Curves of genus 2 covering elliptic curves and an arithmetical application

GERHARD FREY and ERNST KANI

Introduction

The purpose of the following paper is to show how one can relate elliptic curves E with covering curves C of genus 2 and arithmetical properties of E and C in the case that the ground field is a global field.

In the center of our interest is the height conjecture for elliptic curves (cf. [5]) which would have nice implications for elliptic curves as well as for ternary diophantine equations; as it is well known it would imply an asymptotic version of Fermat's last theorem. It turns out that the height of E is closely connected with the self intersection number of the canonical sheaf of the arithmetical surface corresponding to C. This procedure should be compared with the very interesting approach of Parshin [14], and in fact a (stronger) version of a general inequality for self intersections of canonical sheaves conjectured by Parshin in [14] and known as Bogomolov-Miyaoka-Yau inequality in the geometric case would suffice to prove the height conjecture for E. We have to make the (hopefully only) technical restriction that the absolute values of the j-invariant of E are bounded. The difference to Parshin's approach is that we need the inequality "only" for curves of genus 2 (Corollary 4.5).

In the first section we give a short but systematic report on how to construct curves of genus 2 covering elliptic curves. It turns out that the choice of level-n-structures of pairs of elliptic curves is the essential datum

for these coverings. For the arithmetic of C the Weierstraß points play an important role; in fact one has to know their configuration on the special fibres of the minimal model of C. In §2 we study this configuration in detail (cf. [13]).

In §3 we state height conjectures for curves and abelian varieties over global fields (all known to be true if the ground field is a function field), and in the last section we show, as announced above already, how the self intersection of canonical sheaves of curves of genus 2 is related to the height of elliptic curves covered by them. Here the essential tool is the relation between Néron-Tate heights on Jacobians and heights on curves which can be found in [20] and which is applied to Weierstraß points.

Acknowledgements: The authors are very thankful for helpful discussions with A. Brumer and L. Szpiro. The first author wants to thank Queen's University, Kingston, Canada, for its warm hospitality during a visit supported by NSERC and especially the organizers of the conference at Texel, Netherlands, who provided a generous and stimulating athmosphere which made the visit at Texel both pleasant and mathematically fruitful.

This research was supported in part by the Natural Science and Engeneering Research Council of Canada (NSERC) through a research grant hold by the second author.

1 Construction of coverings of genus 2 of elliptic curves

Our aim in this section is to construct curves of genus 2 covering two given elliptic curves. In order to get an idea what one has to expect we begin by looking at the situation that we have already a curve C of genus 2 defined over a field K and a K-morphism

$$\varphi_1 : C \longrightarrow E_1$$

of degree n prime to $\mathrm{char}(K)$ where E_1 is an elliptic curve defined over K. We assume that there is no non trivial unramified covering between E_1 and C. Let J be the Jacobian of C and

$$\varphi_1^* : E_1 \longrightarrow J \qquad \text{resp.}$$

$$\varphi_{1,*} : J \longrightarrow E_1$$

be the maps induced by φ_1.

The maximality of $(C \xrightarrow{\varphi_1} E_1)$ implies that φ_1 is injective and that $\ker(\varphi_{1,*})$ is an elliptic curve E_2^* (cf. Serre [16], p. 130).

Obviously we have

$$\varphi_{1*} \cdot \varphi_1^* = n \cdot \mathrm{id}_{E_1}$$

and hence $\varphi_1^*(E_1) =: E_1^*$ intersects E_2^* exactly in $E_1^*[n]$, the n-torsion points of E_1^*.

The projection $\varphi_{2,*}: J \longrightarrow J/E_1^* =: E_2$ induces a covering:

$$\varphi_2: C \longrightarrow E_2$$

of degree n, too, and the map

$$h = \varphi_1^* \times \varphi_2^*: E_1 \times E_2 \longrightarrow J$$

is an isogeny of degree n^2.

Let $H := \ker(h)$. Since $H \cap E_i = \{0_{E_i}\}$ we get a map

$$\alpha: E_1[n] \longrightarrow E_2[n]$$

with graph H which is defined over K. Let e_n be the Weil pairing on $(E_1 \times E_2)[n]$. Then H is isotropic with respect to e_n, i. e.:

$$e_n(\alpha(P), \alpha(Q)) = e_n(P, Q)^{-1}$$

for all P, $Q \in E_1[n]$.
We summarize: To

$$\varphi_1: C \longrightarrow E_1$$

we associated

$$\varphi_2: C \longrightarrow E_2$$

and a K-rational isomorphism

$$\alpha: E_1[n] \longrightarrow E_2[n]$$

whose graph H is isotropic in $(E_1 \times E_2)[n]$ such that $H = \ker(\varphi_1^* \times \varphi_2^*)$.

In fact α is the essential datum of C and this is what we want to describe in the case that n is odd. Although the following construction seems to be known in principle (cf. Serre [17], Ibukiyama, Katsura, Oort [7]) it does not to our knowledge appear explicitly in the literature and we therefore sketch the essential steps of the construction.

So begin with elliptic curves E_1 and E_2 defined over K with zero points 0_1 and 0_2. Let $n > 1$ be an odd number prime to $\mathrm{char}(k)$ and assume that

$$\alpha: E_1[n] \longrightarrow E_2[n]$$

is a K-rational isomorphism with $H_\alpha := \text{graph}(\alpha)$ isotropic in $(E_1 \times E_2)[n]$ (with respect to the e_n-pairing).

The divisor $\Theta := 0_1 \times E_2 + E_1 \times 0_2 \in \text{Div}(E_1 \times E_2)$ defines a principal polarization with corresponding map

$$\theta: E_1 \times E_2 \longrightarrow (E_1 \times E_2)^\wedge \ .$$

Let

$$h: E_1 \times E_2 \longrightarrow E_1 \times E_2/H_\alpha =: J_\alpha$$

be the canonical map.

By $\mathcal{D}_\alpha$ we denote the set of effective divisors D on $E_1 \times E_2 \otimes \bar{K}$ (where $\bar{K}$ = alg. closure of K) satisfying

i) $D \sim n\Theta$, and
ii) $T_x(D) = D$ for all $x \in H_\alpha \otimes \bar{K}$.

$\mathcal{C}_\alpha$ is the set of effective divisors C on $J_\alpha \otimes \bar{K}$ with

i) $h^*(C) \sim n\Theta$, and
ii) $(C \cdot C) = 2$.

Since h is etale we have: A divisor D on $(E_1 \times E_2) \otimes \bar{K}$ is invariant under translations by all $x \in H_\alpha \otimes \bar{K}$ if and only if $D \in h^*(\text{Div}(J_\alpha))$ and so h^* induces a bijection between $\mathcal{C}_\alpha$ and $\mathcal{D}_\alpha$.

The isotropy condition on H_α ensures (use [11], p. 231) that there is a divisor $\bar{D}$ on J_α with $h^*(\bar{D}) \sim n\Theta$ and so $h^0(\bar{D}) > 0$ and hence $\mathcal{C}_\alpha \neq 0$.

Choose $C \in \mathcal{C}_\alpha$ and define

$$\lambda_C =: \lambda: J_\alpha \longrightarrow J_\alpha^\wedge$$

by

$$\lambda(x) := [T_x(C) - C] \quad .$$

Since $n\Theta$ is ample each $C \in \mathcal{C}_\alpha$ is ample and the Riemann-Roch theorem (cf. [11], p. 150) yields:

$$\deg(\lambda) = [1/2(C \cdot C)] = 1 \quad .$$

Hence λ is an isomorphism.
The map

$$h' := \theta^{-1} \circ h^\wedge \circ \lambda$$

has a kernel which acts freely and transitively on $\mathcal{C}_\alpha$ and so λ and h' are defined over K and independent of the choice of C.

Moreover $\#\mathcal{C}_\alpha = \#\ker(h') = \#\ker(h) = n^2$. Using [11], p. 59 and 143 and [9], p. 131 one checks that we have the following commutative diagram

$$\begin{array}{ccc} E_1 \times E_2 & \xrightarrow{\theta} & (E_1 \times E_2)^\wedge \\ \downarrow h & & \downarrow (h')^\wedge \\ J_\alpha & \xrightarrow{\lambda} & J_\alpha^\wedge \\ \downarrow h' & & \downarrow h^\wedge \\ E_1 \times E_2 & \xrightarrow{\theta} & (E_1 \times E_2)^\wedge \end{array}$$

with $h' \circ h = n \cdot \mathrm{id}$ and $h^\wedge \circ h'^\wedge = n \cdot \mathrm{id}$.

For $i = 1, 2$ denote by e_i the natural injection of E_i into $E_1 \times E_2$ and by p_i the projections.
The maps

$$h_i := h \circ e_i \qquad \textit{and}$$
$$h_i' := p_i \circ h'$$

obviously satisfy

$$h_i' \circ h_j = n \cdot \delta_{ij} \circ \mathrm{id}_{E_i}$$

and the sequences

$$0 \longrightarrow E_j \xrightarrow{h_j} J_\alpha \xrightarrow{h_i'} E_i \longrightarrow 0$$

are exact for $i, j \in \{1, 2\}$, $i \neq j$.
Put $\iota = -\mathrm{id}_{J_\alpha}$.

Proposition 1.1: *There exists a unique curve $C \in \mathcal{C}_\alpha$ such that $h^*(C) \sim n\Theta$ and $\iota(C) = C$.*

Proof. For $C' \in \mathcal{C}_\alpha$ we have: $h^*(\iota C') = -\mathrm{id}_{E_1 \times E_2}(h^*(C'))$ $\sim -\mathrm{id}_{E_1 \times E_2}(n\Theta) = n\Theta$, and so ι operates on $\mathcal{C}_\alpha$.

The order of $\mathcal{C}_\alpha$ is odd and so ι has to have a fixed element C in $\mathcal{C}_\alpha$. Let $C' \in \mathcal{C}_\alpha$ be another fixed element, $C' = T_x C$ with $x \in \ker(h')$.

So $C' = T_x C = T_{-x} C$ and so $2x = 0$ or: $x = 0$ since the kernel of h' has odd order. Hence $C = C'$. Q.E.D.

Corollary 1.2: *The curve $C \in \mathcal{C}_\alpha$ with $\iota C = C$ is defined over K and there exists a unique $D \in \mathcal{D}_\alpha$ with $-\mathrm{id}_{E_1 \times E_2}(D) = D$.*

Let $\rho: C \longrightarrow J_\alpha$ resp. $\tilde{\rho}: D \longrightarrow E_1 \times E_2$ be the canonical injections. The restriction of h' to $\rho(C)$ gives a morphism $\bar{\pi}: C \longrightarrow \bar{C} \subset E_1 \times E_2$, and the restriction of h to $\rho(D)$ defines a morphism $\pi: D \longrightarrow C$.

Put $\varphi_i := h_i'|_C$ and $\tilde{\varphi}_i := p_i|_D$. Then we get the commutative diagram

$$\begin{array}{ccccc} E_1 & \xleftarrow{\tilde{\varphi}_1} & D & \xrightarrow{\tilde{\varphi}_2} & E_2 \\ \downarrow{\scriptstyle \mathrm{noid}_{B_1}} & & \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \mathrm{noid}_{B_2}} \\ E_1 & \xleftarrow{\varphi_1} & C & \xrightarrow{\varphi_2} & E_2 \\ & & \downarrow{\scriptstyle \bar{\pi}} & & \\ & & \bar{C} & & \end{array}$$

and so we are in a situation as described in the beginning of the section. We would have finished our task if C would be an irreducible curve of genus 2. In fact this is not true in general:

Proposition 1.3: *The following statements are equivalent:*
(i) D *is irreducible*
(ii) D *is a smooth connected curve of genus* n^2+1
(iii) C *is irreducible*
(iv) C *is a smooth connected curve of genus* 2.

The proposition easily follows if one uses the adjunction formula on abelian surfaces:

$$p_a(D) = 1/2(D \cdot D) + 1$$

resp.

$$p_a(C) = 1/2(C \cdot C) + 1$$

"In general" C will be irreducible. To be more precise we state

Proposition 1.4 *Suppose that* C *is reducible. Then*

$$C = E + E' \qquad \textit{(as divisors)}$$

where E *and* E' *are* K*-rational elliptic curves meeting transversally in a unique* K*-rational point* P_0*, and* E, E', E_1 *and* E_2 *are all isogenous.*

Proof: Since $(C \cdot C) = 2$ the first assertion is a well known result of Weil ([23] Satz 2). Now assume that $(E \cdot h_i(E_i)) = 0$. This implies that $E = T_x(h_i(E_i))$ for some $x \in J(K)$. It follows that $(E \cdot h_j(E_j)) = \#H_\alpha = n^2$.

On the other side we have: $((E+E') \cdot h_j(E_j)) = (n\Theta \cdot e_j(E_j)) = n$, and so we get a contradiction.

Hence $(E \cdot h_i(E_i))$ and similarly $(E' \cdot h_i(E_i))$ are positive numbers, and thus E and E' are not translates of $h_1(E_1)$ and $h_2(E_2)$. Therefore E_1 and E_2 and hence also E and E' have to be all isogenous. Q.E.D.

Remark: It is easy to construct examples where C is reducible. For example, choose elliptic curves E_1, E_2 admitting an isogeny $f: E_1 \longrightarrow E_2$ of degree $n-1$. Then $\alpha = f|_{E_1[n]}$ satisfies the isotropy condition, but its associated curve C is always reducible.

We now assume that E_1 is an elliptic curve defined over K with an "anti-canonical" K-rational level-n-structure $\alpha_1: E_1[n] \longrightarrow \mathbf{Z}/n \times \mathbf{Z}/n$ with $e_n(\alpha_1^{-1}(1,0), \alpha_1^{-1}(0,1)) = \exp(\frac{-2\pi i}{n})$. Let M_n be the modular curve parametrizing elliptic curves with canonical level-n-structures. A consequence of our results is:

Proposition 1.5: *Let $x \in M_n(K)$ correspond to the pair (E_2, α_2), where α_2 is a canonical level-n-structure of the curve E_2. There is a unique projective K-rational curve C_x of (arithmetic) genus 2 covering E_1 and E_2 of degree n such that the induced morphism $\alpha: E_1[n] \longrightarrow E_2[n]$ is given by $\alpha_2^{-1} \circ \alpha_1$. If E_2 is not isogenous to E_1 then C_x is irreducible without singularities.*

One gets even more: Fixing (E_1, α_1) as above the map $(E_2, \alpha_2) \longrightarrow C_{\alpha_2^{-1} \circ \alpha_1}$ induces a morphism of M_n/K to the moduli space of stable curves of genus 2 over K which is birational onto its image.

Remark: In Proposition 1.5 we have fixed E_1 since we shall be interested in this situation later on. Of course, there is a version of 1.5 with E_1, E_2 both variable, too.

2 The configuration of Weierstraß points

1.) The generic situation

We now assume that C is a smooth irreducible curve of genus 2 covering E_1 and E_2 as described in the last section. Let $\varphi_i: C \longrightarrow E_i$ be the covering maps. We continue to assume that $\deg(\varphi_i)$ is prime to $\mathrm{char}(K)$ and odd. Moreover we assume that $\mathrm{char}(K)$ is odd or zero. By $\bar{K}$ we denote as before the algebraic closure of K.

Let w be the hyperelliptic involution on C. The fixed point set $W \subset C(\bar{K})$ of w consists of 6 points, the Weierstraß points of C.

We can choose zero points of E_1 and E_2 such that

$$\varphi_i \circ w = -\mathrm{id}_{E_i} \circ \varphi_i \quad \text{, and so}$$

$$\varphi_i(W) \subset E_i[2]\,.$$

Lemma 2.1 *i)* $\varphi_i(W) = E_i[2]$

ii) There is exactly one point $P_{0,i} \in E_i[2]$ with $\#\varphi_i^{-1}(P_{0,i}) \cap W = 3$[1].

Proof: More generally we claim: For all $P \in E_i[2]$ we have: $\#\varphi_i^{-1}(P) \equiv 1 \bmod 2$.

Since w permutes $\varphi_i^{-1}(P)$ it has a fixed point inside $\varphi_i^{-1}(P)$ and hence the lemma follows by the pigeonhole principle. So look at the claim. If $\varphi_i^{-1}(P)$ contains no ramified point then $\#\varphi_i^{-1}(P) = n \equiv 1 \bmod 2$.

Next assume that there is a $Q \in \varphi_i^{-1}(P)$ with ramification $e_Q = 2$. The Hurwitz genus formula implies that there is exactly one point Q' different from Q on C which is ramified over E_1 of degree 2, too, and so $Q + Q'$ is a canonical divisor of C. Hence $(Q + Q')$ is linearly equivalent to $2 \cdot \tilde{Q}$ for all $\tilde{Q} \in W$ and so Q and Q' are not in W.

Thus $w(Q) = Q'$ and so $Q' \in \varphi_i^{-1}(P)$. But then all points in $\varphi_i^{-1}(P) \setminus \{Q, Q'\}$ are unramified, and hence $\varphi_i^{-1}(P)$ contains $(n-4)+2 = n-2$ points.

The last case is that there is a point $Q \in \varphi_i^{-1}(P)$ with ramification index $e_Q = 3$. Then all other points of $\varphi_i^{-1}(P)$ are unramified, and so $\#\varphi_i^{-1}(P) = (n-3)+1 = n-2 \equiv 1 \bmod 2$. Q.E.D.

Now define $W_i := \varphi_i^{-1}(P_{0,i})$.

Proposition 2.2 *We have: $W = W_1 \dot{\cup} W_2$ and $\varphi_j(W_i) = E_j[2] \setminus \{P_{0,j}\}$ for $i \neq j$. In particular, the zero point of J does not lie on C.*

Because of the uniqueness of $P_{0,i}$ it follows that this point is rational over any field over which C and φ_1, φ_2 are rational. In the following we choose $P_{0,i}$ as zero point of E_i.

Proof: Suppose first that $E_1[2](K) = \{P_{0,1}\}$. Suppose that there is a point $Q \in \varphi_i^{-1}(P_{0,1}) \cap \varphi_i^{-1}(P_{0,2}) \cap W$. Then $h'(Q) = (P_{0,1}, P_{0,2})$ and so $Q \in \ker(h')$ and $\operatorname{ord}(Q) | \gcd(n, 2) = 1$. So $Q = \{0_J\}$ and hence $\#\{\varphi_1^{-1}(P_{0,1}) \cap \varphi_2^{-1}(P_{0,2}) \cap W\} = 1$. So $\#(W_1 \cup W_2) = 5$ and there is a point $P \in W$ with $\{P\} = W \setminus (W_1 \cup W_2)$. P has to be Galois invariant, hence $\varphi_1(P) \in E_1[2](K) = \{P_{0,1}\}$ and $P \in W_1$ which is a contradiction. This proves the first assertion of the proposition, and from lemma 2.1 the second part follows immediately.

Now we get rid of the condition that $E_1[2](K) = \{P_{0,1}\}$. We can assume that K is algebraically closed. We find an extension $F|K$ and an elliptic curve $\tilde{E}_1$ defined over F which specializes to E_1 such that $\tilde{E}_1[2](F) = \{\tilde{P}_{0,1}\}$. Clearly we can choose $\tilde{\alpha}: \tilde{E}_1[n] \longrightarrow E_2[n]$ which lifts the isomorphism $\alpha: E_1[n] \longrightarrow E_2[n]$ determined by C (cf. Proposition 1.5) and which is rational over a field F_1 with $\tilde{E}_1[2](F_1) = \{\tilde{P}_{0,1}\}$. Since the assertion of the proposition is true for the covering $\tilde{C}$ of $\tilde{E}_1$ and E_2 corresponding to $\tilde{\alpha}$ it follows also for C. Q.E.D.

---

[1] *To ease notation we interpret $\varphi_i^{-1}(P)$ as a subset of $C(\bar{K})$.*

Let's have a brief look at the "degenerated situation" in which the data (E_1, E_2, α) lead to a reducible curve $C = E \cup E'$. Since $wC = C$ it permutes E and E' and so it fixes $\{P_0\} = E \cap E'$. So $P_0 \in J[2](K)$. Now assume that $E_i[2](K) = \{P_{0,i}\}$. Then $J[2](K)$ consists only of the zero point and so P_0 is the zero point. Hence E and E' are abelian subvarieties of J and the set of fixed points of $w|_C$ has seven elements and is the union of the points of order 2 of E and E'.

Hence we get a nice "irreducibility criterion":

Corollary 2.3: *Let E_1, E_2 be elliptic curves over K without K-rational points of order 2 and $\alpha: E_1[n] \longrightarrow E_2[n]$ an isomorphism with isotropic graph H in $(E_1 \times E_2)[n]$, and let C be the corresponding covering curve embedded into $J = (E_1 \times E_2)/H$ according to 1.2. Then C is irreducible if and only if $0_J \notin C(K)$.*

2.) The local situation

We continue to assume that $C|K$ is an irreducible projective curve of genus 2 covering the elliptic curves E_1 and E_2 with covering maps φ_1 and φ_2 of odd degree n. For simplicity we assume that all points of order 2 of E_1 and E_2 (and hence of J) are K-rational. Let $\mathfrak{p}$ be a non-archimedean place of K with ring of integers $O_\mathfrak{p}$, residue field $k_\mathfrak{p}$ and normed valuation $v_\mathfrak{p}$. We assume that E_1 and E_2 (and hence J and C) have semi-stable reduction at $\mathfrak{p}$.

By $\mathcal{C}$, $\mathcal{E}_1$, $\mathcal{E}_2$ and $\mathcal{J}$ we denote the regular minimal (resp. Néron) models of C, E_1, E_2 and J at $\mathfrak{p}$. By $\mathcal{C}^*$ we denote the closure of C in $\mathcal{J}$. The maps $\varphi_{i,*}$ resp. φ_i^* extend to $\mathcal{J}$ resp. $\mathcal{E}_i$ in a unique way, and the same is true for the hyerelliptic involution w. These extensions are denoted by the same letters. Let $\mathcal{W}$ resp. $\mathcal{W}^*$ be the closure of W in $\mathcal{C}$ resp. $\mathcal{J}$. The index $\mathfrak{p}$ at objects mentioned above always means that we look at the special fibre of this object over $k_\mathfrak{p}$. By $\delta_\mathfrak{p}$ we denote the number of singular points on $\mathcal{C}_\mathfrak{p}$. We want to describe $\mathcal{C}_\mathfrak{p}$ and the configuration of $\mathcal{W}_\mathfrak{p}$ inside of $\mathcal{C}_\mathfrak{p}$.

For our purposes it is enough to do this in the case that E_1 has good reduction at $\mathfrak{p}$. Hence we distinguish two cases: 1.) E_2 has good reduction modulo $\mathfrak{p}$, and 2.) E_2 has multiplicative reduction at $\mathfrak{p}$. The results we need can be found in an article of Parshin (cf. [13], p. 80ff) based on work of Ogg [12]. Since the argumentation of Parshin is very short we sketch how to obtain them in the two most interesting cases.

α) The case of good reduction

In this case the special fibre $\mathcal{J}_\mathfrak{p}$ of $\mathcal{J}$ is an Abelian variety. If $\mathcal{C}_\mathfrak{p}$ is irreducible then $\mathcal{C}_\mathfrak{p}$ is a non-singular curve of genus 2 and $\delta_\mathfrak{p} = 0$. Now assume that $\delta_\mathfrak{p} > 0$ and so $\mathcal{C}_\mathfrak{p}^*$ is the union of two elliptic curves intersecting

in the zero point of $\mathcal{J}_\mathfrak{p}$ (cf. the discussion in the last section). It follows that the reductions of points in $\mathcal{W}^*$ lie in the non-singular part of $\mathcal{C}_\mathfrak{p}^*$. From this fact we can conclude that each point $\mathcal{P}_\mathfrak{p}$ of $\mathcal{W}_\mathfrak{p}$ lies on a component of $\mathcal{C}_\mathfrak{p}$ on which w acts non-trivially: Let Q_0 be a regular point on $\mathcal{C}^*$. We take a desingularization

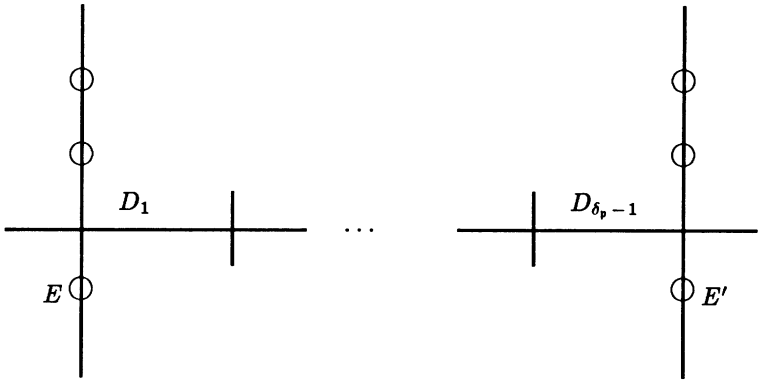
$$\tau: \tilde{\mathcal{C}} \longrightarrow \mathcal{C}^*$$

which is an isomorphism in a neighbourhood of Q_0 of $\mathcal{C}^*$. We can assume that w acts on this neighbourhood. By the universal property of $\mathcal{C}$ we find a map

$$\Pi: \tilde{\mathcal{C}} \longrightarrow \mathcal{C}$$

which continues the identity map on the generic fibre of $\mathcal{C}$ resp. $\mathcal{C}^*$ and which is an isomorphism near the preimage $\tilde{Q}_0$ of Q_0. Since w has only finitely many fixed points on $\mathcal{C}_\mathfrak{p}^*$ we see that the image under Π of $\tilde{Q}_0$ lies in a component on which the action of w is non-trivial.[1)]

Now look closer at $\mathcal{C}_\mathfrak{p}$: By [12] or [13] one knows that $\mathcal{C}_\mathfrak{p}$ has the following shape:



where E and E' are elliptic curves isogenous to $E_{1,\mathfrak{p}}$ and D_i is a projective line with self intersection -2 (on $\mathcal{C}$) for $i = 1$ to $\delta_\mathfrak{p} - 1$. w maps D_i into itself and fixes the singular points. If $P_\mathfrak{p} \in \mathcal{W}_\mathfrak{p}$ would lie on some D_i w

[1)] In the simple situation we are looking at our argument is unnecessarily involved. But since we'll have to use it in the next case we have preferrred to give it here already.

would have to act trivially on D_i and we would get a contradiction. Hence (as is to be expected) $\mathcal{W}_\mathfrak{p} \subset (E \cup E')$, as indicated by small circles in the picture.

Remarks: 1.) Of course for $v_\mathfrak{p}(n) = 0$ this result would follow immediately from the discussion of the degenerated situation above (corollary 2.3). 2.) For the arithmetical applications we'll discuss in §4 the degeneration described above causes the major trouble since neither the number $\delta_\mathfrak{p}$ nor the partition of $\mathcal{W}_{1,\mathfrak{p}}$ and $\mathcal{W}_{2,\mathfrak{p}}$ on E and E' can be controlled by help of $\mathcal{J}$.

β) The case of mixed reduction

We now assume that E_1 has good reduction and that E_2 has multiplicative reduction at $\mathfrak{p}$. We shall assume that the points of order n of E_1 (and hence of E_2, too) are K-rational. Let $\mathcal{J}_\mathfrak{p}^0$ be the connected component of the unity of $\mathcal{J}_\mathfrak{p}$. Let Z be the group of connected components of $\mathcal{J}_\mathfrak{p}$:

$$Z = \mathcal{J}_\mathfrak{p}/\mathcal{J}_\mathfrak{p}^0 .$$

We get

Lemma 2.4: *Z is a cyclic group of order dividing $v_\mathfrak{p}(j_2)$ where j_2 is the absolute invariant of E_2. If $\mathfrak{p} \nmid n$ then $|Z| = \frac{-1}{n} v_\mathfrak{p}(j_2)$.*

Proof: The kernel of $\varphi_{1,*} \times \varphi_{2,*}$ is equal to $E_1[n]$ and so its reduction lies in $\mathcal{J}_\mathfrak{p}^0$. Hence $\varphi_{1,*} \times \varphi_{2,*}$ induces an injective map of Z into the group of components of $\mathcal{E}_{1,\mathfrak{p}} \times \mathcal{E}_{2,\mathfrak{p}}^0$ which is isomorphic to $\mathcal{E}_{2,\mathfrak{p}}/\mathcal{E}_{2,\mathfrak{p}}^0 \cong \mathbf{Z}/v_\mathfrak{p}(j_2)$.

Now assume that $v_\mathfrak{p}(n) = 0$. Let p be a prime and $p^s || n$. Let $\mathcal{J}_\mathfrak{p}^1$ be a component of $\mathcal{J}_\mathfrak{p}$ generating the p-primary part of Z.

Let Q_0 be a point of $J(K)$ with reduction in $\mathcal{J}_\mathfrak{p}^1$. If $p^k || |Z|$ we have: The reduction of $p^k Q_0$ lies in $\mathcal{J}_\mathfrak{p}^0$. We find a point $\tilde{Q}$ rational over a $\mathfrak{p}$-unramified extension K' of K with $p^k \tilde{Q} = p^k Q_0$ and $\tilde{Q}$ reducing to $\mathcal{J}_\mathfrak{p}^0$ mod $\mathfrak{p}$. Hence by replacing K by K' and Q_0 by $Q_0 - \tilde{Q} =: Q$ we can assume that Q has order p^k.

Take $Q' = (Q_1, Q_2) \in (E_1 \times E_2)(\bar{K})$ with $(\varphi_1^* \times \varphi_2^*)(Q') = Q$.

Claim: Q' is rational over a field extension K'' which is unramified at $\mathfrak{p}$.

For: Let $\mathfrak{P}$ be an extension of $\mathfrak{p}$ to $\bar{K}$ and $\tau \in G_\mathfrak{P}$, the inertia group of $\mathfrak{P}$. Q' is a point of finite order and this order is prime to $\mathfrak{p}$ and so $\tau Q_1 = Q_1$. So $\tau Q' - Q' = (0, \tau Q_2 - Q_2) \in H$, and so $\tau Q_2 = Q_2$.

It follows that $v_\mathfrak{p}(j_2) \cdot Q' \in (\mathcal{E}_{1,\mathfrak{p}} \times \mathcal{E}_{2,\mathfrak{p}})^0$. Let p^m be the maximal p-power dividing $v_\mathfrak{p}(j_2)$. Then $p^{m-s} Q'$ has a second component $p^{m-s} Q_2$ which differs from a second component of a point in H only by a point of

order prime to p, and so $(\varphi_1^* \times \varphi_2^*)p^{m-s}Q' = p^{m-s}$. Q is a point which differs from a point with reduction in $\mathcal{J}_\mathfrak{p}^0$ only by a point of order prime to p and hence $p^{m-s}Q$ lies in $\mathcal{J}_\mathfrak{p}^0$ mod $\mathfrak{p}$. Hence $k \leq m - s$.

The converse estimate is clear since the group of connected components of $(\mathcal{E}_1 \times \mathcal{E}_2)_\mathfrak{p}$ is cyclic of order $-v_\mathfrak{p}(j_2)$ and H mod $(\mathcal{E}_1 \times \mathcal{E}_2)_\mathfrak{p}^0$ is cyclic of order n.

A consequence of lemma 2.3 is that we have a fairly natural way to compactify $\mathcal{J}$: First recall that $\mathcal{E}_2$ is constructed as open part (i.e. the regular part) of the projective minimal model $\tilde{\mathcal{E}}_2$ of E_2 at $\mathfrak{p}$. Next, the extension $\mathcal{H}$ of H to $\mathcal{E}_1 \times \mathcal{E}_2$ is a finite group scheme whose actions extends to $\tilde{\mathcal{P}} := \mathcal{E}_1 \times \tilde{\mathcal{E}}_2$ (on the second component it maps the Néron polygon into itself).

Then $\mathcal{P} := \tilde{\mathcal{P}}/\mathcal{H}$ is a proper $0_\mathfrak{p}$-scheme containing $\mathcal{J} \times 0_\mathfrak{p}$ for we claim:

Corollary 2.5: $(\varphi_1^* \times \varphi_2^*)(\mathcal{E}_1 \times \mathcal{E}_2) = \mathcal{J}$.

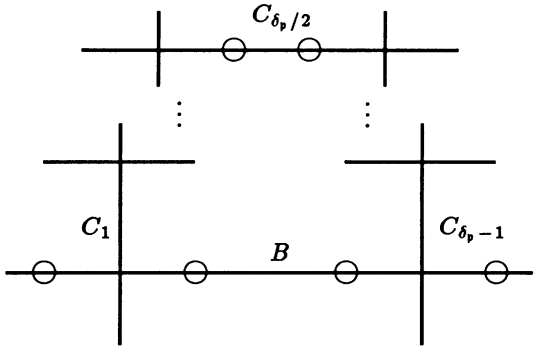
Proof: We have to show the surjectivity of the map in the special fibre. It is clear that $(\mathcal{E}_1 \times \mathcal{E}_2)_\mathfrak{p}^0$ is mapped surjectively to $\mathcal{J}_\mathfrak{p}^0$. Lemma 2.4 implies that $\varphi_1^* \times \varphi_2^*$ induces a surjection of the group of connected components, and hence the corollary follows.

The special fibre of $\mathcal{C}$

Since the abelian part of $\mathcal{J}_\mathfrak{p}$ has dimension 1 the components of $\mathcal{C}_\mathfrak{p}$ have genus ≤ 1, and there is exactly one component, which we call B, of genus 1. The other components are projective lines. Because of the semi-stability all singular points on $\mathcal{C}_\mathfrak{p}$ are ordinary double points.

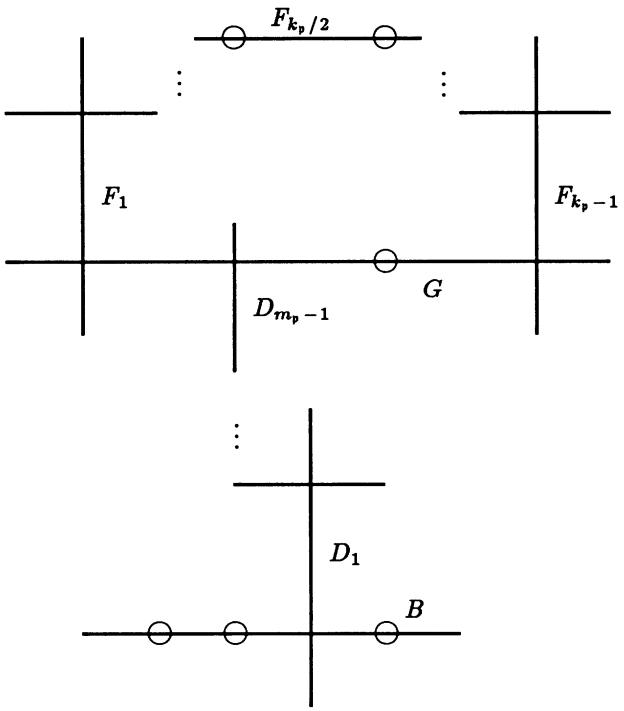
In order to analyse $\mathcal{C}_\mathfrak{p}$, let us, for simplicity, work over $\bar{k}_\mathfrak{p}$ = alg. closure of $k_\mathfrak{p}$. We'll distinguish two cases.

β_1) First assume that divisors of the form $(\mathcal{P}_\mathfrak{p} - \mathcal{Q}_\mathfrak{p})$ with $\mathcal{P}_\mathfrak{p}, \mathcal{Q}_\mathfrak{p} \in B_{\mathrm{reg}}(\bar{k}_\mathfrak{p})$ generate $\mathrm{Pic}^0(\mathcal{C}_\mathfrak{p}) = \mathcal{J}_\mathfrak{p}^0$. Then $\mathcal{C}_\mathfrak{p}$ is equal to $B \cup C_1 \cup \ldots \cup C_{\delta_\mathfrak{p}-1}$ with C_i projective lines of self intersection -2, and we have the following configuration:



The number of rational components of $\mathcal{C}_\mathfrak{p}$ is linked to the number of connected components of $\mathcal{J}_\mathfrak{p}$ by results of Grothendieck [6](cf. also [15], p. 4ff). In our simple situation one gets by a short computation: $\delta_\mathfrak{p} = \#(\mathcal{J}_\mathfrak{p}/\mathcal{J}_\mathfrak{p}^0)$. Hence $\delta_\mathfrak{p} | v_\mathfrak{p}(j_2)$ and for $\mathfrak{p} \nmid n$ we have: $\delta_\mathfrak{p} = -\frac{1}{n} v_\mathfrak{p}(j_2)$. The special fibres of Weierstraß points of $\mathcal{C}$ are located as indicated by the circles (cf. [13]) but since we don't need this we don't go into details of the proof.

β_2) Now assume that $\{(\mathcal{P}_\mathfrak{p} - \mathcal{Q}_\mathfrak{p}) : \mathcal{P}_\mathfrak{p}, \mathcal{Q}_\mathfrak{p} \in B_{\mathrm{reg}}(\bar{k}_\mathfrak{p})\}$ does not generate $\mathcal{J}_\mathfrak{p}^0$. Then $\mathcal{C}_\mathfrak{p}$ looks like this (circles denote special fibres of Weierstraß points again):



Obviously $\delta_\mathfrak{p} = m_\mathfrak{p} + k_\mathfrak{p}$ and again by Grothendieck's results [6] one

computes:

$$k_\mathfrak{p} = \#(\mathcal{J}_\mathfrak{p}/\mathcal{J}_\mathfrak{p}^0)\,.$$

Since for the arithmetical applications we have in mind it is essential where elements of $\mathcal{W}_\mathfrak{p}$ lie we'll give a sketch of the proof that the picture is correct. Let $\mathcal{C}^*$ be the closure of C in $\mathcal{J}$. We restrict the maps h_i' to $\mathcal{C}^*$. Each component of $\mathcal{C}_\mathfrak{p}^*$ is mapped surjectively either under h_1' or h_2' onto a component of $\mathcal{E}_{1,\mathfrak{p}}$ resp. $\mathcal{E}_{2,\mathfrak{p}}$ and is reduced. Hence it contains regular points and the discussion made in section α) above implies that these regular points correspond to points on $\mathcal{C}_\mathfrak{p}$ on which w acts non-trivial. In particular, it follows that there is one component B^* of genus 1 of $\mathcal{C}_\mathfrak{p}^*$ and on this component there is at most one singular point, namely the intersection of at most one rational component of $\mathcal{C}_\mathfrak{p}^*$ with B^*.

Rational components D^* of $\mathcal{C}_\mathfrak{p}^*$ are of the form $D^* = h(P \times D)$ with $P \in \mathcal{E}_{1,\mathfrak{p}}$ and D a component of $\mathcal{E}_{2,\mathfrak{p}}$. Looking at the action of the finite group scheme $\mathcal{H}$ (which is the extension of H to $\mathcal{E}_1 \times \mathcal{E}_2$) one sees that the points of order two of $\mathcal{J}_\mathfrak{p}$ which lie on $\mathcal{C}_\mathfrak{p}^* \setminus B^*$ are regular, and so it follows again by using the argument above that the special fibres of Weierstraß points lying in W_1 are situated on $F_{k_\mathfrak{p}/2}$ resp. G as indicated, and so the special fibres of points in W_2 are on $B \cup D_1 \cup \ldots \cup D_{m_\mathfrak{p}-1}$. Moreover, the intersection of rational components of $\mathcal{C}_\mathfrak{p}^*$ with B^* is mapped under h_1 to the zero point of $\mathcal{E}_{1,\mathfrak{p}}$, and since $2 \not| \mathfrak{p}$ this point is not the special fibre of the closure of a point in W_2 on $\mathcal{C}^*$ and hence W_2 is reduced into B (again use the action of w as above), and this concludes the discussion.

3 A digression about heights of curves

We now assume that K is a global field, i.e. either a finite extension of $\mathbb{Q}$ or a function field of one variable over a field of constants K_0 which we assume to be perfect and of characteristic not equal to 2.

$$m_k := \begin{cases} [K:\mathbb{Q}] & \text{if } K \supset \mathbb{Q} \\ 1 & \text{else.} \end{cases}$$

By Σ_K we denote the set of non-archimedean places of K, $S_{K,\infty}$ is the set of archimedean places. Take $\mathfrak{p} \in \Sigma_K$ and denote as above by $0_\mathfrak{p}$ its ring of integers and by $k_\mathfrak{p}$ its residue field. Define

$$\deg(\mathfrak{p}) := \begin{cases} [k_\mathfrak{p} : K_0] & \text{if } K \text{ is a function field,} \\ \log(\#k_\mathfrak{p}) & \text{if } K \supset \mathbb{Q}. \end{cases}$$

$v_\mathfrak{p} \in \mathfrak{p}$ is the normed valuation in $\mathfrak{p}$ and for the divisor $D = \prod_{\mathfrak{p} \in \Sigma_K} \mathfrak{p}^{z_\mathfrak{p}}$ define

$$\deg(D) = \sum_{\mathfrak{p} \in \Sigma_K} z_{\mathfrak{p}} \deg(\mathfrak{p}) .$$

For $\mathfrak{p} \in S_{K,\infty}$ we choose an embedding σ of K into $\mathbb{C}$ and define for $x \in K$:

$$|x|_{\mathfrak{p}} = |\sigma x| ,$$
$$v_{\mathfrak{p}}(x) = -\log(|\sigma x|) \text{ and}$$
$$\deg(\mathfrak{p}) = \begin{cases} 1 & \text{if } \sigma K \subset \mathbb{R}, \\ 2 & \text{if } \sigma K \not\subset \mathbb{R}. \end{cases}$$

By B we denote the arithmetical curve corresponding to K: In the function field case it is the regular irreducible projective curve over K_0 with function field K, in the number field case it corresponds to $\mathrm{Spec}(0_K) \cup S_{K,\infty}$ where 0_K is the ring of integers of K.
The genus of K is defined by

$$g(K) := \begin{cases} \text{genus of } B & \text{if } K \text{ is a function field} \\ \frac{1}{2} \log |\Delta_{K/\mathbb{Q}}| & \text{if } K \text{ is a number field with discriminant } \Delta_{K/\mathbb{Q}}. \end{cases}$$

Let x be an element of K^*. The height of x is defined by

$$h_K(x) := \sum_{\mathfrak{p} \in \Sigma_K \cup S_{K,\infty}} \max\{0, v_{\mathfrak{p}}(x) \deg \mathfrak{p}\} .$$

Clearly for $K' \supset K$ and $x \in K$ we get:

$$h_{K'}(x) = [K' : K] h_K(x) .$$

Now take a projective irreducible smooth curve C of genus $g \geq 1$ defined over K. By $J(C)$ we denote its Jacobian.

Let $\mathcal{C}$ be the regular minimal (arithmetical) surface over B with generic fibre C and morphism

$$f: \mathcal{C} \longrightarrow B .$$

Let $\mathcal{J}(C)$ denote the Néron model of $J(C)$ over K.

For $\mathfrak{p} \in S_{K,\infty}$ and corresponding embedding $\sigma: K \longrightarrow \mathbb{C}$ let $C_{\mathfrak{p}}$ resp. $\mathcal{J}(C)_{\mathfrak{p}}$ be equal to $\sigma C \otimes \mathbb{C}$ resp. $\sigma(J(C)) \otimes \mathbb{C}$ together with the Arakelov metric μ_σ on $C_{\mathfrak{p}}$ which is induced by the flat metric on $\mathcal{J}(C)_{\mathfrak{p}}$.

We always assume that $\mathcal{C}_{\mathfrak{p}}$ is semi-stable for all $\mathfrak{p} \in \Sigma_K$. Divisors on $\mathcal{C}$ are Arakelov divisors and intersections of such divisors are taken in the sense of Arakelov ([1]). We are especially interested in the divisor

$$\omega := \omega_{\mathcal{C}/B},$$

the relative dualizing sheaf of $\mathcal{C}/B$.

The Faltings height of C is defined by

$$h_K(C) := \deg f_*\omega$$

(cf. Lang [10]).

Example (cf. [3], p. 29). If C is an elliptic curve E with absolute invariant $j_E \neq 0$ then

$$h_K(E) \sim \frac{1}{12} h_K(j_E).$$

Noether's formula. For $\mathfrak{p} \in \Sigma_K$ let $\delta_\mathfrak{p}$ denote the number of singular points in $\mathcal{C}_\mathfrak{p}$. For $\mathfrak{p} \in S_{K,\infty}$ Faltings (cf. [4]) has defined invariants $\delta_\mathfrak{p}$ of $\mathcal{C}_\mathfrak{p}$ such that

$$\omega^2 + \sum_{\mathfrak{p} \in \Sigma_K \cup S_{K,\infty}} \delta_\mathfrak{p} = 12 h_K(C).$$

We want to state some conjectures related with the height of curves. In the center of our interest are elliptic curves.

So assume that E/K is a semi-stable elliptic curve with absolute invariant j_E and conductor

$$\mathcal{N}_E = \sum_{\substack{v_\mathfrak{p}(j_E) < 0 \\ \mathfrak{p} \in \Sigma_K}} \mathfrak{p}.$$

Conjecture (H_E): *There are constants $c_1(K)$ and $d_1(K)$ such that for all semi-stable elliptic curves E/K one has:*

$$h_K(E) \leq c_1(K) \deg \mathcal{N}_E + d_1(K).$$

It is clear that (H_E) is a stronger version of

Szpiro's conjecture(SZ): *Let Δ_E be the minimal discriminant divisor of E. Then*

$$\deg(\Delta_E) \leq c_2(K) \deg \mathcal{N}_E + d_2(K)$$

with $c_2(K)$, $d_2(K)$ depending only on K.

Obviously (H_E) is equivalent to (SZ) if we restrict ourselves to elliptic curves whose absolute invariants are bounded for all $\mathfrak{p} \in S_{K,\infty}$. Consequences of (H_E) or (SZ) can be found in [5].

The height conjecture (H_E) for elliptic curves can be generalized in two obvious ways: First we state the height conjecture for abelian varieties:

(H_A): *Fix $n \in \mathbb{N}$. There exist constants $c_n(K)$ and $d_n(K)$ such that for all semi-stable abelian varieties A of dimension n defined over K one has:*

$$h_K(A) \leq c_n(K) \deg \mathcal{N}_A + d_n(K)$$

where $h_K(A)$ is the Faltings height of A over K and $\mathcal{N}_A = \prod_{\substack{\mathfrak{p} \in \Sigma_K \\ A \text{ has bad reduction} \\ \text{modulo } \mathfrak{p}}} \mathfrak{p}$.

Secondly:

Conjecture (H_C). *Fix $n \in \mathbb{N}$. There exist constants $c'_n(K)$ and $d'_n(K)$ such that for all arithmetical semi-stable surfaces C/B whose generic fibres have genus n one has*

$$h_K(C) \leq c'_n(K) \deg \mathcal{N}_C + d'_n(k) \quad \text{with}$$
$$\mathcal{N}_C = \prod_{\substack{\mathfrak{p} \in \Sigma_K \\ \delta_\mathfrak{p} > 0}} \mathfrak{p}$$

For applications one would like to have even stronger versions:

$c_n(K)$ and $c'_n(K)$ depend on n only, and $d_n(K)$ resp. $d'_n(K)$ depend on n, linearly on $g(K)$ and polynomially on m_K.

These conjectures are known to be true in the function field case: If K is a function field over K_0 then Szpiro ([18], p. 55) has shown that for $n \geq 2$ and curves with non-trivial Kodaira-Spencer class one can take $c'_n(K) = \frac{1}{3}n(n-1)$ and $d'_n(K) = \frac{2}{3}n(n-1)(g(K)-1)$. For $n = 1$ (cf. [5]) one can take $c_1(K) = 1/2(g(K)-1)$. The height conjecture for abelian varieties over K has been proven by Griffiths. For $K_0 = \mathbb{C}$ one can take $c_n(K) = 4\pi \cdot n$ and $d_n(K) = 8\pi \cdot n(g(K)-1)$ (cf. [19], p. 87).

There is an important case in which (H_A) and (H_C) can be compared: Assume that A is the Jacobian $J(C)$ of a curve C/K. Then $h_K(A) = h_K(C)$ and $\mathcal{N}_A$ divides $\mathcal{N}_C$.

Hence the height conjecture (H_A) is stronger than the height conjecture for curves.

Now we can use Noether's formula to get weaker version of (H_C) resp. (H_A) for Jacobians.

Conjecture (S_J): *There exist constants $c(n)$ and $d(g(K),n)$ such that for each arithmetical semi-stable surface $\mathcal{C}/B$ whose generic fibre has genus n one has:*

$$\omega^2 \leq c(n) \deg \mathcal{N}_{J(C)} + d(g(K),n)$$

with $c(n)$ and $d(g(K),n)$ depending polynomially on n, $d(g(K),n)$ depending linearly on $g(K)$ and polynomially on m_K.

To get the version (S_C) corresponding to conjecture (H_C) one has to replace $\mathcal{N}_{J(C)}$ by $\mathcal{N}_C$.

In the function field case (S_C) follows from the Bogomolov-Miyaoka-Yau inequality for Chern classes (cf. [14]). In the same paper Parshin shows that (S_C) implies the height conjecture for elliptic curves. We thus have the following implications:

$$\begin{array}{ccccccc} (H_A) & \Rightarrow & (H_C) & \Rightarrow & (H_E) & \Rightarrow & (SZ) \\ \Downarrow & & \Downarrow & \nearrow & \text{Parshin} & & \\ (S_J) & \Rightarrow & (S_C) & & & & \end{array}$$

The purpose of the next section of this paper is to show that the conjecture (S_J) for curves of genus 2 implies the height conjecture at least for families of elliptic curves E with bounded absolute values of the invariants j_E. We hope that the condition about the boundedness of j_E is not necessary.

4 Application to elliptic curves

Again we assume that K is a global field with $\mathrm{char}(K) \nmid 2n$, and that E_1 and E_2 are non-isogenous semi-stable elliptic curves over K with all points of order $2n$ in $E_i(K)$. Let H be isotropic in $(E_1 \times E_2)[n]$ and C the corresponding covering curve which is assumed to be semi-stable over K with regular minimal model $\mathcal{C}$. For $P \in C(K)$ let $\mathcal{P}$ be the closure of P in $\mathcal{C}$ and $X_P := (\omega_{\mathcal{C}/B} - 2\mathcal{P}) \in \mathcal{J}$.

There is a close relation between the Néron-Tate height on J and the intersection form on $\mathcal{C}$ (cf. e.g. [20] or [8]). To state this relation it is useful to introduce a divisor $\Phi(\mathcal{P})$ whose support lies in the fibres of bad reduction of $\mathcal{C}$ with the following properties: For all $\mathfrak{p} \in \Sigma_K$ we have:

i) $\mathcal{P}_\mathfrak{p} \notin \Phi(\mathcal{P})$, and

ii) for all divisors D with $\mathrm{support}(D) \subset \mathcal{C}_\mathfrak{p}$ one has: $\Phi(\mathcal{P})_\mathfrak{p} \cdot D = 0$.

$\Phi(\mathcal{P})$ exists and is uniquely determined (cf. [20] again). In our situation we'll be able to determine $\mathcal{P}$ explicitely. But before doing so we state the mentioned relation in the special case that P, $P' \in C(K)$ are two different points whose image in $J(K)$ has finite order:

$$1/2\omega_{\mathcal{C}/B}^2 = \sum_{p \in \Sigma_K} \Delta(\mathcal{P}, \mathcal{P}')_\mathfrak{p} - 4(\mathcal{P} \cdot \mathcal{P}').$$

where

$$\Delta(\mathcal{P}, \mathcal{P}')_\mathfrak{p} := -\frac{1}{4}\left(\Phi(\mathcal{P})_\mathfrak{p}^2 + \Phi(\mathcal{P}')_\mathfrak{p}^2\right) + \Phi(\mathcal{P})_\mathfrak{p} \cdot \Phi(\mathcal{P}')_\mathfrak{p}.$$

Now we determine $\Phi(\mathcal{P})_\mathfrak{p}$ and $\Delta(\mathcal{P}, \mathcal{P}')_\mathfrak{p}$ for P, $P' \in W$ and $\mathfrak{p} \nmid 2$. We use the notation from §2.

In the case of good reduction we get: $\Delta(\mathcal{P}, \mathcal{P}')_\mathfrak{p} = 0$.

Now assume that $\mathfrak{p} | \mathcal{N}_C$.

Case α: $\mathcal{C}_\mathfrak{p}$ has two elliptic components E and E' connected by rational components $D_1, \ldots, D_{\delta_\mathfrak{p}-1}$. The intersection numbers are: $E^2 = E'^2 = -1$ and $D_i^2 = -2$, $(\omega_{\mathcal{C}/B} \cdot E) = (\omega_{\mathcal{C}/B} \cdot E') = 1$ and $(\omega_{\mathcal{C}/B} \cdot D_i) = 0$.

Hence one easily checks:

$$\Phi(\mathcal{P}_\mathfrak{p} = \begin{cases} D_1 + 2D_2 + \ldots + (\delta_\mathfrak{p} - 1)D_{\delta_\mathfrak{p}-1} + \delta_\mathfrak{p} E' & \text{if } \mathcal{P}_\mathfrak{p} \in E, \\ D_{\delta_\mathfrak{p}-1} + 2D_{\delta_\mathfrak{p}-2} + \ldots + (\delta_\mathfrak{p} - 1)D_1 + \delta_\mathfrak{p} E & \text{if } \mathcal{P}_\mathfrak{p} \in E'. \end{cases}$$

and $\Phi(\mathcal{P})_\mathfrak{p}^2 = -\delta_\mathfrak{p}$.

If $P' \in W$ is a different point then

$$\Phi(\mathcal{P})_\mathfrak{p} \cdot \Phi(\mathcal{P}')_\mathfrak{p} = \begin{cases} -\delta_\mathfrak{p} & \text{if } P_\mathfrak{p} \text{ and } P'_\mathfrak{p} \text{ are on the same elliptic component} \\ \delta_\mathfrak{p} & \text{else.} \end{cases}$$

So:

$$\Delta(\mathcal{P}, \mathcal{P}')_\mathfrak{p} = \begin{cases} -1/2\,\delta_\mathfrak{p} & \text{if } \mathcal{P}_\mathfrak{p} \text{ and } \mathcal{P}'_\mathfrak{p} \text{ are on the same elliptic component} \\ \frac{3}{2}\delta_\mathfrak{p} & \text{else.} \end{cases}$$

We come to the case of mixed reduction:

Case β_1: $\mathcal{C}_\mathfrak{p}$ consists of $\frac{1}{n}v_\mathfrak{p}(j_2)$ components, if $\mathfrak{p} \nmid n$, and of at most $v_\mathfrak{p}(j_2)$ components if $\mathfrak{p} | n$. Hence there exists an absolute constant c (independent of n) such that

$$|\Delta(\mathcal{P}, \mathcal{P}')_\mathfrak{p}| \leq \begin{cases} c \cdot \frac{1}{n}|v_\mathfrak{p}(j_2)| & \text{if } \mathfrak{p} \nmid n \\ c \cdot |v_\mathfrak{p}(j_2)| & \text{if } \mathfrak{p} | n \end{cases}$$

Case β_2: Again we use the notation introduced in §2. In addition we number the points in W as follows: P_0, P_1 and P_2 are the points in W_2 and P_3, P_4 and P_5 are the points in W_1. We assume that $P_{3,\mathfrak{p}} \in G$.

Since $D_i^2 = F_j^2 = -2$, $G^2 = -3$, $\omega_{\mathcal{C}/B} \cdot B = \omega_{\mathcal{C}/B} \cdot G = 1$, $\omega_{\mathcal{C}/B} \cdot D_i = \omega_{\mathcal{C}/B} \cdot F_j = 0$, one easily checks: $\Phi(\mathcal{P}_i)_\mathfrak{p} = D_1 + \ldots + (m_\mathfrak{p} - 1)D_{m_\mathfrak{p}-1} + m_\mathfrak{p}(G + F_1 + \ldots + F_{k_\mathfrak{p}-1})$ for $i = 0, 1, 2$.
$\Phi(\mathcal{P}_3)_\mathfrak{p} = D_{m_\mathfrak{p}-1} + \ldots + (m_\mathfrak{p} - 1)D_1 + m_\mathfrak{p} \cdot B$ and

$$\Phi(\mathcal{P}_4)_\mathfrak{p} = \Phi(\mathcal{P}_5)_\mathfrak{p} = \sum_{i=1}^{\frac{k_\mathfrak{p}}{2}-1} i\left(F_{\frac{k_\mathfrak{p}}{2}-i} + F_{\frac{k_\mathfrak{p}}{2}+i}\right) + \frac{k_\mathfrak{p}}{2} \cdot H + \left(\frac{k_\mathfrak{p}}{2} + 1\right) D_{m_\mathfrak{p}-1} + \ldots + \left(\frac{k_\mathfrak{p}}{2} + m_\mathfrak{p}\right) \cdot B\,.$$

Hence

$$\Phi(\mathcal{P}_i)_\mathfrak{p}^2 = \begin{cases} -m_\mathfrak{p} & \text{for } 0 \leq i \leq 3 \\ -(k_\mathfrak{p} + m_\mathfrak{p}) & \text{for } i = 4,\ 5 \end{cases}$$

and

$$\Phi(\mathcal{P}_0)_\mathfrak{p} \cdot \Phi(\mathcal{P}_j)_\mathfrak{p} = \begin{cases} -m_\mathfrak{p} & \text{for } j = 1,\ 2 \\ m_\mathfrak{p} & \text{for } j = 3,\ 4,\ 5 \end{cases}$$

Hence

$$\Delta(\mathcal{P}_0, \mathcal{P}_j)_\mathfrak{p} = \begin{cases} -\frac{m_\mathfrak{p}}{2} & \text{for } j = 1,\ 2 \\ \frac{3}{2}m_\mathfrak{p} & \text{for } j = 3 \\ \frac{3}{2}m_\mathfrak{p} + \frac{1}{4}k_\mathfrak{p} & \text{for } j = 4,\ 5 \end{cases}$$

We continue to assume that $\mathfrak{p} \nmid 2$ and that E_1 has good reduction modulo $\mathfrak{p}$. Then $\mathcal{P}_{j,\mathfrak{p}} \neq \mathcal{P}_{0,\mathfrak{p}}$ for $j = 1, \ldots, 5$ and hence $(\mathcal{P}_0 \cdot \mathcal{P}_j)_\mathfrak{p} = 0$.

A remark concerning the contribution of divisors of 2: Let $\mathfrak{p}|2$. We assume that E_1 has good reduction at $\mathfrak{p}$ and that E_1 is not isogenous to E_2 modulo $\mathfrak{p}$ if $\mathfrak{p} \nmid \mathcal{N}_{E_2}$ and that E_1 is not supersingular modulo $\mathfrak{p}$ if $\mathfrak{p}|\mathcal{N}_{E_2}$. Then $(\mathcal{P}_0 \cdot \mathcal{P}_j)_\mathfrak{p}$ as well as $\Delta(\mathcal{P}_0, \mathcal{P}_j)_\mathfrak{p}$ can be estimated by $0(e_\mathfrak{p})$ where $e_\mathfrak{p}$ is the absolute ramification of $\mathfrak{p}$ in $K/\mathbb{Q}$.

By putting things together and summing up we get:

Proposition 4.1: *Let E_1 be an elliptic curve defined over K with good reduction at all non-archimedean places of K and E_2 a semi-stable elliptic curve over K which is not isogenous to E_1. If $\mathfrak{p}|2$ we assume that either E_1 is not supersingular modulo $\mathfrak{p}$ or that $\mathfrak{p} \nmid \mathcal{N}_{E_2}$ and E_1 is not isogenous to E_2 modulo $\mathfrak{p}$. Let $\alpha: E_1[n] \longrightarrow E_2[n]$ be a K-isomorphism such that the graph of α is isotropic in $E_1[n] \times E_2[n]$.*

Let C be the corresponding curve of genus 2 with Weierstraß points P_0, P_1, $P_2 \in W_2$ and P_3, P_4, $P_5 \in W_1$. Then

$$\frac{5}{2}\omega^2_{\mathcal{C}/B} = \frac{7}{2}\sum_{\mathfrak{p}\in\Sigma_K}\delta_{\mathfrak{p}} + O(h_{K,n}(E_2)) + O(\frac{1}{n}h_K(E_2)) + O(m_K) + s_\infty$$

with

$$s_\infty = -4\sum_{\mathfrak{p}\in S_{K,\infty}}\left(\sum_{j=1}^{5}(\mathcal{P}_0\cdot\mathcal{P}_i)_{\mathfrak{p}}\right)$$

and

$$h_{K,n}(E_2) = \sum_{\substack{\mathfrak{p}|n\\ \mathfrak{p}\in\Sigma_K}}\max\{0, -v_{\mathfrak{p}}(j_2)\cdot\deg\mathfrak{p}\}$$

and the term $O(m_K)$ estimates the contribution of primes $\mathfrak{p}|2$.

Using Noether's formula we get

Corollary 4.2 *The height of $\mathcal{C}$ over K is given by*

$$h_K(C) = \frac{1}{7}\omega^2_{\mathcal{C}/B} + O(k_{K,n}(E_2)) + O(\frac{1}{n}h_K(E_2)) + O(m_K) + O(s_\infty) + \sum_{\mathfrak{p}\in S_{K,\infty}}\delta_{\mathfrak{p}}$$

On the other hand the Jacobian of C is isogenous to $E_1\times E_2$ under an isogeny of degree n^2, and using the behaviour of heights under isogenies (cf. [3]) one gets

Corollary 4.3:

$$h_K(E_2) = \frac{1}{7}\omega^2_{\mathcal{C}/B} + O(h_{K,n}(E_2)) + O(\frac{1}{n}h_K(E_2)) + O(m_K) + O(g(K)\cdot\log n) + O(s_\infty) + \sum_{\mathfrak{p}\in S_{K,\infty}}\delta_{\mathfrak{p}}\,.$$

One could hope that the "∞-part" on the right hand side can be estimated using results of Bost ([2]) and the explicit construction of C. At least the following is true (use [2] and Proposition 1.5):

Assume that $M\in\mathbb{R}$ such that for all $\mathfrak{p}\in S_{K,\infty}$ the absolute value $|j_2|_{\mathfrak{p}}$ is bounded by M. Then $O(s_\infty) + \sum_{\mathfrak{p}\in S_{K,\infty}}\delta_{\mathfrak{p}}$ is bounded by $O(M, m_K)$.

Now we want to exploit corollary 4.3. We fix a global field K. We take a constant c such that the terms $O(h_{K,n}(E_2))$ and $O(\frac{1}{n}h_K(E_2))$ are bounded by $c \cdot h_{K,n}(E_2)$ resp. $c \cdot \frac{1}{n}h_K(E_2)$. There is a number N such that for all elliptic curves E/K we find an odd number $n_E \leq N$ with $h_{K,n_E}(E) \leq \frac{1}{2c}h_K(E)$ and $n_E > 3c$.

We find finitely many elliptic curves $\{E_{1,i}\}$ with integral j-invariants such that for all semi-stable curves $\tilde{E}/K$ there is one $E_1 \in \{E_{1,i}\}$ which satisfies: If $\mathfrak{p}|2$ and $\mathfrak{p} \not| \mathcal{N}_E$ then E_1 is not isogenous to $\tilde{E}$, and if $\mathfrak{p}|2$ and $\mathfrak{p}|\mathcal{N}_E$ then E_1 is not supersingular modulo $\mathfrak{p}$.

The necessary number of these curves $\{E_{1,i}\}$ depends on m_K only. There is a finite extension K' of K such that all curves $E_{1,i}$ have good reduction at all places of K' and such that the genus of K' and $m_{K'}$ depend only on K.

Now take a semi-stable curve E/K and assume that for all $\mathfrak{p} \in S_{K,\infty}$ we have: $|j_E|_\mathfrak{p} \leq M$.

Choose $n := n_E \leq N$ such that $h_{K,n}(E) \leq \frac{1}{2c}h_K(E)$ and take $E_1 \in \{E_{1,i}\}$ suitable for E. Define $K'' := K'(E_1[2n], E[2n])$.

The pair (E_1, E) has over K'' all the properties which are necessary to choose $\alpha: E_1[2n] \longrightarrow E[2n]$ and to construct a corresponding curve C such that the corollary 4.3 can be applied:

$$h_{K''}(E) \leq \frac{1}{7}\omega^2_{C/B} + \frac{5}{6}h_{K''}(E) + c_1 \cdot M_{K''} + c_2 g(K'') \log N \quad \text{or :}$$
$$\frac{1}{6}h_{K''}(E) \leq \frac{1}{7}\omega^2_{C/B} + c_1 \cdot M_{K''} + c_2 g(K'') \log N\,.$$

Now $m_{K''}$ is bounded by $O(m_{K'} \cdot N^7)$ and $g(K'')$ is bounded by a linear function of $\deg(\mathcal{N}_E)$ (depending on $g(K)$, m_K and n_E), and hence we get

Theorem 4.4: *Let $E|K$ be a semi-stable elliptic curve. Then there are constants c_1, c_2 depending on K only, and r_∞ depending on K and $\max_{\mathfrak{p} \in S_{K,\infty}}(|j|_\mathfrak{p})$ such that*

$$h_K(E) \leq c_1 \omega^2_{C/B} + c_2 \deg \mathcal{N}_E + r_\infty$$

where C is the arithmetical surface belonging to a curve of genus 2 covering E and an elliptic curve E_1 with potentially good reduction everywhere.

Corollary 4.5: *Assume that the conjecture (S_J) is true for curves of genus 2 with split Jacobians. Then $\omega^2_{C/B} \leq c(K) \deg \mathcal{N}_E + d(K)$, and hence the height conjecture is true for elliptic curves for which the absolute values of the j-invariants are bounded.*

REFERENCES

[1] S. Ju. Arakelov: Intersection theory on an arithmetic surface (Russian). Izv. Akad. Nauk. SSSR 38 (1974) = Math. USSR Izv. 8 (1974), 1167–1180.

[2] J. B. Bost: Fonctions de Green-Arakelov, fonctions thêta et courbes de genre 2. C. R. Acad. Sci. Paris 306 (1987), 643–646.

[3] P. Deligne: Preuve des conjectures de Tate et Shafarevich [d'après G. Faltings]. Sem. Bourbaki (1983/84, no. 616, Astérisque 121/122 (1985), 25–41.

[4] G. Faltings: Calculus on arithmetic surfaces. Ann. Math. 119 (1984), 387–424.

[5] G. Frey: Links between solutions of $A - B = C$ and elliptic curves. Number Theory, Ulm 1987, Springer Lecture Notes in Math. 1380 (1989).

[6] A. Grothendieck: Modèles de Néron et monodromie (SGA 7, X). Springer Lecture Notes in Math. 288 (1972), 313–523.

[7] T. Ibukiyama, T. Katsura, F. Oort: Supersingular curves of genus two and class numbers. Comp. Math. 57 (1986), 127–152.

[8] E. Kani: Weil heights, Néron pairings and v-metrics on curves. Rocky Mt. J. 15 (1985), 417–449.

[9] S. Lang: Abelian Varieties. Interscience Publ., New York, 1959.

[10] S. Lang: Introduction to Arakelov Theory. Springer Verlag, New York, 1988.

[11] D. Mumford: Abelian Varieties. Oxford U. Press, London, 1970.

[12] A. Ogg: On pencils of curves of genus two. Topology 5 (1966), 355–362.

[13] A. N. Parshin: Minimal models of curves of genus 2. Izv. Akad. nauk. SSSR 36 (1972) = Math. USSR Izv. 6 (1972), 65–108.

[14] A. N. Parshin: The Bogomolov-Miyaoka-Yau inequality for arithmetical surfaces and its applications. Sem. Théorie des Nombres Paris 1986/87 (C. Goldstein, ed.) Progress in Math. 75, Birkhäuser, Boston (1989), 299–312.

[15] K. Ribet: On modular representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms. Preprint MSRI 06420-87, June 1987 (68 pp.).

[16] J.-P. Serre: Groupes algébriques et corps de classes. Hermann, Paris, 1959.

[17] J.-P. Serre: Nombres des points des courbes algébriques sur $\mathbb{F}_q$. Sem. Théorie des Nombres Bordeaux 1982/83, no. 22 = Oeuvres/Collected Papers III, 664-668.

[18] L. Szpiro: Proprietés numériques du faisceaux dualisant relatif. In: Sem. sur les pinceaux des courbes de genre au moins deux (L. Szpiro,

ed.) Astérisque 86 (1981), 44–78.
[19] L. Szpiro: La Conjecture de Mordell [d'après G. Faltings]. Sém. Bourbaki 1983/84, no. 619 Astérisque 121/122 (1985), 83–103.
[20] L. Szpiro: Un peu d'effectivité. in: Sém. sur les pinceaux arithmétiques: La Conj. de Mordell (L. Szpiro, ed.), Astérisque 127 (1985), 275–287.
[21] L. Szpiro: Sur les propriétés numériques du dualisant relatif d'une surface arithmétique. To appear.
[22] P. Vojta: Diophantine inequalities and Arakelov theory. Appendix to [10].
[23] A. Weil: Zum Beweis des Torellischen Satzes. Göttinger Nachrichten 2957, Nr. 2 = Oeuvres Scientifiques/Collected Papers II, pp. 302–327.