TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 344, Number 1, July 1994

INTEGER POINTS ON CURVES OF GENUS 2 AND THEIR JACOBIANS

DAVID GRANT

ABSTRACT. Let C be a curve of genus 2 defined over a number field, and Θ the image of C embedded into its Jacobian J. We show that the heights of points of J which are integral with respect to $[2]_*\Theta$ can be effectively bounded. As a result, if P is a point on C, and $\overline{P}$ its image under the hyperelliptic involution, then the heights of points on C which are integral with respect to P and $\overline{P}$ can be effectively bounded, in such a way that we can isolate the dependence on P, and show that if the height of P is bigger than some bound, then there are no points which are S-integral with respect to P and $\overline{P}$.

We relate points on C which are integral with respect to P to points on J which are integral with respect to Θ, and discuss approaches toward bounding the heights of the latter.

INTRODUCTION

Let C be a curve of genus 2 defined over a number field K, and S a finite set of places of K. The image of C embedded into its Jacobian J is a theta divisor Θ. Let U be $J - \Theta$ and $Z = J - [2]_*\Theta$, where $[2]_*\Theta$ is the image of Θ under the multiplication-by-2 map. Using Faltings's proof of the Mordell Conjecture [5], Silverman showed that the number of S-integer points on U and Z are finite [26, 28]. These results now follow from Faltings's [6] proof of Lang's conjecture that the number of points on an Abelian variety which are S-integral with respect to an ample divisor is finite. Silverman's and Faltings's results are ineffective. Silverman also showed that S-integer points on U and Z are "widely-spaced" [27].

In this paper we show that the heights of S-integer points on Z can be effectively bounded (although we do not write down such a bound). So far as we know, this is the first example of the effective bounding of integer points on an affine portion of a generically simple Abelian surface. This has an application to integer points on C.

In 1929 Siegel proved the number of S-integer points on C is finite [24]. (This of course was superseded by Faltings's proof that $C(K)$ is finite.) Although these results are ineffective, Siegel provided a separate proof in the case that C was given by a hyperelliptic model, which reduces the search for S-integer points to one of Diophantine approximation via the famed "S-unit equation" [25]. This, when coupled with A. Baker's lower bound for linear

Received by the editors January 7, 1992.
1991 *Mathematics Subject Classification.* Primary 11G30, 11G10.
Partially supported by NSF grant DMS-9102652.

0002-9947/94 $1.00 + $.25 per page

forms in logarithms, gives an effective bound for the heights of S-integer points on C [1].

Let P be a point on C, and $\overline{P}$ its image under the hyperelliptic involution. Then an effective version of the Riemann-Roch theorem transforms points on C which are integral with respect to P and $\overline{P}$ to integer points on a hyperelliptic model, whose heights can be effectively bounded, but with a bound depending on the height of P. The effective bounding of the integer points on Z allows us to bound the heights of points on C which are integral with respect to P and $\overline{P}$ in such a way that we can isolate the dependence on P, and show that if the height of P is bigger than some bound depending on C, K, and S, then there are no points which are S-integral with respect to P and $\overline{P}$.

If C is given by a model with points $Q = \{Q_1, \ldots, Q_n\}$ at infinity, then points on C which are S-integral with respect to Q are transformed into S-integer points on a hyperelliptic model only when Q contains a nonempty subset invariant under the hyperelliptic involution on C. We discuss an approach to the problem of effectively bounding the heights of S-integer points on C no matter what Q is. First we "reduce" the problem of effectively bounding the heights of S-integer points on C to the harder task of bounding the heights of S-integer points on U. Then in turn we relate these points to solutions of linear equations involving special S-integer elements of GL_2. These form curious "non-Abelian S-unit equations." It is intriguing to note that the effective solution of these equations would effectively bound the heights of S-integer points on U and hence on C.

In §§1 and 2 we cull together facts about integer points on varieties and about the geometry of curves of genus 2. In §§3 and 4 we investigate integer points on Z and U, respectively.

I would like to thank L. Walling for helpful discussions, and L. Cassuto, W. Schmidt, and J. Silverman for their helpful comments on an earlier version of this paper.

1. Preliminaries on integer points

General references for this section are [15, 20, 22, and 30].

Let K be a number field, and S a finite set of places of K which we will always assume contains the archimedean places and those places lying over 2. We let O_S denote the S-integers of K, and $O_S^\times$ the S-units. Let D_K be the discriminant of K over the rationals $\mathbf{Q}$, and d_K the degree $[K : \mathbf{Q}]$ of K over $\mathbf{Q}$. We will always assume that we have a normalized set of absolute values $M_K = \{|\ |_v\}$. We define the relative height $H_K(P)$ of a point $P = (p_0, \ldots, p_n)$ in projective n-space $\mathbf{P}^n(K)$ as

$$H_K(P) = \prod_{v \in M_K} \max_i |p_i|_v .$$

We define the absolute height as $H(P) = H_K(P)^{1/d_K}$. Henceforth all heights shall be absolute. We define the height of a point $(p_1, \ldots, p_n)$ in affine n-space $\mathbf{A}^n(K)$ as the height of the projection point represented by $(1, p_1, \ldots, p_n)$. The height $H(f)$ of a polynomial f is defined to be the height of its coefficient vector considered as a point in projective space.

If V is a nonsingular variety, and f is a function on V, we let (f) denote its divisor. If ω is a differential on a curve, we let (ω) denote its divisor. For

a divisor W on V we let $L(W)$ denote the vector space of functions such that $(f)+W$ is effective, and we let $l(W)$ denote the dimension of $L(W)$. If W_1, W_2 are divisors on a variety, we write $W_1 \equiv W_2$ to indicate that they are linearly equivalent.

If V is an affine variety defined over K, we will always assume that it is embedded into $\mathbf{A}^n(K)$, so that it is defined by a definite model $f_1 = 0, \ldots, f_m = 0$, with $f_i \in K[X_1, \ldots, X_n]$. We use a naive notion of height for V by letting $H(V)$ be the maximum of the heights of the defining polynomials $H(f_i)$. An S-integer point P is defined to be a point $P \in V(K)$ whose coordinates lie in O_S. Equivalently, we can extend V to give it the structure of a scheme over O_S. Indeed, we might as well assume that $f_1, \ldots, f_m \in O_S[X_1, \ldots, X_n]$, in which case we can form the O_S-algebra $A = O_S[X_1, \ldots, X_n]/(f_1, \ldots, f_m)$. Then an S-integer point of V (or A) is defined to be an O_S-point of $\mathrm{Spec}(A)$, i.e., a homomorphism from A into O_S. We call A an O_S-algebra associated to V. For an ample divisor W on V, it will be convenient to use the phrase "P is S-integral with respect to W," by which we mean that we take some very ample multiple jW of W, and use a basis for $L(jW)$ to define a definite model V' for V, with P an S-integer point of V'. Equivalently, we make a choice of an associated O_S-algebra A such that $V - W$ is the generic fibre of $\mathrm{Spec}(A)$ (i.e., $\Gamma = K \otimes_{O_S} A$ is the coordinate ring of $V - W$ over K), in which case we mean that P is an O_S-point of $\mathrm{Spec}(A)$.

Basic to our study is

Theorem 1 (Hermite-Minkowski). *Given a number field K, there are only finitely-many extensions of bounded degree and bounded discriminant.*

As a corollary, given K and a finite set of places S of K, there are only finitely-many extensions of bounded degree in which only places in S ramify. These extensions can be explicitly determined.

The only tool from Diophantine approximation we employ is the "2-variable S-unit equation" which is based on A. Baker's lower bound for linear forms in logarithms.

Theorem 2 (S-unit equation) [12]. *There is a constant c effectively depending on D_K, d_K, the class number and regulator of K, and the norms of the finite primes in S, such that if x_1 and x_2 give a solution to*

$$x_1 + x_2 = 1, \qquad x_i \in O_S^{\times},$$

then $H(x_i) < c$.

Minkowski proved that the class number of K is bounded in terms of d_K and D_K, and the "easy" direction of the Brauer-Siegel theorem shows that the regulator is also so bounded (see [16, pp. 120 and 322]). So the constant in Theorem 2 can be made to depend only on d_K and D_K. (In fact, d_K is also bounded in terms of D_K, but for the unperformed task of explicitly writing bounds, it is convenient to keep d_K present in the discussion.)

Therefore, when describing a set of points in $V(K)$, we use the phrase "effectively bounded" to indicate that there exists an effective bound for the heights of the points, where the bound depends on K only in that it depends on d_K, D_K, and a bound P_S for the "absolute norm" of each finite prime p in S, which we define as $(\mathbf{N}_{K/\mathbf{Q}}(p))^{1/d_K}$.

Since we need to keep track of P_S, the phrase "extending S if necessary" means that we will form a new set S' by adjoining to S all primes of K of absolute norm less than some $P_{S'}$, where $P_{S'}$ is some effectively computable bound which depends on K only in that it depends on P_S, D_K, and d_K. By abuse of notation, we also denote the new set by S. The phrase "extending K if necessary" means that we will replace K by a finite extension K' with $[K' : \mathbf{Q}] < d_{K'}$, and with only primes of absolute norm less than $P_{S'}$ ramifying in K'/K. Here $d_{K'}$ and $P_{S'}$ are some effectively computable bounds which depend on K only in that they depend on P_S, D_K, and d_K. By the Hermite-Minkowski theorem, there are only finitely many such K', and they can be effectively determined. Again, by abuse of notation, we also denote the new field by K. When we take a finite extension K' of K, we will also use S to denote the places of K' which divide those in S, and keep P_S the same. The absolute height is unaffected by a finite extension of fields.

If $\phi: V \to W$ is a rational map of projective varieties represented by a morphism ψ, we define the height of ϕ (relative to ψ) to be the maximum of the heights of the component polynomials of ψ.

Proposition 1. *Let C, C' be (possibly singular) projective curves over K, and let $\phi: C \to C'$ be a birational map defined over K, with domain $E \subseteq C$. Then effectively-bounding the heights of a set of points R in $C(K)$ is equivalent to effectively-bounding the heights of $\phi(R \cap E)$ in $C'(K)$, with a bound that depends on the heights and degrees of ϕ, C, and C'.*

Proof. This follows immediately from [22, p. 13] so long as R is in E and $\phi(R)$ is in the domain of ϕ^{-1}. But since C and C' are curves, the points where ϕ and ϕ^{-1} are not defined is a zero-dimensional set defined by equations of height and degree bounded by those defining the curves and ϕ. Therefore, by classical elimination theory, the heights of the points when ϕ and ϕ^{-1} are not defined can be effectively bounded.

Proposition 2. *Suppose that C is an affine curve defined by polynomials $f_1, \ldots, f_m \in O_S[X_1, \ldots, X_n]$, with $H(f_i) \leq \mathscr{H}$, and degree of $f_i \leq N$, for all i. Then there is an affine plane curve C' defined by a polynomial $f \in O_S[Y, Z]$, and a birational polynomial map $\phi: C \to C'$ defined over O_S, such that the degrees and heights of f and ϕ are bounded in terms of $\mathscr{H}$ and N, and ϕ maps S-integer points of C into S-integer points of C'.*

Proof. This is just an effective version of Noether's normalization lemma. Let $\Gamma = K[X_1, \ldots, X_n]/(f_1, \ldots, f_m)$ be the coordinate ring of C over K, and x_i the image of X_i in Γ. Then the proof of the normalization lemma in [18, p. 262] gives an effective procedure for writing

$$\Gamma = K[Y_1, \ldots, Y_n]/J = K[y_1, \ldots, y_n]$$

where: J is an ideal generated by some $g_1, \ldots, g_l \in K[Y_1, \ldots, Y_n]$; the heights and degrees of the g_i are bounded in terms of $\mathscr{H}$ and N; the y_j are the images of the Y_j in Γ, and are K-linear combinations of the x_j with coefficients whose heights are bounded in terms of $\mathscr{H}$ and N; and $y_2, \ldots, y_n$ are integral over $K[y_1]$. (The proof only requires the well-known fact that a polynomial over K which is not identically zero takes on a nonzero value at a K-point whose height is bounded in terms of the height, degree, and number

of variables of the polynomial.) Multiplying the y_j by constants of bounded height, we can assume that they are O_S-linear combinations of the x_j, and that $y_2, \ldots, y_n$ are integral over $K[y_1]$.

Now by Galois theory, there is a linear combination $z = \sum_2^n a_j y_j$, where the a_j are in the rational integers $\mathbf{Z}$, the a_j are bounded in terms $\mathscr{H}$ and N, and such that $K[y_1, z]$ is a subring of Γ whose fraction field is the function field of C. Further, we can choose an equation $f(Y, Z) \in O_S[Y, Z]$ expressing the algebraic dependence of z and y_1 that has degree and height bounded in terms of $\mathscr{H}$ and N.

Let C' be the curve defined by f, which is birationally-equivalent to C. Our construction gives a polynomial birational map $\phi: C \to C'$, which has height and degree bounded in terms of $\mathscr{H}$ and N, and maps S-integer points of C into those of C'.

As a corollary to the two propositions, to effectively bound the S-integer points on C, it suffices to do so on the birationally-equivalent plane model C'.

Henceforth we shall assume that all our affine curves C are defined by a single irreducible equation in 2 variables.

We will need to know how S-integer points behave under unramified morphisms of varieties [22].

Theorem 3 (Chevalley-Weil). *Let $f: W \to V$ be a finite, unramified morphism of affine nonsingular varieties defined over K. Then, extending S if necessary, there is a finite set T of places of K, such that for every S-integer point $P \in V(K)$, $Q \in f^{-1}(P)$ is an S-integer point of W, defined over an extension L of K, of bounded degree, in which only primes in T ramify.*

Since we are concerned with effectivity, we will be careful in all our applications to pick associated O_S-algebras A_W and A_V for W and V respectively, such that A_W is integral over A_V. In this way we do not need to extend S. Also, given f, W, and V, the theory states that T can be explicitly determined, but in practice this may be difficult. We will only be dealing in simpler situations, either with explicit double covers of varieties, or with coverings of Abelian varieties, where we can explicitly determine T.

Corollary 1. (1) *Let $f: W \to V$ be a finite, unramified morphism of nonsingular affine varieties. Then, extending S if necessary, there is a finite extension L of K, of bounded degree and discriminant, such that for every S-integer point $P \in V(K)$, $Q \in f^{-1}(P)$ is an S-integer point of W defined over L.*

(2) *If V and W are subvarieties of an Abelian variety A, and $f = [m]$, the multiplication-by-m map, then L/K is ramified only at primes of bad reduction for A and those dividing m.*

Proof. (1) This is just the theorem of Chevalley-Weil combined with the theorem of Hermite-Minkowski.

(2) This follows from the criterion of Néron-Ogg-Shafarevich [23]. The primes of bad reduction for A can be effectively bounded in terms of the heights and degrees of the defining equations for A.

Suppose now that C is a curve defined by an irreducible equation $f(x, y) = 0$, of degree N and of height $\mathscr{H}$, defined over a number field K. We think of the function x on C as defining a cover of the projective line $\mathbf{P}^1$. Let

X be the projective normalization of C, and $\psi: X \to \overline{C}$ the natural map to the projective closure of C. Let P be a point in $X(K)$, and let e be the ramification index of P over $\mathbf{P}^1$. We take t to be the local parameter at P defined by $(1/x)^{1/e}$ if P lies above the point at infinity on $\mathbf{P}^1$, and $t = (x - \alpha)^{1/e}$ if $\psi(P) = (\alpha, \beta)$ lies above a finite point of $\mathbf{P}^1$.

The following is a special case of an effective Riemann-Roch theorem, first proved by Coates [3], and recently improved by Schmidt [19].

Theorem 4 (effective Riemann-Roch). *Let W be a divisor on X defined over K. Then there is a basis $\{f_i\}$ for $L(W)$, such that f_i has a Puiseux expansion at P*

$$f_i = \sum_{s \geq s_0} a_{is} t^s,$$

with t the prescribed local parameter at P, $a_{is} \in K$, and with the height of a_{is} bounded in terms of s, $\mathscr{H}$, N, the multiplicities of points in the support of W, and the heights of the points in the support of W.

Further, if W is supported at points on the normalization of C which lie over the points at infinity, then the f_i can be chosen to be integral over $\mathbf{Z}[x]$.

The proof of the first part is given in [19]. The second part follows with only minor modification from §7 of [21]. In brief, the additional condition on W forces f_i to be integral over $K[x]$, and hence over $\mathbf{Q}[x]$. The minimal polynomial of f_i over $\mathbf{Q}[x]$ can be written explicitly, say with coefficients c_{ij} in $\mathbf{Q}[x]$. The bounds on the coefficients of the Puiseux expansions of f_i at every point lying over infinity show that the coefficients of c_{ij} have bounded height in $\mathbf{Q}$. Hence there is an integer c_i of bounded height such that $c_i f_i$ is integral over $\mathbf{Z}[x]$.

2. Curves of genus 2 and their Jacobians

Let C be a curve of genus 2 defined over a number field K. In keeping with the conventions of the last section, we assume that C is defined by a single equation $f(u, v) = 0$ of degree N and height $\mathscr{H}$. Let $\overline{C}$ be the projective closure of C: then $\overline{C} - C$ are the points at infinity of C. Let X be the projective normalization of $\overline{C}$, and $Q = \{Q_1, \ldots, Q_n\}$ be the points of X which lie over $\overline{C} - C$. The points of $\overline{C} - C$ are defined over an extension whose degree and ramification over K are bounded in terms of N and $\mathscr{H}$. Therefore extending K if necessary, we can assume that the points of $\overline{C} - C$ are all defined over K. Now the inverse image of a point $P \in \overline{C} - C$ on X is a set of points, each defined over a field which splits the tangents at P on $\overline{C}$. This splitting is achieved over an extension whose degree and ramification over K are bounded in terms of N and $\mathscr{H}$. So extending K again if necessary, we can assume that the points of Q are all defined over K. We use the natural morphism $X \to \overline{C} \xrightarrow{u} \mathbf{P}^1$ to define a height function H on X. The heights of points in Q are bounded in terms of N and $\mathscr{H}$.

There is a canonical hyperelliptic involution on X, determined as follows. Let ω be a holomorphic differential on X. Then $L((\omega))$ is 2-dimensional, spanned, say, by functions $\{1, x\}$. The function x defines a degree 2 map $\lambda: X \to \mathbf{P}^1$. Note that a change in the choice of ω or x only changes λ by a projective transformation. The quadratic extension given by λ is automatically

Galois, and the nontrivial element in the Galois group of $K(X)$ over $K(x)$ gives the hyperelliptic involution. We denote the image of a point $P \in X$ under the hyperelliptic involution as $\overline{P}$. The Hurwitz formula guarantees that there are 6 points $W_0, \ldots, W_5$ fixed under the hyperelliptic involution, called the Weierstrass points of X.

Theorem 5. *Let $C: F(u, v) = 0$ be a curve of genus 2, of degree N, and height $\mathscr{H}$ defined over a number field K of discriminant D_K and degree d_K. Let X be the projective normalization of C.*

(1) *Suppose that $W_0 \in X(K)$ is a Weierstrass point. Then there is a model for X of the form*

$$\mathrm{Hyp}_5: y^2 = f(x),$$

where f is a monic quintic polynomial in $K[x]$ with distinct roots in an algebraic closure $\overline{K}$ of K, $\{1, x\}$ is a basis for $L(2W_0)$, and $\{1, x, x^2, y\}$ is a basis for $L(5W_0)$.

(2) *Suppose that $P \in X(K)$ is not a Weierstrass point. Then there is a model for X of the form*

$$\mathrm{Hyp}_6: y^2 = f(x),$$

where f is a sextic polynomial in $K[x]$ with distinct roots in $\overline{K}$, $\{1, x\}$ is a basis for $L(P + \overline{P})$, and $\{1, x, x^2, x^3, y\}$ is a basis for $L(3(P + \overline{P}))$.

(3) *Suppose once again that $P \in X(K)$ is not a Weierstrass point. Then there is also a model for X of the form*

$$\mathrm{Nonhyp}: y^3 + g_1(x)y^2 + g_2(x)y = x^4 + g_3(x),$$

where g_i is a polynomial in $K[x]$ of degree $\leq i$, $\{1, x\}$ is a basis for $L(3P)$, and $\{1, x, y\}$ is a basis for $L(4P)$.

(4) *In (1) assume further that $H(W_0)$ is bounded; in (2) assume further that $H(P)$ and $H(\overline{P})$ are bounded; in (3) assume further that $H(P)$ is bounded. Then* Hyp_5, Hyp_6, *and* Nonhyp *can be chosen to be of bounded height, and to bound the height of a set of points in $C(K)$ it suffices to bound the heights of the corresponding points of* Hyp_5, Hyp_6, *or* Nonhyp.

(5) *With assumptions as in (4), in (1) assume further that $W_0 \in Q$; in (2) assume further that $P, \overline{P} \in Q$; in (3) assume further that $P \in Q$. Then* Hyp_5, Hyp_6, *and* Nonhyp *can be chosen to be of bounded height, and such that x is integral over $\mathbf{Z}[u]$. Hence to bound the height of S-integer points on C, it suffices to bound the heights of the S-integer points of* Hyp_5, Hyp_6, *or* Nonhyp.

Proof. Parts (1) and (2) are well-known applications of the Riemann-Roch theorem. Likewise, the proofs of (4) and (5) pertaining to Hyp_5 and Hyp_6 require only minor modifications of the arguments in §§6 and 7 of [21], so we omit them. We will prove (3) *en passant* as we prove the parts of (4) and (5) pertaining to Nonhyp.

Suppose that $P \in X(K)$ is a point of bounded height. Using the effective Riemann-Roch theorem, we can produce $z \in L(5P)$, $y \in L(4P)$, and $x \in L(3P)$ with Puiseux expansions

$$z = t^{-5} \sum_{s \geq 0} a_s t^s, \quad y = t^{-5} \sum_{s \geq 1} b_s t^s, \quad x = t^{-5} \sum_{s \geq 2} c_s t^s,$$

where t is the prescribed local parameter at P, the heights of the $a_s, b_s, c_s \in K$ are bounded in terms of $s, \mathscr{H}, N$, and $H(P)$, and with $a_0 b_1 c_2 \neq 0$. The functions $1, x, x^2, y, xy, y^2, z, xz$ are all in the 7-dimensional space $L(8P)$, and $L(8P) \cup \{x^3, yz\} \subseteq L(9P)$, an 8-dimensional space. Hence there are nontrivial linear relations

$$A_1 + A_2 x + A_3 x^2 + A_4 y + A_5 xy + A_6 y^2 + A_7 z + A_8 xz = 0,$$
$$B_1 + B_2 x + B_3 x^2 + B_4 x^3 + B_5 y + B_6 xy + B_7 y^2 + B_8 z + B_9 xz + B_{10} yz = 0,$$

where the $A_i, B_i \in K$, and $A_6 A_8 B_4 B_{10} \neq 0$. Applying Siegel's lemma twice, we can assume that the coefficients have height bounded in terms of $\mathscr{H}, N$, and $H(P)$. Now eliminating z and rescaling x and y gives Nonhyp.

This establishes (3) and (4) for Nonhyp. Part (5) then follows by applying the second part of the effective Riemann-Roch theorem to the construction above.

We have now reduced the problem of effectively bounding the heights of S-integer points on a curve of genus 2 to the cases where the curve is given in the hyperelliptic forms Hyp_5 and Hyp_6, or the form Nonhyp. Effectively bounding the heights of S-integer points on Hyp_5 and Hyp_6 is accomplished by coupling Theorem 2 with a classic argument of Siegel (for current results, see [31]). Effectively bounding the heights of S-integer points on Nonhyp remains an open problem, which we relate in §4 to an S-integer point problem on the Jacobian of C.

It is easiest to describe a specific model for the Jacobian of C in the case when C is defined by a model of the form Hyp_5. We want to guarantee that rational points on any curve of genus 2 can be bounded in terms of the rational points of this model of the Jacobian.

Theorem 6. *Let C be a curve of genus 2 of height $\mathscr{H}$ and degree N. Then there is a model for C in the form Hyp_5, and a birational map $\phi\colon C \to \mathrm{Hyp}_5$, where the heights of ϕ and Hyp_5 are bounded in terms of $\mathscr{H}$ and N.*

Proof. By Theorem 5 (4), it suffices to prove this when C is of the form Hyp_6 or Nonhyp. The first case is easy: suppose C is given by $y^2 = f(x)$, where f is a sextic of bounded height. Then the Weierstrass points on C are the points $(r, 0)$ on C, where r is a root of f. Hence the Weierstrass points are of bounded height. So extending K if necessary, Theorems 5(4) gives a model Hyp_5 of bounded height.

Assume now that C is of the form Nonhyp. By what we just proved, it suffices to show that C has a model of the form Hyp_6 of bounded height. So by Theorem 5(4), if P is the unique point at infinity on Nonhyp, it suffices to show that the height of $\overline{P}$ is bounded in terms of $\mathscr{H}$. It is just as easy to make the desired transformation explicitly.

Let Nonhyp be given by $f(x, y) = x^4 + g_3(x) - y^3 - g_1(x)y^2 - g_2(x)y$. It is well known that a quartic plane curve has genus 2 only when it has a unique double point [9, p. 214]. It is easy to check that the lone point at infinity on the model is nonsingular, so the double point has some coordinates (x_0, y_0) with height bounded in terms of $\mathscr{H}$. (Indeed, if $\Delta(x)$ is the discriminant of $f(x, y)$ thought of as a cubic in y, then $\Delta(x)$ is an octic of bounded height which has x_0 as a root.) If we replace x and y by $x - x_0$ and $y - y_0$ respectively, then

the double point moves to $(0, 0)$, and Nonhyp takes the form

$$x^4 + f_3(x, y) + f_2(x, y),$$

where f_i is homogeneous of degree i for $i = 2, 3$, and f_2 and f_3 are not identically 0. Let $X = y/x$, and $Y = (x^4 - f_2(x, y))/x^3$. Then

$$Y^2 = \left(\frac{x^4 + f_2(x, y)}{x^3}\right)^2 - 4\frac{f_2(x, y)}{x^2} = f_3(1, X)^2 - 4f_2(1, X),$$

which is the desired sextic in X.

Let J be the Jacobian of C. To get explicit models for J we will now assume that C is defined by a model of the form Hyp_5: $y^2 = f(x)$.

Extending K if necessary, we can assume that f splits, so that

$$y^2 = x^5 + b_1x^4 + b_2x^3 + b_3x^2 + b_4x + b_5 = \prod_{i=1}^{5}(x - a_i),$$

where the a_i are distinct elements of K. Let W_0 denote the Weierstrass point which is the unique point at infinity on this model. The other five Weierstrass points are given by $W_i = (a_i, 0)$. Points on J can be considered as divisor classes on C, and the Riemann-Roch theorem shows that every point other than the origin O on J can be represented uniquely by a divsior of the form $P_1 + P_2 - 2W_0$, where P_1 and P_2 are points of C, with $P_2 \neq \overline{P_1}$. The divisor classes of the form $P + \overline{P} - 2W_0$ all represent the origin. Hence J can be realized by taking the symmetric product $C^{(2)}$ and blowing down the line $\{(P, \overline{P}) \mid P \in C\}$.

We embed C into J via

$$\phi\colon C \to J, \quad \phi(P) = P - W_0.$$

The image is a theta divisor which we denote by Θ. Let $U = J - \Theta$, $Y = J - [2]^*\Theta$, and $Z = J - [2]_*\Theta$, where $[2]^*\Theta$ and $[2]_*\Theta$ denote the inverse and forward image of Θ under the multiplication-by-2 maps [2].

We will be studying the S-integer points on these surfaces and need specific models. The following is an explicit model for U derived in [11].

Since J is birationally equivalent to $C^{(2)}$, we can describe functions on J as symmetric functions on C. For a point $z = (x_1, y_1) + (x_2, y_2) - 2W_0 \in J$, there are functions defined in [11]:

$$X_{22}(z) = x_1 + x_2, \quad X_{12}(z) = -x_1x_2,$$

$$X_{11} = \frac{X_{22}X_{12}^2 + 2b_1X_{12}^2 - b_2X_{22}X_{12} - 2b_3X_{12} + b_4X_{22} + 2b_5 - 2y_1y_2}{X_{22}^2 + 4X_{12}}$$

$$X_{222}(z) = (y_1 - y_2)/(x_1 - x_2), \quad X_{122}(z) = (x_1y_2 - x_2y_1)/(x_1 - x_2),$$

which are regular on U, in $L(3\Theta)$, and generate the coordinate ring $\Gamma(U)$. It was proven in [11] that

g_1: $X_{122}^2 = X_{22}X_{12}^2 - X_{11}X_{12} + b_1X_{12}^2 + b_5$,

g_2: $X_{222}^2 = X_{22}^3 + X_{12}X_{22} + b_1X_{22}^2 + b_2X_{22} + X_{11} + b_3$,

g_3: $2X_{122}X_{222} = 2X_{12}X_{22}^2 - X_{11}X_{22} + X_{12}^2 + 2b_1X_{12}X_{22} + b_2X_{12} + b_4$,

are a set of defining equations for U in $\mathbf{A}^5(K)$.

With this, we can now give the explicit model for Y, as derived in [10].

The 2-torsion points on J are the origin O and the points corresponding to the divisors $e_i = W_i - W_0$, $1 \le i \le 5$, and $e_{ij} = W_i + W_j - 2W_0$ $(1 \le i < j \le 5)$. For a point $P \in J$ let T_P denote the translation-by-P map. Then $\Theta_P = (T_P)^*\Theta$ is the divisor Θ translated by P.

Let

$$h_i = -X_{12} - a_i X_{22} + a_i^2,$$

and

$$h_{ij} = X_{11} - X_{11}(e_{ij}) + (a_i + a_j)X_{12} + a_i a_j X_{22}.$$

In [10] it is shown that the ring $\Gamma(Y)$ of regular functions on Y is generated by functions t_i, $1 \le i \le 5$, and t_{ij}, $1 \le i < j \le 5$, defined by

$$t_i(z)^2 = h_i([2]z) \quad \text{and} \quad t_{ij}(z)^2 = h_{ij}([2]z). \tag{1}$$

Furthermore,

$$(h_i) = 2T_{e_i}^*\Theta - 2\Theta, \quad (h_{ij}) = 2T_{e_{ij}}^*\Theta - 2\Theta, \tag{2}$$

so we have given Y as an unramified cover of U. We now want the equations that define Y.

Let $\mathbf{T}$ denote the set of 15 functions t_i and t_{ij}. As a convention, we let $\{i, j, k, l, m\}$ stand for any permutation of $\{1, 2, 3, 4, 5\}$.

Theorem 7 [10]. *The following* 72 *equations of six types give a nonsingular model for* Y *in* $\mathbf{A}^{15}(K)$:

$$\text{Type I } (i, j, k)\text{: } (a_j - a_i)t_k^2 + (a_i - a_k)t_j^2 + (a_k - a_j)t_i^2 = (a_j - a_i)(a_k - a_i)(a_k - a_j),$$

where $(i, j, k) = (1, 2, 3), (1, 2, 4), (1, 2, 5)$.

$$\text{Type II } (i, j, k)\text{: } t_{ij}^2 - t_{ik}^2 = (a_k - a_j)(t_i^2 - (a_i - a_l)(a_i - a_m)),$$

where $(i, j, k) = (1, 2, 3), (1, 2, 4), (1, 2, 5), (2, 1, 3), (2, 1, 4), (2, 1, 5), (3, 1, 4), (3, 1, 5), (4, 1, 5)$.

$$\text{Type III } (i, j, l, m)\text{: } t_{il}t_{im} - t_{jl}t_{jm} = (a_j - a_i)t_l t_m,$$

where $\{l, m\}$ *is any pair of indices, and* $\{i, j\}$ *is taken in turn to be any* 2 *pairs chosen from the remaining* 3 *indices.*

$$\text{Type IV } (i, j, k, l, m)\text{: } t_i t_{jk} - t_j t_{ik} = (a_i - a_j)t_{lm},$$

where $\{l, m\}$ *is any pair of indices, and* $\{i, j\}$ *is taken in turn to be any* 2 *pairs chosen from the remaining* 3 *indices.*

$$\text{Type V } (i, j, k, l, m)\text{: } t_{jk}t_{lm} - t_{jl}t_{km} = (a_j - a_m)(a_l - a_k)t_i,$$

where i *is any index, and* $\{\{j, k\}, \{l, m\}\}$ *is taken in turn to be any* 2 *partitions of the remaining* 4 *indices into pairs.*

$$\text{Type VI } (i, j, k, l)\text{: } (a_j - a_k)t_{il}t_i + (a_k - a_i)t_{jl}t_j + (a_i - a_j)t_{kl}t_k = 0,$$

where l *is any index, and* $\{i, j, k\}$ *is taken in turn to be any* 2 *triplets chosen from the remaining* 4 *indices.*

Homogenizing these equations gives a nonsingular projective model for J in $\mathbf{P}^{15}(K)$.

In fact, one can get an isomorphic variety with fewer variables (see §4), but we will need all these equations in §3. Since $a_i \in K$, this model is isomorphic to one given by Flynn [7].

A model for Z is not hard to derive from one for U. First note that $(x_1 - x_2)^2 = X_{22}(z)^2 + 4X_{12}(z) \in L(4\Theta)$ vanishes on $[2]_*\Theta$, an irreducible divisor. Since $[2]^*\Theta \equiv 4\Theta$, and the self-intersection number $\Theta \cdot \Theta = 2$, it follows that $[2]^*\Theta \cdot \Theta = 8$, and so by the projection formula, $\Theta \cdot [2]_*\Theta = 8$. Hence by the criterion of Nakai-Moishezon [13, p. 365], the divisor of zeroes of $X_{22}^2 + 4X_{12}$ must be precisely $[2]_*\Theta$. So to build a model for Z, it suffices to take a projective model for J given by a basis of $L(4\Theta)$, and to divide the basis of $X_{22}^2 + 4X_{12}$.

Specifically, define the functions

$$X_{112} = X_{12}X_{222} - X_{22}X_{122},$$
$$X_{111} = -X_{11}X_{222} - X_{12}X_{122} + 2X_{22}X_{112} + 2b_1X_{112} - b_2X_{122},$$
$$X = \tfrac{1}{2}(X_{11}X_{22} - X_{12}^2 + b_2X_{12} - b_4),$$

in $L(3\Theta)$, and

$$X_{1111} = X_{11}^2, \quad X_{1112} = X_{11}X_{12}, \quad X_{1122} = X_{11}X_{22},$$
$$X_{1222} = X_{12}X_{22}, \quad X_{2222} = X_{22}^2,$$
$$X_1 = X_{111}X_{22} + X_{11}X_{122} - 2X_{112}X_{12},$$
$$X_2 = X_{112}X_{22} + X_{11}X_{222} - 2X_{122}X_{12},$$

in $L(4\Theta)$.

It is shown in [11] that these ten functions, along with $\{X_{11}, X_{12}, X_{22}, X_{222}, X_{122}, 1\}$ give a set $\mathbf{X}$ which is a basis for $L(4\Theta)$. Since $4\Theta \equiv [2]^*\Theta$, we can get—as in the case of Theorem 7—a projective nonsingular model for J by homogenizing 72 quadrics in the variables $\mathbf{X}$. Fortunately, there is no need to write them all down. Let X_0 be the homogenizing variable. We will use

$$\begin{aligned} &X^2 + b_4X_{2222}X_{12} + X_{1111}X_{12} - b_1X_{11}(X_{1122} - 2X) \\ &\quad + b_2X_{12}X_{1122} - 2b_2XX_{12} - b_3X_{22}(X_{1122} - 2X) - b_5X_{22}X_{2222} \\ &\quad + (b_2^2 - b_3b_1)X_{1122}X_0 + 2(b_3b_1 - b_2^2)XX_0 + (b_1b_4 - b_2b_3 - b_5)X_{12}X_{22} \\ &\quad - b_5b_1X_{22}^2 + (b_3b_4 - b_5b_2)X_{22}X_0 + (b_1b_3b_4 - b_2^2b_4 - b_3b_5)X_0^2 \\ &\quad + (b_3 - b_1b_2)X_{12}X_{11} + b_2(b_2^2 - b_1b_3)X_{12}X_0 + (b_1b_4 - b_5)X_{11}X_0 = 0, \end{aligned} \tag{3}$$

$$XX_0 = \tfrac{1}{2}(X_{11}X_{22} - X_{12}^2 + b_2X_{12}X_0 - b_4X_0^2),$$
$$X_{1111}X_0 = X_{11}^2, \quad X_{1112}X_0 = X_{11}X_{12}, \quad X_{1122}X_0 = X_{11}X_{22},$$
$$X_{1222}X_0 = X_{12}X_{22}, \quad X_{2222}X_0 = X_{22}^2,$$

where the first equation in (3) comes from subtracting g_3 squared minus 4 times the product of g_1 and g_2.

Finally, to get the model for Z, we define $\rho = X_{2222} + 4X_{12}$, and then set $\xi_0 = X_0/\rho$, $\xi = X/\rho$, $\xi_i = X_i/\rho$, $\xi_{ij} = X_{ij}/\rho$, $\xi_{ijk} = X_{ijk}/\rho$, and

$\xi_{ijkl} = X_{ijkl}/\rho$, for $i \le j \le k \le l \in \{1, 2\}$. Note that $\xi_{2222} = 1 - 4\xi_{12}$. The model for Z then comes from the associated O_S-algebra

$$A_Z = O_S[\xi_0, \xi_{11}, \xi_{12}, \xi_{22}, \xi, \xi_{111}, \xi_{112}, \xi_{122}, \xi_{222}, \xi_1, \xi_2, \xi_{1111}, \xi_{1112}, \xi_{1122}, \xi_{1222}].$$

By construction, Z is nonsingular, and although we will not write down a full set of defining equations for it, we see from (3) that the set includes

$$\begin{aligned}
&\xi^2 + b_4\xi_{2222}\xi_{12} + \xi_{1111}\xi_{12} - b_1\xi_{11}(\xi_{1122} - 2\xi) + b_2\xi_{12}\xi_{1122} \\
&\quad - b_2\xi\xi_{12} - b_3\xi_{22}(\xi_{1122} - 2\xi) - b_5\xi_{22}\xi_{2222} + (b_2^2 - b_3b_1)\xi_{1122}\xi_0 \\
&\quad + 2(b_3b_1 - b_2^2)\xi\xi_0 + (b_1b_4 - b_5)\xi_{11}\xi_0 + (b_1b_4 - b_2b_3 - b_5)\xi_{12}\xi_{22} \\
&\quad - b_5b_1\xi_{22}^2 + (b_3b_4 - b_5b_2)\xi_{22}\xi_0 + (b_1b_3b_4 - b_2^2b_4 - b_3b_5)\xi_0^2 \\
&\quad + (b_3 - b_1b_2)\xi_{12}\xi_{11} + b_2(b_2^2 - b_1b_3)\xi_{12}\xi_0 = 0,
\end{aligned} \tag{4}$$

$$\xi_{2222} + 4\xi_{12} = 1, \quad \xi\xi_0 = \tfrac{1}{2}(\xi_{11}\xi_{22} - \xi_{12}^2 + b_2\xi_{12}\xi_0 - b_4\xi_0^2),$$
$$\xi_{1111}\xi_0 = \xi_{11}^2, \quad \xi_{1112}\xi_0 = \xi_{11}\xi_{12},$$
$$\xi_{1122}\xi_0 = \xi_{11}\xi_{22}, \quad \xi_{1222}\xi_0 = \xi_{12}\xi_{22}, \quad \xi_{2222}\xi_0 = \xi_{22}^2.$$

Finally, in §3 we will need one more relation from [10]. If

$$\begin{aligned}
h_{ijklm} = &- X + a_iX_{11} + (a_ja_k + a_la_m + a_i(a_j + a_k + a_l + a_m))X_{12} \\
&+ a_i(a_ja_k + a_la_m)X_{22} \\
&- a_i(a_ja_ka_l + a_ja_ka_m + a_ja_la_m + a_ka_la_m + a_i(a_la_m + a_ja_k)),
\end{aligned}$$

then

$$t_i(z)t_{jk}(z)t_{lm}(z) = h_{ijklm}([2]z). \tag{5}$$

3. S-INTEGER POINTS ON $Z = J - [2]_*\Theta$

The divisor $W = [2]_*\Theta$ was the first divisor for which it was shown (ineffectively) that $J - W$ contains only finitely many S-integer points [26]. By the Corollary to Theorem 3 it suffices to replace W by $E = [2]^*[2]_*\Theta = \sum_{e \in J[2]} \Theta_e$. By Vojta's generalization of Siegel's theorem [30], for any divisor W' whose support contains 4 distinct hyperplane sections (as E does), the integer points on $J - W'$ are degenerate; that is, they lie on a finite union of curves. An Abelian surface contains no lines, so Siegel's theorem on the finiteness of integer points on a curve of genus at least 1 gives another ineffective proof that the integer points on $J - W$ are finite. The following is an effective argument, which emulates Siegel's famous proof for reducing the study of integer points on hyperelliptic curves to the S-unit equation (see [29, Theorem IX.4.3]).

Theorem 8. *Let C be a curve of genus 2 defined over a number field K with rational Weierstrass points, one of which we denote by W_0. Let J be its Jacobian, and $C \to J$ be the embedding $P \to P - W_0$ whose image we denote by Θ. Let S be any finite set of places of K. Then the heights of the S-integer points of $Z = J - [2]_*\Theta$ can be effectively bounded.*

Proof. By the results of §§1 and 2, we can assume that C is defined by

$$y^2 = x^5 + b_1x^4 + b_2x^3 + b_3x^2 + b_4x + b_5 = \prod_{1\le i\le 5} (x - a_i),$$

where the a_i are distinct elements of K. Therefore we can use the models for U, Y, and Z given in §2. Extending S if necessary, we can assume the a_i are S-integers, and that the $a_i - a_j$ are S-units. As noted above, the Corollary to Theorem 3 shows that to bound S-integer points in $Z(K)$, extending S if necessary, it suffices to bound S-integer points on $Z' = J - \sum_{e\in J[2]} \Theta_e$ over the compositum of all quadratic extensions of K in which only primes dividing 2 or those of bad reduction for J can ramify. Applying the Corollary to Theorem 3 again, and extending K and S if necessary, it suffices to bound S-integer points on $Z'' = J - \sum_{e\in J[2]} [2]^*\Theta_e$. To make sure that we do not need to extend S in either lifting, we want to carefully choose O_S-algebras associated to Z' and Z''.

Lemma 1. *We can form associated O_S-algebras for Z' and Z'' by taking*

$$A_{Z''} = O_S[\{t \in \mathbf{T}\}, 1/\tau],$$
$$A_{Z'} = O_S[X_{11}, X_{12}, X_{22}, X_{122}, X_{222}, 1/h],$$

where $\tau = \prod_{t\in\mathbf{T}} t$, and $h = h_{12345}h_{23451}h_{31425}h_{41235}h_{51324}$.

Further, $A_{Z''}$ is integral over $A_{Z'}$, which in turn is integral over A_Z.

Proof. From (1) we see immediately that $t \in \mathbf{T}$ is integral over $A_{Z'}$, and (2) shows that $(t_i) = [2]^*\Theta_{e_i} - [2]^*\Theta$, and $(t_{ij}) = [2]^*\Theta_{e_{ij}} - [2]^*\Theta$. Hence $A_{Z''}$ defines a model for Z''. From (5) we see that $\tau(z) = h([2]z)$, so $A_{Z''}$ is integral over $A_{Z'}$, and $A_{Z'}$ defines a model for Z'. To show that $A_{Z'}$ is integral over A_Z, we must first note that

$$\xi_0([2]z) = \frac{1}{X_{22}([2]z)^2 + 4X_{12}([2]z)} = \frac{-(k(z))^4}{2^4 h(z)}, \tag{6}$$

and that

$$h_{ij}([2]z) = 4(k_{ij}(z)/k(z))^2, \tag{7}$$

where

$$k = X_{111} - X_{12}X_{122} + X_{22}X_{112},$$

and

$$\begin{aligned}
k_{ij} = {} & X_{11}^2 + 2a_ia_jX_{11}X_{22} - 2(a_ia_j(a_k + a_l + a_m) + a_ka_la_m)X_{11} \\
& + (a_ia_j + (a_i + a_j)(a_k + a_l + a_m) - a_ka_l - a_ka_m - a_la_m)X_{12}^2 \\
& + (a_ia_j(a_ka_l + a_ka_m + a_la_m) - (a_i + a_j)a_ka_la_m)X_{22}^2 \\
& + 2(a_i + a_j)X_{11}X_{12} + 2(a_ia_j(a_k + a_l + a_m) - a_ka_la_m)X_{12}X_{22} \\
& + 2((a_i^2 + a_j^2)a_ka_la_m - a_ia_j(a_i + a_j)(a_ka_l + a_ka_m + a_la_m))X_{22} \\
& - 2a_ia_j(-a_ia_j + (a_i + a_j)(a_k + a_l + a_m) + (a_ka_l + a_ka_m + a_la_m))X_{12} \\
& + (a_ia_j)^2(a_ka_l + a_ka_m + a_la_m) + 2(a_i + a_j)a_ia_ja_ka_la_m \\
& - a_ia_j(a_k^2a_l^2 + a_k^2a_m^2 + a_l^2a_m^2) + a_ka_la_m(a_i + a_j)(a_ka_l + a_ka_m + a_la_m) \\
& + a_ia_j(a_i + a_j)(a_k^2a_l + a_k^2a_m + a_l^2a_m + a_ka_l^2 + a_ka_m^2 + a_la_m^2) \\
& - a_ka_la_m(a_i^2 + a_j^2)(a_k + a_l + a_m).
\end{aligned}$$

These relations follow from the group law on the Jacobian, and were derived from the analytic theory as described in [11]. See [8] for an alternate description of the group law.

Let $\mathbf{H} = \{h_{ij} \mid 1 \le i < j \le 5\}$. Then for every quadruplet $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbf{H}$, we know that $\alpha_1\alpha_2/(X_{22}^2 + 4X_{12})$ and $\alpha_3\alpha_4/(X_{22}^2 + 4X_{12})$ are in $A(Z)$, so if we apply (6) and (7) to

$$\frac{\alpha_1([2]z)\alpha_2([2]z)\alpha_3([2]z)\alpha_4([2]z)}{(X_{22}([2]z)^2 + 4X_{12}([2]z))^2},$$

then we find that $\beta_1\beta_2\beta_3\beta_4/h$ is integral over $A(Z)$ for any $\beta_1, \beta_2, \beta_3, \beta_4 \in \mathbf{K} = \{k_{ij} \mid 1 \le i < j \le 5\}$. In other words, if we let M be the O_S-module $\sum_{\kappa\in\mathbf{K}} O_S \cdot \kappa$, and $M^{\otimes 4}$ the degree 4 terms of the algebra $O_S[\mathbf{K}]$ considered as a polynomial ring in the variables of $\mathbf{K}$, then all elements of the module $\frac{1}{h} \cdot M^{\otimes 4}$ are integral over $A(Z)$. Since $a_i - a_j$ is a unit in O_S, to complete the proof of the lemma it suffices to show that for any i, j, that $\frac{1}{h}$, h_i, h_{ij}, and $\eta_{ij} = X_{112} + (a_i + a_j)X_{122} + a_ia_jX_{222}$, are integral over $A(Z)$. But in [10] it is shown that $\eta_{ij}^2 = h_ih_jh_{ij}$, so it suffices to show that $\frac{1}{h}$, h_i, and h_{ij} are integral over $A(Z)$. Let $\mathbf{X}' = \{1, X_{12}, X_{22}, X_{11}, X_{12}^2, X_{12}X_{22}, X_{12}X_{11}, X_{22}X_{11}, X_{11}^2, X_{22}^2\}$, and let μ be the matrix expressing $\mathbf{K}$ in terms of $\mathbf{X}'$. Elementary row operations transform μ into the matrix that expresses the base of O_S^{10} obtained by taking the exterior square of the "Vandermonde base" $\{(1, a_i, a_i^2, a_i^3, a_i^4) \mid i = 1, \ldots, 5\}$ for O_S^5, in terms of the standard base for O_S^{10}. Since the determinant of the Vandermonde base with respect to the standard base is an S-unit, so too is the determinant of μ. Therefore

$$M = \sum_{g\in\mathbf{X}'} O_S \cdot g. \tag{8}$$

To finish the proof of the lemma we note that (8) immediately puts $\frac{1}{h}$ in $\frac{1}{h} \cdot M^{\otimes 4}$, and likewise

$$h_i = \frac{h_ih_1h_2h_3h_4h_5h_{12}h_{13}}{h} \frac{h_{14}h_{15}h_{23}h_{24}h_{25}h_{34}h_{35}h_{45}}{h}$$

expresses h_i as a product of elements in $\frac{1}{h} \cdot M^{\otimes 4}$. A similar expression holds for h_{ij}.

As a corollary to the lemma, with these choices of models and extending K if necessary, we have guaranteed that S-integer points of Z lift to S-integer points of Z''. So to complete the proof of the theorem, we just have to show that the heights of the S-integer points on Z'' can be effectively bounded.

First note that a point in $Z''(K)$ will be S-integral if and only if the functions in $\mathbf{T}$ take on S-unit values.

We will use the notation $\varepsilon_1 \sim \varepsilon_2$ to indicate that ε_1 and ε_2 are S-units in K whose ratio has a height which can be effectively bounded. For example, equations of types III, IV, and V in Theorem 7, and Theorem 2 show that

$$t_{il}t_{im} \sim t_lt_m, \tag{9}$$

$$t_it_{jk} \sim t_{lm}, \tag{10}$$

and that

$$t_{jk}t_{lm} \sim t_i. \tag{11}$$

Consider the S-unit

$$\tau = (t_i t_{jl})(t_{jm} t_{kl}) t_{km} (t_j t_{ik})(t_l t_{im})(t_m t_{ij})(t_{jk} t_{lm})(t_k t_{il}).$$

Then repeated use of (9), (10), and (11) gives

$$\tau \sim t_{km}(t_i t_{km})(t_{lm} t_{jk})(t_{kl} t_i) t_{jm} \sim (t_{km} t_{jl}) t_i t_{jm} t_{jm}.$$

So

$$\tau \sim t_i^2 t_{jm}^2, \tag{12}$$

and by (10),

$$\tau \sim t_{kl}^2. \tag{13}$$

By symmetry, (12) shows that $\tau \sim t_i^2 t_{kl}^2$, so combining with (13) gives $t_i^2 \sim 1$, and hence that $t_i \sim 1$. By symmetry, this holds for all i, so (10) and (11) give $t_{jk} \sim t_{lm}$, and $t_{jk} t_{lm} \sim 1$, which together give $t_{jk}^2 \sim 1$, or $t_{jk} \sim 1$. Hence all coordinate functions in $\mathbf{T}$ have bounded height at S-integer points of Z'', which completes the proof of the theorem.

Remark. The success of the proof depends on the fact that the equations of Types III, IV, and V in Theorem 7 contain only 3 monomials. The corresponding relations on the Jacobians of hyperelliptic curves of higher genus contain more monomials.

We now apply this result to integer points on C.

For any $P \in C$ we can define an embedding ϕ_P of C into J by setting

$$\phi_P(Q) = Q + P - 2W_0.$$

Recall that Θ_R denotes the translation of Θ by a point R of J. Then identifying P with its image $P - W_0$ under ϕ, the image of ϕ_P is Θ_P. We let $\mathrm{supp}(W)$ denote the support of an algebraic set $W \subseteq J$.

Proposition 3. *Let* $P \in C$.

(a) $\mathrm{supp}([2]_*\Theta \cap \Theta_P) = (P + P - 2W_0) \cup O = \phi_P(P) \cup \phi_P(\overline{P})$.

(b) *With the correct choice of models,* ϕ_P *maps points of* $C(K)$ *which are* S*-integral with respect to* P *and* $\overline{P}$ *to* S*-integer points of* $Z(K)$.

Proof. (a) Recall that every point on J other than the origin has a unique representative as a divisor on C of the form $R + S - 2W_0$, where $\{R, S\}$ is an unordered set of points of C. Points on Θ are uniquely represented in the form $R - W_0$ for R a point of C. So points on Θ_P are uniquely represented in the form $P + R - 2W_0$. If $P + R - 2W_0$ also lies on $[2]_*\Theta$, then

$$P + R - 2W_0 \equiv S + S - 2W_0,$$

for some S in C. Therefore either $P = R = S$, or $P + R - 2W_0$ represents the origin O, in which case $R = \overline{P}$.

(b) Since Θ is defined over K, K-rational functions g of J regular off $[2]_*\Theta$ restrict to K-rational functions g_P on $\phi_P(C)$, which are then integral over the coordinate ring of a model for C over K with P and $\overline{P}$ as the only points at infinity. If A is an O_S-algebra associated to this model of C, then some multiple of g_P is integral over A.

We can explicitly write down this model for C, and control which multiple of g_P we need to take.

By the geometry of numbers, extending S if necessary we can assume that O_S is a principal ideal domain. Hence if $\alpha \in K$ is nonzero, then we can write $\alpha = a/b$ with a and b relatively prime—i.e., the O_S-ideal they generate $(a, b)O_S$ is equal to O_S—and be sure that there are S-integers c and d such that $bd - ac = 1$.

If $f(x)$ is a polynomial in x, we let $f^{(i)}(x)$ denote its ith-derivative divided by $i!$.

Theorem 9. *Let C be a curve of genus 2 defined over a number field K by an equation*

$$\mathrm{Hyp}_5\colon y^2 = f(x) = x^5 + b_1x^4 + b_2x^3 + b_3x^2 + b_4x + b_5,$$

and S a finite set of places of K, chosen large enough so that O_S is a principal ideal domain which contains the b_i.

Let $P = (x_P, y_P) \in C(K)$ be a non-Weierstrass point. Write $x_P = a/b$, such that $(a, b)O_S = O_S$. Pick c, d in O_S such that $bd - ac = 1$. Then there is an effectively computable bound B which depends on $H(b_i)$, d_K, D_K, and S, but not on P, such that

(i) *The S-integer points (u, w, z) on the model for C given by*

$$\mathrm{Hyp}_6(P)\colon w^2 = 4y_P^2 \sum_{i=0}^{5} f^{(i)}(x_P) z^{6-i}, \qquad z = b^2u + bc,$$

have $H(z) < B$; and

(ii) *If $H(x_P) > B$, then the model $\mathrm{Hyp}_6(P)$ has no S-integer points.*

Remark. Of course, Faltings's theorem [5] gives an ineffective bound B, depending on $H(b_i)$, d_K, and D_K, such that $C(K)$ has no points at all satisfying $H(x_P) > B$.

Proof. It follows from the group law on J [11] that the function

$$-\xi_{12} - x_P\xi_{22} + x_P^2\xi_0$$

has $\Theta_P + \Theta_{\overline{P}}$ as its divisor of zeroes. Hence writing $(\Xi)_P$ for the restriction of a function Ξ to Θ_P, we have

$$-(\xi_{12})_P - x_P(\xi_{22})_P + x_P^2(\xi_0)_P = 0. \tag{14}$$

We define a function z on Θ_P by setting $z = (\xi_{22})_P - 2x_P(\xi_0)_P$. Then sequential calculations with (4) and (14) give us

$$(\xi_0)_P = z^2, \quad (\xi_{22})_P = z + 2x_Pz^2, \quad (\xi_{12})_P = -x_Pz - x_P^2z^2. \tag{15}$$

We now define a function v on Θ_P by setting

$$(\xi_{11})_P = zv. \tag{16}$$

Then from (4) we get

$$\begin{aligned} (\xi_{1111})_P &= v^2, \quad (\xi_{1112})_P = v(-x_P - x_P^2z), \\ (\xi_{1122})_P &= v(1 + 2x_Pz), \quad (\xi_{1222})_P = (1 + 2x_Pz)(-x_P - x_P^2z), \\ (\xi)_P &= \tfrac{1}{2}(v(1 + 2x_Pz) - (x_P + x_P^2z)^2 - b_2(x_Pz + x_P^2z^2) - b_4z^2). \end{aligned} \tag{17}$$

Finally, plugging these values into (4), we get the equation

$$w^2 = 4y_P^2 \sum_{i=0}^{5} f^{(i)}(x_P) z^{6-i},$$

where $w = v - 2z^3 f(x_P) - z^2 f^{(1)}(x_P) - z(4x_P^3 + 2b_1 x_P^2 + b_2 x_P) - x_P^2$.

From g_1, g_2, g_3, and the definitions of X_{112}, X_{111}, X_1, and X_2, it can be shown that ξ_{111}, ξ_{112}, ξ_{122}, ξ_{222}, ξ_1, and ξ_2 are integral over

$$\mathcal{O}_S[\xi_0, \xi_{11}, \xi_{12}, \xi_{22}, \xi, \xi_{1111}, \xi_{1112}, \xi_{1122}, \xi_{1222}].$$

So if we now set $z = b^2 u + bc$, using the definition of w above, (15), (16), and (17) show that S-integer points of $\mathrm{Hyp}_6(P)$ map into S-integer points of Z, and z has height bounded independently of P.

To prove (ii), we note that if Q is an S-integer point of $\mathrm{Hyp}_6(P)$, then $((\xi_{22} \pm \sqrt{\xi_0})/2\xi_0)(\phi_P(Q)) = x_P$, and hence if such a Q exists, then $H(x_P)$ must also be bounded.

Remark. Since $u = -c/b$, $z = w = 0$, is a K-point on $\mathrm{Hyp}_6(P)$ which is S-integral whenever P is S-integral on Hyp_5, we recover the effective bounding of S-integer points on Hyp_5.

4. S-INTEGER POINTS ON $U = J - \Theta$

This section is a rather extended comment about how one might attempt to effectively bound the heights of points in $C(K)$ which are S-integral with respect to any $P \in C$. For such a P we can define an embedding ψ_P of C into J by setting $\psi_P(Q) = 2P - Q - W_0$. Hence the image of ψ_P is Θ_{2P}.

Proposition 4. *Suppose $P \in C$ is not a Weierstrass point.*

(a) $$\mathrm{supp}(\Theta \cap \Theta_{2P}) = P - W_0 = \psi_P(P).$$

(b) *With the correct choice of models, ψ_P maps points of $C(K)$ which are S-integral with respect to P to S-integer points of $U(K)$.*

Proof. (a) If a point $R - W_0$ on Θ also lies on Θ_{2P}, then

$$R - W_0 \equiv S - W_0 + 2(P - W_0)$$

for some S in C. Therefore $R + \overline{S} - 2W_0 \equiv 2P - 2W_0$, and hence $R = \overline{S} = P$, for otherwise $2P - 2W_0$ represents the origin. But the latter case cannot hold when P is not a Weierstrass point.

(b) Since Θ is defined over K, K-rational functions g and J regular off Θ restrict to K-rational functions g_P on $\psi_P(C)$, which are then integral over the coordinate ring of a model for C over K with P as the only point at infinity. If A is an O_S-algebra associated to this model of C, then some multiple of g_P is integral over A.

We can explicitly write down this model. We can also control which multiple of g_P we need to take, but not so uniformly as in Theorem 9.

Proposition 5. *Let C be a curve of genus 2 defined over a number field K by an equation*

$$\mathrm{Hyp}_5 : y^2 = f(x) = x^5 + b_1 x^4 + b_2 x^3 + b_3 x^2 + b_4 x + b_5,$$

and S a finite set of places of K, chosen large enough so that O_S is a principal ideal domain which contains the b_i. Let $P = (x_P, y_P) \in C(K)$ be a non-Weierstrass point. Write $x_P = a/b^2$, $y_P = c/b^5$ such that $(a, b)O_S = O_S$. Extend S so that bc is invertible. Let f_i denote $f^{(i)}(x_P)$ for $0 \le i \le 4$. Then the S-integer points on the model for C given by

(18)

$$\begin{aligned}\text{Nonhyp}(P)\colon\ & v^3\{-64f_0^3\} + v^3\{(64f_0^2f_1)u + (16f_2^2f_0^2 - 64f_0^3f_4 + f_1^4 - 8f_1^2f_2f_0)\} \\ & + v\{-8f_0(f_1^2 + 4f_0f_2)u^2 - 8f_0(4f_0f_2f_3 - f_1^2f_3 - 8f_0f_1f_4 + 8f_0^2)u \\ & \qquad + 8f_0(4f_0f_1f_2 - 8f_0^2f_3 - f_1^3)\} \\ = {} & -\{16f_0^2\}u^4 - \{32f_0^2f_3\}u^3 + \{16f_0(f_1^2f_4 - 2f_0f_1 - f_0f_3^2)\}u^2 \\ & - \{4f_1(f_1^3 + 8f_3f_0^2 - 4f_0f_1f_2)\}u\end{aligned}$$

map under ψ_P into integer points of $U(K)$.

Proof. It follows from the group law on J that the function

$$X_{11} - X_{11}([2]P) + 2x_PX_{12} + x_P^2X_{22}$$

has $\Theta_{2P} + \Theta_{2\overline{P}}$ as its divsior of zeroes. Hence writing $(\chi)_P$ for the restriction of a function χ to Θ_{2P}, we have

$$(X_{11})_P - X_{11}([2]P) + 2x_P(X_{12})_P + x_P^2(X_{22})_P = 0. \tag{19}$$

We define functions u and v on Θ_{2P} by setting

$$u = (X_{12})_P + x_P(X_{22})_P - x_P^2, \quad v = (X_{22})_P - 2x_P.$$

Then we have

$$(X_{12})_P = u - x_Pv - x_P^2, \quad (X_{22})_P = v + 2x_P. \tag{20}$$

Then from (19) and g_2:

$$\begin{aligned}(X_{11})_P &= X_{11}([2]P) + x_P^2v - 2x_Pu \\ &= \frac{b^{10}(f^{(1)}(a/b))^2}{4c^2} - 6(a/b^2)^3 - 4b_1(a/b^2)^2 \\ &\quad - 2b_2(a/b^2) - b_3 + x_P^2v - 2x_Pu.\end{aligned} \tag{21}$$

Plugging these values into (3) gives (18). Since X_{111}, X_{112}, X_{122}, X_{222}, and X are integral over $O_S[X_{11}, X_{12}, X_{22}]$, and since

$$C \xrightarrow{\psi_P} J \xrightarrow{\pi} K,$$

but this is sufficient because $\psi_P(C)$ maps isomorphically onto $\pi(\psi_P(C))$. Since $2bc$ is invertible, (20) and (21) show that S-integer points of Nonhyp(P) map into S-integer points of $U(K)$.

Remark. Faltings has proved that there are only finitely many S-integer points in $U(K)$. If there were an effective bound for these points, then the proof of the proposition would give an effective bound for the S-integer points on Nonhyp(P).

The heights of integer points on hyperelliptic curves have been effectively bounded by employing Siegel's reduction to the S-unit equation. One might try, *à la Siegel*, to turn the problem of effectively bounding the S-integer points

on U into that of solving "S-unit" equations, where now the S-units lie in some algebraic group other than the multiplicative group $\mathbf{G}_m$! We can build linear relations among the entries of 3×3-S-integer orthogonal matrices of determinant 1, which in several ways give us linear relations among special elements of $GL_2(O_S)$ which are reminiscent of the classical S-unit equation.

By the Corollary of Theorem 3, once again extending K if necessary, it suffices to effectively bound the S-integer points on $Y = J - [2]^*\Theta$. That is, we need to effectively bound the heights of points in $J(K)$ for which the functions in $\mathbf{T}$ take on S-integer values.

We now expand S so that $a_i - a_j$ is invertible, and adjoin all the square roots $\zeta_{ij} = \sqrt{a_i - a_j}$, $1 \le i < j \le 5$ to K, where the choice of square roots is fixed once and for all. Also adjoin a fixed square root $\sqrt{-1}$ and set $\zeta_{ji} = \sqrt{-1}\zeta_{ij}$ for $i < j$.

It now follows from Theorem 7 that the matrix M_{ijklm} given by

$$\begin{pmatrix} \dfrac{t_i}{\zeta_{ij}\zeta_{ik}} & \dfrac{t_j}{\zeta_{ji}\zeta_{jk}} & \dfrac{t_k}{\zeta_{ki}\zeta_{kj}} \\ \dfrac{t_{il}}{\zeta_{ij}\zeta_{ik}\zeta_{lm}} & \dfrac{t_{jl}}{\zeta_{ji}\zeta_{jk}\zeta_{lm}} & \dfrac{t_{kl}}{\zeta_{ki}\zeta_{kj}\zeta_{lm}} \\ \dfrac{t_{im}}{\zeta_{ij}\zeta_{ik}\zeta_{ml}} & \dfrac{t_{jm}}{\zeta_{ji}\zeta_{jk}\zeta_{ml}} & \dfrac{t_{km}}{\zeta_{ki}\zeta_{kj}\zeta_{ml}} \end{pmatrix}$$

is an S-integral element of the determinant 1 subgroup of the orthogonal group, which we denote as O_3^+. This is an algebraic version of a classical result in theta functions explicitly stated by Hudson [14] and H. F. Baker [2]. It can also be derived from Frobenius's relations on hyperelliptic theta functions [17].

Theorem 7 also shows that $\overline{\mathbf{T}} = \{t_1, t_2, t_3, t_4, t_{15}, t_{25}, t_{35}, t_{45}\}$ generates $\Gamma(Y)$. Lemma 6 of [10] then states that the orthogonality of M_{12354} and M_{12453} determines generators for the ideal of relations among the variables in $\overline{\mathbf{T}}$. Note that the third row of an orthogonal matrix can be found by taking the cross-product of the first two rows, so finding S-integer points on Y is equivalent to finding S-integer values of $\overline{\mathbf{T}}$ such that M_{12354} and M_{12453} are orthogonal.

This compares nicely with the last line of p. 255 of [29], which implies that integer points on an elliptic curve give rise to orthogonal 2×2-S-integer matrices over an extension field. But the analogy soon ends. Unlike $O_2^+ = \mathbf{G}_m$, which has unramified covers of every degree, O_3^+ has only a degree 2 unramified spinor cover from the group of quaternions of norm 1. However, there are relations among the entries of the M_{ijklm} analogous to those of the orthogonal matrices which arise in the elliptic case.

Indeed, comparing the top two rows of the orthogonal matrices M_{12354}, M_{12453}, M_{13452}, and M_{23451} gives us

$$(22)\quad \sum_{i=1}^{4} \beta_i \mu_i = 0, \quad \sum_{i=1}^{4} \beta_i \nu_i = 0, \quad \operatorname{trace}(\mu_i \nu_i^{-1}) = 0, \qquad (i = 1, \dots, 4),$$

where

$$\begin{aligned} \beta_1 &= \zeta_{42}(\zeta_{14}\zeta_{23} + \zeta_{12}\zeta_{34} - \zeta_{13}\zeta_{24}), \\ \beta_2 &= \zeta_{23}(\zeta_{41}\zeta_{23} + \zeta_{12}\zeta_{34} - \zeta_{31}\zeta_{24}), \\ \beta_3 &= (\sqrt{-1} - 1)\zeta_{12}\zeta_{23}\zeta_{24}, \end{aligned}$$

and

$$\beta_4 = \zeta_{12}(\zeta_{13}\zeta_{24} - \zeta_{41}\zeta_{23} - \zeta_{12}\zeta_{34})$$

are S-units, and

$$\mu_1 = \begin{pmatrix} t_2\zeta_{13} - t_1\zeta_{23} & t_3\zeta_{12} \\ -t_3\zeta_{12} & -t_1\zeta_{23} - t_2\zeta_{13} \end{pmatrix},$$

$$\mu_2 = \begin{pmatrix} t_1\zeta_{24} + t_2\zeta_{14} & t_4\zeta_{21} \\ t_4\zeta_{21} & t_1\zeta_{24} - t_2\zeta_{14} \end{pmatrix},$$

$$\mu_3 = \begin{pmatrix} t_1\zeta_{34} & t_3\zeta_{41} + t_4\zeta_{31} \\ t_4\zeta_{31} - t_3\zeta_{41} & t_1\zeta_{34} \end{pmatrix},$$

$$\mu_4 = \begin{pmatrix} -t_2\zeta_{43} & t_3\zeta_{42} + t_4\zeta_{32} \\ t_4\zeta_{32} - t_3\zeta_{42} & t_2\zeta_{43} \end{pmatrix},$$

$$\nu_1 = \begin{pmatrix} t_{25}\zeta_{13} - t_{15}\zeta_{23} & t_{35}\zeta_{12} \\ -t_{35}\zeta_{12} & -t_{15}\zeta_{23} - t_{25}\zeta_{13} \end{pmatrix},$$

$$\nu_2 = \begin{pmatrix} t_{15}\zeta_{24} + t_{25}\zeta_{14} & t_{45}\zeta_{21} \\ t_{45}\zeta_{21} & t_{15}\zeta_{24} - t_{25}\zeta_{14} \end{pmatrix},$$

$$\nu_3 = \begin{pmatrix} t_{15}\zeta_{34} & t_{35}\zeta_{41} + t_{45}\zeta_{31} \\ t_{45}\zeta_{31} - t_{35}\zeta_{41} & t_{15}\zeta_{34} \end{pmatrix},$$

$$\nu_4 = \begin{pmatrix} -t_{25}\zeta_{43} & t_{35}\zeta_{42} + t_{45}\zeta_{32} \\ t_{45}\zeta_{32} - t_{35}\zeta_{42} & t_{25}\zeta_{43} \end{pmatrix}$$

are in $GL_2(O_S)$, and of fixed determinant given by Theorem 7. Although the μ and ν have the same form, they have different determinants.

Somewhat more appealing are the relations between the left columns and top rows of M_{51234}, M_{51324}, M_{52413}, and M_{53412}. They give us

$$\sum_{i=1}^{4} M_i = 0, \quad \sum_{i=1}^{4} N_i = 0, \tag{23}$$

where

$$M_1 = \begin{pmatrix} t_5(\zeta_{15} - \zeta_{25}) & -t_{15} + t_{25} \\ t_{15} + t_{25} & t_5(\zeta_{15} + \zeta_{25}) \end{pmatrix},$$

$$M_2 = \begin{pmatrix} t_5(\zeta_{25} - \zeta_{35}) & -t_{25} + t_{35} \\ -t_{25} - t_{35} & -t_5(\zeta_{25} + \zeta_{35}) \end{pmatrix},$$

$$M_3 = \begin{pmatrix} t_5(\zeta_{35} - \zeta_{45}) & -t_{35} + t_{45} \\ t_{35} + t_{45} & t_5(\zeta_{35} + \zeta_{45}) \end{pmatrix},$$

$$M_4 = \begin{pmatrix} t_5(\zeta_{45} - \zeta_{15}) & -t_{45} + t_{15} \\ -t_{45} - t_{15} & -t_5(\zeta_{45} + \zeta_{15}) \end{pmatrix},$$

$$N_1 = \begin{pmatrix} t_5(\frac{1}{\zeta_{15}} - \frac{1}{\zeta_{25}}) & t_1/\zeta_{15} - t_2/\zeta_{25} \\ t_1/\zeta_{15} + t_2/\zeta_{25} & t_5(\frac{1}{\zeta_{15}} + \frac{1}{\zeta_{25}}) \end{pmatrix},$$

$$N_2 = \begin{pmatrix} t_5(\frac{1}{\zeta_{25}} - \frac{1}{\zeta_{35}}) & t_2/\zeta_{25} - t_3/\zeta_{35} \\ -t_2/\zeta_{25} - t_3/\zeta_{35} & -t_5(\frac{1}{\zeta_{25}} + \frac{1}{\zeta_{35}}) \end{pmatrix},$$

$$N_3 = \begin{pmatrix} t_5(\frac{1}{\zeta_{35}} - \frac{1}{\zeta_{45}}) & t_3/\zeta_{35} - t_4/\zeta_{45} \\ t_3/\zeta_{35} + t_4/\zeta_{45} & t_5(\frac{1}{\zeta_{35}} + \frac{1}{\zeta_{45}}) \end{pmatrix},$$

$$N_4 = \begin{pmatrix} t_5(\frac{1}{\zeta_{45}} - \frac{1}{\zeta_{15}}) & t_4/\zeta_{45} - t_1/\zeta_{15} \\ -t_4/\zeta_{45} - t_1/\zeta_{15} & -t_5(\frac{1}{\zeta_{45}} + \frac{1}{\zeta_{15}}) \end{pmatrix}$$

are matrices in $GL_2(O_S)$, again with fixed determinant given by Theorem 7.

Note that aside from matrices of the form

$$\begin{pmatrix} \pm 1 & 0 & 0 \\ 0 & * & * \\ 0 & * & * \end{pmatrix}, \tag{24}$$

a matrix in O_3^+ is determined by its left column and top row. The matrix M_{ijklm} is of the form (24) only at points of Y which lie over $e_{jk} \in J[2]$.

I have no idea how to solve (22) or (23), nor whether it is any easier to restrict the equations to $[2]^*\psi_P(C)$. It is curious to wonder whether (22) or (23) expresses a tractable question about S-units which simultaneously lie in different quadratic extensions of K.

References

1. A. Baker, *Bounds for the solutions of hyperelliptic equations*, J. London Math. Soc. **43** (1968), 1–9.
2. H. F. Baker, *An introduction to the theory of multiply periodic functions*, Cambridge Univ. Press, 1907.
3. J. Coates, *Construction of rational functions on a curve*, Proc. Cambridge Philos. Soc. **67** (1970), 105–123.
4. K. Coombes and D. Grant, *On heterogeneous spaces*, J. London Math. Soc. (2) **40** (1989), 385–397.
5. G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366.
6. ———, *Diophantine approximation on abelian varieties*, Ann. of Math. **133** (1991), 549–576.
7. E. V. Flynn, *The Jacobian and formal group of a curve of genus* 2 *over an arbitrary ground field*, Math. Proc. Cambridge Philos. Soc. **107** (1990), 425–441.
8. ———, *The group law on the Jacobian of a curve of genus* 2, J. Reine Angew. Math. **439** (1993), 45–69.
9. W. Fulton, *Algebraic curves*, Addison-Wesley, 1989.
10. D. Gordon and D. Grant, *Computing the Mordell-Weil rank of Jacobians of curves of genus* 2, Trans. Amer. Math. Soc. **337** (1993), 807–824.
11. D. Grant, *Formal groups in genus two*, J. Reine Angew. Math. **411** (1990), 96–121.
12. K. Győry, *On the number of solutions of linear equations in units of an algebraic number field*, Comment. Math. Helv. **54** (1979), 583–600.
13. R. Hartshorne, *Algebraic geometry*, Springer-Verlag, 1977.
14. R. W. H. T. Hudson, *Kummer's quartic surface*, Cambridge Univ. Press, 1905.
15. S. Lang, *Fundamentals of Diophantine geometry*, Springer-Verlag, 1983.
16. ———, *Algebraic number theory*, Springer-Verlag, 1986.
17. D. Mumford, *Tata lectures on theta,* I, II, Progress in Math., vols. 28, 43, Birkhäuser, Boston, Mass., 1983, 1984.
18. H. Matsumura, *Commutative ring theory*, Cambridge Univ. Press, 1989.
19. W. Schmidt, *Construction and estimation of bases in function fields*, J. Number Theory **39** (1991), 181–224.
20. ———, *Diophantine approximation and Diophantine equations*, Lecture Notes in Math., vol. 1467, Springer-Verlag, 1991.
21. ———, *Integer points on curves of genus* 1, Compositio Math. **91** (1992), 33–59.
22. J.-P. Serre, *Lectures on the Mordell-Weil Theorem*, Vieweg, 1989.
23. J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. of Math. **88** (1968), 492–517.

24. C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen* (1929), Abh. Preuss. Akad. d. Wiss. Math. Phys. Kl., Nr. 1; Collected Works, Springer-Verlag, 1966, pp. 209–266.
25. ——— (Under the pseudonym X), *The integer solutions of the equation* $y^2 = ax^n + bx^{n-1} + \cdots + k$, J. London Math. Soc. **1** (1926), 66–68; Collected Works, Springer-Verlag, 1966, pp. 207–208.
26. J. Silverman, *Integral points on abelian varieties*, Invent. Math. **81** (1985), 341–346.
27. ———, *Integral points on abelian surfaces are widely spaced*, Compositio Math. **61** (1987), 253–266.
28. ———, *Integral points on curves and surfaces*, Lecture Notes in Math., vol. 1380, Springer-Verlag, 1989.
29. ———, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1986.
30. P. Vojta, *Diophantine approximations and value distribution theory*, Lecture Notes in Math., vol. 1239, Springer-Verlag, 1987.
31. P. Voutier, *An upper bound for the size of solutions of* $y^m = f(x)$, J. Number Theory (to appear).

Department of Mathematics, University of Colorado at Boulder, Boulder, Colorado 80309
E-mail address: grant@boulder.colorado.edu