ON THE HEIGHT CONSTANT FOR CURVES OF GENUS TWO

MICHAEL STOLL

Abstract. Let $y^2 = f(x)$ (with f of degree 5 or 6) define a curve C of genus two over some non-archimedean local field k of characteristic different from 2. Suppose that f has integral coefficients. Let $K \subset \mathbb{P}^3$ be the Kummer surface associated to C, and denote by $\delta : K \longrightarrow K$ the duplication map. For a point $P \in \mathbb{P}^3(k)$ with specified homogeneous coordinates $(x_1 : x_2 : x_3 : x_4)$, denote $|P| = \max\{|x_1|, |x_2|, |x_3|, |x_4|\}$ (where $|\cdot|$ is the absolute value on k). We derive a general bound on the *height constant* $c = \min_{P \in K(k)} |\delta(P)|/|P|^4$, namely

$$c \geq |2^4 \operatorname{disc}(f)|\,,$$

where $\operatorname{disc}(f)$ is the discriminant of f, viewed as a polynomial of degree 6.

Together with some bounds for the archimedean places, this gives an upper bound for the difference $h - \hat{h}$ between a certain naive height and the canonical height on the Jacobian of a curve of genus two defined over a number field. In particular, we get a bound on the naive height of a torsion point, which can be used to find the rational torsion subgroup of the Jacobian.

Contents

Date: July 27, 1998.

1991 *Mathematics Subject Classification.* 11G30, 14H45, 14H40, 11G10.

Key words and phrases. curves of genus two, Jacobians, local fields, number fields, height constant, torsion points.

1. Introduction

In many contexts, it is important to bound the naive height of a point on an abelian variety in terms of its canonical height. There is a quite extensive literature on this subject concerning elliptic curves (see for example [5] for a recent result), but general results for Jacobians of curves of higher genus are sparse. This paper aims at filling this gap for Jacobians of curves of genus two, building on work done by Victor Flynn and Nigel Smart.

The motivation for this work arose from discussions with Bjorn Poonen on the design of a program for computing the rational torsion subgroup of such a Jacobian. One of the more straight-forward approaches requires a bound on the (naive) height of a torsion point. A rough sketch of the algorithm is given at the end of Section 8.

Let h_K be the naive logarithmic height function on the Jacobian J induced from a certain embedding of its Kummer surface K into $\mathbb{P}^3$, and let $\hat{h}$ denote the canonical height on J. Assume for simplicity that $\mathbb{Q}$ is our base field. Then for every $P \in J(\mathbb{Q})$, we have

$$h_K(P) \le \hat{h}(P) + \tfrac{1}{3} \sum_v \gamma_v$$

(cf. [3]), where v runs through the places of $\mathbb{Q}$ and the γ_v are certain local *height constants*, which measure locally how far $h_K(2P)$ is from $4h_K(P)$. The main result of this paper is that

$$\sum_{v \text{ non-arch.}} \gamma_v \le \log |2^4 \operatorname{disc}(F)| \,,$$

where F is the polynomial defining the curve. Together with some estimate on γ_∞, which can also be got by our method, this yields an upper bound on $h_K - \hat{h}$. (Note that $\gamma_v = \log c_v^{-1}$ in terms of the notation used in this paper. The notation in [3] is $c_1^{(v)}$ instead of γ_v.)

The following section introduces the basic notions. The three sections after that use some elementary representation theory to describe the action of the 2–torsion subgroup of J on the Kummer surface and its ambient projective space. In hindsight, this is mainly motivational, since the explicit formulas one can deduce (which are given later in Section 10) are generically valid and can be checked without referring to the theory. The key results are Lemmas 4.1 and 5.2, which immediately imply the main theorem given in Section 6. The following section discusses some refinements of the bounds which can be obtained by using the formulas explicitly. It also gives a method for finding a bound on γ_∞. Section 8 states the application to curves over number fields. A discussion relating our work to earlier work by Victor Flynn follows, and a section giving the relevant formulas closes the paper.

I wish to thank Bjorn Poonen for providing me with the motivation for this work and for many stimulating and fruitful discussions.

2. Basics

Let k be a non-archimedean local field of characteristic different from 2 with (multiplicative) absolute value $|\cdot|$ (in Section 8, we will also consider number fields). Let $\mathcal{O}$ be the integers of k, let $F \in \mathcal{O}[X, Z]$ be a homogeneous polynomial of degree 6 without multiple factors and define $f(X) = F(X, 1)$. Then the affine equation

$$Y^2 = f(X) \tag{2.1}$$

defines a curve of genus two; let C be its smooth projective model over k. We let J denote the Jacobian of C, which is an abelian surface defined over k. Its quotient by the multiplication-by-(-1) map is the associated Kummer surface K; it can be embedded as a hypersurface into $\mathbb{P}^3$. For the basic facts regarding K, see Chapter 3 in the book [1]. We will use the embedding of K into $\mathbb{P}^3$ as given there. Since addition of a 2–torsion point and multiplication by 2 both commute with -1, they descend to give morphisms on K.

The duplication map on K is given by four polynomials $\delta_1, \delta_2, \delta_3, \delta_4 \in \mathcal{O}[x_1, x_2, x_3, x_4]$, homogeneous of degree 4, in the homogeneous coordinates x_1, x_2, x_3, x_4. We will denote by δ_0 the equation of K, which is again a homogeneous polynomial of degree 4; the reason for doing this will soon become apparent. Explicit expressions for these polynomials can be obtained by anonymous ftp at `ftp://ftp.liv.ac.uk/~ftp/pub/genus2`. The Kummer surface equation δ_0 is also given in [1] and [3].

Now the *height constant* of C (over k) is defined to be

$$c = \min_{x=(x_1 : x_2 : x_3 : x_4) \in K(k)} \frac{\max\{|\delta_1(x)|, |\delta_2(x)|, |\delta_3(x)|, |\delta_4(x)|\}}{(\max\{|x_1|, |x_2|, |x_3|, |x_4|\})^4}\,. \tag{2.2}$$

Recall that we are using a specific embedding of K into $\mathbb{P}^3$. In general, the height constant will depend on the embedding chosen.

3. The first representation

For the elementary representation theory of finite groups needed in what follows, we refer to the first two chapters of the book [4].

In this and the next two sections, we will assume that our base field k has characteristic zero. This is necessary to make the representation theory work. Note, however, that the explicit formulas given in Section 10 are completely generic. Since the main results only depend on these formulas, they also hold in positive (odd) characteristic.

For the following, we assume that F splits completely over k. To satisfy this assumption, we can simply replace k with the splitting field of F over k; this will not affect the result. Write

$$F = \prod_{j=1}^{6} (\beta_j X - \alpha_j Z)$$

with $\alpha_j, \beta_j \in \mathcal{O}$.

The non-trivial 2–torsion points of J are parametrised by 2-subsets $\{i, j\} \subset \{1, 2, 3, 4, 5, 6\}$, corresponding to divisors of F of degree two. The addition of the 2–torsion point $t_{\{i,j\}}$ on K is given by a projective linear transformation of the ambient $\mathbb{P}^3$. In [1, p. 21], to each $t = t_{\{i,j\}}$, a 4×4–matrix $M_t = M_{\{i,j\}}$ with entries in $\mathcal{O}$ is associated that defines this transformation. Furthermore, we have $M_{\{i,j\}}^2 = r(i,j)I$ (I being the identity matrix), where

$$r(i,j) = \prod_{m \in \{i,j\}} \prod_{\ell \notin \{i,j\}} (\beta_\ell \alpha_m - \beta_m \alpha_\ell)$$

is the resultant of the factor of F corresponding to $\{i,j\}$ and the the remaining factor. We also define $M_0 = I$. Let $r(t) = r(i,j)$ if $t = t_{\{i,j\}}$ and $r(0) = 1$. We have the relation

$$M_t M_{t'} = c(t,t') M_{t+t'} = e(t,t') M_{t'} M_t \,,$$

where e denotes the Weil pairing on $J[2]$, which is given by

$$e(t_{\{i,j\}}, t_{\{k,m\}}) = (-1)^{\#\{i,j\} \cap \{k,m\}} \,,$$

and $c(t,t') \in \mathcal{O}$ is given explicitly in [1, p. 22].

So we see that $T = J[2]$ embeds into $\mathrm{PGL}(4,k)$, but this does not lift to an embedding into $\mathrm{GL}(4,\bar{k})$, where $\bar{k}$ is some algebraic closure of k. We can, however, consider the subgroup

$$\tilde{T} = \{\rho M_t \mid t \in T, \rho^4 = r(t)^{-2}\} \subset \mathrm{GL}(4,\bar{k}) \,,$$

which is a four-fold cover of T. The kernel of the map $\tilde{T} \longrightarrow T$ consists of the matrices ζI, where ζ is a fourth root of unity, and coincides with the center of $\tilde{T}$. The group $\tilde{T}$ acts on $\bar{k}[x_1,x_2,x_3,x_4]$, and ζI acts as multiplication by ζ on the vector space V of linear polynomials. Let χ be the character of the representation of $\tilde{T}$ on V. Then $\chi(\zeta I) = 4\zeta$, and since every element not in the center is conjugate to its negative, $\chi(\tilde{t}) = 0$ for all other elements $\tilde{t} \in \tilde{T}$. This implies that this representation is irreducible.

For a subring R of $\bar{k}$, we denote by V_R the free R–submodule of $R[x_1,x_2,x_3,x_4]$ generated by x_1,x_2,x_3,x_4.

4. The second representation

There is a group T' between $\tilde{T}$ and T. It consists of pairs (ε, t) with $\varepsilon = \pm 1$ and $t \in T$, with multiplication given by

$$(\varepsilon, t)(\varepsilon', t') = (\varepsilon\varepsilon' e(t,t'), t + t') \,.$$

The map $T' \longrightarrow T$ is projection onto the second component, and the map $\tilde{T} \longrightarrow T'$ is given by $\rho M_t \mapsto (\rho^2 r(t), t)$. The group T' is elementary abelian of order 2^5, so there are sections $T \longrightarrow T'$, but there is no canonical such section. The preimage in $\tilde{T}$ of the image of such a section is a so-called extraspecial 2–group of order 2^5; the representation on V is its (irreducible) 4–dimensional spin representation.

Now look at the representation of $\tilde{T}$ on homogeneous polynomials of degree two, which is $\mathrm{Sym}^2 V$. By the usual formulas, we get for its character ψ that

$$\psi(\zeta I) = 10\zeta^2 \qquad \text{and} \qquad \psi(\rho M_t) = 2\rho^2 r(t) \text{ for } t \neq 0.$$

This shows that the representation factors through T', and on T', we have

$$\psi(\varepsilon, 0) = 10\varepsilon \qquad \text{and} \qquad \psi(\varepsilon, t) = 2\varepsilon \text{ for } t \neq 0.$$

Since T' is abelian, the representation has to split into one-dimensional irreducibles. Every partition of $\{1, 2, 3, 4, 5, 6\}$ into two sets with three elements (there are 10 such partitions—the ordering of the two sets is irrelevant) determines a character on T' as follows. Let S and S' be the two sets. Then

$$\chi_{S,S'}(\varepsilon, 0) = \varepsilon$$

and

$$\chi_{S,S'}(\varepsilon, t_{\{i,j\}}) = -\varepsilon \text{ if } \{i, j\} \subset S \text{ or } \{i, j\} \subset S', \qquad \chi_{S,S'}(\varepsilon, t_{\{i,j\}}) = \varepsilon \text{ otherwise.}$$

Since $\psi = \sum_{\{S,S'\}} \chi_{S,S'}$, we see that

$$\operatorname{Sym}^2 V_k = \bigoplus_{\{S,S'\}} k \cdot y_{S,S'}$$

with $y_{S,S'} \in k[x_1, x_2, x_3, x_4]$ suitable homogeneous polynomials of degree 2 such that T' acts on $y_{S,S'}$ via $\chi_{S,S'}$. (Everything is defined over k, since the characters have values in k.) We can choose the $y_{S,S'}$ to have coefficients in $\mathcal{O}$ with one of them being a unit. Formula 10.1 gives an explicit expression. Let

$$\Delta = \prod_{i<j} (\beta_j \alpha_i - \beta_i \alpha_j) \,.$$

Since the action of $(\varepsilon, t) \in T'$ on $\operatorname{Sym}^2 V$ is given by $\varepsilon/r(t)$ times the action of M_t, and since $r(t)$ divides Δ, we see that $2^4 \Delta \operatorname{Sym}^2 V_{\mathcal{O}}$ is contained in the $\mathcal{O}$–module generated by the $y_{S,S'}$. ($2^5\Delta$ times the projection operator onto the $\chi_{S,S'}$–eigenspace has integral coefficients. By using a section $T \longrightarrow T'$, we can reduce 2^5 to 2^4.) By doing the calculations explicitly, we get the following slightly better result.

Lemma 4.1.

$$\bigoplus_{\{S,S'\}} \mathcal{O} \cdot y_{S,S'} \supset 2^2 \Delta \operatorname{Sym}^2 V_{\mathcal{O}}$$

Proof: This follows from formulas 10.3 and 10.4 □

5. The third representation

The next step is to consider the representation of $\tilde{T}$ or T' on $\operatorname{Sym}^4 V$, the homogeneous polynomials of degree four. Let φ be its character. Then by the usual formulas, we get (first on $\tilde{T}$, then on T')

$$\varphi(\varepsilon, 0) = 35 \qquad \text{and} \qquad \varphi(\varepsilon, t) = 3 \text{ for } t \neq 0.$$

We see that this representation actually is a representation of T itself and that it contains five copies of the trivial representation and two copies of each of the 15 non-trivial irreducible representations. We have the following result.

Lemma 5.1. *The elements* $\delta_0, \delta_1, \delta_2, \delta_3, \delta_4 \in \operatorname{Sym}^4 V_k$ *give a basis of the subspace of* T*–invariant elements.*

PROOF: This is because the Kummer surface is invariant under T and so is the duplication map. One can also check the claim directly. □

Now, since the action of T' on $y_{S,S'}$ is given by a quadratic character, $y_{S,S'}^2 \in \operatorname{Sym}^4 V$ is invariant under T. This means that we can express $y_{S,S'}^2$ in terms of the δ_j. Doing this explicitly yields the following.

Lemma 5.2. *For every partition* $\{S, S'\}$*, we have* $y_{S,S'}^2 \in \bigoplus_{j=0}^{4} \mathcal{O} \cdot \delta_j$.

PROOF: This follows from formula 10.2. □

If we look at the product of two different $y_{S,S'}$, then we will get an element in some nontrivial eigenspace of $\operatorname{Sym}^4 V_k$. For example (and without loss of generality) if we take $y = y_{\{1,3,4\},\{2,5,6\}}$ and $y' = y_{\{1,5,6\},\{2,3,4\}}$, then $t \in T$ acts on yy' as multiplication by $e(t, t_{\{1,2\}})$. The set $\{1, 2\}$ showing up here consists of the two elements that have to be interchanged in order to transform one partition into the other. There are two other such products in this eigenspace, namely $y_{\{1,3,5\},\{2,4,6\}} y_{\{1,4,6\},\{2,3,5\}}$ and $y_{\{1,3,6\},\{2,4,5\}} y_{\{1,4,5\},\{2,3,6\}}$. Since the eigenspace is only two-dimensional, there has to be a linear relation between these three products. This relation is given in formula 10.5.

Together, formulas 10.2, 10.3, 10.4, and 10.5 give a method to compute preimages under δ on the Kummer surface in the following way. First find the $y_{S,S'}^2$ from the values of the δ_j via 10.2. The nonzero values of the $y_{S,S'}^2$ must all lie in the same coset of $k^\times$ modulo squares. Otherwise, there is no preimage in $K(k)$. By multiplying through with a suitable factor, we may assume that they are squares. Then extract square roots to get at possible values for the $y_{S,S'}$ themselves. Now adjust the signs in such a way that relations 10.5 hold. Pick some i such that x_i^2 as given by 10.3 is non-zero. Then $(x_1 : x_2 : x_3 : x_4)$ is determined by $(x_1 x_i : x_2 x_i : x_3 x_i : x_4 x_i)$ as given in 10.3 and 10.4.

REMARK: One can take this game a step further and look at $\operatorname{Sym}^8 V$, the homogeneous polynomials of degree 8. This splits into 15 copies of the trivial representation and 10 copies of each of the non-trivial irreducible representations. If we split $\operatorname{Sym}^4 V_k = W \oplus W'$, where W is the invariant part, then $\operatorname{Sym}^8 V_k = \operatorname{Sym}^2 W \oplus (W' \otimes_k W)$. In particular, the ideal generated by the δ_j contains the eighth power of the irrelevant ideal. It would be interesting to find the 'best' constant $A \in \mathcal{O}$ such that

$$A \cdot (x_1, x_2, x_3, x_4)^8 \subset (\delta_0, \delta_1, \delta_2, \delta_3, \delta_4)$$

as ideals of $\mathcal{O}[x_1, x_2, x_3, x_4]$. I have not yet been able to do the necessary computations because of the complexity of the expressions involved.

As noted at the beginning of Section 3, Lemmas 4.1 and 5.2 remain true over local fields of odd positive characteristic, since they only depend on the explicit formulas of Section 10.

6. The main result

It is now an easy matter to prove our main result.

Theorem 6.1. *Let k be a non-archimedean local field of characteristic different from 2, with absolute value $|\cdot|$. Define the height constant c by*

$$c = \min_{(k_1:k_2:k_3:k_4)\in K(k)} \frac{\max\{|\delta_j(k_1,k_2,k_3,k_4)| \mid j=1,2,3,4\}}{(\max\{|k_1|,|k_2|,|k_3|,|k_4|\})^4}\,.$$

Then

$$c \geq |2^4 \operatorname{disc}(F)|\,.$$

Proof: Let $(k_1 : k_2 : k_3 : k_4) \in K(k)$ be some point. Consider the $y_{S,S'}$ evaluated at this set of homogeneous coordinates. By Lemma 5.2, we have

$$|y_{S,S'}(k_1,k_2,k_3,k_4)|^2 \leq \max\{|\delta_j(k_1,k_2,k_3,k_4)| \mid j=1,2,3,4\}$$

(note that $\delta_0(k_1,k_2,k_3,k_4)=0$ since the point is on K). On the other hand, by Lemma 4.1, for each $j \in \{1,2,3,4\}$, we also have

$$|2^2\Delta|\cdot|k_j|^2 \leq \max_{\{S,S'\}} |y_{S,S'}(k_1,k_2,k_3,k_4)|\,.$$

So (with $\Delta^2 = \operatorname{disc}(F)$) we get

$$|2^4 \operatorname{disc}(F)|\cdot(\max\{|k_1|,|k_2|,|k_3|,|k_4|\})^4 \leq \max\{|\delta_j(k_1,k_2,k_3,k_4)| \mid j=1,2,3,4\}\,,$$

which proves the theorem. □

Remark: The result of the theorem is unchanged when we replace k with a finite extension and extend the absolute value of k to that extension. Hence the bound on c is valid on $K(\bar{k})$.

Remark: (See also [3, Lemma 3].) If we define

$$c' = \max_{(k_1:k_2:k_3:k_4)\in K(k)} \frac{\max\{|\delta_j(k_1,k_2,k_3,k_4)| \mid j=1,2,3,4\}}{(\max\{|k_1|,|k_2|,|k_3|,|k_4|\})^4}\,,$$

then $c' = 1$. We have $c' \leq 1$, since the δ_j have integral coefficients, and $c' \geq 1$, since for $(k_1,k_2,k_3,k_4) = (0,0,0,1)$, we get $(\delta_1,\delta_2,\delta_3,\delta_4) = (0,0,0,1)$.

7. Refinements

If k is archimedean, we can still use our setup to find a bound on the height constant. In this case, we need to find the coefficients in the relations of Lemmas 4.1 and 5.2 explicitly and then have to use the usual archimedean triangle inequality.

To be more specific, write for $i \in \{1,2,3,4\}$

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

and for a partition $\{S,S'\}$

$$y_{S,S'}^2 = \sum_{j=0}^{4} b_{\{S,S'\},j}\delta_j \,.$$

Then for archimedean k, we get

$$\frac{1}{c} \le \max_i \left(\sum_{\{S,S'\}} |a_{i,\{S,S'\}}| \sqrt{\sum_{j=1}^{4} |b_{\{S,S'\},j}|} \right)^2 . \tag{7.1}$$

For non-archimedean k, we similarly have

$$\frac{1}{c} \le \max_i \max_{\{S,S'\}} |a_{i,\{S,S'\}}|^2 \,, \tag{7.2}$$

since we can use the non-archimedean triangle inequality and the fact that $b_{\{S,S'\},4} = 1$ and $|b_{\{S,S'\},j}| \le 1$ for all j. This can be used to obtain refined bounds, using the explicit formulas given in section 10.

A first refinement is

$$c \ge |2|^4 \min_{\{S,S'\}} |R(S,S')^2| \,, \tag{7.3}$$

where

$$R(S,S') = \prod_{i\in S}\prod_{j\in S'} (\alpha_i\beta_j - \alpha_j\beta_i)$$

is the resultant of the two factors of F corresponding to S and S'. In order to find this improved bound in practice for some F with (rational) integral coefficients, say, one can proceed as follows. First find the (complex) roots of f to sufficiently high precision, then compute the $R(S,S')$ numerically and find the polynomial $\prod_{\{S,S'\}}(x - R(S,S')^2)$, which has integral coefficients, so they can be found by rounding. Finally, look at the Newton polygon of this polynomial and take its largest slope as an upper bound for the (additive) valuation of c.

A still better bound can be got in some cases by really considering the $a_{i,\{S,S'\}}$. We know by Lemma 4.1 that $4\Delta a_{i,\{S,S'\}}$ is integral. Hence we can, for each i, form the polynomial

$$p_i(x) = \prod_{\{S,S'\}} (x - 16\,\mathrm{disc}(F) a_{i,\{S,S'\}}^2) \in \mathcal{O}[x]$$

and look at its Newton polygon. The absolute value γ corresponding to the minimum of all the slopes in the Newton polygons gives the refinement

$$\frac{1}{c} \le \frac{\gamma}{|2^4\,\mathrm{disc}(F)|}\,. \tag{7.4}$$

This approach can be used to obtain a better general bound in case F is not primitive. Let F_{red} denote the primitive part of F, and let λ be the content of F (so that $F = \lambda\, F_{\mathrm{red}}$). Tracing the content through the various formulas leads to the following general refinement.

Proposition 7.1. *We have*

$$c \ge |(2\lambda)^4\,\mathrm{disc}(F_{\mathrm{red}})|\,,$$

with the refinement

$$c \ge |2\lambda|^4 \min_{\{S,S'\}} |R_{\mathrm{red}}(S,S')^2|\,,$$

where $\{S,S'\}$ runs through all partitions of $\{1,2,3,4,5,6\}$ into two three-element subsets, and where $R_{\mathrm{red}}(S,S')$ means $R(S,S')$ evaluated for F_{red} instead of F.

This is indeed better than the bounds in the theorem and in (7.3), since $R(S,S') = \lambda^3\,R_{\mathrm{red}}(S,S')$ and $\mathrm{disc}(F) = \lambda^{10}\,\mathrm{disc}(F_{\mathrm{red}})$.

In order to get some indication of how good the bounds are, let us try to find an upper bound on c. Since the 2–torsion points play a special role, it is natural to use them for this purpose. Let $U = \{i,j\}$ be some two-element subset of $\{1,2,3,4,5,6\}$, and let U' denote its complement. Write

$$(\beta_i X - \alpha_i Z)(\beta_j X - \alpha_j Z) = A(X,Z) = a_0\,X^2 - a_1\,XZ + a_2\,Z^2 \qquad \text{and}$$
$$\prod_{m\in U'} (\beta_m X - \alpha_m Z) = B(X,Z) = b_0\,X^4 - b_1\,X^3Z + b_2\,X^2Z^2 - b_3\,XZ^3 + b_4\,Z^4\,.$$

Then the image of t_U in K is given by $(a_0 : a_1 : a_2 : -(a_2^2 + a_2b_2 + b_4))$, and the duplication map evaluated at these coordinates gives $(0 : 0 : 0 : R(U,U')^2)$. Here, $R(U,U') = r(i.j)$ denotes the resultant of A and B. If we again write λ for the content of F and $R_{\mathrm{red}}(U,U')$ for the resultant of the primitive parts of A and B, then we get the following result.

Proposition 7.2. *We have the following upper bound on c.*

$$c \le |\lambda|^4 \min_{\{U,U'\}} |R_{\mathrm{red}}(U,U')|^2\,,$$

where $\{U,U'\}$ runs through all partitions of $\{1,2,3,4,5,6\}$ into a two-element and a four-element subset.

8. The number field case

Now suppose k is a number field and assume that F has coefficients in $\mathcal{O}_k$, the integers of k. Then we get bounds on the various local height constants c_v for all the places v of k. Let H_K denote the naive height induced on K by the embedding into $\mathbb{P}^3$; we will also denote by H_K the function induced on the Jacobian J. Let $h_K = \log H_K$ denote the corresponding logarithmic height, and let finally $\hat{h}$ denote the canonical height on J. By Theorem 4 in [3], we have

$$h_K(P) \le \hat{h}(P) - \tfrac{1}{3} \sum_v \log c_v$$

for all $P \in J(k)$. In particular, taking $k = \mathbb{Q}$ for simplicity, we get the following.

Corollary 8.1. *Let $P \in J(\mathbb{Q})$ be a torsion point. Then*

$$H_K(P) \le 2^{4/3} |\operatorname{disc}(F)|^{1/3} c_\infty^{-1/3} .$$

(Here, $|\cdot|$ denotes the usual absolute value on $\mathbb{Q}$.)

This yields a practical algorithm for computing the rational torsion subgroup of J as follows. We first find some bound on the size of the torsion subgroup (by looking at $\#J(\mathbb{F}_p)$ for a few primes p of good reduction). Then we systematically try to lift possible torsion points from $J(\mathbb{F}_p)$ (p good and prime to the order of the point in question) to $J(\mathbb{Q})$. It is fairly easy to lift them to $J(\mathbb{Q}_p)$ to any desired accuracy, and the height bound of the corollary gives us the possibility to decide that the point cannot come from $J(\mathbb{Q})$ if its naive height would have to be too big. This algorithm is currently being implemented by the author as part of a Magma package for dealing with hyperelliptic curves and their Jacobians.

9. Discussion

A somewhat related approach to finding the height constant is introduced in Flynn's paper [2]. Instead of using all of the 2–torsion at once, he splits the duplication map into two Richelot isogenies. Accordingly, he uses the action of the kernels of these isogenies at each step. This has the advantage that these kernels embed into GL(4) without problems. The disadvantage of Flynn's approach is that it does not take into account that we are only interested in points on K. The method of [2] effectively gives a bound for $\min |\delta(k)|/|k|^4$ over all of $\mathbb{P}^3$.

The results of [2] are also quoted in [3]. The examples given there show that the bound one gets with this method are (usually) considerably worse than the bound given by our theorem. These examples also show that our bound is usually quite sharp.

Here are some tables comparing the various bounds for the examples given in [3].

First example: $Y^2 = X^6 + 8\,X^5 + 22\,X^4 + 22\,X^3 + 5\,X^2 + 6\,X + 1$.

	[3]	Thm. 6.1	(7.3)	(7.4)	$J(\overline{\mathbb{Q}_p})[2]$
γ_2	$6\ \log 2$	$16\ \log 2$	$16\ \log 2$	$12\ \log 2$	$\geq 8\ \log 2$
γ_{3701}	$\log 3701$	$\log 3701$	$\log 3701$	$\log 3701$	$\geq \log 3701$

The last column in each table gives the lower bound on γ_p from Prop. 7.2. This is a lower bound for the height constant taken over all *algebraic* points. The bound from [3] was obtained by an exhaustive search over the points of K, and hence should be best possible. The same applies to the other two examples below. For the infinite place, [3] gives the bound 4.422, whereas (7.1) gives 7.798. On the other hand, Flynn and Smart's bound was obtained by a numerical method and might not be accurate. In fact, a sort of 'guided random search' for points on $K(\mathbb{R})$ reveals the point $(1 : -34.47\ldots : 96.79\ldots : -661.88\ldots) \in K(\mathbb{R})$ which gives a value of $\gamma_\infty \geq 6.723$, contradicting the bound given in [3]. Indeed, looking only at the three real 2–torsion points already gives $\gamma_\infty \geq 4.439$.

Second example: $Y^2 = X^5 + 16\,X^4 - 274\,X^3 + 817\,X^2 + 178\,X + 1$.

	[3]	Thm. 6.1	(7.3)	(7.4)	$J(\overline{\mathbb{Q}_p})[2]$
γ_2	$4\ \log 2$	$4\ \log 2$	$4\ \log 2$	$4\ \log 2$	≥ 0
γ_{191}	$2\ \log 191$	$2\ \log 191$	$2\ \log 191$	$2\ \log 191$	$\geq 2\ \log 191$
γ_{941}	$2\ \log 941$	$4\ \log 941$	$\frac{12}{5}\ \log 941$	$\frac{12}{5}\ \log 941$	$\geq \frac{12}{5}\ \log 941$

The bound of $\frac{12}{5}\log 941$ for γ_{941} gives $2\log 941$ over $\mathbb{Q}_{941}$, of course. From (7.1), we get $\gamma_\infty \leq 4.264$, whereas Flynn and Smart claim that $\gamma_\infty \leq 0$. Looking at 10^5 randomly chosen points on $K(\mathbb{R})$ gives that $\gamma_\infty \geq 0.268$, and the real 2–torsion gives $\gamma_\infty \geq 0.2127$.

Third example: $Y^2 = (X^2 + 6\,X + 7)(X^2 + 4\,X + 1)(X^2 + 2\,X + 3)$.

	[2]	[3]	Thm. 6.1	(7.3)	(7.4)	$J(\mathbb{Q}_p)[2]$	$J(\overline{\mathbb{Q}_p})[2]$
γ_2	$97\ \log 2$	$16\ \log 2$	$34\ \log 2$	$23\ \log 2$	$21\ \log 2$	$\geq 16\ \log 2$	$\geq 17\ \log 2$
γ_3	$3\ \log 3$	$2\ \log 3$	$3\ \log 3$	$2\ \log 3$	$2\ \log 3$	$\geq 2\ \log 3$	$\geq 2\ \log 3$

Here, the next-to-last column gives the lower bound one gets from looking at the $\mathbb{Q}_p$–rational 2–torsion only.

From (7.1), we get $\gamma_\infty \leq 13.528$, whereas Flynn and Smart claim that $\gamma_\infty \leq 2.6836$. The same method as was used for the first example gives that $\gamma_\infty \geq 12.963$; this value comes from $Q = (9 : -49 : 60 : -1180.8716\ldots) \in K(\mathbb{R})$. The $\mathbb{Q}$–rational (!) 2–torsion point coming from the first factor already yields $\gamma_\infty \geq 8.56$. Note that the image $(1 : -6 : 7 : -136)$ on K of this torsion point is quite near to Q. This shows that $|\delta(P)|/|P|^4$ can vary quite fast, which makes numerical methods difficult to apply safely. As a last facet of this example, consider the $\mathbb{Q}$–rational point

$$P = \Big\{\Big(\tfrac{-281+\sqrt{12286}}{105}, \tfrac{-411296-4784\sqrt{12286}}{1157625}\Big), \Big(\tfrac{-281-\sqrt{12286}}{105}, \tfrac{-411296+4784\sqrt{12286}}{1157625}\Big)\Big\}$$

on the Jacobian, It has image $(105 : -562 : 635 : -12656)$ on the Kummer surface, so $h_K(P) = \log 12656 = 9.446$, but using the method of [3], one computes $\hat{h}(P) = 4.007$, hence

$$h_K(P) - \hat{h}(P) = 5.439\,,$$

which is larger than the bound 5.3237 given in [3]. Content-Length: 9795 X-Lines: 209 Status: RO

It is clear that the archimedean bound of (7.1) will usually not be sharp, since the archimedean triangle inequality gives only a crude estimate, but the examples show that the bound is not too bad in practice. On the other hand, the examples indicate that Thm. 6.1 and its refinements usually give quite good bounds at odd primes, whereas at $p = 2$, there might still be some room for improvement.

As already remarked after Thm. 6.1, the bounds obtained (and this also holds for the various refinements) are valid on the algebraic closure of k. This means that the bound fails to be sharp when the minimum is attained outside the k–rational points. In some cases, however, we can use integrality properties of the valuation to improve the bound as in the second example above.

The approach given here should (at least in principle) generalize to Jacobians of higher genus hyperelliptic curves. The corresponding Kummer variety is a g–dimensional subvariety of $\mathbb{P}^{2^g-1}$, and the 2–torsion subgroup of the Jacobian acts on it by linear transformations. To get an explicit bound, however, one needs sufficiently explicit expressions for the matrices giving these linear maps and for the polynomials defining the Kummer variety and the duplication map. Since the dimension of the projective space grows exponentially with the genus, it might be quite difficult to obtain such expressions.

10. Explicit formulas

In this section, we will make the relations given in Lemmas 4.1 and 5.2 explicit. The calculations have been done with the Magma system for computer algebra. We fix some partition $\{S, S'\}$. Let

$$\prod_{j\in S}(\beta_j X - \alpha_j Z) = \sigma_0\, X^3 + \sigma_1\, X^2 Z + \sigma_2\, X Z^2 + \sigma_3\, Z^3 \qquad \text{and}$$
$$\prod_{j\in S'}(\beta_j X - \alpha_j Z) = \tau_0\, X^3 + \tau_1\, X^2 Z + \tau_2\, X Z^2 + \tau_3\, Z^3\,.$$

Then $y_{S,S'}$ can be taken as follows.

Formula 10.1.

$$
\begin{aligned}
y_{S,S'} = {} & x_4^2 \\
& + 2\,(\sigma_2\tau_0 + \sigma_0\tau_2)x_3x_4 \\
& - 2\,(\sigma_3\tau_0 + \sigma_0\tau_3)x_2x_4 \\
& + 2\,(\sigma_3\tau_1 + \sigma_1\tau_3)x_1x_4 \\
& + ((\sigma_1\tau_0 - \sigma_0\tau_1)(\sigma_3\tau_0 - \sigma_0\tau_3 + \sigma_2\tau_1 - \sigma_1\tau_2) + 4\,\sigma_0\sigma_2\tau_0\tau_2)x_3^2 \\
& + 2\,(-\sigma_1\tau_1(\sigma_3\tau_0 + \sigma_0\tau_3) + \sigma_1^2\tau_0\tau_3 + \sigma_0\sigma_3\tau_1^2 - 2\,\sigma_0\tau_0(\sigma_3\tau_2 + \sigma_2\tau_3))x_2x_3 \\
& + 2\,(-(\sigma_3\tau_0 - \sigma_0\tau_3)^2 + (\sigma_1\tau_2 + \sigma_2\tau_1)(\sigma_3\tau_0 + \sigma_0\tau_3))x_1x_3 \\
& + (\sigma_1\sigma_3\tau_0\tau_2 + \sigma_0\sigma_2\tau_1\tau_3 - \sigma_1\sigma_2\tau_0\tau_3 - \sigma_0\sigma_3\tau_1\tau_2 + 4\,\sigma_0\sigma_3\tau_0\tau_3)x_2^2 \\
& + 2\,(-\sigma_2\tau_2(\sigma_3\tau_0 + \sigma_0\tau_3) + \sigma_2^2\tau_0\tau_3 + \sigma_0\sigma_3\tau_2^2 - 2\,(\sigma_1\tau_0 + \sigma_0\tau_1)\sigma_3\tau_3)x_1x_2 \\
& + (\sigma_3^2\tau_0\tau_2 + \sigma_0\sigma_2\tau_3^2 + \sigma_2\tau_2(\sigma_3\tau_1 + \sigma_1\tau_3) - (\sigma_2\tau_0 + \sigma_0\tau_2)\sigma_3\tau_3 \\
& \qquad - \sigma_2^2\tau_1\tau_3 - \sigma_1\sigma_3\tau_2^2 + 4\,\sigma_1\sigma_3\tau_1\tau_3)x_1^2
\end{aligned}
$$

The following expresses $y_{S,S'}^2$ in terms of the δ_j (needed for Lemma 5.2).

Formula 10.2.

$$
\begin{aligned}
y_{S,S'}^2 = -(&(\sigma_3\tau_0 + \sigma_0\tau_3)^2 + 2\,(\sigma_1\sigma_2\tau_0\tau_3 + \sigma_0\sigma_3\tau_1\tau_2) \\
&\quad + 3\,(\sigma_1\sigma_3\tau_0\tau_2 + \sigma_0\sigma_2\tau_1\tau_3) + 5\,(\sigma_2\sigma_3\tau_0\tau_1 + \sigma_0\sigma_1\tau_2\tau_3))\delta_0 \\
& + (\sigma_3\tau_1 + \sigma_1\tau_3)\delta_1 - (\sigma_3\tau_0 + \sigma_0\tau_3)\delta_2 + (\sigma_2\tau_0 + \sigma_0\tau_2)\delta_3 + \delta_4
\end{aligned}
$$

Now, let

$$R = R(S, S') = \prod_{i \in S} \prod_{j \in S'} (\alpha_i\beta_j - \alpha_j\beta_i)\,.$$

Then we can express the x_j^2 in terms of the $y_{S,S'}$ as follows. We only give the coefficient of one $y = y_{S,S'}$; the others can be found by symmetry. Note that R changes sign when we interchange S and S'; since the second factor in each of the expressions below does the same, the coefficient of y is well-defined.

Formula 10.3.

$$
\begin{aligned}
x_1^2 &= -\frac{1}{4\,R}(\sigma_1\tau_0 - \sigma_0\tau_1)\, y + \cdots \\
x_2^2 &= -\frac{1}{4\,R}(\sigma_3\tau_0 - \sigma_0\tau_3 + \sigma_2\tau_1 - \sigma_1\tau_2)\, y + \cdots \\
x_3^2 &= -\frac{1}{4\,R}(\sigma_3\tau_2 - \sigma_2\tau_3)\, y + \cdots \\
x_4^2 &= -\frac{1}{4\,R}(\sigma_1\sigma_3^2\tau_0^2\tau_2 - \sigma_0^2\sigma_2\tau_1\tau_3^2 + \sigma_1\sigma_2\tau_1\tau_2(\sigma_3\tau_0 - \sigma_0\tau_3) - \sigma_3\tau_3(\sigma_1\sigma_2\tau_0^2 - \sigma_0^2\tau_1\tau_2) \\
&\qquad - \sigma_1\tau_1(\sigma_2^2\tau_0\tau_3 - \sigma_0\sigma_3\tau_2^2) - \sigma_1^2\sigma_3\tau_0\tau_2^2 + \sigma_0\sigma_2^2\tau_1^2\tau_3 + 4\,\sigma_1\sigma_3\tau_1\tau_3(\sigma_1\tau_0 - \sigma_0\tau_1) \\
&\qquad + \sigma_2\tau_2(\sigma_1^2\tau_0\tau_3 - \sigma_0\sigma_3\tau_1^2) - \sigma_0\tau_0(\sigma_3^2\tau_1\tau_2 + \tau_3^2\sigma_1\sigma_2) \\
&\qquad + \sigma_0\tau_0(4\,\sigma_3\tau_3(\sigma_3\tau_0 - \sigma_0\tau_3) + 4\,\sigma_2\tau_2(\sigma_3\tau_2 - \sigma_2\tau_3) - 3\,\sigma_3\tau_3(\sigma_2\tau_1 - \sigma_1\tau_2)))\, y + \cdots
\end{aligned}
$$

Since R divides Δ, these formulas show that $4\Delta x_j^2$ is an integral linear combination of the $y_{S,S'}$ for each j. In a similar way, we get formulas for the mixed monomials $x_i x_j$. Together, these formulas prove Lemma 4.1.

Formula 10.4.

$$
\begin{aligned}
x_1x_2 &= -\frac{1}{4\,R}(\sigma_2\tau_0 - \sigma_0\tau_2)\, y + \cdots \\
x_1x_3 &= -\frac{1}{4\,R}(\sigma_3\tau_0 - \sigma_0\tau_3)\, y + \cdots \\
x_1x_4 &= -\frac{1}{4\,R}(-\sigma_1\tau_1(\sigma_3\tau_0 - \sigma_0\tau_3) - (\sigma_1^2\tau_0\tau_3 - \sigma_0\sigma_3\tau_1^2) - 2\,\sigma_0\tau_0(\sigma_3\tau_2 - \sigma_2\tau_3))\, y + \cdots \\
x_2x_3 &= -\frac{1}{4\,R}(\sigma_3\tau_1 - \sigma_1\tau_3)\, y + \cdots \\
x_2x_4 &= -\frac{1}{4\,R}(\sigma_3^2\tau_0^2 - \sigma_0^2\tau_3^2 - (\sigma_2\sigma_3\tau_0\tau_1 - \sigma_0\sigma_1\tau_2\tau_3) - (\sigma_1\sigma_3\tau_0\tau_2 - \sigma_0\sigma_2\tau_1\tau_3))\, y + \cdots \\
x_3x_4 &= -\frac{1}{4\,R}(-\sigma_2\tau_2(\sigma_3\tau_0 - \sigma_0\tau_3) + (\sigma_2^2\tau_0\tau_3 - \sigma_0\sigma_3\tau_2^2) - 2\,\sigma_3\tau_3(\sigma_1\tau_0 - \sigma_0\tau_1))\, y + \cdots
\end{aligned}
$$

For the three products of two of the $y_{S,S'}$ lying in the same nontrivial eigenspace in $\mathrm{Sym}^4 V$, we get the following relation. As a representative, we take the eigenspace of the character given by the Weil pairing with $t_{\{1,2\}}$.

Formula 10.5.

$$
\begin{aligned}
0 \quad = \quad & (\alpha_3\beta_4 - \alpha_4\beta_3)(\alpha_5\beta_6 - \alpha_6\beta_5)\, y_{\{1,3,4\},\{2,5,6\}} y_{\{1,5,6\},\{2,3,4\}} \\
& + (\alpha_3\beta_5 - \alpha_5\beta_3)(\alpha_6\beta_4 - \alpha_4\beta_6)\, y_{\{1,3,5\},\{2,4,6\}} y_{\{1,4,6\},\{2,3,5\}} \\
& + (\alpha_3\beta_6 - \alpha_6\beta_3)(\alpha_4\beta_5 - \alpha_5\beta_4)\, y_{\{1,3,6\},\{2,4,5\}} y_{\{1,4,5\},\{2,3,6\}}
\end{aligned}
$$

References

[1] *J.W.S. Cassels, E.V. Flynn:* Prolegomena to a middlebrow arithmetic of curves of genus 2, Cambridge University Pres, Cambridge, UK, 1996.
[2] *E.V. Flynn:* An explicit theory of heights, Trans. Amer. Math. Soc. **347** (1995), 3003–3015.
[3] *E.V. Flynn, N.P. Smart:* Canonical heights on the Jacobians of curves of genus 2 and the infinite descent, Acta Arith. **79**, 333-352 (1997).
[4] *W. Fulton, J. Harris:* Representation Theory, Springer GTM 129, 1991
[5] *S. Siksek:* Infinite descent on elliptic curves, Rocky Mountain J. Math. **25**, 1501–1538 (1995).

Max-Planck-Institut für Mathematik, Gottfried-Claren-Str. 26, D–53225 Bonn, Germany, Mathematisches Institut, Universitätsstr. 1, D–40225 Düsseldorf, Germany.

E-mail address: stoll@mpim-bonn.mpg.de, stoll@math.uni-duesseldorf.de