we can (possibly after applying another transformation) read off the component that  $P$  maps to directly from the Kummer coordinates of  $P$ .

The discussion of this section shows that we get the following results on the local height constant  $\beta = \max\{\mu(P) : P \in J(k)\}$ . Recall that  $\gamma = \max\{\varepsilon(P) : P \in J(k)\}$  and that  $\frac{1}{4}\gamma \leq \beta \leq \frac{1}{3}\gamma$ . We will see that in many cases the lower bound is attained.

Let  $P$  be a node on  $\mathcal{C}_v$ ; it is defined over a finite extension of  $\mathfrak{k}$ . We say that the node  $P$  is *split* if the two tangent directions of the branches at  $P$  are defined over every extension that  $P$  is defined over, otherwise  $P$  is *nonsplit*. We say that  $P$  is *even* if its contribution  $m_i$  to the valuation of the discriminant is even, and *odd* otherwise.

**Corollary 9.7.** *Suppose that  $C/k$  is a smooth projective curve of genus 2 given by an integral Weierstrass model  $\mathcal{C}$  such that there is a unique node in the special fiber of  $\mathcal{C}$  and let  $m = v(\Delta)$ . Then we have*

$$\beta = \frac{1}{2m} \left\lfloor \frac{m^2}{2} \right\rfloor \leq \frac{v(\Delta)}{4}$$

if the node is split or even, and  $\beta = 0$  otherwise.

*Proof.* This follows from [Proposition 9.1](#), taking into account that if  $m$  is odd and the node is nonsplit, then the group  $\Phi(\mathfrak{k})$  is trivial. □

**Remark 9.8.** Using the relation  $\varepsilon(P) = 4\mu(P) - \mu(2P)$ , one can check that

$$\varepsilon(P) = 2 \min\{i, m - i\} \quad \text{if } P \text{ maps to } [B_i - A] \text{ in } \Phi(\mathfrak{k}).$$

If  $m$  is even (and  $\beta > 0$ ), then  $\beta = \frac{1}{4}m = \frac{1}{4}\gamma$ . If  $m$  is odd, then  $\beta = \frac{1}{4}(m - \frac{1}{m})$  and  $\gamma = m - 1$ , so  $\beta/\gamma = \frac{1}{4}(1 + \frac{1}{m})$  approaches  $\frac{1}{4}$  as  $m \rightarrow \infty$ , but for  $m = 3$  (the worst case), we have  $\beta = \frac{1}{3}\gamma$ .

**Corollary 9.9.** *Suppose that  $C/k$  is a smooth projective curve of genus 2 given by an integral Weierstrass model  $\mathcal{C}$  such that there are exactly two nodes in the special fiber of  $\mathcal{C}$ . Let  $v(\Delta) = m_1 + m_2$  as above. Then we have*

$$\beta = \frac{1}{2m_1} \left\lfloor \frac{m_1^2}{2} \right\rfloor + \frac{1}{2m_2} \left\lfloor \frac{m_2^2}{2} \right\rfloor \leq \frac{v(\Delta)}{4}$$

if each of the nodes is split or even,

$$\beta = \frac{1}{2m_i} \left\lfloor \frac{m_i^2}{2} \right\rfloor$$

if the node corresponding to  $m_i$  is split or even and the other node is nonsplit and odd, and  $\beta = 0$  if both nodes are nonsplit and odd.

*Proof.* This follows from Proposition 9.3, taking into account the action of Frobenius on  $\Phi(\bar{\mathbb{F}})$ . □

If we have three nodes, then it helps to take the field of definition of the nodes into account.

**Corollary 9.10.** *Suppose that  $C/k$  is a smooth projective curve of genus 2 given by an integral Weierstrass model  $\mathcal{C}$  such that there are three nodes in the special fiber of  $\mathcal{C}$ . We say that  $\mathcal{C}$  is split if the two components  $A$  and  $E$  of the special fiber of  $\mathcal{C}^{\min}$  are defined over  $\mathbb{F}$ ; otherwise  $\mathcal{C}$  is nonsplit. Let  $v(\Delta) = m_1 + m_2 + m_3$  as above and set  $M = m_1m_2 + m_1m_3 + m_2m_3$ .*

(a) *If all nodes are  $\mathbb{F}$ -rational,  $\mathcal{C}$  is split, and we have  $m_1 \geq m_3$  and  $m_2 \geq m_3$ , then*

$$\beta = \frac{1}{2M} \left( m_2 \left\lfloor \frac{m_1^2}{2} \right\rfloor + m_3 \left\lfloor \frac{(m_1 + m_2)^2}{2} \right\rfloor + m_1 \left\lfloor \frac{m_2^2}{2} \right\rfloor \right) \leq \frac{m_1 + m_2}{4} < \frac{v(\Delta)}{4}.$$

(b) *If all nodes are  $\mathbb{F}$ -rational, but  $\mathcal{C}$  is nonsplit, then*

$$\beta = \max\{0\} \cup \left\{ \frac{1}{4}(m_i + m_j) : 1 \leq i < j \leq 3, m_i \text{ and } m_j \text{ even} \right\}.$$

(c) *If two of the nodes lie in a quadratic extension of  $\mathbb{F}$  and are conjugate over  $\mathbb{F}$  and one is  $\mathbb{F}$ -rational, then*

$$\beta = \begin{cases} \frac{m_1}{M} \max \left\{ \left\lfloor \frac{m_1^2}{2} \right\rfloor + m_1m_3, \left\lfloor \frac{m_3^2}{2} \right\rfloor + m_1 \left\lfloor \frac{m_3}{2} \right\rfloor \right\} & \text{if } \mathcal{C} \text{ is split,} \\ \frac{m_1}{2} & \text{if } \mathcal{C} \text{ is nonsplit and } m_1 \text{ is even,} \\ 0 & \text{otherwise,} \end{cases}$$

where  $m_3$  corresponds to the rational node (and  $m_1 = m_2$ ).



(d) *If all nodes are defined over a cubic extension of  $\mathfrak{k}$  and are conjugate over  $\mathfrak{k}$ , then  $m_1 = m_2 = m_3 = \frac{1}{3}v(\Delta)$  and*

$$\beta = \begin{cases} \frac{1}{9}v(\Delta) & \text{if } C \text{ is split,} \\ 0 & \text{otherwise.} \end{cases}$$

*Proof.* The proof of (a) follows easily from [Proposition 9.4](#).

For the other cases, note that in the nonsplit case some power of Frobenius acts as negation on the component group  $\Phi(\bar{\mathfrak{k}})$ , so the only elements of  $\Phi(\mathfrak{k})$  are elements of order 2 in  $\Phi(\bar{\mathfrak{k}})$ , which correspond to  $[B_{m_1/2} - C_{m_2/2}]$  if  $m_1$  and  $m_2$  are even (where  $\mu$  takes the value  $\frac{1}{4}(m_1 + m_2)$ ), and similarly with the obvious cyclic permutations.

In the situation of (c), we must have  $m_1 = m_2$ . If  $P = [(P_1) - (P_2)] \in J(k)$  and  $P_1 \in C(\bar{k})$  maps to one of the conjugate nodes, then  $P_2$  must map to the other, so all  $P \in J(k)$  must map to a component of the form  $[B_i - C_j]$  or  $[D_i - D_j]$ . Now the result in the split case follows from a case distinction depending on whether  $m_1 \leq m_3$  or not. In the nonsplit case, the only element of order 2 that is defined over  $\mathfrak{k}$  is  $[B_{m_1/2} - C_{m_1/2}]$  if it exists.

In the situation of (d), the group  $\Phi(\mathfrak{k})$  is of order 3 (generated by  $[E - A]$ ) in the split case and trivial in the nonsplit case. □

Extending the valuation  $v: k^\times \rightarrow \mathbb{Z}$  to  $\bar{v}: \bar{k}^\times \rightarrow \mathbb{Q}$ , we get extensions of  $\varepsilon$  and  $\mu$  to  $J(\bar{k})$ . Denote  $\max\{\mu(P) : P \in J(\bar{k})\}$  by  $\bar{\beta}$  and  $\max\{\varepsilon(P) : P \in J(\bar{k})\}$  by  $\bar{\gamma}$ . Then by the discussion at the beginning of [Section 8](#) and the results above, we find that

$$\bar{\beta} = \frac{1}{4}\bar{\gamma} = \frac{1}{4}v(\Delta),$$

when there are one or two nodes, and

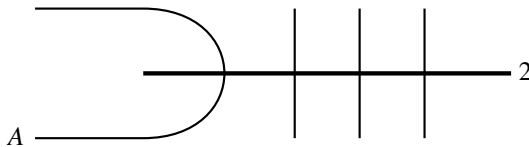
$$\frac{1}{6}v(\Delta) \leq \bar{\beta} = \frac{1}{4}\bar{\gamma} = \frac{1}{4}(v(\Delta) - \min\{m_1, m_2, m_3\}) < \frac{1}{4}v(\Delta),$$

when there are three nodes. (Equality is achieved as soon as the Galois action on  $R(C)$  is trivial and the ramification index is even.)

### 10. Formulas and bounds for $\mu(P)$ in the cuspidal reduction case

In this section we consider the case of a stably minimal Weierstrass model  $\mathcal{C}$  such that there are (one or two) points of multiplicity 3 on the special fiber. These points are either both  $\mathfrak{k}$ -rational or they are defined over a quadratic extension of  $\mathfrak{k}$  and are conjugate over  $\mathfrak{k}$ .

In the notation of [\[Namikawa and Ueno 1973\]](#), the reduction type is of the form  $[\mathcal{K}_1 - \mathcal{K}_2 - l]$ , where  $l \geq 0$  and  $\mathcal{K}_j$  is an elliptic Kodaira type for  $j \in \{1, 2\}$ . We can



**Figure 4.** The special fiber of reduction type  $[I_0 - I_0^* - 0]$ .

compute  $\mathcal{K}_1$ ,  $\mathcal{K}_2$  and  $l$  as in [Liu 1994, §6.1]. By [Liu 1994, §7], we have

$$\Phi(\bar{\mathfrak{f}}) \cong \Phi_1(\bar{\mathfrak{f}}) \times \Phi_2(\bar{\mathfrak{f}}),$$

where  $\Phi_j$  is the component group of an elliptic curve with Kodaira type  $\mathcal{K}_j$ . As in the previous section, we write  $\Delta = \Delta(\mathcal{C})$  for the discriminant of the model  $\mathcal{C}$ .

If  $\mathcal{C}$  is not regular, then we can compute the minimal proper regular model  $\mathcal{C}^{\min}$  of  $\mathcal{C}$  from  $\mathcal{C}$  by a sequence of blowups in the singular point(s) of  $\mathcal{C}$ , so the corresponding morphism  $\zeta : \mathcal{C}^{\min} \rightarrow \mathcal{C}$  is the minimal desingularization of  $\mathcal{C}$ .

Suppose that  $l > 0$ . Then the special fiber of  $\mathcal{C}^{\min}$  consists of Kodaira types  $\mathcal{K}_1$  and  $\mathcal{K}_2$ , connected by a chain of  $l - 1$  rational curves. See for example Figure 5. The desingularization  $\zeta$  contracts  $\mathcal{K}_2$  to one of the singular points; in this case we say that this point *corresponds to*  $\mathcal{K}_2$ . If there is another singular point in  $\mathcal{C}_v(\bar{\mathfrak{f}})$ , then it corresponds to  $\mathcal{K}_1$ ; otherwise we must have  $\mathcal{K}_1 = I_0$ .

Suppose now that  $l = 0$ . If both  $\mathcal{K}_1$  and  $\mathcal{K}_2$  are good or multiplicative, then we are in the situation  $[I_{m_1 - m_2 - 0}]$  for some  $m_1, m_2 \geq 0$ , which we have discussed in the previous section. So we may assume that at least one of the  $\mathcal{K}_j$  is additive, say  $\mathcal{K}_2$ . Then  $\mathcal{C}_v^{\min}$  looks like Kodaira type  $\mathcal{K}_2$ , but with one of the rational curves replaced by (see [Namikawa and Ueno 1973]):

- a curve  $A$  of genus 1 if  $\mathcal{K}_1 = I_0$  (see Figure 4 for the case  $\mathcal{K}_2 = I_0^*$ );
- one of the rational components of  $\mathcal{K}_1$ , otherwise; the remainder of  $\mathcal{K}_1$  is then attached to this component.

We say that a singularity corresponds to one of the Kodaira types  $\mathcal{K}_1$  or  $\mathcal{K}_2$  similarly to the case  $l > 0$ .

**Lemma 10.1.** *Suppose that the residue characteristic of  $k$  is not 2. Let  $\mathcal{C}$  be given by a stably minimal Weierstrass model with reduction type  $[\mathcal{K}_1 - \mathcal{K}_2 - l]$ . Then after at most a quadratic unramified extension of  $k$  there is a stably minimal Weierstrass model*

$\mathcal{C} : Y^2 = F(X, Z) = f_6 X^6 + f_5 X^5 Z + f_4 X^4 Z^2 + X^3 Z^3 + f_2 X^2 Z^4 + f_1 X Z^5 + f_0 Z^6$   
of  $\mathcal{C}$ , isomorphic to the given model of  $\mathcal{C}$ , such that the elliptic curve with Weierstrass model

$$\mathcal{E}_1 : Y^2 Z = X^3 + f_2 X^2 Z + f_1 X Z^2 + f_0 Z^3$$

has Kodaira type  $\mathcal{K}_1$  and the elliptic curve with Weierstrass model

$$\mathcal{E}_2: Y^2Z = X^3 + f_4X^2Z + f_5XZ^2 + f_6Z^3$$

has Kodaira type  $\mathcal{K}_2$ .

*Proof.* After possibly making a quadratic unramified extension and applying a transformation, we can assume that there is a unique point  $\infty \in C_v(\mathbb{k})$  at infinity on the special fiber and that it is a cusp, corresponding to  $\mathcal{K}_2$ ; see the discussion preceding the lemma. Moreover, we can assume that if there is another singular point in  $C_v(\mathbb{k})$ , then this point is  $P = (0, 0) \in C_v(\mathbb{k})$  (in which case it must correspond to  $\mathcal{K}_1$ ).

Because the residue characteristic is not 2, we may assume that  $\mathcal{C}$  has  $H = 0$  and that  $f_3$  is a unit. By Hensel’s lemma there is a factorization  $F = F_1F_2$ , where  $F_2$  is a cubic form reducing to  $Z^3$ . Similarly, we may assume that  $F_1$  reduces to  $X^3$  if there is a cusp at  $P$  and to  $X^2(X + aZ)$  with  $a \neq 0$  if there is a node at  $P$ ; otherwise  $F_1$  is squarefree. Consider the elliptic curves given by the Weierstrass models

$$\mathcal{D}_1: Y^2Z = F_1(X, Z) \quad \text{and} \quad \mathcal{D}_2: Y^2Z = F_2(Z, X).$$

We first show that  $\mathcal{D}_1$  has Kodaira type  $\mathcal{K}_1$  and  $\mathcal{D}_2$  has Kodaira type  $\mathcal{K}_2$ .

If  $\mathcal{D}_1$  is not minimal, then we can apply a transformation to  $\mathcal{C}$  which makes  $\mathcal{D}_1$  minimal. This decreases the valuation of the discriminant  $\Delta(\mathcal{D}_1)$ , but increases the valuation of  $\Delta(\mathcal{D}_2)$  by the same amount. The resulting model is still stably minimal and the resulting  $F_2$  still reduces to  $Z^3$ . Hence we may assume that  $\mathcal{D}_1$  is minimal.

Let  $Q = (0, 0) \in \mathcal{D}_{1,v}(\mathbb{k})$ ; then  $\mathcal{D}_1$  is smooth outside  $Q$ . Note that  $F_2$  is a unit in  $\mathcal{O}_{\mathcal{C},P}$ , so that  $P$  is a smooth point if and only if  $Q$  is a smooth point, in which case  $\mathcal{D}_1$  has reduction type  $I_0 = \mathcal{K}_1$ . More generally,  $\mathcal{C}$  is regular at  $P$  if and only if  $\mathcal{D}_1$  is regular at  $Q$ , and  $P$  is a node (resp. a cusp) if and only if  $Q$  is a node (resp. a cusp). Recall that  $P$  corresponds to  $\mathcal{K}_1$ , so that  $\mathcal{D}_1$  has reduction type  $I_1$  (resp.  $II$ ) if and only if  $\mathcal{K}_1 = I_1$  (resp.  $\mathcal{K}_1 = II$ ).

Now suppose that  $\mathcal{C}$  is not regular at  $P$  and  $\mathcal{D}_1$  is not regular at  $Q$ . The minimal desingularization  $\xi: \mathcal{C}' \rightarrow \mathcal{C}$  in  $P$  can be computed by a sequence of blowups, starting with the blowup of  $\mathcal{C}$  in  $P$ . The preimage of  $P$  under the latter map is contained in the chart  $\mathcal{C}^1$  obtained by dividing the  $x$ - and  $y$ -coordinates by the uniformizing element  $\pi$ . Similarly, in order to compute the minimal desingularization  $\xi_1: \mathcal{D}'_1 \rightarrow \mathcal{D}_1$  in  $Q$ , we first blow up  $\mathcal{D}_1$  in  $Q$ ; then the chart  $\mathcal{D}^1_1$  obtained by dividing the  $x$ - and  $y$ -coordinates by  $\pi$  contains the preimage of  $Q$ . But because  $F_2$  reduces to  $Z^3$ , the special fibers of  $\mathcal{C}^1$  and  $\mathcal{D}^1_1$  are identical. This continues to hold after further blowups (if any are necessary), so we have  $\xi^{-1}(P) = \xi_1^{-1}(Q)$ . There are no exceptional components in these preimages, since we assumed that  $\mathcal{D}_1$  is minimal. Therefore  $\mathcal{D}'_1$  is in fact the minimal proper regular model of the elliptic curve defined by  $\mathcal{D}_1$ . Since the minimal desingularization of  $\mathcal{C}'$  in the point  $\infty \in \mathcal{C}'_v(\mathbb{k})$  leads to  $\mathcal{C}^{\min}$ , and since  $P$  corresponds to  $\mathcal{K}_1$ , we deduce that  $\mathcal{D}_1$  has Kodaira type  $\mathcal{K}_1$ .

A similar argument (for which we first apply a transformation to make  $\mathcal{D}_2$  minimal) shows that  $\mathcal{D}_2$  has Kodaira type  $\mathcal{K}_2$ . To complete the proof of the lemma, we therefore only need to make sure that  $\mathcal{E}_i$  has the same reduction type as  $\mathcal{D}_i$  for  $i = 1, 2$ . This is certainly satisfied if the coefficients of  $\mathcal{E}_i$  and  $\mathcal{D}_i$  agree modulo  $\pi^{N_i+1}$ , where  $N_i$  is the number of blowups needed to construct the minimal desingularization of  $\mathcal{D}_i$ . Suppose that  $F_1 = a_0Z^3 + a_1XZ^2 + a_2X^2Z + a_3X^3$  and  $F_2 = b_3Z^3 + b_2XZ^2 + b_1X^2Z + b_0X^3$ . Writing out the coefficients of  $F$  in terms of the coefficients of  $F_1$  and  $F_2$ , we see that it suffices to have

$$\begin{aligned} v(a_0b_2) &> v(a_1), & v(a_0b_1 + a_2b_2) &> v(a_2), \\ v(b_0a_2) &> v(b_1), & v(a_1b_0 + a_2b_1) &> v(b_2). \end{aligned}$$

If this is not satisfied, it can be achieved by acting on the given stably minimal Weierstrass model via a suitable element of  $\text{GL}_2(\mathcal{O})$  as in Section 4. Finally, we scale the variables to get  $f_3 = 1$ . □

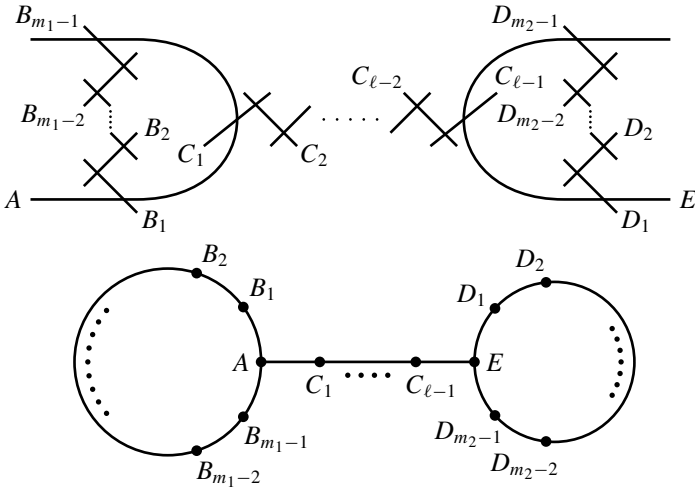
**Remark 10.2.** If the residue characteristic is 2, then it is not hard to see that one can also construct a stably minimal Weierstrass model  $\mathcal{C}$  and corresponding elliptic Weierstrass models  $\mathcal{E}_1$  and  $\mathcal{E}_2$  as in the lemma in a similar way. The construction is more cumbersome, since we cannot assume  $H = 0$ .

In view of Theorem 7.4 we want a condition for  $\mathcal{C}$  to have rational singularities.

**Lemma 10.3.** *The model  $\mathcal{C}$  has rational singularities if and only if  $l = 0$ .*

*Proof.* We may assume that  $\mathcal{C}$  is as in Lemma 10.1 or Remark 10.2. Then all points in  $\mathcal{C}_v(\mathbb{k}) \setminus \{\infty, P\}$  are nonsingular, where  $\infty \in \mathcal{C}_v(\mathbb{k})$  is the unique point at infinity, and  $P = (0, 0) \in \mathcal{C}_v(\mathbb{k})$ . If  $\mathcal{C}$  is regular in  $P$ , then  $P$  is a rational singularity. If not, then, by [Artin 1966, Theorem 3],  $P$  is a rational singularity if and only if the fundamental cycle of  $\xi^{-1}(P)$  has arithmetic genus 0, where  $\xi$  is any desingularization of  $P$ . In particular, the assertion that  $P$  is a rational singularity depends only on the configuration of  $\xi^{-1}(P)$ , where  $\xi: \mathcal{C}' \rightarrow \mathcal{C}$  is the minimal desingularization of  $P$ . Now let  $\mathcal{E}_1$  be as in Lemma 10.1 or Remark 10.2, and let  $\xi_1: \mathcal{E}'_1 \rightarrow \mathcal{E}_1$  denote the minimal desingularization of the singular point  $Q = (0, 0) \in \mathcal{E}_{1,v}(\mathbb{k})$ ; then the assertion that  $Q$  is a rational singularity depends only on the configuration of  $\xi_1^{-1}(Q)$ . We have  $\xi^{-1}(P) = \xi_1^{-1}(Q)$  as in the proof of Lemma 10.1 (this also works when  $\text{char } \mathbb{k} = 2$  and does not require minimality of  $\mathcal{E}_1$ ). In particular,  $P$  is a rational singularity if and only if  $Q$  is a rational singularity.

A similar argument proves the corresponding statement for  $\mathcal{E}_2$ . Hence  $\mathcal{C}$  has rational singularities if and only if both  $\mathcal{E}_1$  and  $\mathcal{E}_2$  have rational singularities. By [Conrad 2005, Corollary 8.4] a Weierstrass model of an elliptic curve has rational singularities if and only if it is minimal. But it is easy to see that  $\mathcal{E}_1$  and  $\mathcal{E}_2$  are both minimal if and only if  $l = 0$ . □



**Figure 5.** The special fiber of reduction type  $[I_{m_1} - I_{m_2} - l]$  and its reduction graph.

According to [Lemma 10.3](#), not all singularities of the given stably minimal Weierstrass model  $\mathcal{C}$  are rational when  $l > 0$ . The following example shows that in this situation  $\varepsilon(P) \neq 0$ , and hence  $\mu(P) \neq 0$ , can indeed occur for  $P \in J_0(k)$ .

**Example 10.4.** Let  $p$  be an odd prime and let  $C/\mathbb{Q}_p$  be given by

$$Y^2 = Z(X^2 + Z^2)(X^3 + p^5 XZ^2 + p^8 Z^3).$$

Let  $P_1 = (0, p^4) \in C(\mathbb{Q}_p)$  and  $P_2 = \iota(P_1)$ . The reduction type is  $[I_0 - III - 1]$  and hence  $\#\Phi(\bar{\mathfrak{k}}) = 2$ . It turns out that both  $P_1$  and  $P_2$  map to the same component and so we have  $P = [(P_1) - (P_2)] \in J_0(k)$ . The image of  $P$  on the Kummer surface is of the form  $(x_1 : 0 : 0 : x_4)$ , where  $v(x_4) - v(x_1) = 2$ . We get  $\varepsilon(P) = \varepsilon(2P) = 6$  and  $\mu(P) = \mu(2P) = 2$ .

The case of semistable reduction, corresponding to reduction type  $[I_{m_1} - I_{m_2} - l]$  (see [Figure 5](#)) deserves special attention. Here  $l \geq 1$ , by the discussion above. Note that  $m_1 = 0$  (or  $m_2 = 0$ ) is possible; in that case  $A$  (or  $E$ ) is a curve of genus 1 and there are no components  $B_i$  (or  $D_i$ ). If  $m_1 = 1$  (or  $m_2 = 1$ ), then  $A$  (or  $E$ ) is a nodal curve (again there are no  $B_i$  or  $D_i$ ). After perhaps an unramified quadratic extension, we can assume that all components in the “chain” that connects the two polygons in the special fiber of  $\mathcal{C}^{\min}$  are defined over  $\bar{\mathfrak{k}}$ . There are then  $l + 1$  different (meaning pairwise nonisomorphic over  $\mathcal{O}$ ) minimal Weierstrass models of the curve; compare the proof of [Lemma 5.4](#). Explicitly, these models can be taken to have the form

$$\begin{aligned} \mathcal{C}_j : Y^2 + (h_0\pi^{3j}Z^3 + h_1\pi^jZ^2X + h_2\pi^{l-j}ZX^2 + h_3\pi^{3(l-j)}X^3)Y \\ = f_0\pi^{6j}Z^6 + f_1\pi^{4j}XZ^5 + f_2\pi^{2j}X^2Z^4 + X^3Z^3 \\ + f_4\pi^{2(l-j)}X^4Z^2 + f_5\pi^{4(l-j)}X^5Z + f_6\pi^{6(l-j)}X^6 \end{aligned} \quad (10-1)$$

for  $j = 0, 1, \dots, l$ , where

$$y^2 + h_1xy + h_0y = x^3 + f_2x^2 + f_1x + f_0$$

and

$$y^2 + h_2xy + h_3y = x^3 + f_4x^2 + f_5x + f_6$$

are minimal Weierstrass equations of elliptic curves of reduction types  $I_{m_1}$  and  $I_{m_2}$ , respectively. Such a model corresponds to the vertex  $C_j$  of the reduction graph (where we set  $C_0 = A$  and  $C_l = E$ ); the corresponding component of the special fiber of  $\mathcal{C}^{\min}$  is the one that is visible in the special fiber of  $\mathcal{C}_j$ . The valuation of the discriminant of  $\mathcal{C}_j$  is  $m_1 + m_2 + 12l$  and does not depend on  $j$ .

A *simple path* in  $R(C)$  is a subgraph that is a tree without vertices of valency  $\geq 3$ . Let  $P_1, P_2 \in C(k)$  reduce to components  $\Gamma_1$  and  $\Gamma_2$  of the special fiber of  $\mathcal{C}^{\min}$ , respectively. Consider the model  $\mathcal{C}_j$  of  $C$ . If there is a simple path from  $\Gamma_1$  to  $\Gamma_2$  in the reduction graph that passes through  $C_j$ , then we say that  $\mathcal{C}_j$  *lies between*  $P_1$  and  $P_2$ . We denote the  $\mu$ -function computed with respect to  $\mathcal{C}_j$  by  $\mu_j$ .

**Proposition 10.5.** *Assume that  $C$  has semistable reduction of type  $[I_{m_1} - I_{m_2} - l]$ . Let  $P_1, P_2 \in C(k)$  be points reducing to components  $\Gamma_1$  and  $\Gamma_2$  of the special fiber of  $\mathcal{C}^{\min}$  and let  $j \in \{0, 1, \dots, l\}$ . Define  $j_{\min}$  and  $j_{\max}$  to be the smallest and largest  $j' \in \{0, 1, \dots, l\}$  such that  $\mathcal{C}_{j'}$  lies between  $P_1$  and  $P_2$ . Let  $P = [(P_1) - (P_2)] \in J(k)$ . Then*

$$r(\Gamma_1, \Gamma_2) + j_{\max} - j_{\min} \leq \mu_j(P) \leq r(\Gamma_1, \Gamma_2) + |j - j_{\max}| + |j - j_{\min}|.$$

If  $\mathcal{C}_j$  lies between  $P_1$  and  $P_2$ , then the inequalities are equalities.

*Proof.* First note that the last statement follows from the first, since  $j_{\min} \leq j \leq j_{\max}$  implies  $j_{\max} - j_{\min} = |j - j_{\max}| + |j - j_{\min}|$ .

Let  $B_0 = B_{m_1} = A$  and  $D_0 = D_{m_2} = E$ . We prove a number of lemmas.

**Lemma 10.6.** *If  $j = j_{\max} = j_{\min} \in \{0, l\}$ , then  $\mu_j(P) = r(\Gamma_1, \Gamma_2)$ .*

*Proof.* We assume that  $j = j_{\max} = j_{\min} = l$ ; the other case is analogous. Then  $\Gamma_1$  and  $\Gamma_2$  are both of the form  $D_i$ , and we consider the model  $\mathcal{C}_l$ . We first claim that  $\mu(P) = 0$  if  $\Gamma_1 = \Gamma_2$ , but the images of  $P_1$  and  $P_2$  on  $\Gamma_1$  are distinct. This is clear if  $\Gamma_1 = D_0 = E$ , since in this case  $P$  is in the image of  $\alpha$ ; compare Lemmas 7.1 and 7.2. Otherwise, we note that the points with nonzero multiplicity on the special fiber of  $\mathcal{C}_l$  have multiplicities 1, 2 and 3. Transforming the equation over  $\mathcal{O}$  if necessary, we can assume that its reduction is case 7 in Table 1 of [Stoll 2002] or (if the residue characteristic is 2) case 5 in Table 2 here.

Recall that  $\Gamma_1 = \Gamma_2 = D_i$ , where we can assume  $0 < i \leq \frac{1}{2}m_2$ . Applying a transformation, we may assume that the points  $P_1 = (\xi_1 : \eta_1 : 1)$  and  $P_2 = (\xi_2 : \eta_2 : 1)$  both reduce to  $(0 : 0 : 1)$  modulo  $\pi$  and that  $m_2 = \min\{v(f_0), 2v(f_1)\}$ . First suppose

that  $i < \frac{1}{2}m_2$ . We then have  $v(\xi_1) = v(\xi_2) = v(\xi_1 - \xi_2) = i$ . Normalizing the Kummer coordinates  $x$  of  $P$  so that  $x_1 = 1$ , we can check that  $v(x_2)$  and  $v(x_3)$  are positive, but that  $v(x_4) = 0$ . This follows because  $\Gamma_1 = D_i = \Gamma_2$  implies that  $v(f_2\xi_1\xi_2 + 2\eta_1\eta_2) = 2i$  if  $\text{char}(\mathbb{k}) \neq 2$  and  $H = 0$  and that  $v(\xi_1\eta_2 + \xi_2\eta_1) = 2i$  if  $\text{char}(\mathbb{k}) = 2$ . By a similar argument, the reduction of the image of  $P$  on the Kummer surface has nonvanishing last coordinate if  $m_2$  is even and  $i = \frac{1}{2}m_2$ . According to the tables, this implies that  $\varepsilon(P) = 0$  and therefore also  $\mu(P) = 0$ .

Now consider the case that  $\Gamma_1$  and  $\Gamma_2$  do not necessarily coincide. The considerations above imply that the assumptions of [Proposition 8.5](#) are satisfied with  $\mu_1 = \mu_2 = 0$  (where we use [Lemma 3.7](#) for the first assumption); the proposition then establishes the claim. □

**Lemma 10.7.** *Assume that  $\Gamma_1 = \Gamma_2 = C_j$  with  $0 < j < l$ . Then  $\mu_j(P) = 0$ .*

*Proof.* In this case,  $P$  is in the image of  $\alpha$ , so the claim follows by [Proposition 7.3](#). □

Note that [Lemmas 10.6](#) and [10.7](#) establish the claim of [Proposition 10.5](#) in all cases such that  $j = j_{\min} = j_{\max}$ .

**Lemma 10.8.** *Assume that both  $C_j$  and  $C_{j+1}$  lie between  $P_1$  and  $P_2$ , where  $0 \leq j < l$ . Then  $\mu_j(P) = \mu_{j+1}(P)$ .*

*Proof.* Let  $\tau : (\xi : \eta : \zeta) \mapsto (\pi\xi : \eta : \pi^{-1}\zeta)$ ; then  $\tau$  gives an isomorphism from the generic fiber of  $C_j$  to that of  $C_{j+1}$ . The induced map on Kummer coordinates is

$$(x_1, x_2, x_3, x_4) \mapsto (\pi^{-2}x_1, x_2, \pi^2x_3, x_4);$$

we have  $v(\tau) = 0$ . Since both  $C_j$  and  $C_{j+1}$  lie between  $P_1$  and  $P_2$ , assuming that  $\Gamma_1$  is to the left and  $\Gamma_2$  to the right of  $C_j$  and  $C_{j+1}$ , we must have that the  $x$ -coordinate of  $P_1$  on  $C_j$  does not reduce to infinity, whereas that of  $P_2$  does. For normalized Kummer coordinates  $x = (x_1, x_2, x_3, x_4)$  of  $P$  on the Kummer surface associated to  $C_j$ , this implies  $v(x_2) = 0$  (the point is not in the kernel of reduction, so  $v(x_4) \geq \min\{v(x_1), v(x_2), v(x_3)\}$ ) and  $v(x_1) > 0$ . Comparing valuations in the equation of  $C_j$ , we see that  $P_2 = (1 : \eta : \zeta)$  must have  $v(\zeta) \geq 2$ , which implies  $v(x_1) \geq 2$ . It follows that  $v(\tau(x)) = 0 = v(x)$ . By [Corollary 4.6](#) we also have  $\hat{\lambda}(\tau(x)) = \hat{\lambda}(x)$  (recall that  $v(\tau) = 0$ ). Since

$$-v(x) - \mu_j(P) = \hat{\lambda}(x) = \hat{\lambda}(\tau(x)) = -v(\tau(x)) - \mu_{j+1}(P),$$

the claim follows. □

**Lemma 10.9.** *If  $C_j$  lies between  $P_1$  and  $P_2$ , then  $\mu_j(P)$  depends only on  $\Gamma_1$  and  $\Gamma_2$ .*

*Proof.* Let  $P'_1, P'_2 \in C(k)$  be points also mapping to  $\Gamma_1$  and  $\Gamma_2$ , respectively. We assume without loss of generality that  $\Gamma_1$  is to the left of  $\Gamma_2$ . By [Lemma 10.6](#) or

**Lemma 10.7**, we have that  $\mu_{j_{\min}}([(P_1) - (P'_1)]) = 0$  and  $\mu_{j_{\max}}([(P_2) - (P'_2)]) = 0$ . Using Lemmas 10.8 and 3.7, we obtain

$$\begin{aligned} \mu_j([(P'_1) - (P'_2)]) &= \mu_{j_{\min}}([(P'_1) - (P'_2)]) = \mu_{j_{\min}}([(P_1) - (P'_2)]) \\ &= \mu_{j_{\max}}([(P_1) - (P'_2)]) = \mu_{j_{\max}}([(P_1) - (P_2)]) = \mu_j(P). \quad \square \end{aligned}$$

**Lemma 10.10.** *Let  $P'_1, P'_2 \in C(k)$  be points mapping to distinct points on the same component of the special fiber of  $C^{\min}$  and let  $P' = [(P'_1) - (P'_2)] \in J(k)$ . Let  $j_0$  be the unique index such that  $C_{j_0}$  lies between  $P'_1$  and  $P'_2$ . Then  $\mu_j(P') = 2|j - j_0|$ .*

*Proof.* By Lemmas 10.6 and 10.7, we have  $\mu_{j_0}(P') = 0$ . Since the images of  $P'_1$  and  $P'_2$  on the special fiber of  $C^{\min}$  are distinct,  $P'$  is not in the kernel of reduction with respect to  $C_{j_0}$ . If

$$x^{(j_0)} = (x_1^{(j_0)}, x_2^{(j_0)}, x_3^{(j_0)}, x_4^{(j_0)})$$

are normalized Kummer coordinates for  $P'$  on the Kummer surface associated to  $C_{j_0}$ , we therefore have

$$0 = v(x^{(j_0)}) = \min\{v(x_1^{(j_0)}), v(x_2^{(j_0)}), v(x_3^{(j_0)})\}.$$

Applying a suitable power of  $\tau$  (see the proof of Lemma 10.8), we find that

$$x^{(j)} = (\pi^{2(j_0-j)}x_1^{(j_0)}, x_2^{(j_0)}, \pi^{2(j-j_0)}x_3^{(j_0)}, x_4^{(j_0)})$$

are (not necessarily normalized) Kummer coordinates for  $P'$  on the Kummer surface associated to  $C_j$ . For definiteness, assume that  $j > j_0$ , the case  $j = j_0$  being clear. Similarly to the proof of Lemma 10.8, we find that  $0 = v(x^{(j_0)}) = v(x_1^{(j_0)})$ , which implies that  $v(x^{(j)}) = -2(j - j_0)$ . In the same way as in the proof of Lemma 10.8, we deduce  $\mu_j(P') = 2(j - j_0) = 2|j - j_0|$ . □

To continue the proof of the proposition, we now first consider the case that  $C_j$  lies between  $P_1$  and  $P_2$ . In this case, Lemmas 10.9 and 10.10 show that the assumptions in Proposition 8.5 hold with  $\mu_1 = 2|j - j_{\min}|$  and  $\mu_2 = 2|j - j_{\max}|$  or conversely. So the statement follows from Proposition 8.5 and  $|j - j_{\max}| + |j - j_{\min}| = j_{\max} - j_{\min}$ .

Now assume that  $C_j$  does not lie between  $P_1$  and  $P_2$ . We assume for definiteness that  $j > j_{\max}$ . For normalized Kummer coordinates  $x^{(j_{\max})}$  for  $P = [(P_1) - (P_2)]$  on the Kummer surface associated to  $C_{j_{\max}}$ , we have

$$v(x_2^{(j_{\max})}) \leq \min\{v(x_1^{(j_{\max})}), v(x_3^{(j_{\max})})\};$$

compare the proof of Lemma 10.8 above. Then  $x^{(j)} = \tau^{j-j_{\max}}(x^{(j_{\max})})$  are Kummer coordinates for  $[(P_1) - (P_2)]$  on the Kummer surface associated to  $C_j$ , and we have

$$v(x^{(j_{\max})}) - 2(j - j_{\max}) \leq v(x^{(j)}) \leq v(x^{(j_{\max})}).$$



It follows that

$$\begin{aligned} \mu_j(P) - \mu_{j_{\max}}(P) &= (-\hat{\lambda}(x^{(j)}) - v(x^{(j)})) - (-\hat{\lambda}(x^{(j_{\max})}) - v(x^{(j_{\max})})) \\ &= v(x^{(j_{\max})}) - v(x^{(j)}) \in \{0, 1, \dots, 2(j - j_{\max})\}. \end{aligned}$$

As  $\mu_{j_{\max}}(P) = r(\Gamma_1, \Gamma_2) + j_{\max} - j_{\min}$  by the case already discussed, the result follows, and the proof of [Proposition 10.5](#) is finished.  $\square$

**Corollary 10.11.** *Let  $\mathcal{C}$  be a stably minimal Weierstrass model of  $C$  with discriminant  $\Delta$ ; assume that  $C$  has reduction type  $[\mathbf{I}_{m_1} - \mathbf{I}_{m_2} - l]$  with  $l > 0$ . As usual, let*

$$\beta(\mathcal{C}) = \max\{\mu(P) : P \in J(k)\} \quad \text{and} \quad \bar{\beta}(\mathcal{C}) = \max\{\mu(P) : P \in J(\bar{k})\},$$

where  $\mu$  is computed with respect to  $\mathcal{C}$ . Then we have

$$\beta(\mathcal{C}) \leq \bar{\beta}(\mathcal{C}) = \frac{1}{4}(m_1 + m_2) + 2l < \frac{1}{4}v(\Delta) \quad \text{and} \quad \bar{\beta} \geq \frac{1}{6}v(\Delta).$$

*Proof.* The assumption on the reduction type implies that the model is equivalent to one of the form (10-1). [Proposition 10.5](#) then gives upper bounds for  $\mu([(P_1) - (P_2)])$ , with  $P_1, P_2 \in C(\bar{k})$ , depending on the images  $\Gamma_1$  and  $\Gamma_2$  of  $P_1$  and  $P_2$  in the reduction graph. The maximizing case occurs for  $\Gamma_1 = B_{m_1/2}$  and  $\Gamma_2 = D_{m_2/2}$ , giving

$$\mu([(P_1) - (P_2)]) = r(B_{m_1/2}, D_{m_2/2}) + l = \frac{1}{4}m_1 + l + \frac{1}{4}m_2 + l.$$

For the remaining inequalities, recall that  $v(\Delta) = m_1 + m_2 + 12l$  and that  $l > 0$ .  $\square$

We state a technical lemma which will be needed for the proof of [Theorem 10.13](#).

**Lemma 10.12.** *Suppose that the residue characteristic of  $k$  is not 2. Consider a degenerate Weierstrass equation of the form*

$$\mathcal{C}: Y^2 = f_0Z^6 + f_1XZ^5 + f_2X^2Z^4 + X^3Z^3$$

and let

$$\mathcal{E}: y^2 = f_0 + f_1x + f_2x^2 + x^3$$

be an elliptic Weierstrass equation. If  $Q_1 = (x_1, y_1)$  and  $Q_2 = (x_2, y_2)$  are points in  $\mathcal{E}(k)$ , then  $P_1 = (x_1 : y_1 : 1)$  and  $P_2 = (x_2 : y_2 : 1)$  are points in  $\mathcal{C}(k)$ , and if  $x_1, x_2 \in \mathcal{O}$ , then  $\mu_{\mathcal{C}}([(P_1) - (P_2)]) \leq \mu_{\mathcal{E}}(Q_1 - Q_2)$ .

Here  $\mu_{\mathcal{E}}$  is the height correction function for the elliptic curve  $\mathcal{E}$ , and  $\mu_{\mathcal{C}}$  denotes the height correction function defined in the same way as  $\mu$  in the smooth case in terms of the equation  $\mathcal{C}$ .

*Proof.* Let  $\underline{\delta}_{\mathcal{C}} = (\delta_{\mathcal{C},1}, \delta_{\mathcal{C},2}, \delta_{\mathcal{C},3}, \delta_{\mathcal{C},4})$  be the duplication polynomials on the Kummer surface associated to  $\mathcal{C}$ , and let  $\underline{\delta}_{\mathcal{E}} = (\delta_{\mathcal{E},1}, \delta_{\mathcal{E},2})$  be the duplication polynomials for the numerator and denominator of the  $x$ -coordinate associated to  $\mathcal{E}$ . Then a generic computation shows that, if  $(\xi_1 : \xi_2 : \xi_3 : \xi_4)$  is the image of  $[(P_1) - (P_2)]$  on

the Kummer surface, we have  $(\xi_4 : \xi_1) = x(Q_1 - Q_2)$ . In addition, we find that  $\delta_{C,1}(\xi_1, \xi_2, \xi_3, \xi_4) = \delta_{E,2}(\xi_4, \xi_1)$  and  $\delta_{C,4}(\xi_1, \xi_2, \xi_3, \xi_4) = \delta_{E,1}(\xi_4, \xi_1)$  (as polynomials in the  $\xi_j$ ).

That  $P_1, P_2 \in C(k)$  is obvious from the equations. For the last statement, we observe that  $\min\{v(\xi_1), v(\xi_2), v(\xi_3), v(\xi_4)\} = \min\{v(\xi_1), v(\xi_4)\}$  (this is where we use that  $x_1$  and  $x_2$  are integral), which implies

$$\begin{aligned} \mu_C([(P_1) - (P_2)]) &= \lim_{n \rightarrow \infty} 4^{-n} v(\underline{\delta}_C^{on}(\underline{\xi})) - v(\underline{\xi}) \\ &\leq \lim_{n \rightarrow \infty} 4^{-n} v(\underline{\delta}_E^{on}(\xi_4, \xi_1)) - \min\{v(\xi_1), v(\xi_4)\} \\ &= \mu_E(Q_1 - Q_2). \end{aligned} \quad \square$$

The following consequence is useful for practical purposes. For simplicity, we state it for the case of residue characteristic  $\neq 2$ , but we expect that the statement remains true for residue characteristic 2.

**Theorem 10.13.** *Suppose that the residue characteristic of  $k$  is not 2. Let  $C$  be a stably minimal Weierstrass model of  $C$  such that  $C$  has reduction type  $[\mathcal{K}_1 - \mathcal{K}_2 - l]$ . Then*

$$\beta(C) \leq \beta(\mathcal{K}_1) + \beta(\mathcal{K}_2) + 2l,$$

where  $\beta(\mathcal{K})$  denotes the maximum of  $\mu$  for an elliptic curve of reduction type  $\mathcal{K}$ , taking the action of Frobenius into account. (See Table 1 in [Cremona et al. 2006] for the values of  $\beta(\mathcal{K})$ .)

*Proof.* We may assume that the point(s) of multiplicity 3 on the special fiber are defined over  $\mathfrak{k}$ , at the cost of an at most quadratic unramified extension of  $k$ . Then we can move these points to have  $x$ -coordinates 0 and  $\infty$ , respectively, and so we can assume that our model  $C$  is as in Lemma 10.1. Let  $P \in J(k)$ ; we write  $P = [(P_1) - (P_2)]$  with points  $P_1, P_2 \in C(k')$  for a finite extension  $k'$  of  $k$  such that the reduction of  $C$  over  $k'$  is semistable. We can find  $C_0, C = C_j$  and  $C_l$  as vertices in the reduction graph of the minimal proper regular model of  $C$  over  $k'$ . Then the part of the graph to the left of  $C_0$  corresponds to the reduction graph of  $\mathcal{E}_1$  over  $k'$ , in the sense that we consider a semistable model that dominates  $\mathcal{E}_1$  (and is minimal with that property); the graph then is either a line segment (potentially good reduction) or a line segment joined to a circle (potentially multiplicative reduction), with  $\mathcal{E}_1$  corresponding to the end of the line segment joined to the remaining graph of  $C$ . Similarly, the part of the graph to the right of  $C_l$  corresponds to the reduction graph of  $\mathcal{E}_2$  over  $k'$ .

Now assume that both  $P_1$  and  $P_2$  map (strictly) to the left of  $C_0$  in the reduction graph. This means that the  $x$ -coordinates of the points have positive valuation. We can then find points  $P'_1$  and  $P'_2$  in  $\mathcal{E}_1(k')$  with the same  $x$ -coordinates as  $P_1$  and  $P_2$  and nearby  $y$ -coordinates. Then  $P'_1 - P'_2$  is in  $\mathcal{E}_1(k)$  and  $P'_1$  and  $P'_2$  have the same images as  $P_1$  and  $P_2$  in the reduction graph. By our previous results for the semistable

case, the value of (or at least the upper bound given in [Proposition 10.5](#) for)  $\mu_0(P)$  depends only on the part of the graph to the left of  $C_0$ . We can therefore let  $l$  tend to infinity; then [Lemma 10.12](#) and the discussion preceding [Lemma 10.3](#) show that  $\mu_0(P)$  is bounded by the value of  $\mu_{\mathcal{E}_1}$  on the difference  $P'_1 - P'_2$ . By the arguments in the proof of [Proposition 10.5](#), we have

$$\mu_C(P) = \mu_j(P) \leq \mu_0(P) + 2j \leq \beta(\mathcal{K}_1) + 2l.$$

The case that  $P_1$  and  $P_2$  both map to the right of  $C_l$  is similar.

If (say)  $P_1$  maps to the left of  $C_0$  and  $P_2$  maps to the right of  $C_0$ , but not to the right of  $C_l$ , then by the formula of [Proposition 10.5](#), we can bound  $\mu_C(P)$  by  $\mu_1 + 2l$ , where  $\mu_1$  comes from the part of the graph between  $P_1$  and  $C_0$ . By an argument similar to the one used in the previous paragraph,  $\mu_1$  can be bounded by  $\mu_{\mathcal{E}_1}(P'_1)$ , where  $P'_1$  is the point on  $\mathcal{E}_1$  corresponding to  $P_1$  and we take the second point to be on the component visible in  $C_0$ . If  $P_2$  maps to the right of  $C_l$ , then we similarly obtain a bound of the form  $\mu_1 + \mu_2 + 2l \leq \beta(\mathcal{K}_1) + \beta(\mathcal{K}_2) + 2l$ . The remaining cases are similar or follow directly from [Proposition 10.5](#).  $\square$

The example in [Section 19](#) demonstrates the effect of the improved bounds on  $\beta$  as given in the preceding section. For other examples the bounds established in this section will be similarly useful.

### 11. General upper and lower bounds for $\bar{\beta}$

In this section we derive an upper bound for the geometric height constant  $\bar{\beta}(C)$  in the general case by reducing to the semistable situation. We also give a lower bound of the same order of magnitude. We note the following consequence of the results obtained so far; see the discussion at the end of [Section 9](#) and [Corollary 10.11](#).

**Corollary 11.1.** *Assume that  $C$  is a stably minimal Weierstrass model of  $C$  over  $k$  and that the minimal proper regular model  $C^{\min}$  of  $C$  over  $k$  has semistable reduction. Denoting the discriminant of  $C$  by  $\Delta$  and writing  $\bar{\beta}(C) = \max\{\mu_C(P) : P \in J(\bar{k})\}$ , where  $\mu_C$  denotes  $\mu$  with respect to the model  $C$  and  $J$  is the Jacobian of  $C$ , we have*

$$\frac{1}{6}v(\Delta) \leq \bar{\beta}(C) \leq \frac{1}{4}v(\Delta).$$

When  $C^{\min}$  does not have semistable reduction, the idea is to pass to a suitable field extension  $k'/k$  and apply [Corollary 11.1](#) over  $k'$ . In order to compare the corresponding geometric height constants  $\bar{\beta}$ , we need to analyze how  $\mu$  changes under minimization. We first prove the following key lemma:

**Lemma 11.2.** *There exists a transformation  $\tau : C \rightarrow C'$ , defined over  $k$ , such that  $C'$  is a minimal Weierstrass model and*

$$v(\tau(x)) + v(\tau) \leq v(x) \quad \text{for all } x \in \text{KS}_{\mathbb{A}}.$$

*Proof.* If  $\mathcal{C}$  is already minimal, then there is nothing to prove. Otherwise, [Liu 1996, Remarque 11] implies that we can compute a minimal Weierstrass model by going through the following steps for finitely many points  $P$  on the special fiber of  $\mathcal{C}$ .

- (a) Move  $P$  to  $(0, 0)$ .
- (b) Scale  $x$  by  $1/\pi$ .
- (c) Replace  $\mathcal{C}$  by the normalization of the resulting model.

As transformations of the form (a) do not change  $v(x)$  and have determinant of valuation 0, it suffices to prove

$$v(\tau(x)) + v(\tau) \leq v(x) \quad \text{for all } x \in \text{KS}_{\mathbb{A}}$$

for a transformation  $\tau = \sigma \circ \rho$ , where  $\rho$  is as in (b) and  $\sigma$  is as in (c). Note that such a transformation decreases the valuation of the discriminant; cf. [Liu 1996, Lemme 9, Corollaire 2]. By the discussion following Proposition 4.4, the transformation  $\rho$  maps  $x \in \text{KS}_{\mathbb{A}}$  to  $(\pi x_1, x_2, \pi^{-1}x_3, \pi^3x_4)$ .

Suppose  $v(2) = 0$  and, without loss of generality,  $H = 0$ . According to [Liu 1996, Remarque 2], the normalization can be computed using the transformation  $\sigma$  mapping an affine point  $(\xi, \eta)$  to  $\sigma(\xi, \eta) = (\xi, \eta\pi^{-s})$  for some nonnegative integer  $s$ . As  $v(\tau) = 3 - 2s$ , we must have  $s \geq 2$ , since otherwise  $\tau$  would increase the valuation of the discriminant. Because  $\tau(x) = (\pi x_1, x_2, \pi^{-1}x_3, \pi^{3-2s}x_4)$  for  $x \in \text{KS}_{\mathbb{A}}$ , we find that  $v(\tau(x)) \leq v(x) + 1$ , implying

$$v(\tau(x)) + v(\tau) - v(x) \leq -2s + 4 \leq 0.$$

The case  $v(2) > 0$  is slightly more complicated. Here one computes the normalization by repeatedly applying transformations

$$(\xi, \eta) \mapsto \left( \xi, \frac{\eta + R(\xi, 1)}{\pi} \right), \tag{11-1}$$

where  $R \in \mathcal{O}[X, Z]$  is a certain cubic form, until the minimum of the valuations of the coefficients of  $F + RH - R^2$  is equal to 1. See [Liu 1996, Remarque 2]. Such a transformation maps Kummer coordinates  $x = (x_1, x_2, x_3, x_4)$  to

$$(x_1, x_2, x_3, \pi^{-2}x_4 + l_1x_1 + l_2x_2 + l_3x_3)$$

and the expressions for the  $l_i$  given in Section 4 show that  $v(l_i) \geq -2$  for all  $i$ . As the determinant of a transformation (11-1) has valuation  $-2$ , we need to apply at least two such transformations, because otherwise the valuation of the discriminant would increase. In other words,  $\sigma = \sigma_s \circ \dots \circ \sigma_1$ , where  $s \geq 2$  and every  $\sigma_i$  is of the form (11-1).

By the properties of the transformations (11-1), it suffices to show the desired inequality for the case  $s = 2$ , since further applications of transformations  $\sigma_i$  will

only make the left-hand side of the desired inequality smaller and will not change the right-hand side. So suppose that  $\sigma = \sigma_2 \circ \sigma_1$ ; then  $\tau = \sigma \circ \rho$  maps  $x \in \text{KS}_{\mathbb{A}}$  to

$$\tau(x) = (\pi x_1, x_2, \pi^{-1}x_3, \pi^{-1}x_4 + \pi l_1 x_1 + \pi l_2 x_2 + \pi l_3 x_3 + \pi l'_1 x_1 + l'_2 x_2 + \pi^{-1}l'_3 x_3),$$

where the  $l_i$  arise from  $\sigma_1$  and the  $l'_i$  arise from  $\sigma_2$ . As  $v(\tau) = -1$ , it clearly suffices to prove that

$$v(\tau(x)) \leq v(x) + 1. \tag{11-2}$$

But if (11-2) is false, then  $v(x) = v(x_4) < \min\{v(x_1), v(x_2) + 1, v(x_3) + 2\}$ . In this situation it follows from the lower bounds  $v(l_i) \geq -2$  and  $v(l'_i) \geq -2$  that we get

$$v(\pi l_1 x_1 + \pi l_2 x_2 + \pi l_3 x_3 + \pi l'_1 x_1 + l'_2 x_2 + \pi^{-1}l'_3 x_3) > v(x_4) - 1.$$

This implies (11-2) and therefore finishes the proof of the lemma. □

**Theorem 11.3.** *Let  $C$  be a smooth projective curve of genus 2 defined over a nonarchimedean local field  $k$ , given by an integral Weierstrass model  $\mathcal{C}$ . Then we have*

$$\bar{\beta}(\mathcal{C}) \leq \frac{1}{4}v(\Delta(\mathcal{C})).$$

*Proof.* By Lemma 5.4 there is a finite extension  $k'/k$  such that the minimal proper regular model of  $C$  over  $k'$  is semistable and such that all minimal Weierstrass models of  $C$  over  $k'$  are stably minimal. By Corollary 11.1, the claim therefore holds for any minimal Weierstrass model of  $C$  over  $k'$ .

It follows from Lemma 11.2 that there is a transformation  $\tau: C \rightarrow C'$  defined over  $k'$  such that  $C'$  is a minimal (and hence stably minimal) Weierstrass model over  $k'$  and such that

$$v(\tau(x)) + v(\tau) \leq v(x) \tag{11-3}$$

for all  $x \in \text{KS}_{\mathbb{A}}$ .

Then, by the above, we have

$$\mu(\tau(x)) \leq \frac{1}{4}v(\Delta(C')).$$

Now using Corollary 4.6 and the relation (4-2), we find

$$\begin{aligned} \mu(x) &= \mu(\tau(x)) - v(x) + v(\tau(x)) - v(\tau) \\ &\leq \frac{1}{4}v(\Delta(C')) - v(x) + v(\tau(x)) - v(\tau) \\ &= \frac{1}{4}v(\Delta(C)) - v(x) + v(\tau(x)) + \frac{3}{2}v(\tau) \\ &\leq \frac{1}{4}v(\Delta(C)), \end{aligned}$$

where we have used (11-3) and  $v(\tau) \leq 0$ . □

**Remark 11.4.** When the residue characteristic is not 2, then we can easily show that  $\bar{\beta}(C)$  is indeed always comparable to  $v(\Delta(C))$ . We can assume that  $H = 0$  and write  $F = cF_0$  with  $F_0$  primitive. We consider the points of order 2 on  $J$ . Such a point  $P$  is given by a factorization  $F_0 = G_1G_2$  with  $G_1$  and  $G_2$  primitive of degrees 2 and 4, respectively. An explicit computation shows that

$$\varepsilon(P) = 4v(c) + 2v(R(P)),$$

where  $R(P)$  denotes the resultant of  $G_1$  and  $G_2$ , and we have  $4\mu(P) = \varepsilon(P)$ . Since  $v(\Delta(C)) = v(\text{disc}(F)) = 10v(c) + v(\text{disc}(F_0))$  and  $4v(\text{disc}(F_0))$  is the sum of the valuations of the 15 resultants  $R(P)$ , we find that

$$\begin{aligned} \bar{\beta}(C) &\geq \frac{1}{4} \max_{O \neq P \in J[2]} (4v(c) + 2v(R(P))) \geq v(c) + \frac{1}{30} \sum_{O \neq P \in J[2]} v(R(P)) \\ &= v(c) + \frac{2}{15}v(\text{disc}(F_0)) \geq \frac{1}{10}v(\Delta(C)). \end{aligned}$$

A similar statement should be true when the residue characteristic is 2.

Recall that we denote  $\max\{\varepsilon(P) : P \in J(\bar{k})\}$  by  $\bar{\gamma}(C)$ .

**Corollary 11.5.** *Let  $C$  be a smooth projective curve of genus 2 defined over a nonarchimedean local field  $k$ , given by an integral Weierstrass model  $\mathcal{C}$ . Then we have*

$$\bar{\gamma}(C) \leq v(\Delta(C)).$$

If  $H = 0$  and  $\text{char}(k) \neq 2$ , then this can be improved to

$$\bar{\gamma}(C) \leq v(2^{-4}\Delta(C)).$$

*Proof.* The first inequality follows from  $\varepsilon(P) = 4\mu(P) - \mu(2P)$  and [Theorem 11.3](#). The second inequality is [Theorem 6.1 of \[Stoll 1999\]](#). □

**Question 11.6.** If  $\mathcal{C}$  is a minimal Weierstrass model, does  $\bar{\beta}(C)$  only depend on the special fiber of  $\mathcal{C}^{\min}$ ?

Note that the corresponding statement holds for elliptic curves [\[Cremona et al. 2006\]](#). In our situation, however, there may be several nonisomorphic minimal Weierstrass models, which complicates the picture.

### Part III. Efficient computation of canonical heights

In this part we show how to compute the canonical height  $\hat{h}(P)$  efficiently for a point  $P$  over a number field, global function field or more general field with a system of absolute values as in [Section 2](#). We first explain how to compute the local height correction functions. We use  $M(d)$  to denote the time needed to multiply two  $d$ -bit integers.

## 12. Computing $\mu$ at nonarchimedean places

In this section,  $k$  is a nonarchimedean local field again, with valuation ring  $\mathcal{O}$ , uniformizer  $\pi$ , normalized valuation  $v$  and residue class field  $\mathfrak{k}$ . Let  $\mathcal{C}$  be an integral Weierstrass model for a genus-2 curve  $C$  over  $k$ . We make no assumptions on the reduction type of  $C$ . We already discussed a method for the computation of  $\mu(P)$  for a given point  $P \in J(k)$  in [Section 3](#). In this section, we provide an alternative fast algorithm and show that its running time is

$$\ll (\log v(\Delta)) M((\log v(\Delta))v(\Delta)(\log \#\mathfrak{k})),$$

where  $\Delta = \Delta(\mathcal{C})$ .

**Lemma 12.1.** *Assume that  $M$  is a positive integer such that  $M\mu(P) \in \mathbb{Z}$ . Further assume that  $\max\{\varepsilon(P) : P \in J(k)\} \leq B$ . Then*

$$\mu(P) = \frac{1}{M} \left[ M \sum_{n=0}^{\lfloor \log(\frac{1}{3}BM)/\log 4 \rfloor} 4^{-n-1} \varepsilon(2^n P) \right].$$

*Proof.* This follows from  $M\mu(P) \in \mathbb{Z}$  and from

$$0 \leq M \sum_{n \geq m} 4^{-n-1} \varepsilon(2^n P) \leq \frac{BM}{3 \cdot 4^m}. \quad \square$$

If we know that the reduction is nodal, then we get an upper bound  $B$  for  $\varepsilon(P)$  and all possible denominators of  $\mu(P)$  from the results of [Section 9](#). More generally, if we know the smallest positive period  $N$  of the sequence  $(\mu(nP))_n$ , then we can take  $M = N$  (respectively,  $M = 2N$ ) if  $N$  is odd (respectively, even) by [Corollary 3.11](#). Also note that we can always take  $B = v(\Delta)$  (or even  $B = v(2^{-4}\Delta)$  if  $\text{char}(k) \neq 2$  and the equation of the curve has  $H = 0$ ); see [Corollary 11.5](#).

If we only know an upper bound for the denominator of  $\mu(P)$ , then the following alternative approach can be used. This is analogous to [[Müller and Stoll 2016](#), Lemma 4.2].

**Lemma 12.2.** *Assume that  $M \geq 2$  is an integer such that  $M'\mu(P) \in \mathbb{Z}$  for some  $0 < M' \leq M$ . Assume in addition that  $\max\{\varepsilon(P) : P \in J(k)\} \leq B$ , and set*

$$m = \left\lfloor \frac{\log(\frac{1}{3}BM^2)}{\log 4} \right\rfloor.$$

*Then  $\mu(P)$  is the unique fraction with denominator less than or equal to  $M$  in the interval  $[\mu_0, \mu_0 + 1/M^2]$ , where*

$$\mu_0 = \sum_{n=0}^m 4^{-n-1} \varepsilon(2^n P).$$

*Proof.* Note that

$$\mu_0 \leq \mu(P) \leq \mu_0 + \sum_{n>m} 4^{-n-1} B < \mu_0 + \frac{1}{M^2}.$$

But since  $M \geq 2$ , the interval  $[\mu_0, \mu_0 + 1/M^2]$  contains at most one fraction with denominator bounded by  $M$ ; by assumption,  $\mu(P)$  is such a fraction.  $\square$

In order to apply [Lemma 12.2](#), we now find a general upper bound  $M$  on the possible denominators of  $\mu$ . Let  $\mathcal{J}$  denote the Néron model of  $J$  over  $S = \text{Spec}(\mathcal{O})$  and write  $\Phi$  for the component group of  $\mathcal{J}$ .

**Proposition 12.3.** *Let  $N$  denote the exponent of  $\Phi(\bar{\mathbb{F}})$  and let  $P \in J(k)$ . Then we have*

$$\mu(P) \in \frac{1}{2N}\mathbb{Z}.$$

*If  $N$  is odd or if  $C$  has a  $k^{\text{nr}}$ -rational Weierstrass point, then we have*

$$\mu(P) \in \frac{1}{N}\mathbb{Z}.$$

*Proof.* Let  $i \in \{1, \dots, 4\}$  be such that  $\kappa_i(P) \neq 0$ . Recall from [Lemma 8.2](#) that the function  $\hat{\lambda}_i = \hat{\lambda} \circ (\kappa/\kappa_i)$  is a Néron function with respect to the divisor  $D_i$ . As  $P \notin \text{supp } D_i$ , we find

$$\mu(P) \equiv \hat{\lambda}(x) \equiv \hat{\lambda}_i(P) \pmod{\mathbb{Z}}$$

for any set of Kummer coordinates  $x$  for  $P$ . It follows from the results of [\[Néron 1965\]](#) and [\[Lang 1983, §11.5\]](#) that

$$\hat{\lambda}_i(P) \equiv j(D_i, (P) - (O)) \pmod{\mathbb{Z}},$$

where  $j(\cdot, \cdot)$  denotes Néron’s bilinear  $j$ -pairing, defined in [\[Néron 1965, §III.3\]](#).

By [\[Néron 1965, Proposition III.2\]](#), the values of the  $j$ -pairing lie in  $\frac{1}{2N'}\mathbb{Z}$ , where  $N' = \#\Phi(\bar{\mathbb{F}})$ . It is easy to see that we can replace  $N'$  by the exponent  $N$  in the proof of [\[Néron 1965, Proposition III.2\]](#), so the first statement of the proposition follows.

For the second statement, note that the  $j$ -pairing takes values in  $\frac{1}{N}\mathbb{Z}$  if  $N$  is odd, again by [\[Néron 1965, Proposition III.2\]](#) and its proof. If  $C$  has a  $k^{\text{nr}}$ -rational Weierstrass point  $P_0$ , then the divisor  $D_i$  is linearly equivalent over  $k^{\text{nr}}$  to  $2\Theta_{P_0}$ , where  $\Theta_{P_0}$  is the theta divisor with respect to  $P_0$ . The Néron model does not change under unramified extensions, and  $\mu(P) \pmod{\mathbb{Z}}$  does not depend on the Weierstrass model of  $C$  by [Corollary 4.6](#). Hence we can assume that  $i = 1$  and  $D_1 = 2\Theta_{P_0}$ , so the linearity of the  $j$ -pairing in the first variable proves the claim.  $\square$

**Remark 12.4.** In the notation of [\[Namikawa and Ueno 1973\]](#), the only reduction types for which [Proposition 12.3](#) does not show that  $\mu(P) \in \frac{1}{N}\mathbb{Z}$  (where  $N$  is the



exponent of  $\Phi(\bar{\mathfrak{k}})$ , are  $[2\text{III} - l]$  and  $[2\text{III}^* - l]$  for  $l \geq 0$ ;  $[2\text{I}_n^* - l]$  for  $n, l \geq 0$ ; and  $[2\text{I}_n - l]$  for  $n > 0$  even and  $l \geq 0$ . We have not found an example where  $\mu(P) \notin \frac{1}{N}\mathbb{Z}$ .

We can compute the group  $\Phi(\bar{\mathfrak{k}})$  in practice using [Bosch et al. 1990, §9.6]. For this we need to know the intersection matrix of the special fiber of a regular model of  $C$  over  $S$ . This is implemented in Magma, but can be rather slow. If the residue characteristic is not 2, then we can apply Liu's algorithm [1994] to compute the reduction type and read off  $\Phi(\bar{\mathfrak{k}})$ .

In general, an upper bound for the exponent of  $\Phi(\bar{\mathfrak{k}})$  suffices to apply Lemma 12.2. We give a bound which only depends on the valuation of the discriminant  $\Delta = \Delta(C)$ .

**Lemma 12.5.** *The exponent of  $\Phi(\bar{\mathfrak{k}})$  is bounded from above by*

$$M := \max\left\{2, \left\lfloor \frac{1}{3}v(\Delta)^2 \right\rfloor\right\}.$$

Moreover, the denominator of  $\mu(P)$  is bounded from above by  $M$  for all  $P \in J(k)$ .

*Proof.* This follows from a case-by-case analysis, using the list of groups  $\Phi(\bar{\mathfrak{k}})$  from [Liu 1994, §8] for all reduction types in [Namikawa and Ueno 1973], and Proposition 12.3.  $\square$

**Remark 12.6.** By going through all reduction types, it is possible to obtain better upper bounds for the denominator  $M'$  of  $\mu(P)$  from the Igusa invariants discussed in Section 6. First note that if the special fiber of  $C$  is nonreduced, then we have

- (i)  $M' \leq 4$  if  $v(\Delta) \leq 12$ ,
- (ii)  $M' \leq \max\{12, v(\Delta) - 15\}$  otherwise.

Suppose that  $C$  is reduced; then, by Proposition 6.2, we can use the Igusa invariants of the special fiber to distinguish between the multiplicities of its singularities.

- (i) If all points on the special fiber of  $C$  have multiplicity at most 2, then we can bound  $M'$  using Proposition 6.3(i)–(iii) and Propositions 9.1, 9.3, and 9.4.
- (ii) If there is a point of multiplicity 3 on the special fiber, then we have
  - $M' \leq \min\{6, v(\Delta) + 1\}$  if  $v(\Delta) \leq 10$ ,
  - $M' \leq 12$  if  $v(\Delta) \leq 20$ ,
  - $M' \leq \left\lfloor \frac{1}{4}(v(\Delta) - 12)^2 \right\rfloor$  otherwise.
- (iii) If there is a point of multiplicity  $\geq 4$  on the special fiber, then we have
  - $M' \leq 3v(\Delta) - 10$  if  $v(\Delta) \leq 10$ ,
  - $M' \leq 4v(\Delta) - 20$  if  $v(\Delta) > 10$  and the model is minimal,
  - $M' \leq \left\lfloor \frac{1}{3}(v(\Delta) - 10)^2 \right\rfloor$  if the model is not minimal.

The results of this section lead to an efficient algorithm for the computation of  $\mu(P)$ , which is analogous to Algorithm 4.4 of [Müller and Stoll 2016]. We

assume that the coefficients of  $F$  and  $H$  and the coordinates of  $P$  are given to sufficient  $v$ -adic precision (in practice, they will be given exactly as elements of a number field or function field).

1. If  $\text{char}(k) \neq 2$  and  $H = 0$ , set  $B := v(2^{-4}\Delta)$ . Otherwise, set  $B := v(\Delta)$ .
2. Set  $M := \max\{2, \lfloor \frac{1}{3}v(\Delta)^2 \rfloor\}$ .
3. Set  $m := \lfloor \log(\frac{1}{3}BM^2) / \log 4 \rfloor$ .
4. Set  $\mu_0 := 0$ . Let  $x$  be normalized Kummer coordinates for  $P$  with  $(m+1)B+1$   $v$ -adic digits of precision.
5. For  $n := 0$  to  $m$  do:
  - a. Compute  $x' := \delta(x)$  (to  $(m+1)B+1$   $v$ -adic digits of precision).
  - b. If  $v(x') = 0$ , then return  $\mu_0$ .
  - c. Set  $\mu_0 := \mu_0 + 4^{-n-1}v(x')$ .
  - d. Set  $x := \pi^{-v(x')}x'$ .
6. Return the unique fraction with denominator at most  $M$  in the interval between  $\mu_0$  and  $\mu_0 + 1/M^2$ .

The fraction in the final step can be computed easily, for instance, using continued fractions.

For the complexity analysis in the following proposition, we assume that elements of  $\mathcal{O}$  are represented as truncated power series in  $\pi$ , whose coefficients are taken from a complete set of representatives for the residue classes. Operations on these coefficients can be performed in time  $\ll M(\log \#\mathfrak{k})$ .

**Proposition 12.7.** *The algorithm above computes  $\mu(P)$ . Its running time is*

$$\ll (\log v(\Delta)) M((\log v(\Delta))v(\Delta)(\log \#\mathfrak{k}))$$

as  $v(\Delta) \rightarrow \infty$ , with an absolute implied constant.

*Proof.* The following proof is analogous to the proof of [Müller and Stoll 2016, Proposition 4.5]. Corollary 11.5 shows that  $B$  is a suitable upper bound for  $\varepsilon$  and Lemma 12.5 shows that  $M$  is an upper bound for the denominator of  $\mu$ . Because  $M \geq 2$ , the loop in step 5 computes the sum in Lemma 12.2. Note that when  $v(x') = 0$  in step 5b, we have  $\mu(P) = \mu_0$  by Theorem 3.10. At each duplication step, the precision loss is  $\varepsilon(2^n P) \leq B$ , so that with our choice of starting precision, after the  $m+1$  steps in the loop the resulting  $x$  still has at least one digit of precision. This proves the correctness of the algorithm.

Clearly the running time of the algorithm is dominated by the running time of the loop in step 5. Step 5a consists of a fixed number of additions and multiplications of elements of  $\mathcal{O}$  which are given to a precision of  $(m+1)B+1$  digits.

Because steps 5b–5d take negligible time compared to step 5a, each pass through the loop takes

$$\ll M((m + 1)B + 1)(\log \#\mathfrak{k})$$

operations, leading to a total running time that is

$$\begin{aligned} &\ll (m + 1) M((m + 1)B + 1)(\log \#\mathfrak{k}) \\ &\ll m M(mB(\log \#\mathfrak{k})) \\ &\ll (\log v(\Delta)) M((\log v(\Delta))v(\Delta)(\log \#\mathfrak{k})) \end{aligned}$$

as  $v(\Delta) \rightarrow \infty$ . Here we use that  $B \ll v(\Delta)$  and  $M \ll v(\Delta)^2$ , so that  $m \ll \log v(\Delta)$ .  $\square$

**Remark 12.8.** In step 2, we can use [Remark 12.6](#) to compute a sharper upper bound for the denominator of  $\mu$ . See also the discussion following [Remark 12.4](#). Of course, if we want to find  $\mu(P)$  for several points  $P$ , the quantities  $M$ ,  $B$  and  $m$  only have to be computed once.

**Remark 12.9.** We can compute  $\mu(P)$  using the algorithm above in more general situations. Suppose that  $k$  is any discretely valued field with valuation ring  $\mathcal{O}$  and uniformizer  $\pi$ . In that case, the sequence  $(\mu(nP))_n$  might not have a finite period, so the method for the computation of  $\mu(P)$  discussed in [Section 3](#) might not be applicable. However, [Lemmas 12.1](#), [12.2](#) and [12.5](#) and [Proposition 12.3](#) remain valid. If  $\text{char}(k) \neq 2$  and if  $H = 0$ , then we have the upper bound  $\varepsilon(P) \leq v(2^{-4}\Delta)$  (cf. [Remark 3.2](#)), so the algorithm above can be used and [Proposition 12.7](#) remains valid as well, in the sense that the computation can be done using  $\ll \log v(\Delta)$  operations with elements of  $\mathcal{O}/\pi^n\mathcal{O}$ , where  $n \ll v(\Delta) \log v(\Delta)$ . In the remaining cases, we can compute an upper bound  $B$  on  $\varepsilon$  as in [Remark 3.2](#), and we can apply the algorithm with this choice of  $B$ .

### 13. Computing $\mu$ at archimedean places

In this section,  $k$  is an archimedean local field, so  $k = \mathbb{R}$  or  $k = \mathbb{C}$ . We assume that the curve  $C$  is given by a Weierstrass equation  $\mathcal{C}$  with  $H = 0$ . In the following,  $\log_+ x = \max\{0, \log x\}$ .

Let  $x \in k^4$  be a set of Kummer coordinates. Recall that

$$\tilde{\varepsilon}(x) = -[k : \mathbb{R}](\log \|\delta(x)\|_\infty - 4 \log \|x\|_\infty)$$

and

$$\tilde{\mu}(x) = \sum_{n=0}^{\infty} 4^{-n-1} \tilde{\varepsilon}(\delta^{on}(x)).$$

We easily obtain a lower bound for  $\tilde{\varepsilon}$  using the standard estimate for  $\|\delta(x)\|_\infty$ . Since the coefficients of the duplication polynomials  $\delta_j$  are universal polynomials

of degree at most 4 in the coefficients of  $F$ , this gives

$$-\tilde{\varepsilon} \ll 1 + \log_+ \|F\|_\infty,$$

where  $\|F\|_\infty$  is the maximum norm of the coefficient vector of  $F$ . We recall that the method described in Section 7 of [Stoll 1999], leading to equation (7.1) there, provides an upper bound  $\tilde{\gamma}$  for  $\tilde{\varepsilon}$  that can be explicitly computed for any given Weierstrass equation  $\mathcal{C}$  of the curve (provided  $H = 0$ ). It is given by

$$\begin{aligned} \tilde{\gamma} &= \log \max_i \left( \sum_{\{S,S'\}} |a_{i,\{S,S'\}}| \sqrt{\sum_{1 \leq j \leq 4} |b_{\{S,S'\},j}|} \right)^2 \\ &\leq \log 400 + 2 \log \max_{i,\{S,S'\}} |a_{i,\{S,S'\}}| + \log \max_{\{S,S'\},j} |b_{\{S,S'\},j}| \end{aligned}$$

with certain numbers  $a_{i,\{S,S'\}}$ ,  $b_{\{S,S'\},j}$ , where  $i, j \in \{1, 2, 3, 4\}$  and  $\{S, S'\}$  runs through the ten partitions of the set of roots of  $F$  into two sets of three. Using the formulas in [Stoll 1999, §10] and Mignotte’s bound (see, for example, [von zur Gathen and Gerhard 1999, Corollary 6.33]), we see that

$$\log \max_{\{S,S'\},j} |b_{\{S,S'\},j}| \ll 1 + \log_+ \|F\|_\infty$$

and

$$\log \max_{i,\{S,S'\}} |a_{i,\{S,S'\}}| \ll 1 + \log_+ \|F\|_\infty + \log_+ \max_{\{S,S'\}} |R(S, S')|^{-1},$$

where  $R(S, S')$  is the resultant of the two factors  $G, G'$  of  $F$  corresponding to the partition of the roots. Using Mignotte’s bound again, we find that

$$|R(S, S')|^{-1} = \frac{\sqrt{|\text{disc } G| |\text{disc } G'|}}{\sqrt{|\text{disc } F|}} \ll \|F\|_\infty^2 |\Delta(\mathcal{C})|^{-1/2},$$

leading finally to the estimate

$$|\tilde{\varepsilon}| \ll 1 + \log_+ \|F\|_\infty + \log_+ |\Delta(\mathcal{C})|^{-1} =: s(F).$$

If  $|\tilde{\varepsilon}(x)| \leq \tilde{\eta}$  for all  $x \in \text{KS}_\mathbb{A}$ , then we have

$$\left| \sum_{n \geq N} 4^{-n-1} \tilde{\varepsilon}(\delta^{on}(x)) \right| \leq \frac{1}{3} \tilde{\eta} 4^{-N},$$

so we need to sum the first

$$N = \left\lceil \frac{d}{2} + \frac{\log(\frac{1}{3}\tilde{\eta})}{\log 4} \right\rceil \ll d + \log s(F)$$

terms to obtain an accuracy of  $2^{-d}$ . Comparing the largest term in any of the  $\delta_j$  and the lower bound on  $\|\delta(x)\|_\infty$ , we obtain a bound  $\tilde{\theta}$  on the loss of relative precision

(in terms of bits) in the computation of  $\delta(x)$ ; we have  $\tilde{\theta} \ll s(F)$ . To achieve the desired precision at the end, we therefore need to compute with an initial precision of

$$d + 1 + N\tilde{\theta} \ll (d + \log s(F))s(F)$$

bits. The time needed for each duplication is then

$$\ll M((d + \log s(F))s(F)).$$

A logarithm can be computed to  $d$  bits of precision in time  $\ll (\log d) M(d)$  by one of several quadratically converging algorithms (see, for example, [Borwein and Borwein 1987, Chapter 7]), so we obtain the following result.

**Proposition 13.1.** *Given Kummer coordinates  $x$  of a point  $P$  in  $J(k)$  (or  $\text{KS}(k)$ ) to sufficient precision, we can compute  $\tilde{\mu}(P)$  to an accuracy of  $d$  bits in time*

$$\ll (d + \log s(F))(\log d) M((d + \log s(F))s(F)),$$

where

$$s(F) = 1 + \log_+ \|F\|_\infty + \log_+ |\Delta(C)|^{-1}.$$

In the applications,  $k$  will be the completion of a number field at a real or complex place. If the number field is  $\mathbb{Q}$  and the given equation  $\mathcal{C}$  of  $C$  is integral, then  $|\Delta(\mathcal{C})| \geq 1$  and we have  $s(F) = 1 + \log \|F\|_\infty = 1 + h(F)$ , where  $h(F)$  denotes the (logarithmic) height of the coefficient vector of  $F$  as a point in affine space. In general, we have the estimate (denoting the value of  $s(F)$  for a place  $v$  by  $s_v(F)$ )

$$\begin{aligned} \sum_{v|\infty} s_v(F) &\leq [K : \mathbb{Q}] + \sum_{v|\infty} \log_+ \|F\|_v + \sum_{v|\infty} \log_+ |\Delta(\mathcal{C})|_v^{-1} \\ &\leq [K : \mathbb{Q}] + h(F) + h(\Delta(\mathcal{C})) \ll h(F) \end{aligned}$$

for  $h(F)$  large. This implies that we can compute the infinite part of the height correction function in time

$$\ll (d + \log h(F))(\log d) M((d + \log h(F))h(F)),$$

which is polynomial in  $d$  and  $h(F)$ .

## 14. Computing the canonical height of rational points

The first algorithm for computing the canonical height on a genus-2 Jacobian over  $\mathbb{Q}$  was introduced by Flynn and Smart [1997]. It does not require any integer factorization, but can be impractical even for simple examples; see the discussion in [Stoll 2002, §1]. A more practical algorithm was introduced in [Stoll 2002]; here the local height correction functions are computed separately, so some integer factorization is required. Uchida [2011] later introduced a similar algorithm. De Jong and Müller [2014] used division polynomials for a different approach.

Building on the Arakelov-theoretic Hodge index theorem for arithmetic surfaces due to Faltings and Hriljac, Holmes [2012] and Müller [2014] independently developed algorithms for the computation of canonical heights of points on Jacobians of hyperelliptic curves of arbitrary genus over global fields. While these algorithms can be used to compute canonical heights for genus as large as 10 (see [Müller 2014, Example 6.2]), they are much slower than the algorithm from [Stoll 2002] when the genus is 2.

In this section we now combine the results of Sections 12 and 13 into an efficient algorithm for computing the canonical height of a point on the Jacobian of a curve of genus 2 over a global field  $K$ .

If  $K$  is a function field, then there are no archimedean places and factorization is reasonably cheap. So in this case, the best approach seems to be to first find the places  $v$  of  $K$  such that  $\mu_v(P)$  is possibly nonzero (this includes the places at which the given equation of the curve is nonintegral) and then compute the corrections  $\mu_v(P)$  for each place separately as in the algorithm of Proposition 12.7, if necessary changing first to an integral model and correcting for the transformation afterwards. In fact this approach can be used whenever  $K$  is a field with a set of absolute values that satisfy the product formula, because the algorithm before Proposition 12.7 is applicable over any discretely valued field; see Remark 12.9. This includes function fields such as  $\mathbb{Q}(t)$  and  $\mathbb{C}(t)$ .

If  $K$  is a number field, then we compute the contribution from the archimedean places as described in Section 13. The finite part of our algorithm is analogous to our quasilinear algorithm for the computation of the finite part of the canonical height of a point on an elliptic curve in [Müller and Stoll 2016]; see Proposition 14.3 below. For simplicity, we take  $K$  to be  $\mathbb{Q}$  in the following. We write  $\varepsilon_p$  and  $\mu_p$  for the local height correction functions over  $\mathbb{Q}_p$  as given by Definition 3.1 and  $\tilde{\mu}_\infty$  for the local height correction function over  $\mathbb{R}$  as defined in equation (1-1).

We assume that our curve is given by a model  $\mathcal{C}: Y^2 = F(X, Z)$  with  $F \in \mathbb{Z}[X, Z]$ , and we set  $\Delta = \Delta(\mathcal{C})$ . Our goal is to devise an algorithm for the computation of  $\hat{h}(P)$  that runs in time polynomial in  $\log \|F\|_\infty$ ,  $h(P)$  and the required precision  $d$  (measured in bits after the binary dot). We note that  $h(P)$  can be computed in time

$$\ll \log(h(P) + d) M(h(P) + d),$$

since it is just a logarithm. By Proposition 13.1, the height correction function  $\tilde{\mu}_\infty(P)$  can be computed in polynomial time. So we only have to find an efficient algorithm for the computation of the “finite part”  $\tilde{\mu}^f(P) := \sum_p \mu_p(P) \log p$  of the height correction.

Fix  $P \in J(\mathbb{Q})$ . We call a set  $x$  of Kummer coordinates for  $P$  primitive if  $x \in \mathbb{Z}^4$  and  $\gcd(x) = 1$ . We set  $g_n = \gcd(\delta(x^{(n)}))$ , where  $x^{(n)}$  is a primitive set of Kummer

coordinates for  $2^n P$ . Then

$$\tilde{\mu}^f(P) = \sum_{n=0}^{\infty} 4^{-n-1} \log g_n.$$

We also know by [Stoll 1999] that  $g_n$  divides  $D = \frac{1}{2^4} |\Delta| = 2^4 |\text{disc}(F)|$ , which implies that  $\log g_n \leq \log D$  for all  $n$ . To achieve a precision of  $2^{-d}$ , it is therefore enough to take the sum up to

$$n = m := \lfloor \frac{1}{2}d + \log(\frac{1}{3} \log D) \rfloor \ll d + \log \log D \ll d + \log \log \|F\|_{\infty}.$$

Since at each duplication step we have to divide by  $g_n$  to obtain primitive coordinates again, it suffices to do the computation modulo  $D^{m+2}$ . This leads to the following algorithm.

1. Let  $D = \frac{1}{16} |\Delta|$  and set  $m := \lfloor \frac{1}{2}d + \log \log D - \log 3 \rfloor$ .
2. Let  $x$  be primitive Kummer coordinates for  $P$ .
3. Set  $\mu := 0$ .
4. For  $n := 0$  to  $m$  do:
  - a. Compute  $x' := \delta(x) \bmod D^{m+2}$ .
  - b. Set  $g_n := \gcd(D, \gcd(x'))$  and  $x := x'/g_n$ .
  - c. Set  $\mu := \mu + 4^{-n-1} \log g_n$  (to  $d$  bits of precision).
5. Return  $\tilde{\mu}^f(P) \approx \mu$ .

**Proposition 14.1.** *This algorithm computes  $\tilde{\mu}^f(P)$  to  $d$  bits of precision in time*

$$\ll (d + \log \log D) \log(d + \log \log D) M((d + \log \log D) \log D) + h(P).$$

*Proof.* The discussion preceding the algorithm shows that it is correct. The duplication in step 4a can be computed in time

$$\ll M((m+2) \log D) \ll M((d + \log \log D) \log D),$$

while the gcd in step 4b can be computed in time

$$\begin{aligned} &\ll M((m+2) \log D) \log((m+2) \log D) \\ &\ll \log(d + \log \log D) M((d + \log \log D) \log D); \end{aligned}$$

the division is even faster, since  $g_n$  is small. The computation of the logarithm takes time  $\ll \log(d + \log D) M(d + \log D)$ ; this is dominated by the time for computing the gcd. This gives a time complexity of

$$\ll (d + \log \log D) \log(d + \log \log D) M((d + \log \log D) \log D) + h(P),$$

where the last term comes from processing the input  $x$ . □

Note that  $\log D \ll \log \|F\|_\infty$ , so this bound is similar to (and even better by a factor of  $\log d$  than) the complexity for computing  $\tilde{\mu}_\infty(P)$ .

**Remark 14.2.** An alternative way to proceed is to compute

$$x' = \delta^{\circ(m+1)}(x) \bmod D^{m+2}$$

(without dividing out gcds in between) and then use  $\mu = 4^{-m-1} \log \gcd(x')$ . The advantage of the algorithm above is that we can actually work mod  $D^{m+2-n}$ , which makes the computation more efficient. The advantage of the alternative is that it can also be used when working over a number field with nontrivial class group (replacing  $\log \gcd(x')$  by the logarithm of the ideal norm of the ideal generated by  $x'$ ). The resulting complexity is similar, with the implied constant depending on the base field.

We now show that we can in fact do quite a bit better than this, by using the strategy already employed in [Müller and Stoll 2016]. Note that  $\tilde{\mu}^f(P)$  is a rational linear combination of logarithms of positive integers. We can compute such a representation exactly and efficiently by the following algorithm. We again assume that  $x$  is a set of primitive Kummer coordinates for  $P$ .

1. Set  $x' := \delta(x)$ ,  $g_0 := \gcd(x')$  and  $x := x'/g_0$ .
2. Set  $D := \gcd(2^4 \operatorname{disc}(F), g_0^\infty)$  and  $B := \lfloor \log D / \log 2 \rfloor$ .
3. If  $B \leq 1$ , return 0. Otherwise, set  $M := \max\{2, \lfloor \frac{1}{3}(B+4)^2 \rfloor\}$  and  $m := \lfloor \log(\frac{1}{3}B^3M^2) / \log 4 \rfloor$ .
4. For  $n := 1$  to  $m$  do:
  - a. Compute  $x' := \delta(x) \bmod D^{m+1}g_0$ .
  - b. Set  $g_n := \gcd(D, \gcd(x'))$  and  $x := x'/g_n$ .
5. Using the algorithm in [Bernstein 2004] (or in [Bernstein 2005]), compute a sequence  $(q_1, \dots, q_r)$  of pairwise coprime positive integers such that each  $g_n$  (for  $n = 0, \dots, m$ ) is a product of powers of the  $q_i$ :  $g_n = \prod_{i=1}^r q_i^{e_{i,n}}$ .
6. For  $i := 1$  to  $r$  do:
  - a. Compute  $a := \sum_{n=0}^m 4^{-n-1} e_{i,n}$ .
  - b. Let  $\mu_i$  be the simplest fraction between  $a$  and  $a + 1/(B^2M^2)$ .
7. Return  $\sum_{i=1}^r \mu_i \log q_i$  (a formal linear combination of logarithms).

**Proposition 14.3.** *The preceding algorithm computes  $\tilde{\mu}^f(P)$  in time*

$$\ll (\log \log D)^2 M((\log \log D)(\log D)) + M(h(P))(\log h(P)).$$

Note that  $D \leq \frac{1}{16}|\Delta|$  and  $\log D \ll \log \|F\|_\infty$ .



*Proof.* If  $B \leq 1$  in step 3, then we either have  $g_0 = 1$  and  $\tilde{\mu}^f(P) = 0$ , or we have  $D \in \{2, 3\}$ . In the latter case,  $g_0$  is a power of  $p = 2$  or  $3$  and  $v_p(\Delta) = 1$ , which would imply that  $\varepsilon_p(P) = 0$  by [Stoll 2002, Proposition 5.2], so  $g_0 = 1$ , and we get a contradiction.

If a prime  $p$  does not divide  $g_0$ , then  $\varepsilon_p(P) = 0$ , implying  $\mu_p(P) = 0$ . Suppose now that  $p$  divides  $g_0$ ; then we have  $v_p(D) \leq B$  and  $v_p(\Delta) \leq B + 4$ , so  $B, M$  and  $m$  are suitable values for Lemma 12.2. We have  $v_p(g_n) = \varepsilon_p(2^n P)$  for all  $n \leq m$ , because  $p^{(m+1)v_p(D)+1} \mid D^{m+1}g_0$  (compare the proof of Proposition 12.7). All the  $g_n$  are power products of the  $q_i$ , so there will be exactly one  $i = i(p) \in \{1, \dots, r\}$  such that  $p \mid q_{i(p)}$ . Setting  $b_p = v_p(q_{i(p)})$  and  $a = \sum_{n=0}^m 4^{-n-1} e_{i(p),n}$ , we have

$$\sum_{n=0}^m 4^{-n-1} \varepsilon_p(2^n P) = \sum_{n=0}^m 4^{-n-1} v_p(g_n) = b_p a,$$

implying

$$\mu_p(P) = \sum_{n=0}^{\infty} 4^{-n-1} \varepsilon_p(2^n P) = b_p a + \sum_{n=m+1}^{\infty} 4^{-n-1} \varepsilon_p(2^n P).$$

Here the last sum is in  $[0, 1/(B^2 M^2)]$  by the definition of  $m$  (compare the proof of Lemma 12.2). Therefore

$$a \leq \frac{\mu_p(P)}{b_p} \leq a + \frac{1}{b_p B^2 M^2} \leq a + \frac{1}{B^2 M^2}.$$

Since the denominator of  $\mu_p(P)$  is at most  $M$  and since we have  $b_p \leq v_p(D) \leq B$ , the denominator of  $\mu_p(P)/b_p$  is at most  $BM$ . Hence  $\mu_p(P)/b_p$  is the unique fraction in  $[a, a + 1/(B^2 M^2)]$  with denominator bounded by  $BM$ , so  $\mu_p(P)/b_p = \mu_{i(p)}$  by step 6b. Now

$$\sum_p \mu_p(P) \log p = \sum_p \mu_{i(p)} b_p \log p = \sum_{i=1}^r \mu_i \sum_{p \mid q_i} b_p \log p = \sum_{i=1}^r \mu_i \log q_i,$$

so the algorithm is correct.

The complexity analysis is as in the proof of Proposition 6.1 in [Müller and Stoll 2016]. Namely, the computations in step 1 can be done in time  $\ll M(h(P)) \log h(P)$ . The computations in steps 2 and 3 take negligible time. Each pass through the loop in step 4 takes time  $\ll \log((m + 2) \log D) M((m + 2) \log D)$ , so the total time for step 4 is

$$\ll m M(m \log D) \log(m \log D) \ll (\log \log D)^2 M((\log \log D)(\log D)),$$

because  $m \ll \log \log D$ . The coprime factorization algorithm in [Bernstein 2004] (or in [Bernstein 2005]) computes suitable  $q_i$  for a pair  $(a, b)$  of positive integers in time

$\ll (\log ab)(\log \log ab)^2$ . We iterate this algorithm, applying it first to  $g_0$  and  $g_1$ , then to each of the resulting  $q_i$  and  $g_2$ , and so on. There are always  $\ll \log D$  terms in the sequence of the  $q_i$  and we have  $g_n \leq D$  for all  $n$ . Hence step 5 takes time  $\ll \log D(\log \log D)^3$ . Because this is dominated by the time for the loop and because the remaining steps take negligible time, the result follows.  $\square$

Note that the complexity of the algorithm above is quasilinear in  $\log D$  and  $h(P)$ . In practice, the efficiency of this approach can be improved somewhat:

- We can split off the contributions of all sufficiently small primes  $p$  by choosing a suitable bound  $T$  and trial factoring  $\Delta$  up to  $T$ ; the corresponding  $\mu_p$  can then be computed using the algorithm of Proposition 12.7; see also Remark 12.8. In step 3, we can then set  $B := \lfloor \log D' / \log T \rfloor$ , where  $D'$  is the unfactored part of  $D$ , and replace  $B + 4$  by  $B$  in the definition of  $M$ . If the coefficients of  $F$  are sufficiently large, then this trial division can become quite expensive (even for small values of  $T$ ). So when  $h(F)$  is large, it is usually preferable to avoid trial division altogether.
- We can update the  $q_i$  after each pass through the loop in step 4 using the new  $g_n$ ; we can also do the computation in step 4a modulo suitable powers of the  $q_i$  instead of modulo  $D^{m+1}g_0$ . Moreover, it is possible to use separate values of  $B$ ,  $M$  and  $m$  for each  $q_i$ ; these will usually be smaller than those computed in steps 2 and 3. In this way, we can integrate steps 4, 5 and 6 into one loop.

**Remark 14.4.** Over a more general number field  $K$  in place of  $\mathbb{Q}$ , the algorithm as stated does not quite work, since we cannot always divide out greatest common divisors. In this case we first compute  $x^{(1)} = \delta(x)$  and the ideal  $g_0$  generated by  $D$  and the entries of  $x^{(1)}$ . Then we compute  $x^{(2)} = \delta(x^{(1)})$ ,  $\dots$ ,  $x^{(m+1)} = \delta(x^{(m)})$  modulo the ideal  $D^{m+1}g_0$ . Let  $G_j$  be the ideal generated by the entries of  $x^{(j)}$  and  $D^{m+1}$  and set

$$g_1 = g_0^{-4}G_2, \quad g_2 = G_2^{-4}G_3, \quad g_3 = G_3^{-4}G_4, \quad \dots \quad g_m = G_m^{-4}G_{m+1}.$$

The coprime factorization algorithms in [Bernstein 2004; 2005] also work for ideals. In the final result,  $\log q_i$  has to be replaced by  $\log N(q_i)$ , where  $N(q_i)$  is the norm of the ideal  $q_i$ . This should result in a complexity similar to that over  $\mathbb{Q}$  (with the implied constant depending on  $K$ ), or at least one that is dominated by the complexity of computing the naive height and the contributions from the archimedean places. Unfortunately, no complexity analysis for standard operations with ideals in number fields seems to be available in the literature; this prevents us from making a precise statement. Alternatively, we can take the approach described in Remark 14.2.

Combining this with the results for archimedean places, we obtain an efficient algorithm for computing the canonical height  $\hat{h}(P)$  of a point  $P \in J(\mathbb{Q})$ . As

mentioned above, we expect a similar result to hold for any number field  $K$  in place of  $\mathbb{Q}$ , with the implied constant depending on  $K$ .

**Theorem 14.5.** *Let  $C$  be given by the model  $Y^2 = F(X, Z)$  with  $F \in \mathbb{Z}[X, Z]$  and let  $P \in J(\mathbb{Q})$  be given by primitive Kummer coordinates  $x$  (i.e., the coordinates are coprime integers). We can compute  $\hat{h}(P)$  to  $d$  bits of precision in time*

$$\ll \log(d + h(P)) M(d + h(P)) \\ + (d + \log \log \|F\|_\infty)(\log d + \log \log \|F\|_\infty) M((d + \log \log \|F\|_\infty) \log \|F\|_\infty).$$

*Proof.* The first term comes from computing  $h(P)$ . The second term dominates both the complexity bound for  $\tilde{\mu}_\infty(P)$  from Proposition 13.1 and the complexity of computing  $\tilde{\mu}^f(P)$  using the algorithm of Proposition 14.3, since we have  $D \leq \frac{1}{16}|\Delta|$  and  $\log D \ll \log \|F\|_\infty$ . The time for the numerical evaluation of the logarithms  $\log q_i$  to  $d$  bits of precision is also dominated by this term.  $\square$

Note that the complexity is quasilinear in  $\log \|F\|_\infty$  and in  $h(P)$ , and quadratic in  $d$ . The latter is caused by the (only) linear convergence of the computation of  $\tilde{\mu}_\infty(P)$ . For elliptic curves one can use a quadratically convergent algorithm due to Bost and Mestre [1993] (see also [Müller and Stoll 2016]); such an algorithm in the genus-2 case would lead to a complexity that is quasilinear in  $d$  as well.

In Section 15 below we illustrate the efficiency of our algorithm by applying it to a family of curves and points with the property that the number  $g_0$  above is large, so that the previously known algorithms have problems factoring it.

## 15. Examples

We have implemented our algorithm using the computer algebra system Magma [Bosma et al. 1997]. For the factorization into coprimes we have implemented a simple quadratic algorithm due to Buchmann and Lenstra [1994, Proposition 6.5] instead of the quasilinear, but more complicated, algorithms of [Bernstein 2004] or [Bernstein 2005].

Since the estimates for the required precision in the computation of the archimedean contribution as given in Section 13 are too wasteful in practice, we instead compute this contribution repeatedly using a geometrically increasing sequence of digits of precision until the results agree up to the desired number of bits.

We now compare our implementation with Magma's built-in `CanonicalHeight` (version 2.21-2), which is based on [Flynn and Smart 1997] and [Stoll 2002], for a family of genus-2 curves. In `CanonicalHeight`, the duplication on the Kummer surface is done using arithmetic over  $\mathbb{Q}$ , making the implementation slow when points with large coordinates show up during the computation. No factorization of the discriminant is required. However, to find a set of primes such that  $\mu_p(P) \neq 0$

for every prime  $p$  not in the set, `CanonicalHeight` factors the integer  $\gcd(\delta(x))$ , where  $x$  are primitive Kummer coordinates for  $P$ .

**Example 15.1.** For an integer  $a \neq 0$ , consider the curve  $C_a$  of genus 2 defined by the integral Weierstrass model  $y^2 = x^5 + a^2x + a^2$ . Let  $J_a$  denote the Jacobian of  $C_a$ . Then the point  $P = [((0, a) - (\infty))] \in J_a(\mathbb{Q})$  is nontorsion. A set of primitive Kummer coordinates is given by  $x = (0, 1, 0, 0)$  and we have  $\delta(x) = (4a^2, 0, 0, a^4)$ . Hence `CanonicalHeight` needs to factor  $a^2$ .

We choose this family of curves because (a) there is an obvious rational point  $P$  on the Jacobian that is generically nontorsion and (b)  $\gcd(\delta(x))$  involves a large integer, where  $x$  is a set of primitive integral Kummer coordinates for  $P$ . For a random sextic polynomial in  $\mathbb{Z}[x]$ , very likely the discriminant will have a large squarefree part, and so  $\gcd(\delta(x))$  will be fairly small. Of course, the advantages of our algorithm show most clearly when  $\gcd(\delta(x))$  is too large to be factored quickly.

Consider

$$a = 580765860498857094216036712228682450578792019063967819 \\ 607220990444681533984530140793610237063603282,$$

with partial factorization  $2 \cdot 7 \cdot 643 \cdot 804743 \cdot a'$ , where  $a'$  has 89 decimal digits, and its smallest prime factor has 34 decimal digits. Our implementation computes  $\hat{h}(P)$  in 0.51 seconds, whereas Magma's `CanonicalHeight` needs about 15 minutes.

Next, we look at

$$a = 2004037729560594889502897895078536177197017605286267684456693 \\ 371856523790027402225238543540575431528468305556200069359999 \\ 066088091821746622820780762863572550314577271857779581968920.$$

This factors as  $a = 2^3 \cdot 5 \cdot 17 \cdot a'$ , where  $a'$  has 178 decimal digits and no prime divisor with less than 50 decimal digits. Here, our implementation took 1.04 seconds to compute  $\hat{h}(P)$ , whereas Magma did not terminate in 8 weeks.

For  $a = p \cdot q$ , where  $p$  and  $q$  are the smallest primes larger than  $10^{200}$  and  $10^{250}$ , respectively, the canonical height of  $P$  was computed in 5.87 seconds using our implementation.

For the computations in these examples, we used a single-core Xeon CPU E7-8837 having 2.67GHz. All heights were computed to 30 decimal digits of precision.

We conclude this part with an example over the rational function field  $\mathbb{Q}(t)$ .

**Example 15.2.** Consider the curve  $C/\mathbb{Q}(t)$  given by the equation

$$y^2 = x^6 - 2t(t+1)x^5 + (t+1)(t^3 - 5t^2 + 4t - 2)x^4 + 2t(t+1)^2(3t^2 + 1)x^3 \\ - (t+1)(3t^4 - 2t^2 + 4t - 1)x^2 - 4t^2(t+1)^3(t^2 + 2t - 1)x + 4t^4(t+1)^4.$$

It has the points

$$P_1 = (1 : 1 : 0), \quad P_2 = (0, -2t^2(t+1)^2), \quad P_3 = (t+1, 2t(t-1)(t+1))$$

(and also points with  $x$ -coordinate  $t(t+1)$  and a Weierstrass point  $(-t-1, 0)$ ). Let  $Q = [(P_1) - 2(P_2) + (P_3)] \in J(\mathbb{Q}(t))$ . Its image on the Kummer surface has coordinates

$$(1 : -t+1 : -2t^2(t+1) : 0).$$

Applying the duplication polynomials and looking at the gcd of the result, we see that we have to compute the height correction functions at the places given by  $t = 0$ ,  $t = 1$  and  $t = -1$ . We also have to consider the place at infinity, since our model of  $C$  is not integral there. We use the algorithms of [Section 12](#). Consider the place  $t = 0$ . From the valuations of the Igusa invariants (see [Section 6](#)) we can deduce that the reduction type is  $[I_{7-3-2}]$ , which gives us  $M = 41$  for the exponent of the component group and a bound  $B = 10$  for  $\varepsilon$ . We follow [Lemma 12.1](#) and compute

$$\mu_0(Q) = \frac{1}{41} \left[ 41 \sum_{n=0}^3 4^{-n-1} \varepsilon_0(2^n Q) \right] = \frac{1}{41} \left[ 41 \left( \frac{8}{4} + \frac{4}{4^2} + \frac{7}{4^3} + \frac{6}{4^4} \right) \right] = \frac{98}{41}.$$

At  $t = 1$ , the model is not stably minimal. We can deduce from the Igusa invariants that there is a stably minimal model over an extension of ramification index 4, which has reduction type  $[I_{12-2-2}]$ . This shows that the denominator of  $\mu_1$  is divisible by  $4 \cdot 26 = 104$ . With  $M = 104$  and  $B = 9$  we get  $m = 4$  in [Lemma 12.1](#); we obtain

$$\mu_1(Q) = \frac{1}{104} \left[ 104 \sum_{n=0}^4 4^{-n-1} \varepsilon_1(2^n Q) \right] = \frac{1}{104} \left[ 104 \left( \frac{4}{4} + \frac{4}{4^2} + \frac{3}{4^3} + \frac{2}{4^4} + \frac{2}{4^5} \right) \right] = \frac{17}{13}.$$

At  $t = -1$ , the situation is similar. There is a stably minimal model over an extension with ramification index 4 again, which has reduction type  $[I_{20-0-0}]$ . This leads to  $M = 4 \cdot 20 = 80$  and  $B = 20$ , so  $m = 4$ , and

$$\mu_{-1}(Q) = \frac{1}{80} \left[ 80 \sum_{n=0}^4 4^{-n-1} \varepsilon_{-1}(2^n Q) \right] = \frac{1}{80} \left[ 80 \left( \frac{7}{4} + \frac{10}{4^2} + \frac{8}{4^3} + \frac{10}{4^4} + \frac{8}{4^5} \right) \right] = \frac{51}{20}.$$

Finally, at the infinite place, there is a stably minimal integral model over an extension with ramification degree 2, which has reduction type  $[I_{8-0-0}]$ . In a similar way as for  $t = -1$  and taking into account a shift of  $-8$  coming from making the model integral, we obtain  $\mu_\infty(Q) = \frac{19}{4} - 8 = -\frac{13}{4}$ . This results in

$$\begin{aligned} \hat{h}(Q) &= h(Q) - \mu_0(Q) - \mu_1(Q) - \mu_{-1}(Q) - \mu_\infty(Q) \\ &= 3 - \frac{98}{41} - \frac{17}{13} - \frac{51}{20} + \frac{13}{4} = \frac{11}{5330}. \end{aligned}$$

To our best knowledge, the point  $Q$  is the point of smallest known nonzero canonical height on the Jacobian of a curve of genus 2 over  $\mathbb{Q}(t)$ . The curve was found by Andreas Kühn (a student of the second author) in the course of a systematic search for curves with many points mapping into a subgroup of rank 1 in the Jacobian.

**Part IV. Efficient search for points with bounded canonical height**

**16. Bounding the height difference at archimedean places**

We now describe two approaches for getting a better upper bound  $\tilde{\beta}$  on  $\tilde{\mu}$  than the one coming from the bound on  $\tilde{\varepsilon}$  given in [Stoll 1999, Equation (7.1)], when  $k$  is an archimedean local field and  $C/k$  is a smooth projective curve of genus 2, given by a Weierstrass equation  $Y^2 = F(X, Z)$  in  $\mathbb{P}_K(1, 3, 1)$ .

We write  $\|x\|_\infty = \max\{|x_1|, |x_2|, |x_3|, |x_4|\}$  for the maximum norm.

**16A. Bounding  $\tilde{\varepsilon}$  closely.** For the first approach we assume that  $k = \mathbb{R}$ . We describe how to approximate  $\max\{\tilde{\varepsilon}(P) : P \in J(\mathbb{R})\}$  to any desired accuracy, which gives us an essentially optimal bound  $\tilde{\gamma}$ . Recall that

$$\tilde{\varepsilon}(P) = -\log \frac{\max\{|\delta_1(x_1, x_2, x_3, x_4)|, \dots, |\delta_4(x_1, x_2, x_3, x_4)|\}}{\max\{|x_1|, |x_2|, |x_3|, |x_4|\}^4},$$

where  $(x_1 : x_2 : x_3 : x_4)$  is the image of  $P \in J(\mathbb{R})$  on the Kummer surface. We can normalize the Kummer coordinates in such a way that  $\|x\|_\infty = 1$  and one of the coordinates is 1. We then have to minimize  $\max\{|\delta_1|, \dots, |\delta_4|\}$  over four three-dimensional unit cubes, restricted to the points on the Kummer surface that are in the image of  $J(\mathbb{R})$ . This means that the relevant points satisfy the equation defining the Kummer surface and in addition the value of (at least) one of four further auxiliary polynomials is positive. (In general, the values of these polynomials are squares if the point comes from the Jacobian, and the converse holds for any one of the polynomials when its value is nonzero. One can choose four such polynomials in such a way that they do not vanish simultaneously on the Kummer surface.)

The idea is now to successively subdivide the given cubes. For each small cube, we check if it may contain points in the image of  $J(\mathbb{R})$ , by evaluating the various polynomials at the center of the cube and bounding the gradient on the cube. If it can be shown that the defining equation cannot vanish on the cube or that one of the auxiliary polynomials takes only negative values on the cube, then the cube can be discarded. Otherwise, we find upper and lower estimates for  $\max\{|\delta_1|, \dots, |\delta_4|\}$  in a similar way. If the lower bound is larger than our current best upper bound for the minimum, the cube can also be discarded. (At the beginning, we have a trivial upper bound of 1 for the minimum, coming from the origin.) Otherwise, we keep it and subdivide it further. We continue until the difference of the upper and lower

bounds for  $\tilde{\varepsilon}$  on the cube with the smallest lower bound for  $\max\{|\delta_1|, \dots, |\delta_4|\}$  becomes smaller than a specified tolerance. The upper bound for  $\tilde{\varepsilon}$  on that cube is then our bound  $\tilde{\gamma}$ , and we take (as before)  $\tilde{\beta} = \frac{1}{3}\tilde{\gamma}$ .

We have implemented this approach in Magma [Bosma et al. 1997]. After a considerable amount of fine-tuning, our implementation usually takes a few seconds to produce the required bound. In many cases the new bound, which is essentially optimal as a bound on  $\tilde{\varepsilon}$ , is considerably better than the bound of [Stoll 1999, Equation (7.1)], but there are also cases for which it turns out that the old bound is actually pretty good.

We used the following tricks to get the implementation reasonably fast.

- We keep the polynomials shifted and rescaled so that the cube under consideration is  $[-1, 1]^3$ .
- The shifting and scaling is done using linear algebra (working with vectors of coefficients and matrices) and not using polynomial arithmetic.
- The coordinates of the centers and vertices of all cubes are dyadic fractions. We scale everything (by  $2^4 = 16$  at each subdivision step — note that the polynomials involved are of degree 4) so that we can compute with integers instead.

**16B. Iterating Stoll's bound.** We now describe a different approach that also works for complex places. Instead of trying to get an optimal bound on  $\tilde{\varepsilon}$ , we aim at a bound on  $\tilde{\mu}$  by iterating the bound obtained from equation (7.1) in [Stoll 1999]. We recall how this bound was obtained. There is an elementary abelian group scheme  $G$  of order 32 that maps onto  $J[2]$  and acts on the space of quadratic forms in the coordinates of the  $\mathbb{P}^3$  containing the Kummer surface. This representation splits into a direct sum of ten one-dimensional representations that correspond to the ten partitions  $\{S, S'\}$  of the set of ramification points of the double cover  $C \rightarrow \mathbb{P}^1$  into two sets of three. We write  $y_{\{S, S'\}}$  for suitably normalized generators of these eigenspaces ([Stoll 1999] gives explicit formulas in the case  $H = 0$ ). We can then express the squares  $x_i^2$  as linear combinations of these quadratic forms,

$$x_i^2 = \sum_{\{S, S'\}} a_{i, \{S, S'\}} y_{\{S, S'\}}(x),$$

for certain complex numbers  $a_{i, \{S, S'\}}$  that can be explicitly determined. On the other hand,  $y_{\{S, S'\}}^2$  is a quartic form invariant under the action of  $J[2]$  (the representation of  $G$  on quartic forms descends to a representation of  $J[2]$ ) and is therefore a linear combination of the duplication polynomials  $\delta_j$  and the quartic defining the Kummer surface. So there are complex numbers  $b_{\{S, S'\}, j}$  that can also be explicitly determined such that

$$y_{\{S, S'\}}(x)^2 = \sum_{1 \leq j \leq 4} b_{\{S, S'\}, j} \delta_j(x)$$

if  $x$  is a set of Kummer coordinates. Taking absolute values and using the triangle inequality, we obtain

$$\begin{aligned}
 |x_i|^4 &\leq \left( \sum_{\{S,S'\}} |a_{i,\{S,S'\}}| |y_{\{S,S'\}}(x)| \right)^2 \\
 &\leq \left( \sum_{\{S,S'\}} |a_{i,\{S,S'\}}| \sqrt{\sum_{1 \leq j \leq 4} |b_{\{S,S'\},j}| |\delta_j(x)|} \right)^2
 \end{aligned}$$

for all  $(x_1 : x_2 : x_3 : x_4) \in \text{KS}(\mathbb{C})$ . This gives a bound for  $\tilde{\epsilon}$  in terms of the  $a_{i,\{S,S'\}}$  and  $b_{\{S,S'\},j}$  as in equation (7.1) of [Stoll 1999].

We refine this as follows. Define a function  $\varphi : \mathbb{R}_{\geq 0}^4 \rightarrow \mathbb{R}_{\geq 0}^4$  by

$$(d_1, d_2, d_3, d_4) \mapsto \left( \sqrt{\sum_{\{S,S'\}} |a_{i,\{S,S'\}}| \sqrt{\sum_{1 \leq j \leq 4} |b_{\{S,S'\},j}| d_j}} \right)_{1 \leq i \leq 4}.$$

**Lemma 16.1.** *Define a sequence  $(b_n)_n$  in  $\mathbb{R}_{\geq 0}^4$  by*

$$b_0 = (1, 1, 1, 1) \quad \text{and} \quad b_{n+1} = \varphi(b_n).$$

*Then  $(b_n)$  converges to a limit  $b$  and we have*

$$\tilde{\mu}(P) \leq \frac{4^N}{4^N - 1} \log \|b_N\|_\infty$$

*for all  $N \geq 1$  and all  $P \in J(\mathbb{C})$ . In particular,  $\sup \tilde{\mu}(J(\mathbb{C})) \leq \log \|b\|_\infty$ .*

*Proof.* By our previous considerations, it is clear that  $|\delta_j(x)| \leq d_j$  for all  $j$  implies  $|x_i| \leq \varphi_i(d_1, d_2, d_3, d_4)$  for all  $i$ . We deduce by induction on  $N$  that

$$\log \|x\|_\infty \leq \log \|b_N\|_\infty + 4^{-N} \log \|\delta^{\circ N}(x)\|_\infty$$

for all  $N \geq 1$ . Writing

$$\tilde{\mu}(P) = - \sum_{m=0}^{\infty} 4^{-mN} (\log \|\kappa(2^{mN} P)\|_\infty - 4^{-N} \log \|\delta^{\circ N}(\kappa(2^{mN} P))\|_\infty),$$

we obtain an upper bound of  $\log \|b_N\|_\infty$  for each of the terms in parentheses, which gives the desired bound.

To see that  $(b_n)$  converges, we consider

$$\Phi(x) = (\log \varphi_i(\exp(x_1), \dots, \exp(x_4)))_{1 \leq i \leq 4}.$$

It is easy to see that the partial derivatives  $\partial \Phi_i / \partial x_j$  are positive and that, for each  $i$ , summing them over  $j$  gives  $\frac{1}{4}$ . (This comes from the fact that  $\varphi_i$  is homogeneous of degree  $\frac{1}{4}$ .) This implies that  $\|\Phi(x') - \Phi(x)\|_\infty \leq \frac{1}{4} \|x' - x\|_\infty$ , so that  $\Phi$  is contracting with contraction factor  $\leq \frac{1}{4}$ . The Banach fixed point theorem then guarantees the



existence of a unique fixed point of  $\Phi$ , which every iteration sequence converges to. This implies the corresponding statement for  $\varphi$ .  $\square$

If we are dealing with a real place, then we may gain a little bit more by making use of the fact that the  $\delta_j(x)$  are real, while some of the coefficients  $b_{\{S, S'\}, j}$  may be genuinely complex. This can lead to a better bound on  $|y_{\{S, S'\}}|$ .

For example, considering the curve with the record number of known rational points, we get an improvement from 7.726 to 0.973 for the upper bound on  $-\tilde{\mu}$  using [Lemma 16.1](#). See [Section 19](#) for more details. In practice it appears that this second approach is at the same time more efficient and leads to better bounds than the approach described in [Section 16A](#) above.

The approach described here can also be applied in the context of heights on genus-3 hyperelliptic Jacobians; see [\[Stoll 2014\]](#).

### 17. Optimizing the naive height

We now consider an arbitrary local field  $k$ , with absolute value  $|\cdot|$ . Let  $C$  be given by an equation

$$Y^2 = F(X, Z),$$

and let  $W$  be the canonical class on  $C$ . The first three coordinates of the image of a point  $P = [(X_1 : Y_1 : Z_1) + (X_2 : Y_2 : Z_2)] - W \in J$  on the Kummer surface are given by  $Z_1 Z_2, X_1 Z_2 + Z_1 X_2, X_1 X_2$ , whereas the fourth coordinate is homogeneous of degree 1 in the coefficients  $f_j$  of  $F$  (if we consider  $Y_1$  and  $Y_2$  to be of degree  $\frac{1}{2}$ ). This has the effect that the fourth coordinate usually differs by a factor of about  $\|F\| := \max\{|f_0|, |f_1|, \dots, |f_6|\}$  from the other three, which gives this last coordinate a much larger (when  $\|F\|$  is large; this is usually the case when  $k$  is archimedean) or smaller (this may occur when  $k$  is nonarchimedean) influence on the local contribution to the naive height when  $k = K_v$  and  $K$  is a global field. This imbalance tends to increase the difference  $h_{\text{std}} - \hat{h}$  between naive and canonical height. This observation suggests to modify the naive height in the following way, so as to give all coordinates roughly the same weight. Compare [Section 2](#) for the general setup. Let  $x$  be a set of Kummer coordinates over a global field  $K$  and set

$$h'(x) := \sum_{v \in M_K} \log \max\{|x_1|_v, |x_2|_v, |x_3|_v, |x_4|_v / \|F\|_v\}.$$

This is a height as in [Example 2.3](#).

We state the following simple result, which will help us use this modified height.

**Lemma 17.1.** *Let  $F_0 \in k[X, Z]$  be squarefree and homogeneous of degree 6. For  $c \in k^\times$ , let  $C^{(c)}$  denote the curve  $Y^2 = cF_0(X, Z)$ . The Kummer surfaces  $\text{KS}^{(1)}$*

of  $C^{(1)}$  and  $\text{KS}^{(c)}$  of  $C^{(c)}$  are isomorphic via

$$\iota: \text{KS}^{(1)} \rightarrow \text{KS}^{(c)}, \quad (x_1 : x_2 : x_3 : x_4) \mapsto (x_1 : x_2 : x_3 : cx_4).$$

We abuse notation and write  $\iota$  also for the linear map

$$(x_1, x_2, x_3, x_4) \mapsto (x_1, x_2, x_3, cx_4).$$

Write  $\delta^{(c)}$  for the duplication polynomials on  $\text{KS}^{(c)}$ . Then

$$\delta^{(c)}(\iota(x)) = c^3 \iota(\delta^{(1)}(x)) \quad \text{for each } x \in \text{KS}_{\mathbb{A}}^{(1)}.$$

*Proof.* This can be checked by an easy calculation. □

If  $k$  is nonarchimedean and we use the modified local height given by

$$h'_v(x) = \log \max\{|x_1|_v, |x_2|_v, |x_3|_v, |x_4|_v / \|F\|_v\},$$

then we need to change the definition of  $\varepsilon$  accordingly to (compare [Lemma 2.4](#))

$$\varepsilon(x) = \min\{v(\delta_1(x)), v(\delta_2(x)), v(\delta_3(x)), v(\delta_4(x)) - v(F)\} \\ - 4 \min\{v(x_1), v(x_2), v(x_3), v(x_4) - v(F)\},$$

where  $v(F) = v(\{f_0, \dots, f_6\})$ . By [Lemma 17.1](#) with  $c = \pi^{v(F)}$ , where  $\pi$  is a uniformizer of  $k$ , and  $F_0 = c^{-1}F$ , we then have, denoting the objects associated to  $F_0$  by  $\delta_0, \varepsilon_0$  and  $\mu_0$ ,

$$\varepsilon(x) = v(\iota^{-1}(\delta(x))) - 4v(\iota^{-1}(x)) \\ = v(c^3 \delta_0(\iota^{-1}(x))) - 4v(\iota^{-1}(x)) = 3v(F) + \varepsilon_0(\iota^{-1}(x)).$$

This implies  $\mu(x) = v(F) + \mu_0(\iota^{-1}(x))$ . Let  $C_0$  be the curve given by  $Y^2 = F_0(X, Z)$ . We then get that

$$\beta(C) \leq v(F) + \bar{\beta}(C_0).$$

Note that the Jacobians of  $C$  and  $C_0$  are in general only isomorphic over the ramified quadratic extension  $k(\sqrt{\pi})$ , so we cannot necessarily use  $\beta(C_0)$  here. If  $v(F)$  is even, however, then the isomorphism is defined over  $k$ , and we have  $\beta(C) = v(F) + \beta(C_0)$ .

So, except for the correction term  $v(F)$ , the effect is that we use the Kummer surface associated to the quadratic twist  $C_0$  of  $C$ , which has a primitive polynomial on the right-hand side of its equation. Note in addition that this also allows us to deal with nonintegral equations; in this case, we again implicitly scale to make the polynomial on the right integral and primitive.

When  $k = K_v \cong \mathbb{Q}_2$  (say) and we can write  $F = 4F_1 + H^2$  with binary forms  $F_1$  and  $H$  with integral coefficients, then  $C$  is isomorphic to the curve  $C'$  given by

the Weierstrass equation

$$Y^2 + H(X, Z)Y = F_1(X, Z),$$

and we can use the Kummer surface of the latter to define the local contribution to the naive height. The isomorphism between the Kummer surfaces is given by (see [Müller 2010, p. 53]; note that this is the inverse of the map given there)

$$(x_1 : x_2 : x_3 : x_4) \mapsto (x_1 : x_2 : x_3 : \frac{1}{4}x_4 + \frac{1}{2}(h_0h_2x_1 + h_0h_3x_2 + h_1h_2x_3)).$$

The scaling factor this induces for the  $\delta$  polynomials is  $2^6$  in this case. So defining the local component at  $v$  of  $h'(x)$  to be

$$\log \max \left\{ |x_1|_v, |x_2|_v, |x_3|_v, \left| \frac{1}{4}x_4 + \frac{1}{2}(h_0h_2x_1 + h_0h_3x_2 + h_1h_2x_3) \right|_v \right\},$$

we can replace the bound for  $\mu_v$  by the bound we get on  $C'$  plus 2. If we use this at the places above 2 where it applies (instead of, or combined with, the scaling described above), we still obtain a height as in Example 2.3.

If  $v$  is an archimedean place, then the approach described in Section 16B above can easily be adapted to the modified naive height. We just have to replace  $b_{\{S,S'\},4} = 1$  by  $\|F\|_v$  and  $a_{4,\{S,S'\}}$  by  $a_{4,\{S,S'\}}/\|F\|_v^2$ . This will usually lead to a negative upper bound for  $\tilde{\mu}_v$ , which is fairly close to  $-\log \|F\|_v$ , at least when  $F$  is reduced in the sense of [Stoll and Cremona 2003] and its roots are not too close together. This is because the scaled  $a_{i,\{S,S'\}}$  are now all of size  $\approx \|F\|_\infty^{-2}$  and the scaled  $b_{\{S,S'\},j}$  are all of size  $\approx \|F\|_\infty$ , so  $\Phi$  as in the proof of Lemma 16.1 roughly satisfies  $\|\Phi(x)\|_\infty \approx -\frac{3}{4} \log \|F\|_\infty + \frac{1}{4} \|x\|_\infty$ , which has  $-\log \|F\|_\infty$  as its fixed point.

Note that for a point  $(0 : 0 : 0 : 1) \neq P = (x_1 : x_2 : x_3 : x_4) \in \text{KS}(K)$  we have, for all versions  $h'$  of the modified height,

$$h_{\text{std}}((x_1 : x_2 : x_3)) \leq h'(P).$$

We will therefore find all points  $P$  with  $h'(P) \leq B$ , if we can enumerate all  $P$  with  $h_{\text{std}}((x_1 : x_2 : x_3)) \leq B$ . This can be done (over  $\mathbb{Q}$ ) by using the `-a` option of the second author's program `j-points`, which is available at [Stoll 2006]. (This option is also available in Magma version 2.22 or later.) In this way, enumerating all points as above with  $B$  up to roughly  $\log 50\,000$  is feasible. See the discussion in Section 18.

Note that it is quite possible that we end up with a bound

$$h_{\text{std}}((x_1 : x_2 : x_3)) \leq h'(P) \leq \hat{h}(P) + \tilde{\beta} \quad \text{for all } P \in J(\mathbb{Q}) \setminus \{O\}$$

with  $\tilde{\beta} < 0$ . In this case  $-\tilde{\beta}$  is a lower bound on the canonical height of any nontrivial point in  $J(\mathbb{Q})$ ; in particular, the torsion subgroup of  $J(\mathbb{Q})$  must be trivial. To give an indication of when we can expect  $\tilde{\beta}$  to be close to zero or negative, write  $|2^4 \text{disc}(F)| = DD'$  with  $D$  and  $D'$  coprime and  $D'$  squarefree and odd. Then the contribution of the finite places to  $\tilde{\beta}$  can be bounded by  $\frac{1}{4} \log D$ , and we get

$\tilde{\beta} \approx -\log \|F\|_\infty + \frac{1}{4} \log D$ . So if  $D \ll \|F\|_\infty^4$ , we are in good shape. Note that  $|\text{disc}(F)| \ll \|F\|_\infty^{10}$ , so this means that 60% or more of  $\log |\text{disc}(F)|$  comes from primes  $p$  dividing the discriminant exactly once. For curves that are not very special this is very likely to be the case.

In Section 19 we show how this approach can be used to get a very small bound for the height difference even for a curve with ten-digit coefficients.

### 18. Efficient enumeration of points of bounded canonical height

Let  $C : y^2 = f(x)$  be a curve of genus 2 over  $\mathbb{Q}$  with Jacobian  $J$ . In this section we describe the algorithm for enumerating all points  $P \in J(\mathbb{Q})$  with  $\hat{h}(P) \leq B$  that follows from the considerations above. We assume that  $f \in \mathbb{Z}[x]$  and proceed as follows.

1. Compute the complex roots of  $f$  numerically.
2. Compute the coefficients  $a_{i,\{S,S'\}}$  and  $b_{\{S,S'\},j}$  from the roots and the leading coefficient of  $f$  according to the formulas given in [Stoll 1999, §10].
3. Multiply all  $a_{4,\{S,S'\}}$  by  $\|f\|_\infty^{-2}$  and multiply all  $b_{\{S,S'\},4}$  by  $\|f\|_\infty$ .
4. Iterate the function  $\varphi$  from Section 17 (but using the modified coefficients) a number of times, starting at  $(1, 1, 1, 1)$ , until there is little change; let  $\tilde{\beta}_\infty$  be the upper bound for  $\tilde{\mu}_\infty$  as in Lemma 16.1.
5. Factor the discriminant of  $f$ . Let  $g$  be the gcd of the coefficients of  $f$ .
6. For each prime divisor  $p$  of  $2 \text{ disc}(f)$ , do the following.
  - a. Let  $e_p$  be the  $p$ -adic valuation of  $g$  and set  $f_1 = p^{-e_p} f$ .
  - b. If  $p = 2$  and  $f_1 = h^2 + 4f_2$  for polynomials  $f_2, h \in \mathbb{Z}[x]$ , then set  $C_1 : y^2 + h(x)y = f_2(x)$  and replace  $g$  by  $4g$ ; otherwise set  $C_1 : y^2 = f_1(x)$ . Let  $J_1$  be the Jacobian of  $C_1$ .
  - c. If  $e_p$  is even, let  $\beta_p$  be the bound for  $\mu_p$  on  $J_1(\mathbb{Q}_p)$  as obtained in Part II. Otherwise, let  $\beta_p$  be the bound for  $\mu_p$  on  $J_1(\overline{\mathbb{Q}}_p)$ .
7. Set  $\tilde{\beta} = \tilde{\beta}_\infty + \sum_p \beta_p \log p + \log g$ .
8. Use `j-points` with the `-a` option to enumerate all points  $O \neq P \in J(\mathbb{Q})$  such that  $h_{\text{std}}((\kappa_1(P) : \kappa_2(P) : \kappa_3(P))) \leq B + \tilde{\beta}$ .
9. Add  $O$  to this set and return it.

Note that  $\log g$  is the sum of the correction terms  $v_p(f) \log p$ .

It follows from the discussion in the previous sections that the set returned by this algorithm contains all points with canonical height at most  $B$ . If necessary, one can compute the actual canonical heights using the algorithm from Part III and discard the points whose height is too large.

The actual enumeration is done by running through all points  $(x_1 : x_2 : x_3) \in \mathbb{P}^2$  of (standard) height at most  $B + \tilde{\beta}$  and checking whether there are rational numbers  $x_4$

such that  $(x_1 : x_2 : x_3 : x_4)$  is on the Kummer surface. For each of these points on the Kummer surface, we then check if it lifts to the Jacobian. Both these conditions are equivalent to some expression in the coordinates (and the coefficients of  $f$ ) being a square. The `j-points` program tries to do this efficiently by using information modulo a number of primes to filter out triples that do not lift to rational points on  $J$ . Let  $N = \lfloor \exp(B + \tilde{\beta}) \rfloor$ . Then `j-points` usually takes a couple of seconds when  $N = 1000$ , a few minutes when  $N = 5000$  and a few days when  $N = 50\,000$ . The running time scales with  $N^3$ , but the scaling factor depends on how effective the sieving mod  $p$  is. For Jacobians of high rank, the program tends to take longer than for “random” Jacobians.

Since the running time depends exponentially on  $B + \tilde{\beta}$ , it is very important to obtain a small bound  $\tilde{\beta}$  for the difference between naive and canonical height. The improvement at the infinite place that we can achieve by considering a modified naive height is crucial for making the enumeration feasible also in cases when the defining polynomial has large coefficients. This is demonstrated by the example in [Section 19](#).

If the discriminant of  $f$  is too large to be factored, then one can use

$$\tilde{\beta} = \tilde{\beta}_\infty + \frac{1}{4} \log |\text{disc}(f_1)| + \log g$$

(or use information from small prime divisors as in the algorithm above and  $\frac{1}{4} \log D$  for the remaining primes, where  $D$  is the unfactored part of the discriminant). But note that it is usually a great advantage to know the bad primes, since we can take  $\beta_p = 0$  for primes  $p$  such that  $v_p(\text{disc}(f)) = 1$ . In most cases, this leads to a much smaller bound  $\tilde{\beta}$ .

One of the most important applications of this enumeration algorithm is its use in saturating a given finite-index subgroup of  $J(\mathbb{Q})$ , which gives (generators of) the full group  $J(\mathbb{Q})$ . This is a necessary ingredient of the method for obtaining all integral points on  $C$  developed in [\[Bugeaud et al. 2008\]](#), for example, and for computing the regulator of  $J(\mathbb{Q})$ .

There are essentially two ways of performing the saturation. Let  $G \subset J(\mathbb{Q})$  denote the known subgroup.

(i) Let  $\rho$  be (an upper bound for) the covering radius of the lattice  $\Lambda = (G/G_{\text{tors}}, \hat{h})$ . Then  $J(\mathbb{Q})$  is generated by  $G$  together with all points  $P \in J(\mathbb{Q})$  that satisfy  $\hat{h}(P) \leq \rho^2$ ; see [\[Stoll 2002, Proposition 7.1\]](#). This approach is feasible when  $\tilde{\beta} + \rho^2$  is sufficiently small.

(ii) Let  $I = (J(\mathbb{Q}) : G)$  denote the index; we assume  $J(\mathbb{Q})_{\text{tors}} \subset G$ . If  $m_1, \dots, m_r$  are the successive minima of  $\Lambda$  and there are no points  $P \in J(\mathbb{Q}) \setminus G$  with  $\hat{h}(P) < B$ , then

$$I \leq \sqrt{\frac{R \cdot \gamma_r^r}{\prod_{j=1}^r \min\{m_j, B\}}};$$

see [Flynn and Smart 1997, §7]. Here  $\gamma_r$  is (an upper bound for) the Hermite constant for lattices of rank  $r$ , and  $R$  is the regulator of  $G$  (i.e., the determinant of the Gram matrix of any basis of  $\Lambda$ ). This can be used to get a bound on  $I$  whenever  $B$  is strictly positive, so for the enumeration we only need  $\tilde{\beta}$  to be sufficiently small. (If  $\tilde{\beta} < 0$ , then we can do entirely without enumeration to get an index bound.) In a second step, one then has to check that  $G$  is  $p$ -saturated in  $J(\mathbb{Q})$  (or find the largest group  $G \subset G' \subset J(\mathbb{Q})$  with  $(G' : G)$  a power of  $p$  for all primes  $p$  up to the index bound. This can be done by considering the intersection of the kernels of the maps  $J(\mathbb{Q})/pJ(\mathbb{Q}) \rightarrow J(\mathbb{F}_q)/pJ(\mathbb{F}_q)$  for a set of good primes  $q$  (such that the group on the right is nontrivial). If this intersection is trivial, then  $G$  is  $p$ -saturated; otherwise it tells us where to look for points that are potentially divisible by  $p$ . Since the index bound gets smaller with increasing  $B$  (as long as  $B < m_r$ ), it makes sense to pick  $B$  in such a way as to balance the time spent in the two steps of this approach.

### 19. Example

As an example that demonstrates the use of our nearly optimal upper bound for the difference  $h - \hat{h}$  between naive and canonical height (which is based on the optimal bounds for the  $\mu_p$  obtained in Sections 9, 10 and 11 and the variation of the naive height discussed in Section 17), we consider the curve

$$C: y^2 = 82342800x^6 - 470135160x^5 + 52485681x^4 + 2396040466x^3 + 567207969x^2 - 985905640x + 247747600.$$

This curve is of interest, since it holds the current record for the largest number of known rational points (which is 642 for this curve); see [Stoll 2008]. A 2-descent on its Jacobian  $J$  (assuming GRH) as described in [Stoll 2001] and implemented in Magma gives an upper bound of 22 for the rank of  $J(\mathbb{Q})$ , and the differences of the known rational points generate a group of rank 22. The latter statement can be checked by computing the determinant  $R$  of the height pairing matrix of the 22 points in  $J(\mathbb{Q})$  listed in Table 3, which is fairly fast using the algorithm for computing canonical heights described in Section 14. The points are given in Mumford representation  $(a(x), b(x))$ , which stands for  $[(\theta_1, b(\theta_1)) + (\theta_2, b(\theta_2))] - W$ , where  $\theta_1, \theta_2$  are the two roots of  $a(x)$  and  $W$  is the canonical class. Not all of these points are differences of rational points, but they are linear combinations of such differences.

We can easily check that  $J(\mathbb{Q})$  has trivial torsion subgroup by computing the order of  $J(\mathbb{F}_p)$  for a few good primes  $p$ .

The discriminant of  $C$  factors as

$$\Delta = 2^{47} \cdot 3^5 \cdot 5^9 \cdot 11^2 \cdot 13^2 \cdot 17^6 \cdot 19^4 \cdot 23^2 \cdot 41^4 \cdot 73^3 \cdot 2707 \cdot 43579 \cdot 108217976921 \cdot 8723283517315751077.$$

$(x^2 + x, 18868x + 15740),$	$(x^2 - \frac{1}{3}x, \frac{216800}{3}x - 15740),$
$(x^2 + \frac{2}{3}x - \frac{1}{3}, \frac{11747}{3}x + \frac{21131}{3}),$	$(x^2 + 5x + 4, 276256x + 273128),$
$(x^2 + \frac{4}{3}x - \frac{5}{9}, 16315x + \frac{26195}{9}),$	$(x^2 + \frac{53}{12}x + \frac{5}{3}, \frac{1433669}{6}x + \frac{371650}{3}),$
$(x^2 - 3x - 4, 34104x + 30976),$	$(x^2 - 4x - 5, 65987x + 69115),$
$(x^2 + \frac{8}{5}x + \frac{3}{5}, 67671x + 64543),$	$(x^2 - 5x - 6, \frac{883626}{7}x + \frac{905522}{7}),$
$(x^2 - \frac{3}{4}x - \frac{7}{4}, 31875x + 35003),$	$(x^2 + \frac{5}{7}x - \frac{2}{7}, \frac{432898}{49}x + \frac{279626}{49}),$
$(x^2 + \frac{29}{6}x - \frac{178}{9}, \frac{3014179}{6}x - \frac{10824742}{9}),$	$(x^2 + \frac{19}{84}x - \frac{65}{84}, \frac{4287373}{294}x + \frac{5207005}{294}),$
$(x^2 + \frac{97}{42}x - \frac{37}{42}, \frac{23742013}{294}x - \frac{5459431}{294}),$	$(x^2 - \frac{5}{11}x, \frac{1089388}{121}x - 15740),$
$(x^2 + \frac{325}{84}x - \frac{11}{21}, \frac{30014567}{147}x - \frac{2230444}{147}),$	$(x^2 - \frac{683}{140}x - \frac{279}{140}, \frac{45519013}{490}x + \frac{5478709}{490}),$
$(x^2 - \frac{91}{769}x - \frac{584}{769}, \frac{6911886712}{591361}x + \frac{16665656516}{591361}),$	$(x^2 - \frac{259}{96}x + \frac{163}{72}, \frac{52305719}{768}x - \frac{13101271}{576}),$
$(x^2 - \frac{3073}{2307}x - \frac{1252}{769}, \frac{54505985456}{1774083}x + \frac{25990632928}{591361}),$	$(x^2 - \frac{137}{51}x + \frac{40}{51}, \frac{47131040}{867}x - \frac{8471860}{867}).$

**Table 3.** Generators of the known part of  $J(\mathbb{Q})$ .

The results of [Stoll 1999; Stoll 2002] lead to a bound of

$$\frac{1}{3}(43 \log 2 + 3 \log 3 + 9 \log 5 + 2 \log 11 + 2 \log 13 + 6 \log 17 + 4 \log 19 + 2 \log 23 + 4 \log 41 + 3 \log 73) \approx 40.1$$

for the contribution of the finite places to the height difference bound. When trying to get a better bound (for  $\gamma_p$ ) by essentially doing an exhaustive search over the  $p$ -adic points of the Kummer surface, Magma gets stuck at  $p = 2$  for a long while, but eventually finishes with a contribution of 26.434 from the finite places and a total bound of 34.163. This contribution turns out to be  $\frac{1}{3}\gamma_p \log p$  in all cases except for  $p = 73$ , where it is  $\frac{2}{3} \log 73$  instead of  $\frac{1}{3} \log 73$ . Our new results from this paper give bounds on the local contributions as shown in Table 4.  $\Phi_p$  is the component group ( $\varepsilon$  and  $\mu$  factor through it in all cases) and “gain” gives the gain in the bound on the height difference obtained by using the optimal bound on  $\mu$  versus the bound  $\frac{1}{3}\gamma$ , where  $\gamma$  is the maximum of the values of  $\varepsilon$ .

This now gives a bound of  $\approx 20.429$  for the contribution of the finite places. The optimization of the naive height does not give any improvement at the odd finite places, since the polynomial  $f$  defining the curve is primitive. On the other hand, we note that  $f$  is congruent to a square mod 4, so we could use the Kummer surface of the curve  $y^2 + (x^2 + x)y = f_1(x)$  (where  $f(x) = 4f_1(x) + (x^2 + x)^2$ ) for the local height at 2, but this results in no improvement, since we have already used a minimal model to get our bound.

Now we consider the contribution of the infinite place. The bound obtained from [Stoll 1999, Equation (7.1)] is 7.726. Using Lemma 16.1 with  $N = 10$  improves

$p$	reduction type	$\Phi_p$	$\beta_p$	$\frac{1}{3}\gamma_p$	gain
2	$[I_{10-9-8}]$	$\mathbb{Z}/242\mathbb{Z}$	$2 + 11^{45}/242$	$26/3$	1.341
3	$[I_0 - IV - 0]$	$\mathbb{Z}/3\mathbb{Z}$	$2/3$	$2/3$	0.000
5	$[I_{4-3-2}]$	$\mathbb{Z}/26\mathbb{Z}$	$2^2/13$	2	0.495
11	$[I_{2-0-0}]$	$\mathbb{Z}/2\mathbb{Z}$	$1/2$	$2/3$	0.400
13	$[I_{2-0-0}]$	$\mathbb{Z}/2\mathbb{Z}$	$1/2$	$2/3$	0.427
17	$[I_{2-2-2}]$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	1	$4/3$	0.944
19	$[I_{2-1-1}]$	$\mathbb{Z}/5\mathbb{Z}$	$3/5$	$2/3$	0.196
23	$[I_{2-0-0}]$	$\mathbb{Z}/2\mathbb{Z}$	$1/2$	$2/3$	0.523
41	$[I_{2-1-1}]$	$\mathbb{Z}/5\mathbb{Z}$	$3/5$	$2/3$	0.248
73	$[I_{1-1-1}]$	$\mathbb{Z}/3\mathbb{Z}$	$1/3$	$1/3$	0.000

**Table 4.** Bounds for  $\beta_p$ .

this to 0.973; increasing  $N$  further gives no significant improvement. However, modifying the local height at the infinite place by scaling the contribution of the fourth coordinate by  $\|f\|_\infty^{-1}$  reduces this bound drastically to  $\tilde{\mu}_\infty \leq -19.25654$  (compare this to  $-\log \|f\|_\infty \approx -21.59708$ ). This finally gives

$$h'(P) \leq \hat{h}(P) + 1.17273$$

for our modified naive height  $h'$ .

So if we enumerate all points  $P \in J(\mathbb{Q})$  with  $h'(P) \leq \log N$  and do not find points that are not in the known subgroup  $G$ , then we obtain a bound for the index  $I = (J(\mathbb{Q}) : G)$  as follows (see the discussion at the end of [Section 18](#)):

$$I \leq \sqrt{\frac{R \cdot \gamma_{22}^{22}}{\prod_{j=1}^{22} \min\{m_j, \log N - 1.17273\}}}$$

Here  $R$  is the regulator of  $G$  and  $m_1, m_2, \dots, m_{22}$  are the successive minima of the lattice  $(G, \hat{h})$ , which are

- 8.5276, 8.5668, 8.5956, 8.8594, 9.0256, 9.0776, 9.1426, 9.1753,  
 9.4456, 9.7428, 9.7747, 9.9047, 9.9465, 9.9611, 9.9704, 10.1408,  
 10.3472, 10.3784, 10.5284, 10.5356, 10.6318, 10.9287.

With  $N = 10000$  we obtain  $I \leq 6842$ , with  $N = 20000$  we get  $I \leq 2835$  and with  $N \geq 178\,245$  we obtain the best possible bound  $I \leq 900$ . We checked that there are no unknown points  $P$  with  $\kappa(P) = (x_1 : x_2 : x_3 : x_4)$  such that  $h_{\text{std}}((x_1 : x_2 : x_3)) \leq \log 20\,000$  and verified that the index is not divisible by any prime  $p \leq 2835$ . The first computation took about two days on a single core, the second less than half a day. This implies the following.



**Proposition 19.1.** *Assume the generalized Riemann hypothesis. Let*

$$C: y^2 = 82342800x^6 - 470135160x^5 + 52485681x^4 \\ + 2396040466x^3 + 567207969x^2 - 985905640x + 247747600$$

*and denote by  $J$  the Jacobian of  $C$ . Then  $J(\mathbb{Q})$  is a free abelian group of rank 22, freely generated by the points listed in Table 3. In particular,  $J(\mathbb{Q})$  is generated by the differences of rational points on  $C$ .*

### Acknowledgments

We would like to thank David Holmes for suggesting the strategy of the proof of Proposition 7.3, Elliot Wells for pointing out an inaccuracy in the complexity analysis in Propositions 14.1 and 14.3, and the anonymous referee for some useful remarks and suggestions.

### References

- [Artin 1966] M. Artin, “On isolated rational singularities of surfaces”, *Amer. J. Math.* **88** (1966), 129–136. [MR](#) [Zbl](#) 10
- [Artin 1986] M. Artin, “Lipman’s proof of resolution of singularities for surfaces”, pp. 267–287 in *Arithmetic geometry* (Storrs, CT, 1984), edited by G. Cornell and J. H. Silverman, Springer, 1986. [MR](#) [Zbl](#) 7
- [Barth et al. 1984] W. Barth, C. Peters, and A. Van de Ven, *Compact complex surfaces*, *Ergebnisse der Mathematik und ihrer Grenzgebiete* (3) **4**, Springer, 1984. [MR](#) [Zbl](#) 5
- [Bernstein 2004] D. J. Bernstein, “Research announcement: faster factorization into coprimes”, preprint, 2004, <https://cr.yp.to/lineartime/dcba2-20041009.ps>. [5.](#), [14.](#), [14.4.](#), [15](#)
- [Bernstein 2005] D. J. Bernstein, “Factoring into coprimes in essentially linear time”, *J. Algorithms* **54**:1 (2005), 1–30. [MR](#) [Zbl](#) [5.](#), [14.](#), [14.4.](#), [15](#)
- [Bombieri and Gubler 2006] E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, *New Mathematical Monographs* **4**, Cambridge University Press, 2006. [MR](#) [Zbl](#) 4.5
- [Borwein and Borwein 1987] J. M. Borwein and P. B. Borwein, *Pi and the AGM: a study in analytic number theory and computational complexity*, John Wiley & Sons, New York, 1987. [MR](#) [Zbl](#) 13
- [Bosch and Liu 1999] S. Bosch and Q. Liu, “Rational points of the group of components of a Néron model”, *Manuscripta Math.* **98**:3 (1999), 275–293. [MR](#) [Zbl](#) 7
- [Bosch et al. 1990] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, *Ergebnisse der Mathematik und ihrer Grenzgebiete* (3) **21**, Springer, 1990. [MR](#) [Zbl](#) [7.](#), [7.](#), [7.](#), [7.](#), [9.](#), [9.](#), [9.](#), [12](#)
- [Bosma et al. 1997] W. Bosma, J. Cannon, and C. Playoust, “The Magma algebra system, I: The user language”, *J. Symbolic Comput.* **24**:3-4 (1997), 235–265. [MR](#) [Zbl](#) 15, 16A
- [Bost and Mestre 1993] J.-B. Bost and J.-F. Mestre, “Calcul de la hauteur archimédienne des points d’une courbe elliptique par un algorithme quadratiquement convergent et application au calcul de la capacité de l’union de deux intervalles”, unpublished manuscript, 1993. [14](#)
- [Bruin and Stoll 2010] N. Bruin and M. Stoll, “The Mordell–Weil sieve: proving non-existence of rational points on curves”, *LMS J. Comput. Math.* **13** (2010), 272–306. [MR](#) [Zbl](#) 7, 7
- [Buchmann and Lenstra 1994] J. A. Buchmann and H. W. Lenstra, Jr., “Approximating rings of integers in number fields”, *J. Théor. Nombres Bordeaux* **6**:2 (1994), 221–260. [MR](#) [Zbl](#) 15

- [Bugeaud et al. 2008] Y. Bugeaud, M. Mignotte, S. Siksek, M. Stoll, and S. Tengely, “Integral points on hyperelliptic curves”, *Algebra Number Theory* **2**:8 (2008), 859–885. MR Zbl 1, 18
- [Cassels and Flynn 1996] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus 2*, London Mathematical Society Lecture Note Series **230**, Cambridge University Press, 1996. MR Zbl 1, 1, 3, 7
- [Cinkir 2011] Z. Cinkir, “Zhang’s conjecture and the effective Bogomolov conjecture over function fields”, *Invent. Math.* **183**:3 (2011), 517–562. MR Zbl 8.4
- [Conrad 2005] B. Conrad, “Minimal models for elliptic curves”, unpublished manuscript, 2005, <http://math.stanford.edu/~conrad/papers/minimalmodel.pdf>. 7.5, 10
- [Cremona et al. 2006] J. E. Cremona, M. Prickett, and S. Siksek, “Height difference bounds for elliptic curves over number fields”, *J. Number Theory* **116**:1 (2006), 42–68. MR Zbl 10.13, 11
- [Deligne and Mumford 1969] P. Deligne and D. Mumford, “The irreducibility of the space of curves of given genus”, *Inst. Hautes Études Sci. Publ. Math.* **36** (1969), 75–109. MR Zbl 5
- [Flynn and Smart 1997] E. V. Flynn and N. P. Smart, “Canonical heights on the Jacobians of curves of genus 2 and the infinite descent”, *Acta Arith.* **79**:4 (1997), 333–352. MR Zbl 1, a., 4, 14, 15, 18
- [Flynn et al. 2001] E. V. Flynn, F. Leprévost, E. F. Schaefer, W. A. Stein, M. Stoll, and J. L. Wetherell, “Empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves”, *Math. Comp.* **70**:236 (2001), 1675–1697. MR Zbl 1
- [von zur Gathen and Gerhard 1999] J. von zur Gathen and J. Gerhard, *Modern computer algebra*, Cambridge University Press, New York, 1999. MR Zbl 13
- [Greuel and Kröning 1990] G.-M. Greuel and H. Kröning, “Simple singularities in positive characteristic”, *Math. Z.* **203**:2 (1990), 339–354. MR Zbl 5
- [Heinz 2004] N. Heinz, “Admissible metrics for line bundles on curves and abelian varieties over non-Archimedean local fields”, *Arch. Math. (Basel)* **82**:2 (2004), 128–139. MR Zbl 1, 8
- [Hindry and Silverman 2000] M. Hindry and J. H. Silverman, *Diophantine geometry: an introduction*, Graduate Texts in Mathematics **201**, Springer, 2000. MR Zbl 1, 2, 4
- [Holmes 2012] D. Holmes, “Computing Néron–Tate heights of points on hyperelliptic Jacobians”, *J. Number Theory* **132**:6 (2012), 1295–1305. MR Zbl 14
- [Holmes 2014] D. Holmes, “An Arakelov-theoretic approach to naïve heights on hyperelliptic Jacobians”, *New York J. Math.* **20** (2014), 927–957. MR Zbl 2
- [Igusa 1960] J.-I. Igusa, “Arithmetic variety of moduli for genus two”, *Ann. of Math. (2)* **72** (1960), 612–649. MR Zbl 6
- [de Jong and Müller 2014] R. de Jong and J. S. Müller, “Canonical heights and division polynomials”, *Math. Proc. Cambridge Philos. Soc.* **157**:2 (2014), 357–373. MR Zbl 14
- [Lang 1983] S. Lang, *Fundamentals of Diophantine geometry*, Springer, 1983. MR Zbl 8, 12
- [Liu 1993] Q. Liu, “Courbes stables de genre 2 et leur schéma de modules”, *Math. Ann.* **295**:2 (1993), 201–222. MR Zbl 6, 6.1, 6, 6
- [Liu 1994] Q. Liu, “Modèles minimaux des courbes de genre deux”, *J. Reine Angew. Math.* **453** (1994), 137–164. MR Zbl 10, 12, 12
- [Liu 1996] Q. Liu, “Modèles entiers des courbes hyperelliptiques sur un corps de valuation discrète”, *Trans. Amer. Math. Soc.* **348**:11 (1996), 4577–4610. MR Zbl 4, 5, 5, 5, 11, 11, 11
- [Liu 2002] Q. Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics **6**, Oxford University Press, 2002. MR Zbl 7
- [Mestre 1991] J.-F. Mestre, “Construction de courbes de genre 2 à partir de leurs modules”, pp. 313–334 in *Effective methods in algebraic geometry* (Castiglione, 1990), edited by T. Mora and C. Traverso, Progr. Math. **94**, Birkhäuser, Boston, 1991. MR Zbl 6

- [Müller 2010] J. S. Müller, “Explicit Kummer surface formulas for arbitrary characteristic”, *LMS J. Comput. Math.* **13** (2010), 47–64. MR Zbl 1, 1, 3, 17
- [Müller 2014] J. S. Müller, “Computing canonical heights using arithmetic intersection theory”, *Math. Comp.* **83**:285 (2014), 311–336. MR Zbl 14
- [Müller and Stoll 2016] J. S. Müller and M. Stoll, “Computing canonical heights on elliptic curves in quasi-linear time”, *LMS J. Comput. Math.* **19**:suppl. A (2016), 391–405. MR 1, 12, 12, 12, 14, 14, 14, 14
- [Namikawa and Ueno 1973] Y. Namikawa and K. Ueno, “The complete classification of fibres in pencils of curves of genus two”, *Manuscripta Math.* **9** (1973), 143–186. MR Zbl 5, 6.3, 9, 9, 10, 10, 12.4, 12
- [Néron 1965] A. Néron, “Quasi-fonctions et hauteurs sur les variétés abéliennes”, *Ann. of Math. (2)* **82** (1965), 249–331. MR Zbl 1, 12
- [Silverman 1988] J. H. Silverman, “Computing heights on elliptic curves”, *Math. Comp.* **51**:183 (1988), 339–358. MR Zbl 7.5, 9.2
- [Silverman 1994] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics **151**, Springer, 1994. MR Zbl 9
- [Stoll 1999] M. Stoll, “On the height constant for curves of genus two”, *Acta Arith.* **90**:2 (1999), 183–201. MR Zbl 1, 1, 3.2, 11, 13, 14, 16, 16A, 16B, 2., 19, 19
- [Stoll 2001] M. Stoll, “Implementing 2-descent for Jacobians of hyperelliptic curves”, *Acta Arith.* **98**:3 (2001), 245–277. MR Zbl 19
- [Stoll 2002] M. Stoll, “On the height constant for curves of genus two, II”, *Acta Arith.* **104**:2 (2002), 165–182. MR Zbl 1, 1, 3, 3, 3, 3, 3, 3, 10, 14, 14, 15, 18, 19
- [Stoll 2006] M. Stoll, “j-points, a program for searching rational points on genus 2 Jacobians”, computer program, 2006, <http://www.mathe2.uni-bayreuth.de/stoll/programs/index.html>. 17
- [Stoll 2008] M. Stoll, “A genus 2 curve with at least 642 rational points”, electronic reference, 2008, <http://www.mathe2.uni-bayreuth.de/stoll/recordcurve.html>. 1, 19
- [Stoll 2014] M. Stoll, “An explicit theory of heights for hyperelliptic Jacobians of genus three”, preprint, 2014, <http://www.mathe2.uni-bayreuth.de/stoll/papers/Kummer-g3-hyp-2014-05-15.pdf>. 16B
- [Stoll and Cremona 2003] M. Stoll and J. E. Cremona, “On the reduction theory of binary forms”, *J. Reine Angew. Math.* **565** (2003), 79–99. MR Zbl 17
- [Uchida 2011] Y. Uchida, “Canonical local heights and multiplication formulas for the Jacobians of curves of genus 2”, *Acta Arith.* **149**:2 (2011), 111–130. MR Zbl 8, 14
- [Zarkhin 1995] Y. G. Zarkhin, “Local heights and Néron pairings”, *Trudy Mat. Inst. Steklov.* **208** (1995), 111–127. In Russian; translated in *Proc. Steklov Inst. Math.* **208** (1995), 100–114. MR Zbl 2, 4.5
- [Zhang 1993] S. Zhang, “Admissible pairing on a curve”, *Invent. Math.* **112**:1 (1993), 171–193. MR Zbl 1, 8

Communicated by Joseph H. Silverman

Received 2016-03-31

Revised 2016-08-02

Accepted 2016-09-05

[jan.steffen.mueller@uni-oldenburg.de](mailto:jan.steffen.mueller@uni-oldenburg.de)

*Institut für Mathematik, Carl von Ossietzky Universität  
Oldenburg, D-26111 Oldenburg, Germany*

[michael.stoll@uni-bayreuth.de](mailto:michael.stoll@uni-bayreuth.de)

*Mathematisches Institut, Universität Bayreuth,  
D-95440 Bayreuth, Germany*

# Algebra & Number Theory

[msp.org/ant](http://msp.org/ant)

## EDITORS

### MANAGING EDITOR

Bjorn Poonen  
Massachusetts Institute of Technology  
Cambridge, USA

### EDITORIAL BOARD CHAIR

David Eisenbud  
University of California  
Berkeley, USA

## BOARD OF EDITORS

Dave Benson	University of Aberdeen, Scotland	Susan Montgomery	University of Southern California, USA
Richard E. Borcherds	University of California, Berkeley, USA	Shigefumi Mori	RIMS, Kyoto University, Japan
John H. Coates	University of Cambridge, UK	Raman Parimala	Emory University, USA
J-L. Colliot-Thélène	CNRS, Université Paris-Sud, France	Jonathan Pila	University of Oxford, UK
Brian D. Conrad	Stanford University, USA	Anand Pillay	University of Notre Dame, USA
Hélène Esnault	Freie Universität Berlin, Germany	Victor Reiner	University of Minnesota, USA
Hubert Flenner	Ruhr-Universität, Germany	Peter Sarnak	Princeton University, USA
Sergey Fomin	University of Michigan, USA	Joseph H. Silverman	Brown University, USA
Edward Frenkel	University of California, Berkeley, USA	Michael Singer	North Carolina State University, USA
Andrew Granville	Université de Montréal, Canada	Vasudevan Srinivas	Tata Inst. of Fund. Research, India
Joseph Gubeladze	San Francisco State University, USA	J. Toby Stafford	University of Michigan, USA
Roger Heath-Brown	Oxford University, UK	Ravi Vakil	Stanford University, USA
Craig Huneke	University of Virginia, USA	Michel van den Bergh	Hasselt University, Belgium
Kiran S. Kedlaya	Univ. of California, San Diego, USA	Marie-France Vignéras	Université Paris VII, France
János Kollár	Princeton University, USA	Kei-Ichi Watanabe	Nihon University, Japan
Yuri Manin	Northwestern University, USA	Efim Zelmanov	University of California, San Diego, USA
Philippe Michel	École Polytechnique Fédérale de Lausanne	Shou-Wu Zhang	Princeton University, USA

## PRODUCTION

[production@msp.org](mailto:production@msp.org)

Silvio Levy, Scientific Editor

---

See inside back cover or [msp.org/ant](http://msp.org/ant) for submission instructions.

---

The subscription price for 2016 is US \$290/year for the electronic version, and \$485/year (+\$55, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscribers address should be sent to MSP.

---

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

---

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

 **mathematical sciences publishers**  
nonprofit scientific publishing

<http://msp.org/>

© 2016 Mathematical Sciences Publishers

# Algebra & Number Theory

Volume 10    No. 10    2016

---

<a href="#">Weight functions on Berkovich curves</a>	2053
MATTHEW BAKER and JOHANNES NICAISE	
<a href="#">Nonvanishing of Dirichlet <math>L</math>-functions</a>	2081
RIZWANUR KHAN and HIEU T. NGO	
<a href="#">Every integer greater than 454 is the sum of at most seven positive cubes</a>	2093
SAMIR SIKSEK	
<a href="#">Constructible isocrystals</a>	2121
BERNARD LE STUM	
<a href="#">Canonical heights on genus-2 Jacobians</a>	2153
JAN STEFFEN MÜLLER and MICHAEL STOLL	
<a href="#">Combinatorial degenerations of surfaces and Calabi–Yau threefolds</a>	2235
BRUNO CHIARELLOTTO and CHRISTOPHER LAZDA	
<a href="#">The Voronoi formula and double Dirichlet series</a>	2267
EREN MEHMET KIRAL and FAN ZHOU	
<a href="#">Finite dimensional Hopf actions on algebraic quantizations</a>	2287
PAVEL ETINGOF and CHELSEA WALTON	