ACTA ARITHMETICA
XC.2 (1999)

On the height constant for curves of genus two

by

Michael Stoll (Düsseldorf)

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 straightforward 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, and a detailed description can be found in Section 11.

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 $\widehat{h}$ denote the corresponding canonical height on J. Assume for simplicity that $\mathbb{Q}$ is our base field. Then for every $P \in J(\mathbb{Q})$, we have

$$h_K(P) \le \widehat{h}(P) + \frac{1}{3}\sum_v \gamma_v$$

(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

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

where F is the polynomial used to define the curve. Together with some

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, rational torsion subgroup, canonical height.

This work forms part of the author's Habilitation in Düsseldorf.

estimate on γ_∞, which can also be got by our method, this yields an upper bound on $h_K - \widehat{h}$. We remark that it is (obviously!) not necessary to factor the discriminant to obtain this bound or even a slightly better one taking into account the content and the primitive part of F (cf. Cor. 8.1). (Note that $\gamma_v = \log c_v^{-1}$ in the notation of 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 after a section giving the relevant formulas, a description of the algorithm for determining the rational torsion subgroup closes the paper.

Acknowledgements. I wish to thank Bjorn Poonen for providing me with the motivation for this work and for many stimulating and fruitful discussions. I am indebted to Ed Schaefer for his many and useful comments on various versions of this paper.

The Max-Planck-Institut für Mathematik in Bonn has provided me with the opportunity to concentrate on my research during a six months' stay in 1998.

The computations leading to the formulas in Section 10 have been done using the Magma system for Computer Algebra [7].

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 negation map $P \mapsto -P$ 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 [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 negation, they descend to give morphisms on K.

The duplication map, δ, on K is given by four homogeneous polynomials $\delta_1, \delta_2, \delta_3, \delta_4 \in \mathcal{O}[x_1, x_2, x_3, x_4]$ 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 so will soon become apparent. Explicit expressions for these polynomials can be obtained from [6]. 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 [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 $\{i, j\}$ of $\{1, \dots, 6\}$, corresponding to divisors of F of degree two (see [1, p. 3]). 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

$$r(i, j) = \prod_{m\in\{i,j\}} \prod_{l\notin\{i,j\}} (\beta_l \alpha_m - \beta_m \alpha_l)$$

is the resultant of the factor of F corresponding to $\{i, j\}$ and 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

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

(with $c(t,t) = r(t)$), 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 $\mathrm{GL}(4,\overline{k})$, where $\overline{k}$ is some algebraic closure of k. We can, however, consider the subgroup

$$\widetilde{T} = \{\varrho M_t \mid t \in T,\ \varrho^4 = r(t)^{-2}\} \subset \mathrm{GL}(4,\overline{k}),$$

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

For a subring R of $\overline{k}$, we let V_R be the R-submodule of $R[x_1,x_2,x_3,x_4]$ freely generated by x_1,x_2,x_3,x_4.

4. The second representation. There is a group T' between $\widetilde{T}$ 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 $T' \to T$ is projection onto the second component, and the map $\widetilde{T} \to T'$ is given by $\varrho M_t \mapsto (\varrho^2 r(t), t)$. The group T' is elementary abelian of order 2^5, so there are sections $T \to T'$, but there is no canonical such section. The preimage in $\widetilde{T}$ 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 $\widetilde{T}$ on the space of homogeneous polynomials of degree two, which is $\mathrm{Sym}^2 V$. By the usual formulas, for its character ψ we get

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

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

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

Since T' is abelian, the representation has to split into one-dimensional irreducibles. Every partition of $\{1,\dots,6\}$ 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

$$\chi_{S,S'}(\varepsilon,0)=\varepsilon \quad\text{and}\quad \chi_{S,S'}(\varepsilon,t_{\{i,j\}})=\begin{cases}-\varepsilon & \text{if } \{i,j\}\subset S \text{ or } \{i,j\}\subset S',\\ \varepsilon & \text{otherwise.}\end{cases}$$

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. For a given partition $\{S,S'\}$, we will take $y_{S,S'}$ to be the specific polynomial given there. Let

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

(Note that Δ is a square root of the discriminant of F.) The action of $(\varepsilon,t)\in T'$ on $\operatorname{Sym}^2 V$ is given by that of ϱM_t, where $\varrho^2=\varepsilon/r(t)$. Since a scalar matrix $\alpha I\in \mathrm{GL}(4,\overline{k})$ acts as multiplication by α^2 on $\operatorname{Sym}^2 V$, the action of (ε,t) on $\operatorname{Sym}^2 V$ is $\varepsilon/r(t)$ times the action of M_t. Since $r(t)$ divides Δ, and since M_t has integral entries, the projection operator

$$\pi:\operatorname{Sym}^2 V\to\operatorname{Sym}^2 V,\qquad v\mapsto\frac{1}{\#T'}\sum_{\sigma\in T'}\chi_{S,S'}(\sigma)\sigma\cdot v,$$

onto the $\chi_{S,S'}$-eigenspace $k\cdot y_{S,S'}$ maps $2^5\Delta\operatorname{Sym}^2 V_{\mathcal{O}}$ into $\mathcal{O}\cdot y_{S,S'}$. Writing the identity homomorphism as the sum of all the 10 projection operators corresponding to the various partitions $\{S,S'\}$, we see that $2^5\Delta\operatorname{Sym}^2 V_{\mathcal{O}}$ is contained in the $\mathcal{O}$-module generated by the $y_{S,S'}$. (If we use a section $T\to T'$, we can reduce the factor 2^5 to 2^4.) If we do 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 $\widetilde{T}$ 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 $\widetilde{T}$, then on T')

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

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 non-trivial 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 10.2–10.5 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 non-zero 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*

$$c = \min_{(x_1:x_2:x_3:x_4) \in K(k)} \frac{\max\{|\delta_j(x_1, x_2, x_3, x_4)| \mid j = 1, 2, 3, 4\}}{(\max\{|x_1|, |x_2|, |x_3|, |x_4|\})^4}.$$

Then

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

P r o o f. Let $(x_1 : x_2 : x_3 : x_4) \in K(k)$ be some point. Consider the $y_{S,S'}$ evaluated at this set of homogeneous coordinates. By Lemma 5.2, we have

$$|y_{S,S'}(x_1, x_2, x_3, x_4)|^2 \leq \max_{1 \leq j \leq 4} |\delta_j(x_1, x_2, x_3, x_4)|$$

(note that $\delta_0(x_1, x_2, x_3, x_4) = 0$ 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

$$|2^2 \Delta| \cdot |x_j|^2 \leq \max_{\{S,S'\}} |y_{S,S'}(x_1, x_2, x_3, x_4)|.$$

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

$$|2^4 \operatorname{disc}(F)| \cdot (\max\{|x_1|, |x_2|, |x_3|, |x_4|\})^4 \leq \max_{1 \leq j \leq 4} |\delta_j(x_1, x_2, x_3, x_4)|,$$

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 $K(\overline{k})$.

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

$$c' = \max_{(x_1:x_2:x_3:x_4) \in K(k)} \frac{\max\{|\delta_j(x_1, x_2, x_3, x_4)| \mid j = 1, 2, 3, 4\}}{(\max\{|x_1|, |x_2|, |x_3|, |x_4|\})^4},$$

then $c' = 1$. We have $c' \leq 1$, since the δ_j have integral coefficients, and also $c' \geq 1$, since for $(x_1, x_2, x_3, x_4) = (0, 0, 0, 1)$, 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 use the usual archimedean triangle inequality.

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

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

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

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

We take (archimedean) absolute values to obtain

$$|x_i|^2 \le \sum_{\{S,S'\}} |a_{i,\{S,S'\}}| \cdot |y_{S,S'}| \quad \text{and} \quad |y_{S,S'}|^2 \le \sum_{j=0}^{4} |b_{\{S,S'\},j}| \cdot |\delta_j|.$$

This implies

$$\max_i |x_i|^4 \le \max_i \Bigg(\sum_{\{S,S'\}} |a_{i,\{S,S'\}}| \sqrt{\sum_{j=1}^{4} |b_{\{S,S'\},j}|} \Bigg)^2 \max_j |\delta_j|.$$

After dividing by $\max_j |\delta_j|$ and taking the maximum over the left-hand side, we get

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

The remaining parts of this section deal with non-archimedean fields. For such a field, 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 of the bound in Theorem 6.1 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 obtained 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. *In the situation of Theorem* 6.1, *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* $\{1,\dots,6\}$ *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 $\{1,\dots,6\}$, and let U' denote its complement. Write

$$\prod_{m\in U} (\beta_m X - \alpha_m Z) = A(X,Z) = a_0X^2 - a_1XZ + a_2Z^2,$$

$$\prod_{m\in U'}(\beta_m X-\alpha_m Z)=B(X,Z)$$
$$=b_0X^4-b_1X^3Z+b_2X^2Z^2-b_3XZ^3+b_4Z^4.$$

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. *Under the assumption that F splits completely over k, 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 $\{1,\dots,6\}$ into a two-element and a four-element subset.

If the polynomial F does not split completely over the field we are interested in, then we have to restrict to the 2-torsion points defined over k (there may be none) to get a lower bound on the height constant defined with respect to the k-rational points on K.

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. Recall the definition of the height on projective space:

$$H(x_1:\ldots:x_n)=\prod_v\max\{|x_1|_v,\dots,|x_n|_v\},$$

where v runs through the places of k and $|\cdot|_v$ is the normalised absolute value (multiplication by x multiplies volumes in k_v by $|x|_v$). Let $h_K=\log H_K$ denote the corresponding logarithmic height, and let finally $\widehat{h}$ denote the canonical height on J associated with h_K. Recall that this is defined as $\widehat{h}(P)=\lim_{n\to\infty}h_K(nP)/n^2$.

By Theorem 4 of [3], we have

$$h_K(P)\le\widehat{h}(P)+\frac{1}{3}\sum_v\log c_v^{-1}$$

for all $P\in J(k)$. Let $\mathfrak{l}$ be the content of F (i.e., the ideal generated by its coefficients), and let $N_{k/\mathbb{Q}}(\mathfrak{l})=\#\mathcal{O}_k/\mathfrak{l}$ denote its norm. Then we get the following global result. (In this section, $|\cdot|$ denotes the usual absolute value on $\mathbb{Q}$.)

COROLLARY 8.1. *For all points $P \in J(k)$, we have*

$$h_K(P) \le \widehat{h}(P) + \frac{4}{3}[k:\mathbb{Q}]\log 2 - 2\log N_{k/\mathbb{Q}}(\mathfrak{l}) + \frac{1}{3}\log|N_{k/\mathbb{Q}}(\mathrm{disc}(F))| + \frac{1}{3}\sum_{v|\infty}\log c_v^{-1}.$$

The local height constants c_v for the infinite places of k can be estimated using (7.1).

P r o o f. This follows from Proposition 7.1, the above-mentioned theorem of [3] and the definition of the height, taking into account the product formula for the absolute values on k. ∎

REMARK. Since the bounds on the local height constants are valid on algebraic points, a similar result holds for normalised heights of algebraic points—simply divide by the degree $[k:\mathbb{Q}]$.

In particular, taking $k = \mathbb{Q}$ for simplicity, we get the following bound for the naive height of a torsion point.

COROLLARY 8.2. *Let $P \in J(\mathbb{Q})$ be a torsion point. Then*

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

where λ is the content of F.

P r o o f. This is a special case of Corollary 8.1—torsion points have canonical height zero. ∎

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. See Section 11 for a detailed description of this algorithm.

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 indicate that the bound one gets with this method is usually worse than the bound given by our theorem (see the third example below). Another disadvantage is that the bound depends on the choice of a splitting of F as a product of three polynomials of degree two. Furthermore, as described in [2, 3], the method requires the knowledge of the bad primes, and one usually has to perform computations in algebraic extensions of $\mathbb{Q}_p$. (This is the reason why these bounds are given only for the last example—it has a canonical factorisation, and the computation involves only square roots.)

Here are some tables comparing the various bounds for the examples given in [3]. Recall that $\gamma_v = \log c_v^{-1}$ and that this is denoted $c_1^{(v)}$ in [3]. The last column in each table gives the lower bound on γ_p from Proposition 7.2. This is a lower bound for the height constant taken over all *algebraic* points. Hence it is not a contradiction if this entry is larger than the bound given in [3], since the latter refers to the *rational* points only. This lower bound gives an indication, however, of the best possible bound we can obtain with our method.

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

	[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 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: $Y^2 = X^5 + 16X^4 - 274X^3 + 817X^2 + 178X + 1$.

	[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 $\mathbb{Q}_{941}$, since γ_p is the maximum of numbers that are integral multiples of $\log p$. 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 $\gamma_\infty \geq 0.268$, and the real 2-torsion gives $\gamma_\infty \geq 0.2127$.

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

	[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 $\gamma_\infty \geq 12.963$; this value comes from the point $Q = (9 : -49 : 60 : -1180.8716\ldots) \in K(\mathbb{R})$. 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

$$P = \left\{ \left(\frac{-281 + \sqrt{12286}}{105}, \frac{-411296 - 4784\sqrt{12286}}{1157625} \right), \right.$$
$$\left. \left(\frac{-281 - \sqrt{12286}}{105}, \frac{-411296 + 4784\sqrt{12286}}{1157625} \right) \right\}$$

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 $\widehat{h}(P) = 4.007$, hence

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

which is larger than the bound 5.3237 given in [3].

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 Theorem 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 Theorem 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 bounds fail 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) generalise 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

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

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

Formula 10.1.

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

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

Formula 10.2.

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

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.

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

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.

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

$$x_3x_4 = -\frac{1}{4R}(-\sigma_2\tau_2(\sigma_3\tau_0-\sigma_0\tau_3)+(\sigma_2^2\tau_0\tau_3-\sigma_0\sigma_3\tau_2^2) \\ -2\sigma_3\tau_3(\sigma_1\tau_0-\sigma_0\tau_1))y+\dots$$

For the three products of two of the $y_{S,S'}$ lying in the same non-trivial 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.

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

11. An algorithm for determining the rational torsion subgroup. In this section, we give a more detailed description of the algorithm that has been rather tersely summarised at the end of Section 8. We will denote the multiplication-by-m map (on the Jacobian and on the Kummer surface) by $[m]$ in order to distinguish it from scalar multiplication of coordinates.

We assume that C is a curve of genus two over $\mathbb{Q}$, which is given by an equation

$$Y^2 = f(X) = F(X,1)$$

with F homogeneous of degree 6 and with integral coefficients. We want to determine the torsion subgroup T of $J(\mathbb{Q})$, where J is the Jacobian of C.

The first step is to choose a few odd primes p not dividing the discriminant of F (so that C and hence J have good reduction there) and to compute $\#J(\mathbb{F}_p)$ for each of these p. It is not our subject here to discuss ways of doing this, but since these primes are typically small, simply counting the points on C over $\mathbb{F}_p$ and over $\mathbb{F}_{p^2}$ will do in most cases. Then we can use the formula

$$\#J(\mathbb{F}_p) = \tfrac{1}{2}(\#C(\mathbb{F}_p)^2 + \#C(\mathbb{F}_{p^2})) - p$$

to find $\#J(\mathbb{F}_p)$.

Let g be the gcd of all these numbers. Then the order of T divides g.

Now T, being a finite abelian group, is the product of its various q-parts for all primes q. Since we know that $\#T$ divides g, only the primes q dividing g can occur. So we consider each prime divisor q of g in turn and determine the q-part T_q of T.

Among the primes considered in the first step, we choose some $p \neq q$ such that the q-adic valuation of $\#J(\mathbb{F}_p)$ is minimal. Let G be the q-part of $J(\mathbb{F}_p)$. We have the well-known exact sequence [1, §§ 7.3, 7.4]

$$0 \to J^1(\mathbb{Q}_p) \to J(\mathbb{Q}_p) \to J(\mathbb{F}_p) \to 0,$$

where $J^1(\mathbb{Q}_p)$ is the "kernel of reduction", which is a uniquely q-divisible group. This implies that there is a unique section $G \to J(\mathbb{Q}_p)$. Identifying

G and $J(\mathbb{Q})$ with their respective images in $J(\mathbb{Q}_p)$, we have $T_q = G \cap J(\mathbb{Q})$. Our task is therefore the following:

Find the subgroup of G consisting of points that lift to $J(\mathbb{Q})$ (together with their image in $J(\mathbb{Q})$).

Of course, we first need to find G explicitly. Since we know its order and its index in $J(\mathbb{F}_p)$, we can simply take random elements of $J(\mathbb{F}_p)$ and multiply them by the index to get something in G until the group generated by all the elements we have got in this way has the correct order.

We will now describe how to decide whether a point $P \in G$ lifts to $J(\mathbb{Q})$ or not (if it does, its image in $J(\mathbb{Q})$ is also determined). Afterwards, we will give a general algorithm that finds a subgroup in a finite q-group, given that we can check whether an element belongs to the subgroup or not.

In order to find out whether a point $P \in G$ lifts to $J(\mathbb{Q})$, we first have to lift it to $J(\mathbb{Q}_p)$ and then must decide whether this lifted point is in $J(\mathbb{Q})$. Let B be the bound given by Corollary 8.2, and let N' be the smallest integer such that $p^{N'} > 2B^2$. Then it is easy to check that the set of points $P \in \mathbb{P}^3(\mathbb{Q})$ with $H(P) \leq B$ is mapped injectively into $\mathbb{P}^3(\mathbb{Z}/p^{N'}\mathbb{Z})$. So all we have to do is to lift the given point to $J(\mathbb{Z}/p^{N'}\mathbb{Z})$, find its unique approximation of height $\leq B$ in $J(\mathbb{Q})$ (if it exists; if it does not, we are done) and check that this really is a torsion point of the correct order. In practice, we will take N to be the smallest integer such that $p^N > 2^6 B^2$. This will enable us to use the LLL algorithm to find the rational approximation of height $\leq B$ (we have to take into account that LLL produces small vectors with respect to the usual euclidean norm (requiring $2^3 B^2$ instead of $2B^2$) and that it does not necessarily give the smallest vector).

The following method for computing the lifting to $J(\mathbb{Z}/p^N\mathbb{Z})$ of the given torsion point $P \in G$ was suggested to me by Bjorn Poonen. The group $J(\mathbb{Q}_p)$ is a (p-adic) abelian Lie group. Therefore the differential of the multiplication-by-m map on $J(\mathbb{Q}_p)$ is simply scalar multiplication by m on the tangent space (the Lie algebra). Now let $Q \in J(\mathbb{Q}_p)$ be a torsion point of order m (prime to p), and let $\phi : J \to \mathbb{A}^n$ be a rational map defined over $\mathbb{Q}_p$ that is an immersion near Q. Suppose that a is an integer chosen so that p divides $1 + am$. Then for points Q' near Q, we have

$$\phi([1+am]Q') - \phi(Q) = (1+am)(\phi(Q') - \phi(Q)) + O((1+am)^2). \tag{11.1}$$

We want to take some standard affine patch of the map $J \to K \to \mathbb{P}^3$ as our ϕ. This means that we have to treat points P of order 2 separately, since K has singularities there. This is not a problem, since it is straightforward to determine $J(\mathbb{Q})[2]$ explicitly.

So let P have order $m \geq 3$. The following procedure will decide whether P lifts to $J(\mathbb{Q})$ or not. We take some standard affine patch of $\mathbb{P}^3$ which

contains the image of P on K and perform all computations in terms of these coordinates.

1. Choose $a \in \mathbb{Z}$ such that $M = 1 + am$ is divisible by p.
2. Let Q_0 be the image of P in $K(\mathbb{Z}/p\mathbb{Z})$ and set $r = 1$ and $n = 0$.
3. While $r < N$, repeat the following steps.
   3.1. Replace r by $\min\{2r, N\}$.
   3.2. Let Q'_n be some lifting of Q_n to $K(\mathbb{Z}/p^r\mathbb{Z})$.
   3.3. Set $Q_{n+1} = \frac{1}{M-1}(MQ'_n - [M]Q'_n)$.
   (An algorithm for computing the multiplication-by-M map on the Kummer surface is given in [3].)
   3.4. Replace n with $n + 1$.
   Since $p \mid M$, we deduce inductively from (11.1) that at the beginning of step 3.1, Q_n is the m-torsion point in $K(\mathbb{Z}/p^r\mathbb{Z})$ lifting Q_0.
4. Let $(q_1 : q_2 : q_3 : q_4)$ be representatives in $\mathbb{Z}$ of the projective coordinates of Q_n (we can choose some $q_j = 1$). Apply the LLL algorithm to find a small vector R' in the lattice generated by (q_1, q_2, q_3, q_4) and p^N times the standard basis of $\mathbb{Z}^4$. Let R be the point in $\mathbb{P}^3(\mathbb{Q})$ with projective coordinates R'. (By our choice of N, we know that R will be the unique point of height $\le B$ mapping to Q_n if such a point exists.)
5. If $R \notin K(\mathbb{Q})$ or $H(R) > B$, then return "No".
6. If $[m]R$ is not the origin of $K(\mathbb{Q})$ (i.e., the image of the origin on J), then return "No".
   Note that we can use the height bound B to stop this computation as soon as an intermediate result gets too big.
7. If R lifts to $J(\mathbb{Q})$ then return "Yes" and one of its preimages, otherwise return "No".
   (To decide whether R comes from a rational point on J boils down to checking if some expressions in the coordinates are rational squares or not.)

Now we can decide whether any given element $P \in G$ belongs to T or not. To find $G \cap T$ itself, we can use the following procedure.

1. Let $G_0 = G$, $T_0 = \{0\} \subset G$, and $S_0 = G_0 \setminus \{0\}$, $S'_0 = \{0\}$.
2. Set $n = 0$ and repeat the following steps until $S_n = \emptyset$.
   2.1. Let $g \in S_n$ be some (random) element and let $\widetilde{g} \in G$ be an element mapping to g. (It might be a good idea to choose g either primitive or of order q in G_n.)
   2.2. Using the algorithm above, find the smallest $m \ge 0$ such that $q^m \cdot \widetilde{g} \in T$. (Recall that G is a q-group.)

2.3. Set

$$\begin{aligned} T_{n+1} &= \langle T_n, q^m \cdot \widetilde{g} \rangle \\ &= \text{inverse image of } \langle q^m \cdot g \rangle \subset G_n \text{ in } G, \\ G_{n+1} &= G/T_{n+1} = G_n/\langle q^m \cdot g \rangle, \\ S'_{n+1} &= \text{image of } S'_n \cup \langle g \rangle \text{ in } G_{n+1}, \\ S_{n+1} &= G_{n+1} \setminus S'_{n+1}. \end{aligned}$$

2.4. Replace n with $n+1$.

(S_n and S'_n always define a partition of G_n. S'_n contains zero and the elements which are known not to be in T, so S_n contains the elements which we have still to check.)

3. Return T_n, which is the subgroup $T \cap G$. Generators of $T \cap G$ have been found on the way in step 2.3.

This algorithm has been implemented by the author as part of a forthcoming Magma package dealing with hyperelliptic curves and their Jacobians.

References

[1] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus 2*, Cambridge Univ. Press, Cambridge, 1996.

[2] E. V. Flynn, *An explicit theory of heights*, Trans. Amer. Math. Soc. 347 (1995), 3003–3015.

[3] E. V. Flynn and N. P. Smart, *Canonical heights on the Jacobians of curves of genus 2 and the infinite descent*, Acta Arith. 79 (1997), 333–352.

[4] W. Fulton and J. Harris, *Representation Theory*, Grad. Texts in Math. 129, Springer, 1991.

[5] S. Siksek, *Infinite descent on elliptic curves*, Rocky Mountain J. Math. 25 (1995), 1501–1538.

[6] *Kummer surface formulas*, ftp://ftp.liv.ac.uk/~ftp/pub/genus2/.

[7] *Magma homepage*, http://www.maths.usyd.edu.au:8000/u/magma/.

Mathematisches Institut
Universitätsstr. 1
D-40225 Düsseldorf, Germany
E-mail: stoll@math.uni-duesseldorf.de

Received on 29.10.1998
and in revised form on 10.3.1999 (3499)