ACTA ARITHMETICA
104.2 (2002)

On the height constant for curves of genus two, II

by

Michael Stoll (Bonn and Düsseldorf)

1. Introduction. When investigating the arithmetic of a curve and its Jacobian over the rationals (or a number field), it is often required to determine the canonical height of a point on the Jacobian. This is in particular necessary when one wants to find explicit generators of the Mordell–Weil group. It has been a routine matter for some time to compute heights on an elliptic curve. The obvious next step was to consider Jacobians of genus two curves. Flynn and Smart [2, 3] have developed the necessary theory, and they also present an algorithm for computing the canonical height. This algorithm avoids factorisation of integers, but it turns out to be impractical in certain cases. Since this observation was the starting point for the present paper, we give a short sketch of the difficulty.

Let C be a curve of genus two over $\mathbb{Q}$, and let J denote its Jacobian. We choose a point $P \in J(\mathbb{Q})$ and want to compute its canonical height with Flynn and Smart's algorithm. Its first step consists in finding a so-called "good multiple" nP of the given point, by computing $2P$, $3P$, and so on, until we find an n such that $\epsilon_p(nP) = 0$ for all finite primes p. Here, $\epsilon_p(P)$ is defined as follows. Let $x = (x_1, x_2, x_3, x_4)$ be projective coordinates for the image of $P \in J(\mathbb{Q})$ on the Kummer surface $K \subset \mathbb{P}^3$. Then (with the notation $v_p(x) = \min\{v_p(x_1), \ldots, v_p(x_4)\}$)

$$\epsilon_p(P) = v_p(\delta(x)) - 4v_p(x),$$

where v_p is the additive p-adic valuation (such that $v_p(p) = 1$) and where δ is the duplication map on K as defined in [1]; see Section 2 below.

Now take for example the curve given by the affine equation

$$y^2 = 4x^6 + 4x^5 + 3x^4 - 3x^3 - x - 6.$$

Let $\infty_\pm$ denote the two points at infinity (the sign corresponds to the sign of

2000 *Mathematics Subject Classification*: 11G30, 11G50, 11G20, 11G10, 14H45, 14H40, 14H25, 14Q05.

Key words and phrases: curves of genus two, Jacobians, local fields, number fields, canonical height, height constant, Mordell–Weil group.

y/x^3). Then we have rational points P and Q on the Jacobian, represented by the divisors $\infty_+ - \infty_-$ and $(-1,-1) - \infty_-$, respectively. When we try to find the canonical height of their sum $P+Q$, it turns out that the first "good multiple" is $60(P+Q)$. This means that we have to compute all points $n(P+Q)$, along with their doubles, up to $n = 60$. The largest point that occurs in this computation, which is $120(P+Q)$, has coordinates on the Kummer surface of more than 25000 decimal digits. It is therefore not very surprising that this computation requires an insufferable amount of time.

In this paper, we investigate the functions ϵ_p more closely. For this purpose, we replace our base field $\mathbb{Q}$ by some p-adic field (or, more generally, a non-archimedean local field of characteristic different from 2) k with additive valuation v. We define the function ϵ on $J(k)$ as above by

$$\epsilon(P) = v(\delta(x)) - 4v(x),$$

where $x = (x_1, x_2, x_3, x_4)$ is some set of Kummer coordinates of P (meaning projective coordinates for the image of P on K). Our main result is the following.

Theorem 1.1. *Let $U = \{P \in J(k) \mid \epsilon(P) = 0\}$. Then U is a subgroup of finite index in $J(k)$, and $\epsilon(P)$ depends only on the coset of P mod U.*

The first part proves that Flynn and Smart's algorithm is correct. Both statements together lead to an improved algorithm for the height computation.

In the first paper of this series [7], we used representation theory to obtain general bounds on the height constant

$$\gamma = \max_{P \in J(k)} \epsilon(P),$$

in terms of the discriminant of the curve. As a by-product of the results derived in the present paper, we can get considerable improvements in bounding γ. This can be applied in order to find generators of the Mordell–Weil group of the Jacobian of a genus two curve over $\mathbb{Q}$. We discuss this in some detail in Section 7; two examples (of ranks 7 and 12, respectively) are given to demonstrate the method.

It should be noted that similar results hold for elliptic curves. See for example Siksek [5], where this approach is used to get good bounds for the height constant.

Acknowledgements. I wish to thank the anonymous referee for making some useful suggestions. The example given above of the point with the large good multiple was communicated to me by Colin Stahlke.

The computations involved in the proof of Proposition 3.1 have been done using the MAGMA system for Computer Algebra [10].

2. Basics. Let k be an arbitrary field. Let $F \in k[X,Z]$ be homogeneous of degree 6 ($F = 0$ is allowed). We write

$$\begin{aligned} &F(X,Z) \\ &\quad = f_6X^6 + f_5X^5Z + f_4X^4Z^2 + f_3X^3Z^3 + f_2X^2Z^4 + f_1XZ^5 + f_0Z^6. \end{aligned}$$

In Cassels and Flynn [1], which is our basic reference for the following, the authors define surfaces $J \subset \mathbb{P}^{15}$ and $K \subset \mathbb{P}^3$ associated to such a polynomial F. (Cassels and Flynn require F to have no multiple factors. However, their definitions still make sense for arbitrary polynomials as above.) The latter is defined by a quartic equation $\kappa = 0$. There are homogeneous polynomials $\delta = (\delta_1, \delta_2, \delta_3, \delta_4)$ of degree 4 such that $\delta(x)$ is again a point on K if $x = (x_1, x_2, x_3, x_4) \in K$ and $\delta(x) \neq 0$. (Here and in the following, 0 is used as a shorthand for the origin of affine space.) Furthermore, there are biquadratic forms B_{ij} ($i, j \in \{1,2,3,4\}$) in two sets of four homogeneous variables such that if $x = (x_1, x_2, x_3, x_4)$ and $y = (y_1, y_2, y_3, y_4)$ are points on K and if some B_{ij} is non-zero, then there are homogeneous coordinates $w = (w_1, w_2, w_3, w_4)$ and $z = (z_1, z_2, z_3, z_4)$ (which are uniquely determined up to scaling and interchanging w and z) such that $w_iz_i = B_{ii}(x,y)$ and $w_iz_j + w_jz_i = 2B_{ij}(x,y)$ for all $i,j \in \{1,2,3,4\}$. Furthermore, the points w and z are again on K. If x and y are defined over k, then w and z are either defined over k or over a quadratic extension of k and conjugate. (Explicit expressions for all these polynomials can be obtained from [9].)

When F has no multiple factors, we define $f(X) = F(X,1)$. Then the affine equation

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

defines a curve of genus two, and we let C be its smooth projective model over k. Then J as defined above is 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; it is the same as K defined above. Since multiplication by 2 on J commutes with negation, it descends to give a morphism on K. This duplication map on K is given by the polynomials δ. The addition map itself cannot be defined on the Kummer surface, since we cannot distinguish between $P+Q$ and $P-Q$. But the unordered pair $\{P+Q, P-Q\}$ is defined. The biquadratic forms B_{ij} do not all vanish when evaluated on two sets of homogeneous coordinates for points on K, and the coordinates w and z defined above correspond to the points $P+Q$ and $P-Q$ if the coordinates x and y correspond to P and Q.

In order to simplify notation, we write B for the 4-by-4 matrix with diagonal entries B_{ii} and other entries $2B_{ij}$.

3. Some applied computer algebra. In this section, we will sketch a proof of the following result.

Proposition 3.1. *Let k be an arbitrary field, and let $F \in k[X,Z]$ be homogeneous of degree 6 ($F = 0$ is allowed). Consider the objects K, δ, B defined above with respect to F.*

(1) *Let $x = (x_1, x_2, x_3, x_4)$ be homogeneous coordinates of a point on K. Then if $\delta(\delta(x)) = 0$, we must already have $\delta(x) = 0$.*

(2) *Let $x = (x_1, x_2, x_3, x_4)$ and $y = (y_1, y_2, y_3, y_4)$ be homogeneous coordinates of points on K. Then if $B(x,y) = 0$, we have $\delta(x) = \delta(y) = 0$.*

Note that the expression "homogeneous coordinates" is meant to include the assertion that the coordinates do not all vanish.

We will apply this result to the reduction mod p of the model K of the Kummer surface associated to a given model of a genus two curve. Since we do not want to put restrictions on this reduction, we need the full generality of this result.

In principle, we can prove these assertions working generically, i.e., by replacing k with the ring $\mathbb{Z}[f] = \mathbb{Z}[f_0, \ldots, f_6]$, where the f_j are the coefficients of F, which are taken to be independent indeterminates. Let $\sqrt{I}$ denote the radical of an ideal I. Then we have to show that

$$\delta_1(x), \delta_2(x), \delta_3(x), \delta_4(x) \in \sqrt{(\kappa(x), \delta(\delta(x)))} \tag{3.1}$$

in the polynomial ring $\mathbb{Z}[f, x]$ and that

$$\delta_j(x) x_r y_s \in \sqrt{(\kappa(x), \kappa(y), B(x,y))} \tag{3.2}$$

in the polynomial ring $\mathbb{Z}[f, x, y]$, for all $j, r, s \in \{1, 2, 3, 4\}$ (we need not also check the corresponding statement for $\delta_j(y) x_r y_s$ for reasons of symmetry).

Using MAGMA [10], we have indeed succeeded in proving the proposition in this way in the special case that k has characteristic 2 (with $\mathbb{Z}$ replaced by $\mathbb{F}_2$ in the above). This task is simplified by the fact that $\delta_1 = \delta_2 = \delta_3 = 0$ on K, and that δ_4, κ, B_{ii} are all squares (the B_{ij} with $i \neq j$ do not come into play since they are multiplied by 2). The general case, however, is far too complex to be attacked in this way (we did not succeed even with $\mathbb{F}_3$ in place of $\mathbb{Z}$). Hence we must look for simplifications.

The statement is geometric in nature, therefore we can assume that the field k is algebraically closed. When we act on F by a (non-singular) linear transformation of the variables X and Z, we get an isomorphism between the "Kummer surfaces" associated to the old and to the new F, together with their additional structure. This means that we only need to consider one polynomial F in each orbit of the homogeneous polynomials of degree 6 under $\mathrm{GL}_2(k)$. We can choose the following representatives:

$$\begin{gathered} 0, \quad Z^6, \quad XZ^5, \quad X^2Z^4, \quad X^3Z^3, \quad X(X-Z)Z^4, \\ X^2(X-Z)Z^3, \quad X^2(X-Z)^2Z^2, \quad X(X-Z)(X-aZ)Z^3, \\ X^2(X-Z)(X-aZ)Z^2, \quad X(X-Z)(X-aZ)(X-bZ)Z^2 \end{gathered}$$

with $a, b \in k\backslash\{0,1\}$ distinct. We have left out representatives for the orbits of polynomials without multiple factors, since in this case the claim is trivially true (we are in the situation of a genuine Jacobian and Kummer surface, hence δ and B never vanish at points on K).

We now go back and use the ring $\mathbb{Z}[1/2]$ (or $\mathbb{Z}[1/2, a]$ or $\mathbb{Z}[1/2, a, b]$) as the base and prove assertions (3.1) and (3.2). We do not give full details here, which would make for very dull reading, but we sketch a few of the cases to give an impression of the arguments involved, which are fairly elementary.

Case 1: $F = 0$. We have $\delta_4 = x_4^4$ and $\delta_j = 4x_j x_4^3$ for $j \in \{1, 2, 3\}$. Hence $\delta = 0 \Leftrightarrow x_4 = 0 \Leftrightarrow \delta_4 = 0$. This already implies assertion (1). We also have $B_{44}(x, y) = x_4^2 y_4^2$. If (for example) $x_4 = 0$, we see upon substitution into B that we must have either $y_4 = 0$ also (which implies that $\delta(x) = \delta(y) = 0$) or $x = 0$, which is excluded.

Case 2: $F = X(X-Z)Z^4$. We have again $\delta_4 = x_4^4$. The Kummer surface equation is $\kappa = x_1^4 + x_4 R$ with some polynomial R. Hence $x_4 = 0$ implies $x_1 = 0$ for a point on K. If $x_1 = x_4 = 0$, then all δ_j vanish. This means that we again have $\delta = 0 \Leftrightarrow x_4 = 0 \Leftrightarrow \delta_4 = 0$. We also have $B_{44}(x, y) = x_4^2 y_4^2$, and the argument can be finished as in Case 1.

Case 3: $F = X(X - Z)(X - aZ)Z^3$ (with $a \notin \{0, 1\}$). We have $\delta_1(x) = 4x_1x_4(x_1 - x_4)(ax_1 - x_4)$ and $\delta_4(x) = (ax_1^2 - x_4^2)^2$. If both vanish, then $x_1 = x_4 = 0$, which implies that all δ_j vanish. Hence $\delta = 0 \Leftrightarrow x_1 = x_4 = 0 \Leftrightarrow \delta_1 = \delta_4 = 0$, which implies assertion (1).

Similarly, $B_{11}(x, y) = (x_1y_4 - x_4y_1)^2$ and $B_{44}(x, y) = (ax_1y_1 - x_4y_4)^2$. If we assume that $x_1 = 0$, we see that $B(x, y) = 0$ implies $x_4 = 0$ or $y_1 = y_4 = 0$. By symmetry, we can assume $x_1 = x_4 = 0$. This already implies $\delta(x) = 0$.

Setting $x_1 = x_4 = 0$ in B, we find that $B_{22} = (x_2y_4 - x_3y_1)^2$ and that $B_{33} = (ax_2y_1 - x_3y_4)^2$. If $y_1 = 0$, then also $y_4 = 0$ and $\delta(y) = 0$. Otherwise, we can assume $y_1 = 1$ and so $x_3 = x_2y_4$. Then from B_{23}, we must have either $y_4 \in \{0, 1, a\}$ or $x_2 = 0$, and from B_{33}, we must have either $y_4^2 = a$ or $x_2 = 0$. Since $a \notin \{0, 1\}$, the conditions on y_4 are incompatible, and we must have $x_2 = 0$, hence $x = 0$, a contradiction.

Now assume that $x_1 \neq 0$, so without loss of generality $x_1 = 1$ and hence $y_4 = x_4y_1$. From B_{14}, we get $x_4 \in \{0, 1, a\}$ or $y_1 = 0$, and from B_{44}, we have $x_4^2 = a$ or $y_1 = 0$. Hence $y_1 = 0$, and after interchanging x and y, we are in a situation already considered.

Arguing in a similar manner, we obtain Table 1. It lists for each of our chosen representative polynomials two conditions ("Cond. 1" and "Cond. 2") that are each equivalent to $\delta(x) = 0$ for a point x on K. A point in $\mathbb{P}^3$ satisfying Condition 2 is on K if and only if it also satisfies the condition listed under the heading "Additional".

Table 1. Conditions for the vanishing of $\delta(x)$

No.	F	Cond. 1	Cond. 2	Additional
1	0	$\delta_4 = 0$	$x_4 = 0$	
2	Z^6	$\delta_4 = 0$	$x_4 = 0$	
3	XZ^5	$\delta_4 = 0$	$x_4 = 0$	$x_1 = 0$
4	X^2Z^4	$\delta_4 = 0$	$x_4 = 0$	
5	X^3Z^3	$\delta_4 = 0$	$x_4 = 0$	$x_1x_3 = 0$
6	$X(X-Z)Z^4$	$\delta_4 = 0$	$x_4 = 0$	$x_1 = 0$
7	$X^2(X-Z)Z^3$	$\delta_4 = 0$	$x_4 = 0$	$x_1x_3 = 0$
8	$X^2(X-Z)^2Z^2$	$\delta_4 = 0$	$x_4 = 0$	
9	$X(X-Z)(X-aZ)Z^3$	$\delta_1 = \delta_4 = 0$	$x_1 = x_4 = 0$	
10	$X^2(X-Z)(X-aZ)Z^2$	$\delta_4 = 0$	$x_4 = 0$	$x_1x_3 = 0$
11	$X(X-Z)(X-aZ)(X-bZ)Z^2$	$\delta_1 = \delta_4 = 0$	$x_1 = x_4 = 0$	

The fact that Condition 1 can be obtained from Condition 2 by replacing x_j with δ_j amounts to a proof of statement (1) in Proposition 3.1.

This completes the sketch of the proof. For the applications, we will also need the following somewhat technical lemma.

Lemma 3.2. *Let $x = (x_1, x_2, x_3, x_4)$ and $y = (y_1, y_2, y_3, y_4)$ be homogeneous coordinates for points on K and suppose that $B(x, y) \neq 0$. Let $w = (w_1, w_2, w_3, w_4)$ and $z = (z_1, z_2, z_3, z_4)$ be homogeneous coordinates such that $w_iz_i = B_{ii}(x, y)$ and $w_iz_j + w_jz_i = 2B_{ij}(x, y)$ for all $i, j \in \{1, 2, 3, 4\}$. Then $B_{ii}(\delta(x), \delta(y)) = \delta_i(w)\delta_i(z)$ and $2B_{ij}(\delta(x), \delta(y)) = \delta_i(w)\delta_j(z) + \delta_j(w)\delta_i(z)$ for all $i, j \in \{1, 2, 3, 4\}$.*

Proof. We can treat this generically—we assume the coefficients of F to be independent indeterminates. Then K is the Kummer surface of a Jacobian, and from $2(P \pm Q) = (2P) \pm (2Q)$, we see that the set of equalities must hold at least projectively. The expressions $\delta_i(w)\delta_i(z)$ and $\delta_i(w)\delta_j(z) + \delta_j(w)\delta_i(z)$ are bihomogeneous of bidegree $(4, 4)$ and symmetric in w and z, therefore they can be expressed in terms of $B(x, y)$. This gives bihomogeneous polynomials in x and y of bidegree $(8, 8)$. Since $B(\delta(x), \delta(y))$ is also given by bihomogeneous polynomials of bidegree $(8, 8)$, the constant of projectivity must be in the base field, i.e., independent of x and y. Specialising both points to the origin $(0 : 0 : 0 : 1)$, we see that the constant is 1. ∎

4. The main result. We will now deduce the main result of this paper. We let k be a non-archimedean local field with $\mathrm{char}(k) \neq 2$. We denote by v the additive valuation on k (normalised to have image $\mathbb{Z}$) and by $\mathcal{O} = \{\alpha \in k \mid v(\alpha) \geq 0\}$ the valuation ring. We assume that F is in $\mathcal{O}[X, Z]$ and has no multiple factors. Hence J is an abelian surface, the Jacobian of the curve defined by F. We define the map $\epsilon : J(k) \to \mathbb{Z}$ by

$$\epsilon(P) = v(\delta(x)) - 4v(x),$$

where (as always) x is a set of homogeneous coordinates for the image of P on the Kummer surface K. It is clear that this does not depend on the homogeneous coordinates chosen. Since the coefficients of the δ_j are polynomials with integral coefficients in the coefficients of F, we always have $\epsilon(P) \geq 0$.

With this definition, our result is the following.

THEOREM 4.1. *Let $U = \{P \in J(k) \mid \epsilon(P) = 0\}$. Then U is a subgroup* (*of finite index*) *in $J(k)$, and ϵ factors through $J(k)/U$. Furthermore, $\epsilon(P) = \epsilon(-P)$.*

The subgroup is of finite index since it contains the kernel of reduction with respect to the given model (cf. [1, §7.5]). That ϵ vanishes on the kernel of reduction can be seen as follows. If $P \in K$ reduces to $\widetilde{P} = (0 : 0 : 0 : 1)$ mod p, then we have $\widetilde{\delta(P)} = \delta(\widetilde{P}) = (0 : 0 : 0 : 1)$, and so $v(\delta(x)) = v(x) = 0$ for suitably chosen projective coordinates x of P. The last statement is clear, since ϵ is defined via the Kummer surface, which does not distinguish between P and $-P$.

We note that this result is an immediate corollary of the following proposition.

PROPOSITION 4.2. *Let P, Q be points in $J(k)$. Then $\epsilon(P) = 0$ implies that $\epsilon(P + Q) = \epsilon(Q)$.*

Proof. We first note the following simple fact:

$$\min\{v(a_i b_i), v(a_i b_j + a_j b_i) \mid i, j \in \{1, 2, 3, 4\}\} = v(a) + v(b). \tag{4.1}$$

Let P, Q be two points on $J(k)$ and let x, y be homogeneous coordinates for their images on K. Then we define

$$\epsilon(P, Q) = v(B(x, y)) - 2v(x) - 2v(y).$$

Lemma 3.2 and the simple fact (4.1) together imply that

$$\epsilon(2P, 2Q) + 2\epsilon(P) + 2\epsilon(Q) = \epsilon(P + Q) + \epsilon(P - Q) + 4\epsilon(P, Q). \tag{4.2}$$

If we choose homogeneous coordinates that are normalised in such a way that they are in $\mathcal{O}$ with one of them being a unit, then we see by applying Proposition 3.1 to the reductions $\widetilde{P}, \widetilde{Q} \in J(\widetilde{k})$, where $\widetilde{k}$ is the residue field of k, that for all points $P, Q \in J(k)$, $\epsilon(P) = 0$ implies $\epsilon(2P) = 0$ and $\epsilon(P, Q) = 0$. If we plug this into equation (4.2), we see that $\epsilon(P) = 0$ implies

$$2\epsilon(Q) = \epsilon(P + Q) + \epsilon(P - Q) = \epsilon(Q + P) + \epsilon(Q - P) \tag{4.3}$$

for all points Q. Let $a_n = \epsilon(Q + nP)$ (for $n \in \mathbb{Z}$). Replacing Q in (4.3) by $Q + nP$, we obtain the recurrence relation $2a_n = a_{n+1} + a_{n-1}$ for all

$n \in \mathbb{Z}$. Its solutions are of the form $a_n = \alpha + \beta n$. Since ϵ takes on only non-negative values, β must be zero, hence $a_n = \alpha$ is constant. In particular, $\epsilon(P+Q) = a_1 = a_0 = \epsilon(Q)$. ∎

5. Improvement of the height constant. We can use the explicit results of Section 3 to improve the bound on the local height constant $\gamma = \max_{P \in J(k)} \epsilon(P)$. In [7], it was shown that $\gamma \le v(2^4 \operatorname{disc}(F))$, and some possible improvements were discussed. The main disadvantages of the approach followed there are that it always produces a bound that is valid for all *algebraic* points on the *Kummer surface*. But we only need a bound that is valid for all *k-rational* points on the *Jacobian* itself. It is obvious that there is room for improvement here. The following result shows that we can indeed gain something in many cases.

We first remark that a point $x = (x_1, x_2, x_3, x_4)$ on K can lift to J only if the following two expressions are squares in k:

$$\begin{aligned} s_1(x) &= x_1^3 x_4 + f_2 x_1^4 + f_3 x_1^3 x_2 + f_4 x_1^2 x_2^2 \\ &\quad + f_5 x_1 x_2 (x_2^2 - x_1 x_3) + f_6 (x_2^2 - x_1 x_3)^2, \end{aligned} \tag{5.1}$$

$$s_2(x) = x_1^2 x_3 x_4 + f_0 x_1^4 + f_4 x_1^2 x_3^2 + f_5 x_1 x_2 x_3^2 + f_6 x_2^2 x_3^2. \tag{5.2}$$

(Generically, s_1 and s_2 are the squares of the coefficients a and b in the equation $y = ax + b$ of the line joining the two points on the curve that represent a corresponding point on J. We therefore get an equivalence when we have two affine points. If one or both of the points are at infinity, we get a weaker condition.)

Lemma 5.1. *Let k be a p-adic field, $f_0, \ldots, f_6, x_1, x_2, x_3, x_4 \in \mathcal{O}$ and assume that $v(x) = 0$, where v is the normalised additive valuation on k. Then the following set of conditions is contradictory*:

(i) $v(f_6) = 1$, $v(f_5) \ge 1$;
(ii) $v(x_1) \ge 1$, $v(x_4) \ge 1$;
(iii) *the expressions $s_1(x)$ and $s_2(x)$ are squares in k.*

Proof. We assume (i) and (ii) hold and derive a contradiction to (iii).

Let $v_j = v(x_j)$. We must have $v_2 = 0$ or $v_3 = 0$. In the first case, all terms but the last one in $s_1(x)$ have valuation at least 2, whereas the last term has valuation 1. Hence $v(s_1(x)) = 1$, and $s_1(x)$ cannot be a square.

In the second case, let us first assume that $v_1 \le v_2$. Then all terms but the last one in $s_1(x)$ have valuation at least $3v_1 + 1$, whereas the last term has valuation $2v_1 + 1$. Hence $v(s_1(x)) = 2v_1 + 1$ is again odd, and $s_1(x)$ cannot be a square.

Finally, assume that $v_1 > v_2$. Then all terms but the last one in $s_2(x)$ have valuation at least $2v_2 + 2$, whereas the last term has valuation $2v_2 + 1$. Hence $v(s_2(x)) = 2v_2 + 1$ is odd, and $s_2(x)$ cannot be a square. ∎

This implies the following improvement in the bound for γ.

Proposition 5.2. *Assume that the residue characteristic of k is odd and that the reduction of F factors as hl^m with h non-constant and square-free, and l linear and not dividing h. Suppose further that the model of the curve given by F is regular. Then the local height constant γ vanishes* (*i.e.*, $U = J(k)$ *in the notation of Theorem* 4.1).

Proof. Since the assumptions are unaffected when we replace k with its maximal unramified extension k^{nr}, we can assume that $k = k^{\mathrm{nr}}$. The assumption on F means that the reduction of F falls into the GL_2-orbit of one of cases 3, 6, 9 or 11 in Table 1 (unless F has square-free reduction, in which case the claim holds trivially). Since the residue field of k^{nr} is algebraically closed, we can invoke a suitable automorphism of $\mathbb{P}^1_{\mathcal{O}_k}$ in order to transform the reduction of F into the given representative. In all these cases, a point P on $J(k^{\mathrm{nr}})$ with $\epsilon(P) > 0$ would have image on K satisfying the contradictory conditions (i)–(iii) in the lemma above. The regularity implies condition (i), from Table 1 we get condition (ii), and condition (iii) is satisfied because the point lifts to $J(k^{\mathrm{nr}})$. ■

Remark. The assumptions in Proposition 5.2 are certainly satisfied when the residue characteristic p is odd and $v(\operatorname{disc} F) = 1$. This shows that for a "generic" curve over $\mathbb{Q}$, most of the bad primes will not cause trouble (especially the large ones), since one would expect its discriminant to have only a few (and small) multiple prime factors.

More generally, when p is odd, the regularity assumption means that $v(\operatorname{disc} F) = m - 1$ in the notation of Proposition 5.2.

Example. We consider the curve

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

The discriminant of the polynomial on the right hand side factors as $191^2 \cdot 941^4$. It turns out that the bounds $\gamma_2 \le 4$ and $\gamma_{191} \le 2$ given by [7] are sharp. At 941, however, we can improve on the bounds $\gamma_{941} \le 4$ or $\gamma_{941} \le 2$ (which is the improved bound from [7] or the bound from [3] that was obtained by looking at the $\mathbb{Q}_{941}$-rational points on K). Indeed, modulo 941, the polynomial (in homogeneous form) factors as $Z(X-185Z)^5$. Since $v_{941}(\operatorname{disc} F) = 4$, the model must be regular. Hence our result shows that in fact $\gamma_{941} = 0$. This means that the bound for the difference between the (logarithmic) naive and canonical heights on $J(\mathbb{Q})$ can be reduced to 5.84704 (using the height constant at infinity as given by [7]) or even to 4.6 (if we are willing to accept a numerical estimate of the height constant at infinity). We will return to this example at the end of the paper, where we will determine the Mordell–Weil group.

In general, we can try to find γ exactly by searching through the points in $K(k)$ that lift to $J(k)$, in a similar way to the program mentioned in [3]. Table 1 tells us where to start off the search.

6. An improved canonical height algorithm. For definiteness, we let $k = \mathbb{Q}$ in this section. Everything can be done for a general number field as well, but the additional complexities would tend to obscure the main point. We assume that F has coefficients in $\mathbb{Z}$ and no multiple factors. Given a point $P \in J(\mathbb{Q})$ and a set (x_1, x_2, x_3, x_4) of homogeneous coordinates for its image on K, we define its (logarithmic) *naive height* to be

$$h(P) = \sum_v \max\{\log|x_1|_v, \log|x_2|_v, \log|x_3|_v, \log|x_4|_v\},$$

where the sum is over the places of $\mathbb{Q}$, and $|\cdot|_v$ are the corresponding absolute values, normalised in such a way that $|p|_p = p^{-1}$ at a finite place $v = p$ and such that $|\cdot|_\infty$ is the usual archimedean absolute value. By the usual product formula, $h(P)$ does not depend on the specific set of coordinates chosen.

The *canonical height* of P is then

$$\widehat{h}(P) = \lim_{n\to\infty} \frac{h(nP)}{n^2} = \lim_{n\to\infty} 4^{-n} h(2^n P).$$

For a prime p, we denote by ϵ_p the map from $J(\mathbb{Q})$ to $\mathbb{Z}$ obtained by first going from $J(\mathbb{Q})$ into $J(\mathbb{Q}_p)$ and then using the ϵ map defined in the previous section. Similarly, we let

$$\epsilon_\infty(P) = \log\max\{|\delta_j(x)| \mid j \in \{1,2,3,4\}\} - 4\log\max\{|x_1|, |x_2|, |x_3|, |x_4|\},$$

where again (x_1, x_2, x_3, x_4) are homogeneous coordinates for the image of P on K.

From these definitions, we have immediately

$$h(2P) = 4h(P) + \epsilon_\infty(P) - \sum_p \epsilon_p(P)\log p.$$

Hence

$$\widehat{h}(P) = h(P) + \sum_{n=0}^{\infty} 4^{-n-1}\epsilon_\infty(2^n P) - \sum_p (\log p) \sum_{n=0}^{\infty} 4^{-n-1}\epsilon_p(2^n P). \tag{6.1}$$

Flynn and Smart [3] propose the following algorithm for the computation of $\widehat{h}(P)$.

1. Find an $m \geq 1$ such that $\epsilon_p(mP) = 0$ for all p.
2. Compute $\widehat{h}(mP)$ as $h(mP) + \sum_{n=0}^{\infty} 4^{-n-1}\epsilon_\infty(2^n mP)$.
3. Return $\widehat{h}(P) = \widehat{h}(mP)/m^2$.

Note that the condition in step 1 can be checked as follows. Choose Kummer coordinates x for P in such a way that they are relatively prime integers. Then $\epsilon_p(P) = 0$ for all p is equivalent to the $\delta_j(x)$ being relatively prime. In particular, no factorisation is required. The sum in step 2 can be cut off as soon as the precision is high enough (which can be checked when one has a bound on $|\epsilon_\infty|$). The terms in the sum can be computed using floating-point arithmetic by repeated application of δ.

For this algorithm to work it is necessary that $\epsilon_p(2P) = 0$ if $\epsilon_p(P) = 0$ (otherwise we could miss some terms $\epsilon_p(2^n mP)$). Flynn and Smart do not prove this (they seem to have overlooked the necessity). It is, however, an immediate consequence of our theorem. Hence the algorithm is correct.

There are several examples for which the algorithm in this form turns out to be impractical. This is the case when the number m that has to be found in step 1 is large. The length of the coordinates of mP grows roughly as m^2—the numbers grow very big even for fairly moderate values of m, and it takes a very long time to compute these numbers; compare the example given in the introduction. We therefore propose some improvements to the canonical height algorithm that will cut down the number of multiples of P that have to be computed.

Let us consider one prime p. We let $U_p = \{P \in J(\mathbb{Q}) \mid \epsilon_p(P) = 0\}$. Let $P \in J(\mathbb{Q})$ be some point. We know that U_p is a subgroup of finite index in $J(\mathbb{Q})$, hence there is a smallest $m \geq 1$ such that $mP \in U_p$. By Theorem 4.1, $\epsilon_p(nP)$ then only depends on n mod m. When we compute the multiples of P up to mP, we therefore construct a table of these values. Write $m = 2^r s$ with s odd and let t be the order of 2 in the group $(\mathbb{Z}/s\mathbb{Z})^\times$. Then we have $\epsilon_p(2^{n+t}P) = \epsilon_p(2^n P)$ as soon as $n \geq r$. This means that we can write the p-part on the right hand side of (6.1) as a finite number of terms plus a finite number of geometric series. Namely,

$$(6.2)\quad \sum_{n=0}^{\infty} 4^{-n-1}\epsilon_p(2^n P) = \sum_{n=0}^{r-1} 4^{-n-1}\epsilon_p(2^n P) + \frac{4^{-r-1}}{1-4^{-t}} \sum_{n=0}^{t-1} 4^{-n}\epsilon_p(2^{r+n}P).$$

This allows us to find this p-part exactly.

Now let $P \in J(\mathbb{Q})$ be some point and choose Kummer coordinates x that are relatively prime integers. Let $a = \gcd(\delta(x))$ (with the obvious notational shortcut). Then $\epsilon_p(P) = v_p(a)$ (where v_p is the normalised p-adic valuation). Therefore, if p does not divide a, then the p-part in the canonical height is zero. We get the relevant primes by factoring a (which can be a costly operation in principle, but see the discussion below).

This leads to the following algorithm. Let $P \in J(\mathbb{Q})$.

1. Choose Kummer coordinates x for P that are relatively prime integers. Compute $a = \gcd(\delta(x))$. Let S be the set of prime divisors of a. For each prime $p \in S$, begin a table T_p with the pairs $(0, 0)$ and $(1, v_p(a))$. Let $m = 1$ and $S' = S$.

2. While S' is non-empty, do the following. Increase m by 1 and compute mP. Choose Kummer coordinates x for mP as above and let $a = \gcd(\delta(x))$. For each prime $p \in S'$, do the following. If $p \nmid a$, let $m_p = m$ and remove p from S'. Otherwise, add the pair $(m, v_p(a))$ to the table T_p.
3. For each prime $p \in S$, compute the sum in (6.2), where $r = v_2(m_p)$, t is the order of 2 in $(\mathbb{Z}/s\mathbb{Z})^\times$ with $s = 2^{-r}m_p$, and we can compute $\epsilon_p(2^nP)$ as the number associated to $2^n \bmod m_p$ in the table T_p. Call the sum s_p.
4. Compute $s_\infty = \sum_{n=0}^{\infty} 4^{-n-1}\epsilon_\infty(2^nP)$ to the desired accuracy (using a bound on $|\epsilon_\infty|$) by repeated application of δ to a floating-point approximation of the coordinates of P.
5. Return $\widehat{h}(P) = h(P) + s_\infty - \sum_{p\in S} s_p \log p$.

This algorithm requires to go up to $m = \max\{m_p \mid p \in S\}$, whereas the original algorithm goes up to $m = \operatorname{lcm}\{m_p \mid p \in S\}$. This can make a big difference.

A few more remarks on the implementation. If in step 2, we find that $\delta(x)$ (i.e., $2mP$) is in the kernel of reduction at p, then we know that $2mP$ is in U_p. We therefore can complete the table T_p by symmetry (since $\epsilon_p(Q) = \epsilon_p(-Q)$) and remove p from S'. This can save some work, especially for $p = 2$. Similarly, we can compute $(2m+1)P$ in each step without much additional work and check if it is in the kernel of reduction.

In step 4, it is a good idea to keep the multiples of P on $K(\mathbb{R})$ (for example by adjusting the fourth coordinate after each doubling step). Because of rounding errors, the points tend to leave K, which introduces additional errors.

The factorisation in step 1 is probably not so very costly (in most cases, at least). Primes that divide the discriminant only once do not show up (compare the remark following Proposition 5.2), hence normally the primes involved will be fairly small. To avoid expensive factorisations, one could restrict to splitting off all reasonably small primes and use the old algorithm on the remaining part (if any). This means that we have to find the smallest m such that $\epsilon_p(mP) = 0$ for all large p (which we can check using gcd and small factorisation) and then compute $\widehat{h}(mP)$ as before.

The algorithm presented here has been implemented by the author as part of a MAGMA package dealing with hyperelliptic curves and their Jacobians.

7. How to find the Mordell–Weil group. We now assume that we have a curve of genus two over $\mathbb{Q}$ (or, more generally, a number field). Our goal is to find the Mordell–Weil group $J(\mathbb{Q})$. We suppose that we already know its torsion-free rank, r, and that we have found r points $P_1, \dots, P_r \in J(\mathbb{Q})$ that generate a subgroup of rank r (and hence of finite index). See [8] for an algorithm that produces an upper bound for the rank r. Let T be the finite torsion subgroup of $J(\mathbb{Q})$. We are concerned here with finding the free part $J(\mathbb{Q})/T$. (See [7] for an algorithm that computes T.)

Flynn and Smart [3] discuss how we can bound the index of the subgroup $\langle P_1, \dots, P_r \rangle$ in $J(\mathbb{Q})/T$, provided we have found all points in $J(\mathbb{Q})$ of canonical height at most a given bound $b > 0$. We will give a complement to this and establish a bound b such that all points of canonical height up to b, together with the given points P_j, will generate $J(\mathbb{Q})/T$.

We have $\Lambda = J(\mathbb{Q})/T \cong \mathbb{Z}^r$ and the canonical height, $\widehat{h}$, defines a positive definite quadratic form on $V = \Lambda \otimes_{\mathbb{Z}} \mathbb{R}$ (see Silverman [6, VIII, Proposition 9.6]; the proof is valid for general abelian varieties). Hence we can consider Λ as a lattice in the euclidean vector space V. The given points generate a sublattice Λ', and we can find an (almost) reduced basis for it with the LLL algorithm. The *covering radius* $\varrho(\Lambda')$ of Λ' is defined to be the maximal distance a point in V can have from the lattice Λ'.

PROPOSITION 7.1. *In the situation described above*, Λ *is generated by* Λ' *together with all points in* Λ *of height at most equal to* $\varrho(\Lambda')^2$.

Proof. This follows from the fact that (by definition) the ball with radius $\varrho(\Lambda')$ about the origin contains a fundamental domain for Λ'. So all the residue classes in Λ/Λ' must have a representative of height $\le \varrho(\Lambda')^2$. ■

Now it is quite difficult to determine ϱ exactly for a lattice of high rank, but we can easily find an upper bound as follows. Let L be some lattice, and let $V = L \otimes_{\mathbb{Z}} \mathbb{R}$, with positive definite quadratic form q. Let $V_1 \subset V$ be a subspace such that $L_1 = L \cap V_1$ is a full lattice in V_1. Let $V_2 = V_1^{\perp}$ be the orthogonal complement (with respect to q) of V_1 in V, and let L_2 be the orthogonal projection of L to V_2; then L_2 is a full lattice in V_2.

LEMMA 7.2. *We have*

$$\varrho(L)^2 \le \varrho(L_1)^2 + \varrho(L_2)^2.$$

Proof. We claim that the set

$$R = \{v_1 + v_2 \mid v_1 \in V_1,\, v_2 \in V_2,\, q_1(v_1) \le \varrho(L_1)^2,\, q_2(v_2) \le \varrho(L_2)^2\}$$

(where q_j is the form induced by q on V_j) contains a fundamental domain for L. Since R is contained in the ball of radius $\sqrt{\varrho(L_1)^2 + \varrho(L_2)^2}$ about the origin in V, the result follows.

So let $v = v_1 + v_2$ be some element of V, split into its components in V_1 and V_2. We can find an element $\lambda_2 \in L_2$ such that $q_2(v_2 + \lambda_2) \le \varrho(L_2)^2$. Let $\lambda \in L$ be a preimage of λ_2, and let $\lambda' = \lambda - \lambda_2 \in V_1$. We can find an element $\lambda_1 \in L_1 \subset L$ such that $q_1(v_1 + \lambda' + \lambda_1) \le \varrho(L_1)^2$. This shows that $v + \lambda_1 + \lambda \in R \cap (v + L)$, which proves the claim. ∎

The simplest application is when we split the space V into one-dimensional pieces. This amounts to orthogonalising a given basis of the lattice. We then take the sum of the norms of the orthogonalised basis vectors as an upper bound for $4\varrho^2$. This bound is used in the first example in Section 8 below.

In general, the computation of ϱ requires a good knowledge of the Voronoi cell of the lattice, which is a very complex object—a typical Voronoi cell of a lattice of rank r is a polytope with $(r+1)!$ vertices. It seems to be feasible to compute ϱ exactly for lattices of rank up to about 6, but beyond that, the complexity becomes prohibitive. We can, however, split our lattice into pieces of smaller rank and use the bound given by the lemma above. See the second example in Section 8 below.

We remark that in the case $r = 2$, an exact formula for ϱ is

$$\varrho^2 = \frac{\widehat{h}(P_1)\widehat{h}(P_2)\widehat{h}(P_1 \pm P_2)}{4\,\mathrm{Reg}(P_1, P_2)},$$

where Reg is the regulator and the sign is chosen that gives the smaller value. P_1 and P_2 are assumed to be a Minkowski-reduced basis.

These considerations lead to the following algorithm. We are given independent points $P_1, \dots, P_r \in J(\mathbb{Q})$ and want to find the saturation in $J(\mathbb{Q})$ of the subgroup generated by the given points, i.e., the largest subgroup of the finitely generated abelian group $J(\mathbb{Q})$ containing the known subgroup with finite index. In case we know the rank of $J(\mathbb{Q})$ is r, this amounts to finding generators of $J(\mathbb{Q})$ itself.

1. For all bad primes p and for the infinite prime ∞, find a bound γ_p (resp. γ_∞) on the local height constant, and let $\gamma = \sum_p \gamma_p \log p + \gamma_\infty$. These bounds can be obtained using the results of [7] or of Section 5 in this paper.
2. Using the algorithm described in Section 6 above, compute the height pairing matrix $M = \left(\frac{1}{2}(\widehat{h}(P_i + P_j) - \widehat{h}(P_i) - \widehat{h}(P_j))\right)_{i,j}$. Construct the corresponding lattice Λ'.
3. Find a bound ϱ^2 for the square of the covering radius of Λ', either by exact computation or by splitting the lattice into several parts and using Lemma 7.2.
4. Enumerate all points in $J(\mathbb{Q})$ with normalised projective Kummer coordinates bounded in absolute value by $\lfloor \exp(\gamma + \varrho^2) \rfloor$. This set will contain all points of (canonical) height $\le \varrho^2$ (cf. [3] or [7]). By Proposition 7.1, these points, together with the P_i, will generate the group we are looking for.

A few remarks are in order. Note that this algorithm is applicable to any abelian variety, as long as we are able to compute heights, find a bound for the global height constant and can enumerate points of bounded naive height. This is the case for elliptic curves, for example.

The quantity γ_∞ needed in step 1 can be obtained by the method described in [7]. Finally, there is a fairly fast program called `j-points` written by the author that uses a sieving technique in order to enumerate points of bounded height on the Jacobian.

The algorithm presented here is applicable when $\gamma + \varrho^2$ is not too large, since otherwise the enumeration of points in step 3 will be prohibitive. When γ is not too large, but ϱ^2 is, one can use the approach suggested by Flynn and Smart [3]. This consists in enumerating points up to (logarithmic) naive height $\gamma + \varepsilon$ for a suitable $\varepsilon > 0$ and using the result to bound the index in the saturation. In a second step, one tries to exclude the possible index divisors p by collecting information on independence $\bmod p$ in the reduction at suitable primes q. The disadvantage of this approach is that when the rank is high, the first step will nearly always give a nontrivial bound (it gets worse with growing rank), and it is very time-consuming to obtain the necessary information in the second step in order to exclude index divisors below this bound. Compare the examples given below.

8. Examples

Example 1. We return to our earlier example,

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

Schaefer [4] has shown that the classes of the following divisors generate a subgroup of finite index in the Mordell–Weil group:

$$(-17, 1223) - \infty, \quad (-9, 557) - \infty, \quad (-6, 317) - \infty, \quad (-2, 73) - \infty,$$
$$(0, 1) - \infty, \quad (4, 37) - \infty, \quad \left(\tfrac{1}{2}(5 + \sqrt{177}), 191\right) + \left(\tfrac{1}{2}(5 - \sqrt{177}), 191\right) - 2 \cdot \infty.$$

Table 2. Generators for $J(\mathbb{Q})$ in the rank 7 example

Generator	Height
$(2 + \sqrt{10}, 21 - 5\sqrt{10}) + \text{conj.} - 2 \cdot \infty$	1.6473513303
$(0, 1) - \infty$	2.0178003424
$(4, 37) - \infty$	2.9901773857
$(- 2, 73) - \infty$	3.2923263549
$\left(\frac{21+\sqrt{329}}{8}, \frac{965+9\sqrt{329}}{64}\right) + \text{conj.} - 2 \cdot \infty$	3.3796213459
$\left(\frac{1}{2}(15 + \sqrt{129}), 355 + 26\sqrt{129}\right) + \text{conj.} - 2 \cdot \infty$	3.6923148302
$\left(\frac{35+\sqrt{1189}}{9}, \frac{11492+307\sqrt{1189}}{243}\right) + \text{conj.} - 2 \cdot \infty$	3.6956019437

Using the algorithm described in the preceding section, we compute the height pairing matrix of these points. Then we find an LLL-reduced basis, which is listed in Table 2 (together with the heights of the points).

When we orthogonalise this basis, we see that the new basis vectors have norms 1.64724, 1.91458, 2.60517, 3.07602, 2.57622, 2.79642, 2.54511, respectively, hence $\varrho^2 \leq 4.29021$. This, taken together with the bound for the height constant given above, shows that the points in $J(\mathbb{Q})$ with (non-logarithmic) naive height up to 25266 will generate $J(\mathbb{Q})$.

Using `j-points`, we enumerate all 683 points in this range. This took under two hours of CPU time on a 200 MHz Pentium PC. It can be checked that all these points are already in Λ'. Since the torsion subgroup T is trivial in this case, this shows that the above list gives a full set of generators of $J(\mathbb{Q})$.

Note that the method given in [3] for bounding the index of Λ' in Λ can only bound the index by 4, no matter how far we go in the search of points in $J(\mathbb{Q})$. Since in this case, it is known that the index must be odd, we still would have to exclude the possibility that the index is 3.

After we had done this calculation, we succeeded in determining the covering radius of the lattice generated by the known points. It turns out that $\varrho^2 = 2.6658$, hence it would have been sufficient to enumerate all points in $J(\mathbb{Q})$ of (non-logarithmic) naive height up to about 5000. On the other hand, finding the covering radius took much more time than finding the points of height up to 25266.

Example 2. We consider the curve C over $\mathbb{Q}$ given by the affine equation

$$Y^2 = X^6 - 56X^5 + 176X^4 + 74X^3 - 81X^2 - 282X + 169,$$

and let J denote its Jacobian. This curve was found by Colin Stahlke while searching for curves of genus two with small coefficients and many rational points. It has pairs of rational points with x-coordinates in the following list:

$$\infty, -4, -2, -1, 0, 1, 2, 57, 58, -\tfrac{15}{2}, -\tfrac{5}{2}, -\tfrac{1}{2}, \tfrac{1}{2}, \tfrac{7}{2}, \tfrac{1}{3}, \tfrac{4}{3}, \tfrac{5}{3}, \tfrac{7}{3}, \tfrac{8}{3}, -\tfrac{55}{4}, -\tfrac{37}{4}, -\tfrac{9}{4},$$
$$-\tfrac{209}{5}, -\tfrac{112}{5}, -\tfrac{6}{5}, -\tfrac{3}{5}, \tfrac{3}{5}, \tfrac{6}{5}, \tfrac{3}{7}, -\tfrac{7}{8}, \tfrac{27}{8}, \tfrac{18}{11}, \tfrac{4}{13}, \tfrac{53}{17}, -\tfrac{5}{18}, -\tfrac{2322}{23}, \tfrac{25}{24}, \tfrac{43}{28}, \tfrac{95}{29}, -\tfrac{53}{31}, \tfrac{23}{44},$$
$$\tfrac{77}{53}, -\tfrac{10}{63}, \tfrac{116}{65}, -\tfrac{69}{76}, \tfrac{169}{77}, \tfrac{103}{100}, \tfrac{73}{116}, \tfrac{68}{117}, \tfrac{199}{145}, \tfrac{463}{145}, \tfrac{159}{146}, \tfrac{169}{154}, \tfrac{169}{168}, \tfrac{248}{249}, -\tfrac{776}{261}, -\tfrac{425}{286},$$
$$-\tfrac{1865}{309}, \tfrac{196}{333}, \tfrac{187}{366}, -\tfrac{1212}{563}, -\tfrac{1345}{949}, \tfrac{2332}{1043}$$

The set of the classes of divisors $P - Q$ where P and Q are among these rational points on C generates a subgroup of $J(\mathbb{Q})$ of rank 12. Since it can be shown (see [8]) that the rank of $J(\mathbb{Q})$ is at most 12, we have found generators of a finite index subgroup. The torsion subgroup is trivial in this case, hence this subgroup coincides with the lattice Λ'. With the usual algorithms for lattices, we find a Minkowski-reduced basis. It is given in Table 3.

Table 3. Generators for $J(\mathbb{Q})$ in the rank 12 example

Generator	Height
$(1,1) - \infty_+$	3.6069846330
$(1,1) - \infty_-$	3.6248921651
$(0,13) - \infty_-$	3.9724077310
$(-1,23) - \infty_+$	4.4794963440
$(2,31) - \infty_+$	4.5306263681
$\left(\frac{1}{2}, \frac{41}{8}\right) - \infty_-$	4.6541675885
$(1,1) + (-2,67) - \infty_+ - \infty_-$	4.7683627239
$\left(\frac{1}{3}, \frac{227}{27}\right) - \infty_+$	4.9309921342
$\left(\frac{3}{5}, -\frac{283}{125}\right) - \infty_-$	5.1654708604
$\left(\frac{4}{3}, \frac{331}{27}\right) - \infty_-$	5.2192990555
$(1,1) + (-4,-319) - \infty_+ - \infty_-$	5.2817228322
$\left(\frac{5}{3}, \frac{589}{27}\right) - \infty_+$	5.3847930886

We can bound the covering radius of this lattice by splitting it into two parts of rank six. For these two parts, we find that $\varrho_1^2 = 3.2542$ and $\varrho_2^2 = 2.0489$, hence $\varrho^2 \leq 5.3031$.

The discriminant of the polynomial on the right hand side in the equation defining C is a power of two times the product of the two primes 27605791 and 12261635838401. Hence only $p = 2$ contributes to the finite part of the height constant. The global height constant can then be bounded by 3.37131. It will therefore be sufficient to find all points in $J(\mathbb{Q})$ of logarithmic naive height at most 8.6745, or non-logarithmic naive height at most 5851. We can find these points with `j-points` (there are 1347 of them), and it turns out that all of them are already in the known sublattice. This shows that the classes of the divisors listed in Table 3 are indeed generators of $J(\mathbb{Q})$, and the regulator is 316539.273674.

The Flynn–Smart approach can only bound the index by 20 at best in this example, and it would be quite a tedious task to eliminate all primes below 20 as possible index divisors.

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] E. F. Schaefer, *Class groups and Selmer groups*, J. Number Theory 56 (1996), 79–114.

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

[6] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, 1986.

[7] M. Stoll, *On the height constant for curves of genus two*, Acta Arith. 90 (1999), 183–201.

[8] —, *Implementing 2-descent for Jacobians of hyperelliptic curves*, ibid. 98 (2001), 245–277.

[9] Kummer surface formulas, ftp://ftp.liv.ac.uk/˜ftp/pub/genus2.

[10] MAGMA is described in W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system I: The user language*, J. Symbolic Comput. 24 (1997), 235–265. (Also see the Magma home page at http://www.maths.usyd.edu.au:8000/u/magma.)

Max-Planck-Institut für Mathematik
P.O. Box 7280
53072 Bonn, Germany
E-mail: stoll@mpim-bonn.mpg.de

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

Received on 28.6.2001
and in revised form on 12.10.2001 (4063)