Aaron LEVIN

Siegel's theorem and the Shafarevich conjecture

Siegel's theorem and the Shafarevich conjecture

par AARON LEVIN

RÉSUMÉ. Il est connu que dans le cas des courbes hyperelliptiques la conjecture de Shafarevich peut être rendue effective, c'est à dire, pour tout corps de nombres k et tout ensemble fini de places S de k, on peut effectivement calculer l'ensemble des classes d'isomorphisme des courbes hyperelliptiques sur k ayant bonne réduction en dehors de S. Nous montrons ici qu'une extension de ce résultat à une version effective de la conjecture de Shafarevich pour les *Jacobiennes* de courbes hyperelliptiques de genre g impliquerait une version effective du théorème de Siegel pour les points entiers sur les courbes hyperelliptiques de genre g.

ABSTRACT. It is known that in the case of hyperelliptic curves the Shafarevich conjecture can be made effective, i.e., for any number field k and any finite set of places S of k, one can effectively compute the set of isomorphism classes of hyperelliptic curves over k with good reduction outside S. We show here that an extension of this result to an effective Shafarevich conjecture for *Jacobians* of hyperelliptic curves of genus g would imply an effective version of Siegel's theorem for integral points on hyperelliptic curves of genus g.

1. Introduction

The famous 1929 theorem of Siegel [30] on integral points on affine curves states (in a formulation convenient for us):

Theorem 1.1 (Siegel). *Let C be a curve over a number field k, S a finite set of places of k containing the archimedean places, $\mathcal{O}_{k,S}$ the ring of S-integers, and $f \in k(C)$ a nonconstant rational function on C. If C is a rational curve then we assume further that f has at least three distinct poles. Then the set of S-integral points of C with respect to f,*

$$C(f, k, S) = \{P \in C(k) \mid f(P) \in \mathcal{O}_{k,S}\},$$

is finite.

While Siegel's theorem is completely satisfactory from a qualitative viewpoint, all known proofs of the theorem suffer from the defect of being ineffective, i.e., in general there is no known algorithm for explicitly computing

the set $C(f, k, S)$ (when it is finite). In the classical proofs of Siegel's theorem, this ineffectivity arises from the use of Roth's theorem from Diophantine approximation (for a survey on the use of Roth's theorem in Siegel's theorem, including some remarks on effectivity, see [34]). Finding an effective version of Siegel's theorem remains a longstanding important open problem.

Of course, in certain special cases there are known techniques for effectively computing $C(f, k, S)$. In this context, the most powerful and widely used effective techniques come from Baker's theory of linear forms in logarithms [2]. Using these techniques, Baker and Coates [3] proved an effective version of Siegel's theorem for curves of genus zero and genus one. Already for curves of genus two, however, it is an open problem to prove an effective version of Siegel's theorem. More generally, we will be interested here in studying this problem for hyperelliptic curves:

Problem 1.1. *Find an effective version of Siegel's theorem for curves C of genus two. More generally, find an effective version of Siegel's theorem for hyperelliptic curves C.*

Again, in certain special cases, Problem 1.1 has been solved. For instance, if C is a (nonsingular projective) hyperelliptic curve over a number field k, i denotes the hyperelliptic involution of C, and $f \in k(C)$ is a rational function that has a pole at both P and $i(P)$ for some point $P \in C(\bar{k})$ (where we allow $P = i(P)$), then $C(f, k, S)$ is effectively computable for any appropriate finite set of places S. This is essentially equivalent to effectively finding all solutions $x, y \in \mathcal{O}_{k,S}$ to hyperelliptic equations of the form

$$(1.1) \qquad y^2 = a_n x^n + \cdots + a_0, \quad x, y \in \mathcal{O}_{k,S},$$

where $a_0, \ldots, a_n \in k$ are constants and the equation defines a hyperelliptic curve. Explicit bounds for the solutions to (1.1) (when $\mathcal{O}_{k,S} = \mathbb{Z}$) were first given by Baker [1]. Along the lines of equation (1.1), we note that using Riemann-Roch it is possible to restate Problem 1.1 as a question about integral solutions to certain specific types of equations. For instance, if C has genus two, Problem 1.1 is equivalent to solving equations of the form (1.1) (with $n = 5, 6$) and equations of the form

$$y^3 + g_1(x)y^2 + g_2(x)y = x^4 + g_3(x), \quad x, y \in \mathcal{O}_{k,S},$$

where $g_i \in k[x]$ has degree $\leq i$. We refer the reader to [13] or [26] for details.

When C has genus two, Bilu [5] has shown that there exists an infinite set $M \subset C(\bar{k})$ such that if f has poles at two distinct points of M, then $C(f, k, S)$ is effectively computable. The method of [5] combines linear forms in logarithms with functional units and coverings of curves, and the exact limitations of the method do not yet seem to be fully understood. Another interesting alternative approach to an effective Siegel's theorem

for genus two curves is given by Grant in [13]. There, the problem is reduced to questions about integral points on a certain affine subset of the Jacobian of C, which in turn are reduced to certain "non-Abelian S-unit equations".

A final case of particular note where an effective version of Siegel's theorem is known is the case of geometrically Galois coverings of the projective line, proved independently by Bilu [4] and Dvornicich and Zannier [10] (partial results were also obtained in [16] and [26]). This generalizes, in a qualitative way, the aforementioned results of Baker and Coates [3] and Baker [1] on integral points on elliptic curves and hyperelliptic curves, respectively. Quantitative results in this context were proven by Bilu in [6]. We refer the reader to [5] for more general statements and other cases of an effective Siegel's theorem.

When C is a curve of genus $g \geq 2$, Siegel's theorem is superseded by Faltings' theorem (Mordell's Conjecture), which states that in this case the set of rational points $C(k)$ is finite for any number field k. Faltings' proof of the Mordell conjecture [12] used a reduction (due to Parshin) to the Shafarevich conjecture, proved by Faltings in the same paper. Moreover, Rémond has shown [27] that an effective version of the Shafarevich conjecture would imply an effective version of Faltings' theorem. In a similar vein, we will show that Problem 1.1 can be reduced to proving an effective version of a restricted form of the Shafarevich conjecture (hyperelliptic Jacobians). For instance, we will show that an effective version of Siegel's theorem for genus two curves follows from an effective version of the Shafarevich conjecture for abelian surfaces.

Before stating the main theorem, we make a few more definitions. For a nonsingular projective curve C, we let $\mathrm{Jac}(C)$ denote the Jacobian of C. Let $g \geq 2$ be an integer, k a number field, and S a finite set of places of k, which we will always assume contains the archimedean places. Define

$$\mathcal{H}(g, k, S) = \{k\text{-isomorphism classes of (nonsingular projective) hyperelliptic curves over } k \text{ of genus } g \text{ with good reduction outside } S\}$$

and

$$\mathcal{H}'(g, k, S) = \{k\text{-isomorphism classes of hyperelliptic curves } C \text{ over } k \text{ of genus } g \text{ such that } \mathrm{Jac}(C) \text{ has good reduction outside } S\}.$$

As is well known, if C has good reduction at a place v then so does $\mathrm{Jac}(C)$. In other words, we have $\mathcal{H}(g, k, S) \subset \mathcal{H}'(g, k, S)$. In general, this set inclusion is proper. In fact, as we will see, understanding the difference between the two sets is in some sense the key to solving Problem 1.1. It follows from the Shafarevich conjecture for abelian varieties, proved by Faltings, that the set $\mathcal{H}'(g, k, S)$ is finite. We now state our main result.

Theorem 1.2. *Let $g \geq 2$ be an integer. Suppose that for any number field k and any finite set of places S of k the set $\mathcal{H}'(g, k, S)$ is effectively computable (e.g., an explicit hyperelliptic Weierstrass equation for each element of the set is given). Then for any number field k, any finite set of places S of k, any hyperelliptic curve C over k of genus g, and any rational function $f \in k(C)$, the set of S-integral points with respect to f,*

$$C(f, k, S) = \{P \in C(k) \mid f(P) \in \mathcal{O}_{k,S}\},$$

is effectively computable.

We now give a brief outline of the proof of Theorem 1.2. To each point $P \in C(f, k, S)$ we associate a certain double cover $\pi_P : \tilde{C}_P \to C$ such that $\tilde{C}_P$ has good reduction outside some fixed finite set of places T of some number field L (with T and L independent of P). Associated to π_P we have a classical construction, the Prym variety $\mathrm{Prym}(\tilde{C}_P/C)$. When C is hyperelliptic, it will turn out that $\mathrm{Prym}(\tilde{C}_P/C)$ is isomorphic to the Jacobian $\mathrm{Jac}(X_P)$ of some hyperelliptic curve X_P and $\mathrm{Jac}(X_P)$ has good reduction outside of T. This yields a map $C(f, k, S) \to \mathcal{H}'(g, L, T)$, $P \mapsto X_P$, and if $\mathcal{H}'(g, L, T)$ is known then $C(f, k, S)$ can be explicitly computed. We note that an analogous construction essentially works for any curve C (except that $\mathrm{Prym}(\tilde{C}_P/C)$ will not be a hyperelliptic Jacobian, or even a Jacobian, for general C), but we focus on the hyperelliptic case as there are reasons to believe that effectively computing $\mathcal{H}'(g, k, S)$ may be a tractable problem.

Indeed, a primary reason for this hope is that the set $\mathcal{H}(g, k, S)$ is known to be effectively computable, i.e., there is an effective version of the Shafarevich conjecture for hyperelliptic curves.

Theorem 1.3 (Effective Shafarevich conjecture for hyperelliptic curves, von Känel [15])**.** *Let $g \geq 2$ be an integer, k a number field, and S a finite set of places of k. The set $\mathcal{H}(g, k, S)$ is effectively computable.*

The finiteness of $\mathcal{H}(g, k, S)$ goes back to work of Shafarevich [29], Merriman [19], Parshin [24], and Oort [23]. Building on earlier work of Merriman and Smart [20], Smart [33] explicitly computed the set $\mathcal{H}(2, \mathbb{Q}, \{2, \infty\})$ using effective results of Evertse and Györy [11] on related problems concerning discriminants of binary forms. Using the results of Evertse and Györy [11] and a result of Liu [18], von Känel [15] proved explicit bounds for the heights of Weierstrass models of the hyperelliptic curves represented in $\mathcal{H}(g, k, S)$. We note that the much earlier proof of Oort [23] also yields a certain weaker version of Theorem 1.3.[1]

---

[1]Oort's proof of finiteness in [23] (implicitly) yields a fixed computable finite extension L of k and effective bounds for the heights of Weierstrass models *over L* of the hyperelliptic curves represented in $\mathcal{H}(g, k, S)$.

In [25], Poonen raised the problem of extending the computations of Merriman and Smart to an effective computation of $\mathcal{H}'(2, \mathbb{Q}, \{2, \infty\})$. Our results give additional motivation and importance, coming from Siegel's theorem, to the problem of extending Theorem 1.3 from the set $\mathcal{H}(g, k, S)$ to the set $\mathcal{H}'(g, k, S)$. In view of Theorems 1.2 and 1.3, to solve Problem 1.1 it would suffice to solve the following problem:

Problem 1.2. *Find an effective bound $B(g, k, S)$ such that if C is a hyperelliptic curve of genus g over k and $\mathrm{Jac}(C)$ has good reduction outside S, then C has good reduction at all primes $\mathfrak{p}$ of k with norm $\mathrm{N}(\mathfrak{p}) > B(g, k, S)$.*

Note that an ineffective bound $B(g, k, S)$ follows trivially from the finiteness of $\mathcal{H}'(g, k, S)$.

2. Parshin's construction

Parshin [24] was the first to notice that the Mordell conjecture could be obtained as a consequence of the Shafarevich conjecture. The basic idea is to associate to each rational point $P \in C(k)$ a covering $\pi_P : \tilde{C}_P \to C$ such that the curve $\tilde{C}_P$ has good reduction outside a finite set S (independent of P) and π_P has certain specified ramification. We will use a similar construction to study integral points on curves.

Theorem 2.1. *Let C be a nonsingular projective curve over a number field k, $f \in k(C)$ a nonconstant rational function, and S a finite set of places of k containing the archimedean places. Fix a pole $Q \in C(\overline{k})$ of f. There exists an effectively computable number field $L \supset k$ and an effectively computable finite set of places T of L with the following property: for any $P \in C(f, k, S)$ and any double cover $\pi : \tilde{C} \to C$ over $\overline{k}$ ramified exactly above P and Q, there exists a morphism of nonsingular projective curves $\pi' : \tilde{C}' \to C$ with the following properties:*

(a) *There is an isomorphism $\psi : \tilde{C} \to \tilde{C}'$ over $\overline{k}$ such that $\pi = \pi' \circ \psi$.*
(b) *π' and $\tilde{C}'$ are both defined over L.*
(c) *$\deg \pi' = 2$.*
(d) *π' is ramified exactly above P and Q.*
(e) *Both $\tilde{C}'$ and C have good reduction outside T.*

We note that for any P and Q such maps π exist (see Theorem 4.2). We will use the following result proven by Silverman in [31, Prop. 3, Lemma 4], where it is attributed to Szpiro and Ogus.

Lemma 2.1. *Let C be a nonsingular projective curve over a number field L and let $g \in L(C)$. Suppose that*

$$\mathrm{div}(g) = \pm P_1 \pm P_2 \pm \cdots \pm P_n + pD,$$

where $P_1, \ldots, P_n \in C(\overline{L})$, D is some divisor on C, and p is a prime. Let $\mathscr{C}$ be a model for C over $\mathcal{O}_L$. Let T be a finite set of places of L such that:

   (a) T contains all archimedean places of L.
   (b) T contains all places of bad reduction of $\mathscr{C}$.
   (c) T contains all places of L lying above p.
   (d) The ring of T-integers $\mathcal{O}_{L,T}$ has class number one.

There exists an element $\alpha \in L^*$ such that if C' is a nonsingular projective curve with function field $L(C)(\sqrt[p]{\alpha g})$ and $v \notin T$ is a place of L such that $P_1, \ldots, P_n$ are distinct modulo v, then C' has good reduction at v.

We now prove Theorem 2.1.

Proof of Theorem 2.1. Without loss of generality, we may assume that $Q \in C(k)$ and that all of the 2-torsion of $\mathrm{Jac}(C)$ is rational over k. Let L be a number field such that

$$(2.1) \qquad \mathrm{Jac}(C)(k) \subset 2\,\mathrm{Jac}(C)(L).$$

The existence of such an L follows from the (weak) Mordell-Weil theorem and we recall that such a field L can be explicitly given. We may assume without loss of generality that S is a finite set of places of k containing all places of bad reduction of C, all places of k lying above the prime 2, and such that $\mathcal{O}_{k,S}$ has trivial class group. Let $s_1, \ldots, s_n$ be generators of $\mathcal{O}_{k,S}^*$. Then $L = k(\sqrt{s_1}, \ldots, \sqrt{s_n})$ will be a number field satisfying (2.1) ([14, §C.1]). From the explicit description of L it is clear that L is effectively computable.

Let $\mathscr{C}$ be a model of C over $\mathcal{O}_L$. If $R \subset R'$ are rings and X is a scheme over R, we let $X_{R'} = X \times_{\mathrm{Spec}\,R} \mathrm{Spec}\,R'$. Let T be a finite set of places of L satisfying (a)–(d) of Lemma 2.1 (with $p = 2$) and such that

   (e) T contains every place of L lying above a place of S.
   (f) The associated morphism $f : C_L \to \mathbb{P}^1_L$ extends to a morphism $\mathscr{C}_{\mathcal{O}_{L,T}} \to \mathbb{P}^1_{\mathcal{O}_{L,T}}$ over $\mathrm{Spec}\,\mathcal{O}_{L,T}$.

We note that such a finite set T is effectively computable. Let $P \in C(f, k, S)$. Let $\pi : \tilde{C} \to C$ be a double cover (over $\overline{k}$) ramified exactly above P and Q. Then π corresponds to an extension of function fields $\overline{k}(C) \subset \overline{k}(C)(\sqrt{g})$ for some rational function $g \in \overline{k}(C)$. It is a standard fact that π is ramified above a point $R \in C(\overline{k})$ if and only if g has a pole or zero of odd order at R. Since π is ramified exactly above P and Q, we must have

$$\mathrm{div}(g) = P - Q + 2D$$

for some divisor D. Since $\mathrm{Jac}(C)(k) \subset 2\,\mathrm{Jac}(C)(L)$, the divisor class $[D]$ is L-rational and $D \sim E$ for some L-rational divisor E. Then for an appropriate rational function $h \in \overline{k}(C)$ satisfying $\mathrm{div}(h) = E - D$, after replacing g by gh^2 we can assume that $g \in L(C)$.

Let $v \notin T$ be a place of L. Since $f(P) \in \mathcal{O}_{k,S} \subset \mathcal{O}_{L,T}$ by assumption, it follows from the definition of T that P cannot reduce to the pole Q of f modulo v. Then by Lemma 2.1, there exists $\alpha \in L^*$ such that if $\tilde{C}'$ is the nonsingular projective curve with function field $L(C)(\sqrt{\alpha g})$, then $\tilde{C}'$ has good reduction outside T. Let $\pi' : \tilde{C}' \to C$ be the morphism corresponding to the inclusion of function fields $L(C) \subset L(C)(\sqrt{\alpha g})$. Then $\tilde{C}'$ and π' satisfy the required properties. $\qquad\square$

3. Prym varieties

Let $\pi : \tilde{C} \to C$ be a morphism of nonsingular projective curves of degree two. There are two natural maps between the Jacobians $\mathrm{Jac}(\tilde{C})$ and $\mathrm{Jac}(C)$ that one can associate to π. First, we have the pullback map

$$\pi^* : \mathrm{Jac}(C) \to \mathrm{Jac}(\tilde{C}),$$
$$[D] \mapsto [\pi^* D],$$

where $[D]$ denotes the divisor class of a divisor D of degree 0. Second, we have the so-called norm map

$$\mathrm{Nm} : \mathrm{Jac}(\tilde{C}) \to \mathrm{Jac}(C),$$
$$\left[\sum n_P P\right] \mapsto \left[\sum n_P \pi(P)\right].$$

Definition. The Prym variety associated to the double cover $\pi : \tilde{C} \to C$ is defined by

$$\mathrm{Prym}(\tilde{C}/C) = (\ker \mathrm{Nm})^0,$$

the connected component of $\ker \mathrm{Nm}$ containing the identity.

We recall some basic facts about Prym varieties (see [21]). Let $\iota : \tilde{C} \to \tilde{C}$ be the involution of $\tilde{C}$ interchanging the two sheets of π. This induces an involution $\iota : \mathrm{Jac}(\tilde{C}) \to \mathrm{Jac}(\tilde{C})$. Then we have the identities

$$\mathrm{Prym}(\tilde{C}/C) = \ker(1 + \iota)^0 = \mathrm{im}(1 - \iota).$$

Let $i : \mathrm{Prym}(\tilde{C}/C) \to \mathrm{Jac}(\tilde{C})$ be the inclusion. Assume further now that C has positive genus and that π is either étale or ramified above exactly two points of C. We have an isogeny

$$\mathrm{Jac}(C) \times \mathrm{Prym}(\tilde{C}/C) \to \mathrm{Jac}(\tilde{C}),$$
$$(P, Q) \mapsto \pi^*(P) + i(Q).$$

Furthermore, if $\theta_{\tilde{C}}$ is a theta divisor on $\mathrm{Jac}(\tilde{C})$, then $i^* \theta_{\tilde{C}} \equiv 2\Xi$ for some ample divisor Ξ on $\mathrm{Prym}(\tilde{C}/C)$ and Ξ yields a principal polarization of $\mathrm{Prym}(\tilde{C}/C)$. So $\mathrm{Prym}(\tilde{C}/C)$ can naturally be given the structure of a principally polarized abelian variety. We will find the following lemma useful.

Lemma 3.1. *Suppose that $\tilde{C}$, C, and $\pi : \tilde{C} \to C$ are defined over a number field k. Let v be a finite place of k. Then $\mathrm{Jac}(\tilde{C})$ has good reduction at v if and only if both $\mathrm{Prym}(\tilde{C}/C)$ and $\mathrm{Jac}(C)$ have good reduction at v.*

Proof. The result follows [28, Cor. 2] from the fact that the abelian varieties $\mathrm{Jac}(\tilde{C})$ and $\mathrm{Jac}(C) \times \mathrm{Prym}(\tilde{C}/C)$ are k-isogenous. $\qquad\square$

In general, the Prym variety $\mathrm{Prym}(\tilde{C}/C)$ is not the Jacobian of a curve. However, in the important special case where C is hyperelliptic this holds (and the Prym variety is a hyperelliptic Jacobian).

Theorem 3.1 (Dalaljan [8, 9], Mumford [21])**.** *Suppose that C is hyperelliptic and $\pi : \tilde{C} \to C$ is a double cover of C that is either unramified or ramified above exactly two points of C. Then $(\mathrm{Prym}(\tilde{C}/C), \Xi)$ is isomorphic to the Jacobian $(\mathrm{Jac}(C'), \theta_{C'})$ of some hyperelliptic curve C'.*

Suppose that C is a hyperelliptic curve of genus g. For $Q \in C(\overline{k})$ and $P \in C(f, k, S)$ as in Theorem 2.1, we have a double cover $\tilde{C}_P \to C$ ramified exactly above P and Q and having nice reduction properties. By Theorem 3.1, $\mathrm{Prym}(\tilde{C}_P/C) \cong \mathrm{Jac}(X_P)$ for some hyperelliptic curve X_P of genus g. In the next section we will explicitly compute a Weierstrass equation for X_P.

4. Some explicit equations

We begin by recalling some results from [9, §3].

Theorem 4.1 (Dalaljan)**.** *Let k be an algebraically closed field, $\mathrm{char}\, k \neq 2$. Let C be a nonsingular projective hyperelliptic curve over k with hyperelliptic map $p : C \to \mathbb{P}^1$. Let $\pi : \tilde{C} \to C$ be a double cover of nonsingular projective curves, ramified above exactly two points of C. Associated to π and p there exists a tower of curves*

(4.1)

with $C_1 \cong \mathbb{P}^1$, $\tilde{C}_1$ *hyperelliptic,* $\deg \pi_1 = 2$, *and*

$$(\mathrm{Prym}(\tilde{C}/C), \Xi) \cong (\mathrm{Jac}(\tilde{C}_1), \theta_{\tilde{C}_1}).$$

For any positive integer g, the tower (4.1) *induces a bijection between equivalence classes of towers*

$$\{[\tilde{C} \xrightarrow{\pi} C \xrightarrow{p} \mathbb{P}^1] \mid \deg \pi = \deg p = 2, g(\tilde{C}) = 2g, g(C) = g\} \longleftrightarrow$$
$$\{[\tilde{C}_1 \xrightarrow{\pi_1} C_1 \xrightarrow{p_1} \mathbb{P}^1] \mid \deg \pi_1 = \deg p_1 = 2, g(\tilde{C}_1) = g, C_1 \cong \mathbb{P}^1\}.$$

Here, we say that two towers of curves $X \xrightarrow{\pi} Y \xrightarrow{p} Z$ and $X' \xrightarrow{\pi'} Y' \xrightarrow{p'} Z'$ are equivalent if there exists a commutative diagram

$$
\begin{array}{ccc}
X & \longrightarrow & X' \\
\downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle \pi'} \\
Y & \longrightarrow & Y' \\
\downarrow{\scriptstyle p} & & \downarrow{\scriptstyle p'} \\
Z & \longrightarrow & Z'
\end{array}
$$

where the horizontal morphisms are isomorphisms.

Theorem 4.2. *Let k be an algebraically closed field,* $\mathrm{char}\, k \neq 2$. *Let C be a (nonsingular projective) hyperelliptic curve over k of genus g given by an equation*

$$y^2 = \prod_{i=1}^{2g+1} (x - \alpha_i), \quad \alpha_i \in k,$$

and $p : C \to \mathbb{P}^1$ the hyperelliptic map $(x, y) \mapsto x$. Let $P = (x_P, y_P), Q = (x_Q, y_Q) \in C(k)$ with $x_P \neq x_Q$ and $y_P \neq 0$. The tower (4.1) *induces a bijection between the sets*

$$\left\{ \begin{array}{l} \text{double covers } \pi : \tilde{C} \to C, \text{ up to equivalence,} \\ \text{ramified exactly above } P \text{ and } Q \end{array} \right\}$$

and

$$\left\{ \text{hyperelliptic curves } \tilde{C}_1 : y^2 = (x-1) \prod_{i=1}^{2g+1} (x - \beta_i) \,\middle|\, \begin{array}{l} \beta_i^2 = \frac{x_Q - \alpha_i}{x_P - \alpha_i}, \\ \prod_{i=1}^{2g+1} \beta_i = \frac{y_Q}{y_P} \end{array} \right\}.$$

Both sets have cardinality 2^{2g}.

Proof. We first give an explicit description of the set of double covers $\pi : \tilde{C} \to C$ ramified exactly above P and Q. At the function field level, we have $k(\tilde{C}) = k(C)(\sqrt{\phi})$ for some rational function $\phi \in k(C)$. The corresponding

morphism π is ramified exactly above P and Q if and only if $\mathrm{div}(\phi) = P+Q+2D$ for some divisor D. It's easily seen then that there is a bijection

$$\left\{ \begin{array}{l} \text{double covers } \pi : \tilde{C} \to C, \text{ up to equivalence,} \\ \text{ramified exactly above } P \text{ and } Q \end{array} \right\}$$

$$\longleftrightarrow \{[D] \mid D \in \mathrm{Div}(C), 2D \sim -(P+Q)\},$$

where $\mathrm{Div}(C)$ denotes the group of divisors of C and $[D]$ the linear equivalence class of D. As is well-known, the latter (and hence former) set has cardinality 2^{2g}.

Let ∞ denote the (unique) point of C at infinity relative to the equation $y^2 = \prod_{i=1}^{2g+1}(x - \alpha_i)$. Then we have an embedding $C \to \mathrm{Jac}(C)$, pt $\mapsto$ $[\mathrm{pt} - \infty]$. Every element of $\mathrm{Jac}(C)$ can be represented by a divisor of the form $P_1 + \cdots + P_g - g\infty$, $P_1, \ldots, P_g \in C(k)$. Then in each linear equivalence class of divisors D satisfying $2D \sim -(P+Q)$, we can find a divisor D of the form

$$D = P_1 + \cdots + P_g - (g+1)\infty, \quad P_1, \ldots, P_g \in C(k).$$

Let $\pi : \tilde{C} \to C$ be a double cover ramified exactly above P and Q. Then we find that $k(\tilde{C}) = k(C)(\sqrt{\phi})$ for some rational function $\phi \in k(C)$ satisfying

$$\mathrm{div}(\phi) = P + Q + 2P_1 + \cdots + 2P_g - (2g+2)\infty.$$

As usual, let $L(D)$ be the k-vector space $L(D) = \{\psi \in k(X) \mid \mathrm{div}(\psi) \geq -D\}$. By Riemann-Roch, $\dim L((2g+2)\infty) = g+3$ and a basis for $L((2g+2)\infty)$ is given by the rational functions $1, x, \ldots, x^{g+1}, y$. It follows that we can write

$$\phi = ay + h(x)$$

for some $a \in k$ and some $h \in k[x]$ with $\deg h \leq g+1$. Since $x_P \neq x_Q$, we have $a \neq 0$, and so we can assume $a = 1$. Let $f(x) = \prod_{i=1}^{2g+1}(x - \alpha_i)$. Then $\tilde{C}$ has an equation of the form

$$y^2 = f(x),$$
$$z^2 = y + h(x),$$

where $h \in k[x]$ and $\deg h \leq g+1$ (where throughout, we mean that the curve, here $\tilde{C}$, is a projective normalization of the curve defined by the given equations).

We now describe the relevant part of the tower (4.1) (see [9]). For a double cover $\phi : X' \to X$ of nonsingular projective curves, we let i_ϕ denote the corresponding involution of X'. We set $\tilde{C}' = \tilde{C}$ and $\pi' = i_p \circ \pi$, where $p : C \to \mathbb{P}^1$ is the projection onto the x-coordinate. Let $\tilde{\tilde{C}} = \tilde{C} \times_C \times \tilde{C}'$ and let $\tilde{\pi}$ and $\tilde{\pi}'$ be the natural projection maps onto $\tilde{C}$ and $\tilde{C}'$, respectively.

Explicitly, $\tilde{\tilde{C}}$ consists of pairs $(\tilde{P}, \tilde{P}') \in \tilde{C} \times \tilde{C}'$ such that $\pi(\tilde{P}) = \pi'(\tilde{P}')$. Then $\tilde{\tilde{C}}$ can be given by the equations

$$y^2 = f(x),$$
$$z^2 = y + h(x),$$
$$z'^2 = -y + h(x).$$

Let $i_{\tilde{\pi}_0} = i_{\tilde{\pi}'} \circ i_{\tilde{\pi}}$ and let $i_{\tilde{\pi}_1}$ be the involution of $\tilde{\tilde{C}} = \tilde{C} \times_C \times \tilde{C}'$ that switches the coordinates. In the coordinates (x, y, z, z') these are the involutions $(x, y, z, z') \mapsto (x, y, -z, -z')$ and $(x, y, z, z') \mapsto (x, -y, z', z)$, respectively. Taking the quotients of $\tilde{\tilde{C}}$ by $i_{\tilde{\pi}_0}$ and $i_{\tilde{\pi}_1}$, we obtain curves $\tilde{C}_0$ and $\tilde{C}_1$, respectively, and double covers $\tilde{\pi}_0 : \tilde{\tilde{C}} \to \tilde{C}_0$ and $\tilde{\pi}_1 : \tilde{\tilde{C}} \to \tilde{C}_1$, respectively. Note that

$$(z + z')^2 = 2h(x) + 2zz',$$
$$(zz')^2 = h(x)^2 - f(x).$$

Using the above equations, we see that $\tilde{C}_0$ is given by the equations

$$y^2 = f(x),$$
$$z^2 = h(x)^2 - f(x),$$

and $\tilde{C}_1$ by the equations

$$(4.2) \qquad\qquad w^2 = 2h(x) + 2z,$$
$$(4.3) \qquad\qquad z^2 = h(x)^2 - f(x).$$

The involutions $i_{\tilde{\pi}_0}$ and $i_{\tilde{\pi}_1}$ commute and generate a group of order 4. The quotient of $\tilde{\tilde{C}}$ modulo the action of this group yields the curve C_1 in the tower. The curve C_1 is naturally given as the projective normalization of the curve defined by the equation

$$z^2 = h(x)^2 - f(x).$$

The induced maps π'_0 and π_1 are then induced by the natural projection maps onto the x and z coordinates. From the definition of $h(x)$, we have

$$(4.4) \qquad\qquad h(x)^2 - f(x) = (x - x_P)(x - x_Q)F(x)^2,$$

for some polynomial $F \in k[x]$. It follows that $C_1 \cong \mathbb{P}^1$. As $\deg \pi'_0 = \deg \pi_1 = 2$, we see that $\tilde{C}_0$ and $\tilde{C}_1$ are hyperelliptic curves.

A hyperelliptic Weierstrass equation for $\tilde{C}_1$ can be computed as follows. In view of (4.4), we can parametrize (4.3) by setting

$$(4.5) \qquad\qquad t^2 = \frac{x - x_Q}{x - x_P},$$

$$x = x(t) = \frac{x_Q - x_P t^2}{1 - t^2},$$

$$z = z(t) = t(x(t) - x_P)F(x(t)).$$

Substituting into (4.2), we see that we need to consider the polynomial

$$G(t) = (1 - t^2)^{g+1}(h(x(t)) + z(t))$$

$$= (1 - t^2)^{g+1}\left(h\left(\frac{x_Q - x_P t^2}{1 - t^2}\right) + t\left(\frac{x_Q - x_P}{1 - t^2}\right)F\left(\frac{x_Q - x_P t^2}{1 - t^2}\right)\right).$$

Let $\alpha_i, i = 1, \ldots, 2g+1$, be the roots of f. Then when $x = \alpha_i$, (4.3) gives $z = \pm h(\alpha_i)$. From (4.5), it then follows that for some (unique) choice of the square root, $t = \sqrt{\frac{x_Q - \alpha_i}{x_P - \alpha_i}} = \beta_i$ is a root of $G(t)$, $i = 1, \ldots, 2g+1$. From (4.4), it follows that the leading coefficients of $h(x)$ and $F(x)$ are equal up to sign. This easily implies that either $t = 1$ or $t = -1$ is a root of $G(t)$. Replacing $F(x)$ by $-F(x)$, if necessary, we can assume that $t = 1$ is a root of $G(t)$. Since $\deg G \leq 2g+2$, we find that the roots of G are exactly given by the $2g+2$ distinct elements $t = 1, \beta_1, \ldots, \beta_{2g+1}$.

We have $G(0) = h(x_Q) = -y_Q$, from the definition of h. The leading coefficient of G can be computed as

$$\lim_{t \to \infty} (-1)^{g+1} \frac{G(t)}{(1 - t^2)^{g+1}} = (-1)^{g+1} h(x_P) = -(-1)^{g+1} y_P.$$

Thus,

$$1 \cdot \prod_{i=1}^{2g+1} \beta_i = \frac{-y_Q}{-(-1)^{g+1} y_P} = (-1)^{g+1} \frac{y_Q}{y_P}.$$

If g is odd, so that $(1 - t^2)^{g+1}$ is an even power of $1 - t^2$, then it follows from the above and (4.2) and (4.3) that $\tilde{C}_1$ has a Weierstrass equation

$$(4.6) \qquad y^2 = (x - 1)\prod_{i=1}^{2g+1}(x - \beta_i), \qquad \beta_i^2 = \frac{x_Q - \alpha_i}{x_P - \alpha_i}, \quad \prod_{i=1}^{2g+1} \beta_i = \frac{y_Q}{y_P}.$$

If g is even, then

$$\frac{(1 - t^2)^{g+2}}{(t - 1)^2}(h(x(t)) + z(t)) = c'(t + 1)\prod_{i=1}^{2g+1}(t - \beta_i),$$

for some constant c' and where $\prod_{i=1}^{2g+1} \beta_i = -\frac{y_Q}{y_P}$. Replacing t by $-t$, we again see that $\tilde{C}_1$ has a Weierstrass equation (4.6).

In the coordinates of (4.6), the tower $\tilde{C}_1 \xrightarrow{\pi_1} C_1 \xrightarrow{p_1} \mathbb{P}^1$ is given by the hyperelliptic map $(x,y) \mapsto x$ followed by the squaring map $C_1 = \mathbb{P}^1 \to \mathbb{P}^1$, $x \mapsto x^2$. The tower $\tilde{C}_1 \xrightarrow{\pi_1} C_1 \xrightarrow{p_1} \mathbb{P}^1$ is associated to the tower $\tilde{C} \xrightarrow{\pi} C \xrightarrow{p} \mathbb{P}^1$, and from the above, $\tilde{C}_1$ has an equation given by (4.6). Note that there are exactly 2^{2g} possibilities for the curve (4.6), and hence for the tower $[\tilde{C}_1 \xrightarrow{\pi_1} C_1 \xrightarrow{p_1} \mathbb{P}^1]$, given by the 2^{2g} possibilities for β_i subject to the constraint $\prod_{i=1}^{2g+1} \beta_i = \frac{y_Q}{y_P}$. Since the map

$$[\tilde{C} \xrightarrow{\pi} C \xrightarrow{p} \mathbb{P}^1] \mapsto [\tilde{C}_1 \xrightarrow{\pi_1} C_1 \xrightarrow{p_1} \mathbb{P}^1]$$

given by the tower (4.1) is injective and there are 2^{2g} possibilities for $[\tilde{C} \to C \to \mathbb{P}^1]$, it follows that all of the 2^{2g} possibilities for $\tilde{C}_1$ arise from some covering $\tilde{C} \to C$, proving the theorem. $\qquad\square$

Corollary 4.1. *Let C be a hyperelliptic curve over a number field k of genus g given by an equation*

$$y^2 = \prod_{i=1}^{2g+1} (x - \alpha_i), \quad \alpha_i \in k.$$

Let $f \in k(C)$ be a nonconstant rational function and S a finite set of places of k containing the archimedean places. Fix a pole $Q = (x_Q, y_Q) \in C(\bar{k})$ of f. There exists an effectively computable number field $L \supset k$ and an effectively computable finite set of places T of L such that for any $P = (x_P, y_P) \in C(f, k, S)$ with $x_P \neq x_Q$, $y_P \neq 0$, any β_i satisfying $\beta_i^2 = \frac{x_Q - \alpha_i}{x_P - \alpha_i}, \prod_{i=1}^{2g+1} \beta_i = \frac{y_Q}{y_P}$, and some $c = c(\beta_1, \ldots, \beta_{2g+1}) \in L^*$, the Jacobian $\mathrm{Jac}(X_P)$ of the curve

$$X_P : y^2 = c(x - 1) \prod_{i=1}^{2g+1} (x - \beta_i)$$

is defined over L and has good reduction outside of T.

Proof. Without loss of generality, we may assume that $Q \in C(k)$. Let L and T be as in Theorem 2.1. Let $P = (x_P, y_P) \in C(f, k, S)$ with $x_P \neq x_Q$, $y_P \neq 0$. Let β_i, $i = 1, \ldots, 2g+1$, satisfy $\beta_i^2 = \frac{x_Q - \alpha_i}{x_P - \alpha_i}, \prod_{i=1}^{2g+1} \beta_i = \frac{y_Q}{y_P}$. Let S' be a finite set of places of k such that $\mathcal{O}_{k,S'}$ is a principal ideal domain and $\alpha_i \in \mathcal{O}_{k,S'}$, $\alpha_i - \alpha_j \in \mathcal{O}_{k,S'}^*$, for all i and j, $i \neq j$. If $P' = (x', y') \in C(k)$, then we have $x' - \alpha_i = u_i z_i^2$ for some $z_i \in k$ and some S'-unit $u_i \in \mathcal{O}_{k,S'}^*$. Then by the Dirichlet unit theorem, applied to $\mathcal{O}_{k,S'}^*$, there is a fixed finite extension of L (independent of $P' \in C(k)$) containing $\sqrt{x' - \alpha_i} = z_i \sqrt{u_i}$ for all i. By replacing L by this finite extension (and replacing T by the set of places lying above it), we can assume that we always have $\beta_i \in L$, $i = 1, \ldots, 2g+1$. We note that from their construction both L and T are effectively computable.

Let X_P' be the curve $y^2 = (x-1)\prod_{i=1}^{2g+1}(x-\beta_i)$. By Theorem 2.1 and Theorem 4.2, there is a double covering $\pi_P : \tilde{C}_P \to C$, ramified exactly above P and Q, that corresponds to $\tilde{C}_1 = X_P'$ via the tower (4.1), such that both π_P and $\tilde{C}_P$ are defined over L and both $\tilde{C}_P$ and C have good reduction outside T. By Theorem 4.1,

$$\mathrm{Prym}(\tilde{C}_P/C) \cong \mathrm{Jac}(X_P')$$

over $\overline{L}$. In fact, the proofs of Theorems 4.1 and 4.2 show that

$$\mathrm{Prym}(\tilde{C}_P/C) \cong \mathrm{Jac}(X_P)$$

over L, where X_P is some quadratic twist of X_P' given by

$$X_P : y^2 = c(x-1)\prod_{i=1}^{2g+1}(x-\beta_i),$$

for some $c \in L^*$. Since both $\tilde{C}_P$ and C have good reduction outside T, by Lemma 3.1, $\mathrm{Jac}(X_P)$ has good reduction outside T. $\square$

An alternative, more direct proof of this result follows from Theorems 6.2 and 6.4 in Section 6.

5. Main theorem

We now prove the main theorem from the introduction.

Theorem 5.1. *Let $g \geq 2$ be an integer. Suppose that for any number field k and any finite set of places S of k the set $\mathcal{H}'(g,k,S)$ is effectively computable (e.g., an explicit hyperelliptic Weierstrass equation for each element of the set is given). Then for any number field k, any finite set of places S of k, any hyperelliptic curve C over k of genus g, and any rational function $f \in k(C)$, the set of S-integral points with respect to f,*

$$C(f,k,S) = \{P \in C(k) \mid f(P) \in \mathcal{O}_{k,S}\},$$

is effectively computable.

Proof. Without loss of generality, by enlarging k we can assume that every Weierstrass point of C is k-rational and that some pole $Q = (x_Q, y_Q)$ of f is k-rational. Then C can be given by a hyperelliptic Weierstrass equation

$$C : y^2 = \prod_{i=1}^{2g+1}(x-\alpha_i), \quad \alpha_i \in k.$$

Let U consist of the set of Weierstrass points of C along with Q and its image under the hyperelliptic involution. By Corollary 4.1, for some number

field L and some finite set of places T of L, we have a map (arbitrarily choosing among the choices for X_P)

$$C(f, k, S) \setminus U \to \mathcal{H}'(g, L, T),$$
$$P \mapsto X_P.$$

Explicitly, we can compute $C(f, k, S)$ from $\mathcal{H}'(g, L, T)$ as follows. Recall that for $P = (x_P, y_P) \in C(f, k, S) \setminus U$, X_P is defined by an equation

$$y^2 = c_P(x - 1) \prod_{i=1}^{2g+1} \left(x - \sqrt{\frac{x_Q - \alpha_i}{x_P - \alpha_i}} \right),$$

for some $c_P \in L^*$ and some appropriate choice of the square roots. We pick four of the roots of the polynomial on the right-hand side, say $\beta_i = \sqrt{\frac{x_Q - \alpha_i}{x_P - \alpha_i}}, i = 1, 2, 3, 4$, and consider the cross-ratio

$$\mathrm{CR}(\beta_1, \beta_2, \beta_3, \beta_4) = \frac{(\beta_1 - \beta_3)(\beta_2 - \beta_4)}{(\beta_2 - \beta_3)(\beta_1 - \beta_4)}.$$

Alternatively, we consider the rational function

(5.1) $$\frac{(c_1 z_3 - c_3 z_1)(c_2 z_4 - c_4 z_2)}{(c_2 z_3 - c_3 z_2)(c_1 z_4 - c_4 z_1)}$$

on the curve defined by $z_i^2 = x - \alpha_i$, $i = 1, 2, 3, 4$, where we view $c_i = \sqrt{x_Q - \alpha_i}$, $i = 1, 2, 3, 4$, as fixed constants. Note that by Kummer theory, since the α_i are distinct, we have $[\overline{k}(x, z_1, \ldots, z_4) : \overline{k}(x)] = 2^4 = 16$. This immediately implies that the rational function (5.1) is nonconstant and thus that the equation $\mathrm{CR}(\beta_1, \beta_2, \beta_3, \beta_4) = \alpha$ has only finitely many solutions in x_P for any $\alpha \in \overline{k}$. Now let $C' \in \mathcal{H}'(g, L, T)$, given by a Weierstrass equation $C' : y^2 = c' \prod_{i=1}^{2g+2}(x - \gamma_i)$. If $X_P \cong C'$, then $\mathrm{CR}(\beta_1, \beta_2, \beta_3, \beta_4) = \mathrm{CR}(\gamma_i, \gamma_j, \gamma_k, \gamma_l)$ for some $i, j, k, l \in \{1, \ldots, 2g + 2\}$. Since there are only finitely many possible cross-ratios $\mathrm{CR}(\gamma_i, \gamma_j, \gamma_k, \gamma_l)$, we find that there are only finitely many (explicitly computable) possible points $P = (x_P, y_P)$ with $X_P \cong C'$. Finally, for each such possible point P and each point $P \in U$, we check if $P \in C(f, k, S)$. $\qquad\square$

6. Binary Forms

In this section we give a reformulation of some of our results in terms of binary forms. Let k be a number field and S a finite set of places of k (which we always assumes contains the archimedean places). Let $F(X, Z), G(X, Z) \in k[X, Z]$ be binary forms. Let $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $a, b, c, d \in k$, be a matrix. Define $F_U(X, Z) = F(aX + bZ, cX + dZ)$. We will call F and G equivalent if there exists $U \in \mathrm{GL}_2(k)$ and $\lambda \in k^*$ such that $G(X, Z) = \lambda F_U(X, Z)$.

Denote the equivalence class containing F by $[F]$. Let $\text{Disc}(F)$ denote the discriminant of F. Define

$$\mathcal{B}(r,k,S) = \left\{ [F] \,\middle|\, \begin{array}{l} F \in \mathcal{O}_{k,S}[X,Z] \text{ is a binary form of degree } r \\ \text{and } \text{Disc}(F) \in \mathcal{O}_{k,S}^* \end{array} \right\}.$$

Effective finiteness of the set $\mathcal{B}(r,k,S)$ follows from work of Evertse and Győry.

Theorem 6.1 (Evertse, Győry [11]). *Let $r \geq 2$ be an integer, k a number field, and S a finite set of places of k. The set $\mathcal{B}(r,k,S)$ is finite and effectively computable.*

We now define a larger, but related, set $\mathcal{B}'(r,k,S) \supset \mathcal{B}(r,k,S)$. The set $\mathcal{B}'(r,k,S)$ contains equivalence classes of certain binary forms F whose discriminant is an S-unit outside of primes $\mathfrak{p}$ where $F \pmod{\mathfrak{p}}$ has a factor of multiplicity ≥ 3. An effective procedure for computing $\mathcal{B}'(r,k,S)$ would give a solution to Problem 1.1 (Corollary 6.1).

More precisely, define $\mathcal{B}'(r,k,S)$ to be the set of equivalence classes of binary forms over k of degree r such that there exists a representative $F \in \mathcal{O}_{k,S}[X,Z]$ satisfying:

If $\mathfrak{p} \notin S$ and $\text{ord}_\mathfrak{p} \text{Disc}(F) > 0$, then $\text{ord}_\mathfrak{p} \text{Disc}(F) = 2mn(n-1)$, where m is some positive integer, n is an odd integer with $3 \leq n \leq 2[(r+1)/2]-3$, and $f(x) = F(x,1)$ has n distinct roots $\alpha_1, \ldots, \alpha_n \in k$ with $\text{ord}_\mathfrak{p} \alpha_i = 2m$, $i = 1, \ldots, n$.

If $\text{Disc}(F) \in \mathcal{O}_{k,S}^*$ or $r \leq 4$, then the above condition is vacuous. So we trivially have $\mathcal{B}(r,k,S) \subset \mathcal{B}'(r,k,S)$ for all r and $\mathcal{B}(r,k,S) = \mathcal{B}'(r,k,S)$ if $1 \leq r \leq 4$.

Theorem 6.2. *Let C be a hyperelliptic curve over a number field k of genus g given by an equation*

$$y^2 = h(x) = \prod_{i=1}^{2g+1} (x - \alpha_i), \quad \alpha_i \in k.$$

Let $f \in k(C)$ be a nonconstant rational function and S a finite set of places of k containing the archimedean places. Fix a pole $Q = (x_Q, y_Q) \in C(\bar{k})$ of f. Let U be the set of Weierstrass points of C along with Q and its image under the hyperelliptic involution. Then there exists an effectively computable number field L and an effectively computable finite set of places T of L such that we have a well-defined map

$$C(f,k,S) \setminus U \to \mathcal{B}'(2g+2, L, T),$$

$$P = (x_P, y_P) \mapsto \left[(X-Z) \prod_{i=1}^{2g+1} (X - \beta_i Z) \right],$$

where the β_i are chosen such that $\beta_i^2 = \frac{x_Q - \alpha_i}{x_P - \alpha_i}$ and $\prod_{i=1}^{2g+1} \beta_i = \frac{y_Q}{y_P}$.

We will see (Corollary 6.2) that $\mathcal{B}'(2g + 2, k, S)$ is a finite set. Then by essentially the same argument as in the proof of Theorem 5.1, we obtain the following corollary.

Corollary 6.1. *Let $g \geq 2$ be an integer. Suppose that for any number field k and any finite set of places S of k the set $\mathcal{B}'(2g + 2, k, S)$ is effectively computable. Then for any number field k, any finite set of places S of k, any hyperelliptic curve C over k of genus g, and any rational function $f \in k(C)$, the set of S-integral points with respect to f,*

$$C(f, k, S) = \{P \in C(k) \mid f(P) \in \mathcal{O}_{k,S}\},$$

is effectively computable.

Proof of Theorem 6.2. First note that there is an explicit number field L, depending on C and k, such that for any $P \in C(f, k, S)$ we have $\beta_i \in L$ for all i. Then after enlarging k, without of loss of generality it suffices to prove the theorem for points $P \in C(f, k, S)$ such that $\beta_i \in k$, $i = 1, \ldots, 2g + 1$. Similarly, by enlarging S (in an effectively computable way) we can assume without of loss of generality that $\alpha_i \in \mathcal{O}_{k,S}$, $x_Q - \alpha_i \in \mathcal{O}_{k,S}^*$, $i = 1, \ldots, 2g+1$, $\mathrm{Disc}(h) \in \mathcal{O}_{k,S}^*$, $\mathcal{O}_{k,S}$ is a principal ideal domain, every place of k lying above 2 is in S, every prime $\mathfrak{p}$ of $\mathcal{O}_k$ with norm $|\mathcal{O}_k/\mathfrak{p}| \leq 2g+2$ is in S, and

$$(6.1) \qquad \min\{\mathrm{ord}_{\mathfrak{p}}(x_P - x_Q), \mathrm{ord}_{\mathfrak{p}}(y_P - y_Q)\} \leq 0$$

for every $\mathfrak{p} \in M_k \setminus S$ and every $P = (x_P, y_P) \in C(f, k, S)$, where M_k denotes the canonical set of places of k (identifying nonarchimedean places with the corresponding prime ideal).

Let $P \in C(f, k, S)$ with $\beta_i \in k$, $i = 1, \ldots, 2g + 1$, as in the theorem. Since $\mathcal{O}_{k,S}$ is principal, we can write $\beta_i = \frac{\gamma_i}{\delta_i}$, where γ_i and δ_i are relatively prime S-integers, $i = 1, \ldots, 2g + 1$. Consider the binary form

$$F(X, Z) = (X - Z) \prod_{i=1}^{2g+1} (\delta_i X - \gamma_i Z) \in \mathcal{O}_{k,S}[X, Z],$$

which is equivalent to $(X - Z) \prod_{i=1}^{2g+1} (X - \beta_i Z)$. Let $\mathfrak{p} \in M_k \setminus S$.

Suppose that $\mathrm{ord}_{\mathfrak{p}}(x_P - x_Q) = 0$. Then we claim that $\mathrm{ord}_{\mathfrak{p}} \mathrm{Disc}(F) = 0$. For this, it suffices to show that $\mathrm{ord}_{\mathfrak{p}}(\gamma_i \delta_j - \gamma_j \delta_i) = 0$, $i \neq j$, and $\mathrm{ord}_{\mathfrak{p}}(\gamma_i - \delta_i) = 0$ for all i. We have the identity

$$(6.2) \quad \beta_i^2 - \beta_j^2 = \frac{\gamma_i^2 \delta_j^2 - \gamma_j^2 \delta_i^2}{\delta_i^2 \delta_j^2} = \frac{x_Q - \alpha_i}{x_P - \alpha_i} - \frac{x_Q - \alpha_j}{x_P - \alpha_j} = \frac{(x_P - x_Q)(\alpha_j - \alpha_i)}{(x_P - \alpha_i)(x_P - \alpha_j)}.$$

Since $\mathrm{Disc}(h) \in \mathcal{O}_{k,S}^*$, we have $\mathrm{ord}_{\mathfrak{p}}(\alpha_j - \alpha_i) = 0$. By assumption, $\mathrm{ord}_{\mathfrak{p}}(x_P - x_Q) = \mathrm{ord}_{\mathfrak{p}}((x_P - \alpha_i) - (x_Q - \alpha_i)) = 0$. This last equality, along with

$\operatorname{ord}_{\mathfrak{p}}(x_Q - \alpha_i) = 0$, implies that $\operatorname{ord}_{\mathfrak{p}}(x_P - \alpha_i) = 2\operatorname{ord}_{\mathfrak{p}}\delta_i$. Then

$$\begin{aligned}
\operatorname{ord}_{\mathfrak{p}}(\gamma_i^2\delta_j^2 - \gamma_j^2\delta_i^2) &= \operatorname{ord}_{\mathfrak{p}}((\gamma_i\delta_j - \gamma_j\delta_i)(\gamma_i\delta_j + \gamma_j\delta_i)) \\
&= \operatorname{ord}_{\mathfrak{p}}\frac{\delta_i^2\delta_j^2(x_P - x_Q)(\alpha_j - \alpha_i)}{(x_P - \alpha_i)(x_P - \alpha_j)} = 0.
\end{aligned}$$

Since $\gamma_i\delta_j \pm \gamma_j\delta_i$ is an S-integer, we find that $\operatorname{ord}_{\mathfrak{p}}(\gamma_i\delta_j - \gamma_j\delta_i) = 0$. Similarly, we find that $\operatorname{ord}_{\mathfrak{p}}(\gamma_i - \delta_i) = 0$. So $\operatorname{ord}_{\mathfrak{p}}\operatorname{Disc}(F) = 0$ as desired.

Now suppose that $\operatorname{ord}_{\mathfrak{p}}(x_P - x_Q) < 0$. Since $x_Q, \alpha_1, \ldots, \alpha_{2g+1} \in \mathcal{O}_{k,S}$, this implies that $\operatorname{ord}_{\mathfrak{p}}(x_P - x_Q) = \operatorname{ord}_{\mathfrak{p}} x_P = \operatorname{ord}_{\mathfrak{p}}(x_P - \alpha_i) < 0$ for all i. Since $x_Q - \alpha_i \in \mathcal{O}_{k,S}^*$ for all i, we have $\operatorname{ord}_{\mathfrak{p}}\gamma_i = -\frac{1}{2}\operatorname{ord}_{\mathfrak{p}} x_P$ for all i. Let $c \in \mathcal{O}_{k,S}$ be such that $\operatorname{ord}_{\mathfrak{p}} c = \max\{0, -\frac{1}{2}\operatorname{ord}_{\mathfrak{p}} x_P\}$ for $\mathfrak{p} \notin S$. We consider now the binary form

$$G(X, Z) = (cX - Z)\prod_{i=1}^{2g+1}\left(\delta_i X - \frac{\gamma_i}{c}Z\right) \in \mathcal{O}_{k,S}[X, Z].$$

The identity (6.2) easily implies that if $\mathfrak{p} \notin S$ and $\operatorname{ord}_{\mathfrak{p}}(x_P - x_Q) < 0$, then

$$\operatorname{ord}_{\mathfrak{p}}(\gamma_i\delta_j - \gamma_j\delta_i) = -\frac{1}{2}\operatorname{ord}_{\mathfrak{p}} x_P = \operatorname{ord}_{\mathfrak{p}} c, \quad i \neq j.$$

Then computing $\operatorname{Disc}(G)$, we find that $\operatorname{ord}_{\mathfrak{p}}\operatorname{Disc}(G) = 0$ if $\mathfrak{p} \notin S$ and $\operatorname{ord}_{\mathfrak{p}}(x_P - x_Q) \leq 0$.

Finally, suppose that $\operatorname{ord}_{\mathfrak{p}}(x_P - x_Q) > 0$. Then from (6.1), we must have $\operatorname{ord}_{\mathfrak{p}}(y_P - y_Q) = 0$ (the case $\operatorname{ord}_{\mathfrak{p}}(y_P - y_Q) < 0$ being impossible). Since $\operatorname{ord}_{\mathfrak{p}}(x_Q - \alpha_i) = 0$ for all i, $\operatorname{ord}_{\mathfrak{p}}(x_P - x_Q) > 0$ implies that $\operatorname{ord}_{\mathfrak{p}}(x_P - \alpha_i) = 0$ for all i. Then $\operatorname{ord}_{\mathfrak{p}}\beta_i = \operatorname{ord}_{\mathfrak{p}}\delta_i = \operatorname{ord}_{\mathfrak{p}}\gamma_i = 0$ for all i. It follows from (6.2) that

$$\operatorname{ord}_{\mathfrak{p}}(\gamma_i^2\delta_j^2 - \gamma_j^2\delta_i^2) = \operatorname{ord}_{\mathfrak{p}}(x_P - x_Q)$$

for $i \neq j$. Similarly,

$$\operatorname{ord}_{\mathfrak{p}}(\gamma_i^2 - \delta_i^2) = \operatorname{ord}_{\mathfrak{p}}(x_P - x_Q) > 0$$

for all i. In particular, $\gamma_i \equiv \pm\delta_i \pmod{\mathfrak{p}}$ and $\beta_i \equiv \pm 1 \pmod{\mathfrak{p}}$ for all i. Since $x_P \equiv x_Q \pmod{\mathfrak{p}}$ and $y_P \not\equiv y_Q \pmod{\mathfrak{p}}$, we have $y_P \equiv -y_Q \pmod{\mathfrak{p}}$. So

$$\prod_{i=1}^{2g+1}\beta_i \equiv \frac{y_Q}{y_P} \equiv -1 \pmod{\mathfrak{p}}.$$

Then $\beta_i \equiv -1 \pmod{\mathfrak{p}}$ for an odd number $n_{\mathfrak{p}}$ of the elements i. Let $m_{\mathfrak{p}} = \operatorname{ord}_{\mathfrak{p}}(x_P - x_Q)$. Then for $i \neq j$,

$$\operatorname{ord}_{\mathfrak{p}}(\gamma_i\delta_j - \gamma_j\delta_i) = \begin{cases} m_{\mathfrak{p}} & \text{if } \beta_i \equiv \beta_j \pmod{\mathfrak{p}}, \\ 0 & \text{if } \beta_i \not\equiv \beta_j \pmod{\mathfrak{p}}. \end{cases}$$

Now a straight-forward calculation gives

(6.3) $\operatorname{ord}_{\mathfrak{p}} \operatorname{Disc}(G) = m_{\mathfrak{p}} n_{\mathfrak{p}}(n_{\mathfrak{p}} - 1) + m_{\mathfrak{p}}(2g + 2 - n_{\mathfrak{p}})(2g + 2 - n_{\mathfrak{p}} - 1).$

Let

$$\mathcal{P} = \{\mathfrak{p} \in M_k \setminus S \mid \operatorname{ord}_{\mathfrak{p}}(x_P - x_Q) > 0\} = \{\mathfrak{p} \in M_k \setminus S \mid \operatorname{ord}_{\mathfrak{p}} \operatorname{Disc}(G) > 0\}.$$

Let $b \in \mathcal{O}_k$ be such that

$$2bc \equiv -1 \left(\operatorname{mod} \prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}^{m_{\mathfrak{p}}} \right).$$

Let $U = \begin{pmatrix} 1 & b \\ c & 1 + bc \end{pmatrix}$. Then

$$-G_U(X, Z) = Z \prod_{i=1}^{2g+1} \left((\delta_i - \gamma_i)X + \frac{1}{c}(bc\delta_i - (bc + 1)\gamma_i)Z \right).$$

Note that since $\det U = 1$, $\operatorname{Disc}(G_U) = \operatorname{Disc}(G)$. For $\mathfrak{p} \in \mathcal{P}$, let $\pi_{\mathfrak{p}}$ be a generator for $\mathfrak{p}\mathcal{O}_{k,S}$. Let $\epsilon_{i,\mathfrak{p}} = 1$ if $\delta_i \equiv \gamma_i \pmod{\mathfrak{p}}$ and $\epsilon_{i,\mathfrak{p}} = 0$ otherwise (in which case $\delta_i \equiv -\gamma_i \pmod{\mathfrak{p}}$). Define $\theta_i = \prod_{\mathfrak{p} \in \mathcal{P}} \pi_{\mathfrak{p}}^{m_{\mathfrak{p}}\epsilon_{i,\mathfrak{p}}}$ and $\theta_i' = \prod_{\mathfrak{p} \in \mathcal{P}} \pi_{\mathfrak{p}}^{m_{\mathfrak{p}}(1 - \epsilon_{i,\mathfrak{p}})}$. Consider the binary form

$$H(X, Z) = Z \prod_{i=1}^{2g+1} \left(\frac{\delta_i - \gamma_i}{\theta_i}X + \frac{\theta_i'}{c}(bc\delta_i - (bc + 1)\gamma_i)Z \right).$$

Note that the binary form $H(X, Z)$ is a scalar multiple of the form $G_U\left(X, \left(\prod_{\mathfrak{p} \in \mathcal{P}} \pi_{\mathfrak{p}}^{m_{\mathfrak{p}}}\right) Z\right)$. It follows that $\operatorname{ord}_{\mathfrak{p}} \operatorname{Disc}(H) = 0$ if $\mathfrak{p} \in M_k \setminus (\mathcal{P} \cup S)$. For $\mathfrak{p} \in \mathcal{P}$, from (6.3) and the definition of H, a calculation yields

(6.4) $\operatorname{ord}_{\mathfrak{p}} \operatorname{Disc}(H) = 2m_{\mathfrak{p}} n_{\mathfrak{p}}(n_{\mathfrak{p}} - 1).$

For $\mathfrak{p} \in \mathcal{P}$,

$$2(bc\delta_i - (bc + 1)\gamma_i) \equiv -(\delta_i + \gamma_i) \pmod{\mathfrak{p}^{m_{\mathfrak{p}}}}.$$

If $\epsilon_{i,\mathfrak{p}} = 0$, then it follows that $\operatorname{ord}_{\mathfrak{p}}(\frac{\theta_i'}{c}(bc\delta_i - (bc + 1)\gamma_i)) \geq 2m_{\mathfrak{p}}$. In fact, since there are $n_{\mathfrak{p}}$ distinct values of i such that $\epsilon_{i,\mathfrak{p}} = 0$, by (6.4), $\operatorname{ord}_{\mathfrak{p}}(\frac{\theta_i'}{c}(bc\delta_i - (bc + 1)\gamma_i)) > 2m_{\mathfrak{p}}$ for at most one value of i with $\epsilon_{i,\mathfrak{p}} = 0$. Since $|\mathcal{O}_k/\mathfrak{p}| > 2g + 2 > n_{\mathfrak{p}}$, after an appropriate substitution $X \mapsto X + aZ$, we can force $\operatorname{ord}_{\mathfrak{p}}(\frac{\theta_i'}{c}(bc\delta_i - (bc + 1)\gamma_i)) = 2m_{\mathfrak{p}}$ for all i and $\mathfrak{p}$ such that $\epsilon_{i,\mathfrak{p}} = 0$. Then for each $\mathfrak{p} \in \mathcal{P}$, $H(x, 1)$ has $n_{\mathfrak{p}}$ roots α with $\operatorname{ord}_{\mathfrak{p}} \alpha = 2m_{\mathfrak{p}}$. If $n_{\mathfrak{p}} = 2g + 1$, then we can replace $H(X, Z)$ by $\pi_{\mathfrak{p}}^{m_{\mathfrak{p}}} H\left(X, \frac{Z}{\pi_{\mathfrak{p}}^{m_{\mathfrak{p}}}}\right)$, eliminating $\mathfrak{p}$ as a divisor of the discriminant of H. So we have $3 \leq n_{\mathfrak{p}} \leq 2g - 1$ for every $\mathfrak{p} \in M_k \setminus S$ with $\operatorname{ord}_{\mathfrak{p}} \operatorname{Disc}(H) > 0$. Then from all of the above we

have found a binary form equivalent to $(X - Z)\prod_{i=1}^{2g+1}(X - \beta_i Z)$ showing that $[(X - Z)\prod_{i=1}^{2g+1}(X - \beta_i Z)] \in \mathcal{B}'(2g + 2, k, S)$.   □

We have shown that in order to solve Problem 1.1 it suffices to effectively compute, for all values of the parameters, either the set $\mathcal{B}'(2g + 2, k, S)$ or the set $\mathcal{H}'(g, k, S)$. It seems interesting to determine the precise relationship between these two sets. In the case $g = 2$, Liu [17] has given an algorithm to compute, given a Weierstrass equation for a genus two curve, the fibers of a minimal model of the curve (away from primes above 2, at least). In particular (see [17, §6]), Liu's algorithm implies that computing the set $\mathcal{B}'(6, k, S)$ for all k and S and computing the set $\mathcal{H}'(2, k, S)$ for all k and S are equivalent problems. More precisely, Liu's results imply the following relationship.

Theorem 6.3. *Let k be a number field and S a finite set of places of k containing the archimedean places and the places lying above 2. There exists a number field L and a finite set of places T of L such that if C : $y^2 = f(x)$, $\deg f = 6$, is a hyperelliptic curve of genus two representing an element of $\mathcal{H}'(2, k, S)$ and $F(X, Z)$ is the homogenization of f, then $[F] \in \mathcal{B}'(6, L, T)$. Conversely, if $[F] \in \mathcal{B}'(6, k, S)$, then for some constant $c \in k^*$, the equivalence class of the curve $y^2 = cF(x, 1)$ is in $\mathcal{H}'(2, k, S)$.*

In the theorem, we can take L to be any field such that for every curve C representing an element of $\mathcal{H}'(2, k, S)$, the Weierstrass points of C are L-rational. As is well known, such a field L can be explicitly computed and it is a certain extension of k unramified outside of S.

It seems plausible that the analogue of Theorem 6.3 holds in higher genus. We give a proof of one of the directions.

Theorem 6.4. *Let g be a positive integer, k be a number field, and S a finite set of places of k containing the archimedean places and the places lying above 2. If $[F] \in \mathcal{B}'(2g + 2, k, S)$, then for some constant $c \in k^*$ the equivalence class of the curve $y^2 = cF(x, 1)$ is in $\mathcal{H}'(g, k, S)$.*

Proof. Let $[F] \in \mathcal{B}'(2g + 2, k, S)$, with $F \in \mathcal{O}_{k,S}[X, Z]$ as in the definition of $\mathcal{B}'(2g + 2, k, S)$. Let $f(x) = F(x, 1)$ and let C be the hyperelliptic curve defined by $y^2 = f(x)$. It suffices to show that $\mathrm{Jac}(C)$ has good reduction outside S. Let $\mathfrak{p} \in M_k \setminus S$. If $\mathfrak{p}$ doesn't divide the discriminant of f then the curve C, and hence $\mathrm{Jac}(C)$, has good reduction at $\mathfrak{p}$. Otherwise, let $k_\mathfrak{p}$ be the completion of k at $\mathfrak{p}$, $\mathcal{O}_\mathfrak{p}$ the ring of integers of $k_\mathfrak{p}$, and π a uniformizer. Then from the definitions, we can write

$$f(x) = h(x) \prod_{i=1}^{n}(x - u_i \pi^{2m}),$$

where

- m and n are positive integers with n odd, $3 \le n \le 2g - 1$.
- $h \in \mathcal{O}_{\mathfrak{p}}[x]$, h (mod π) has distinct roots, and $\pi \nmid h(0)$.
- $u_i \in \mathcal{O}_{\mathfrak{p}}^*$, $i = 1, \ldots, n$, and $\prod_{i=1}^{n}(x - u_i)$ has distinct roots mod π.

We can define two nonisomorphic models $\mathscr{C}_1$ and $\mathscr{C}_2$ of C over $\mathcal{O}_{\mathfrak{p}}$ via the equations $y^2 = h(x)\prod_{i=1}^{n}(x - u_i\pi^{2m})$ and $y^2 = h(\pi^{2m}x)\prod_{i=1}^{n}(x - u_i)$, respectively [18, §4.3]. Let C_1 and C_2 be the hyperelliptic curves over $\mathcal{O}_k/\mathfrak{p}$ defined by $y^2 = x\bar{h}(x)$ and $y^2 = \overline{h(0)}\prod_{i=1}^{n}(x - \bar{u}_i)$, respectively, where the bar denotes the image in $(\mathcal{O}_k/\mathfrak{p})[x]$. Then C_1 and C_2 are birational to the special fibers of $\mathscr{C}_1$ and $\mathscr{C}_2$, respectively. Let $\mathscr{C}$ be the minimal proper regular model of C over $\mathcal{O}_{\mathfrak{p}}$. Since $\mathscr{C}$ can be obtained by desingularizing $\mathscr{C}_1$ or $\mathscr{C}_2$ and then blowing down exceptional curves, it follows that the special fiber $\mathscr{C}_{\mathfrak{p}}$ of $\mathscr{C}$ contains irreducible components Γ_1 and Γ_2 birational to C_1 and C_2, respectively. Let $\mathscr{C}_{\mathfrak{p}} = \sum_{i=1}^{r} n_i\Gamma_i$, where $\Gamma_1, \ldots, \Gamma_r$ are the distinct components of $\mathscr{C}_{\mathfrak{p}}$. Then $\mathscr{C}_{\mathfrak{p}}$ is connected, $\Gamma_i^2 < 0$ for all i, and letting K denote a canonical divisor, we have $\sum_{i=1}^{r} n_i(\Gamma_i.K) = 2g - 2$ and $\Gamma_i.K \ge 0$ for all i (see [32, pp. 342-343], [22, p. 356]). Let g_i be the genus of C_i, $i = 1, 2$. Then by the adjunction formula,

$$\Gamma_i.K = 2p_a(\Gamma_i) - 2 - \Gamma_i^2 \ge 2g_i - 2 + 1 \ge 2g_i - 1, \quad i = 1, 2,$$

where $p_a(\Gamma)$ denotes the arithmetic genus of Γ. Since $g_1 + g_2 = g$, so $\Gamma_1.K + \Gamma_2.K \ge 2g - 2$, we must have $\Gamma_i^2 = -1$, $p_a(\Gamma_i) = g_i$, and $\Gamma_i \cong C_i$ for $i = 1, 2$. Moreover, $\Gamma_i.K = 0$, $i \ge 3$. This implies that $\Gamma_i^2 = -2$ and Γ_i is a nonsingular rational curve for $i \ge 3$. Since $n_1 = n_2 = 1$ and $\Gamma_i.(\mathscr{C}_{\mathfrak{p}} - \Gamma_i) = 1$, $i = 1, 2$, Γ_i meets the rest of the special fiber in exactly one point for $i = 1, 2$. If Γ_1 intersects Γ_i, $i \ge 3$, then $n_i = 1$ and since $\Gamma_i.(\mathscr{C}_{\mathfrak{p}} - \Gamma_i) = 2$, Γ_i meets the rest of the special fiber in exactly one other point. Since $\mathscr{C}_{\mathfrak{p}}$ is connected, continuing with the same reasoning we find that $n_i = 1$ for all i and the special fiber of $\mathscr{C}$ consists of either C_1 and C_2 intersecting at a single point or C_1, C_2, and an appropriate chain of rational curves joining a point of C_1 with a point of C_2. Then it follows from well-known facts on the relationship between a minimal model of C and the Néron model of $\mathrm{Jac}(C)$ [7, §9.5 Th. 4, §9.6 Prop. 10] that $\mathrm{Jac}(C)$ has good reduction at $\mathfrak{p}$ and the reduction mod $\mathfrak{p}$ is isomorphic to $\mathrm{Jac}(C_1) \times \mathrm{Jac}(C_2)$. $\qquad\square$

Finally, since $\mathcal{H}'(g, k, S)$ is finite by the Shafarevich conjecture, we can conclude the (ineffective) finiteness of the set $\mathcal{B}'(2g + 2, k, S)$.

Corollary 6.2. *For any positive integer g, number field k, and finite set of places S of k, the set $\mathcal{B}'(2g + 2, k, S)$ is finite.*

detailed reading of the paper and comments that improved the quality of the paper.

References

1. A. BAKER, *Bounds for the solutions of the hyperelliptic equation*. Proc. Cambridge Philos. Soc. **65** (1969), 439–444.

2. A. BAKER, *Transcendental number theory*. Second ed., Cambridge Mathematical Library, Cambridge University Press, Cambridge, 1990.

3. A. BAKER AND J. COATES, *Integer points on curves of genus 1*. Proc. Cambridge Philos. Soc. **67** (1970), 595–602.

4. YU. BILU (BELOTSERKOVSKIĬ), *Effective analysis of a new class of Diophantine equations*. Vestsī Akad. Navuk BSSR Ser. Fīz.-Mat. Navuk (1988), no. 6, 34–39, 125.

5. YU. BILU, *Effective analysis of integral points on algebraic curves*. Israel J. Math. **90** (1995), no. 1-3, 235–252.

6. YU. BILU, *Quantitative Siegel's theorem for Galois coverings*. Compositio Math. **106** (1997), no. 2, 125–158.

7. S. BOSCH, W. LÜTKEBOHMERT, AND M. RAYNAUD, *Néron models*. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 21, Springer-Verlag, Berlin, 1990.

8. S. G. DALALJAN, *The Prym variety of an unramified double covering of a hyperelliptic curve*. Uspehi Mat. Nauk **29** (1974), no. 6(180), 165–166.

9. S. G. DALALJAN, *The Prym variety of a two-sheeted covering of a hyperelliptic curve with two branch points*. Mat. Sb. (N.S.) **98(140)** (1975), no. 2 (10), 255–267, 334.

10. R. DVORNICICH AND U. ZANNIER, *Fields containing values of algebraic functions*. Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) **21** (1994), no. 3, 421–443.

11. J.-H. EVERTSE AND K. GYŐRY, *Effective finiteness results for binary forms with given discriminant*. Compositio Math. **79** (1991), no. 2, 169–204.

12. G. FALTINGS, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*. Invent. Math. **73** (1983), no. 3, 349–366.

13. D. GRANT, *Integer points on curves of genus two and their Jacobians*. Trans. Amer. Math. Soc. **344** (1994), no. 1, 79–100.

14. M. HINDRY AND J. H. SILVERMAN, *Diophantine geometry*. Graduate Texts in Mathematics, vol. 201, Springer-Verlag, New York, 2000, An introduction.

15. R. VON KÄNEL, *An effective proof of the hyperelliptic Shafarevich conjecture and applications*. PhD thesis, Eidgenössische Technische Hochschule Zürich, 2010.

16. H. KLEIMAN, *On the Diophantine equation $f(x, y) = 0$*. J. Reine Angew. Math. **286/287** (1976), 124–131.

17. Q. LIU, *Modèles minimaux des courbes de genre deux*. J. Reine Angew. Math. **453** (1994), 137–164.

18. Q. LIU, *Modèles entiers des courbes hyperelliptiques sur un corps de valuation discrète*. Trans. Amer. Math. Soc. **348** (1996), no. 11, 4577–4610.

19. J. R. MERRIMAN, *Binary forms and the reduction of curves*. 1970, D.Phil, thesis, Oxford University.

20. J. R. MERRIMAN AND N. P. SMART, *Curves of genus 2 with good reduction away from 2 with a rational Weierstrass point*. Math. Proc. Cambridge Philos. Soc. **114** (1993), no. 2, 203–214.

21. D. MUMFORD, *Prym varieties. I*. Contributions to analysis (a collection of papers dedicated to Lipman Bers), Academic Press, New York, 1974, pp. 325–350.

22. A. P. OGG, *On pencils of curves of genus two*. Topology **5** (1966), 355–362.

23. F. OORT, *Hyperelliptic curves over number fields*. Classification of algebraic varieties and compact complex manifolds, Springer, Berlin, 1974, pp. 211–218. Lecture Notes in Math., Vol. 412.

24. A. N. PARSHIN, *Minimal models of curves of genus* 2. *and homomorphisms of abelian varieties defined over a field of finite characteristic.* Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), 67–109.

25. B. POONEN, *Computational aspects of curves of genus at least* 2. Algorithmic number theory (Talence, 1996), Lecture Notes in Comput. Sci., vol. 1122, Springer, Berlin, 1996, pp. 283–306.

26. D. POULAKIS, *Points entiers et modèles des courbes algébriques.* Monatsh. Math. **118** (1994), no. 1-2, 111–143.

27. G. RÉMOND, *Hauteurs thêta et construction de Kodaira.* J. Number Theory **78** (1999), no. 2, 287–311.

28. J.-P. SERRE AND J. TATE, *Good reduction of abelian varieties.* Ann. of Math. (2) **88** (1968), 492–517.

29. I. R. SHAFAREVICH, *Algebraic number fields.* Proc. Internat. Congr. Mathematicians (Stockholm, 1962), Inst. Mittag-Leffler, Djursholm, 1963, pp. 163–176.

30. C.L. SIEGEL, *Über einege Anwendungen Diophantischer Approximationen.* Abh. Preuss. Akad. Wiss. Phys. Math. Kl. (1929), 41–69.

31. J. H. SILVERMAN, *Integral points on abelian varieties.* Invent. Math. **81** (1985), no. 2, 341–346.

32. J. H. SILVERMAN, *Advanced topics in the arithmetic of elliptic curves.* Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.

33. N. P. SMART, *S-unit equations, binary forms and curves of genus* 2. Proc. London Math. Soc. (3) **75** (1997), no. 2, 271–307.

34. U. ZANNIER, *Roth's theorem, integral points and certain ramified covers of* $\mathbb{P}_1$. Analytic number theory, Cambridge Univ. Press, Cambridge, 2009, pp. 471–491.

Aaron LEVIN
Department of Mathematics
Michigan State University
East Lansing, MI 48824
E-mail: `adlevin@math.msu.edu`