Pure and Applied Mathematics Quarterly
Volume 4, Number 3
(*Special Issue: In honor of
Fedya Bogomolov, Part 2 of 2*)
715—728, 2008

A Shafarevich-Faltings Theorem for Rational Functions

Lucien Szpiro and Thomas J. Tucker

*This paper is dedicated to Fedya Bogomolov
on the occasion of his 60th birthday.*

Abstract: Using an alternative notion of good reduction, a generalization of the Shafarevich finiteness theorem for elliptic curves is proved for self-maps of the projective line over number fields.

1. Introduction

In 1963, Shafarevich ([Sha63]) proved that for any finite set S of primes in a number field K, there are finitely many isomorphism classes of elliptic curves with good reduction at all primes outside of S (see also [Ser98, IV.1.4] for a quick proof of this result). Shafarevich also conjectured that there were only finitely many isomorphism classes of abelian varieties over K of any fixed dimension, with polarization of fixed degree d, that have good reduction at all primes outside of S. This conjecture, often called the Shafarevich conjecture, was later proved by Faltings ([Fal83]) as part of his celebrated proof of the Mordell conjecture.

Shafarevich's result implies that that the minimal discriminant of an elliptic curve can be bounded in terms of the conductor of the curve. Indeed, this follows trivially from the fact that his result implies that there are finitely many isomorphism classes of elliptic curves having fixed conductor. An explicit bound for the

Received March 14, 2006.

minimal discriminant in terms of the conductor was later proposed by the first author ([Szp90]). This conjecture was proved for function fields ([HS88, PS00]), but it remains open in the number field case. Note that the *abc*-conjecture of Masser and Oesterlé (which is closely related to this conjecture) has been proved for function fields by Mason [Mas84] (in fact, it might be more accurate to say that Mason's result along with a conjecture of [Szp90] helped motivate the *abc*-conjecture) and that Arakelov, Paršin, and the first author ([Ara71, Par68, Szp79]) proved the Shafarevich conjecture over function fields several years before Faltings proved it for number fields. Bogomolov, Katzarkov, and Pantev ([BKP02]) have even managed to prove a version of the conjecture of [Szp90] for hyperelliptic curves over function fields.

Perhaps the most natural definition for good reduction in the context of non-constant morphisms $\varphi : \mathbb{P}^1_K \to \mathbb{P}^1_K$ over a number field K is to say that such a map φ has good reduction at a finite place v if φ extends to a map $\mathbb{P}^1_{\mathfrak{o}_v} \to \mathbb{P}^1_{\mathfrak{o}_v}$, where $\mathfrak{o}_v$ is the localization of the ring of integers $\mathfrak{o}_K$ at v. When this is the case, we will say that φ has **simple good reduction** at v. Note that this is equivalent to saying that there is a choice of $\mathfrak{o}_v$-coordinates for $\mathbb{P}^1_{\mathfrak{o}_v}$ such that φ can be written as $\varphi([x : y]) = [P(x, y) : Q(x, y)]$ where P and Q are homogeneous polynomials of the same degree in $\mathfrak{o}_v[x, y]$ that do not have common roots in the algebraic closure of the residue field at v. The situation here, however, is quite different from the case of elliptic curves since any monic polynomial $f(x) \in \mathfrak{o}_K[x]$ gives rise to a morphism that has simple good reduction at all finite places. Thus, one is led to consider alternative notions of good reduction, one of which we will now explain.

Let K be a number field, let $\mathfrak{o}_K$ be its ring of integers, let S be a finite set of finite places of $\mathfrak{o}_K$, and let $\overline{K}$ be an algebraic closure of K. We define

$$\mathfrak{o}_S = \{z \in K \quad | \quad |z|_v \leq 1 \text{ for all } v \notin S\}.$$

The ring $\mathfrak{o}_S$ is often referred to as the ring of S-integers in K. Let $\mathbb{P}^1_{\mathfrak{o}_S}$ be the usual projective line over $\operatorname{Spec} \mathfrak{o}_S$ (which can be defined as $\operatorname{Proj} \mathfrak{o}_S[T_0, T_1]$, as in [Har77, p. 103]), and let $g : \mathbb{P}^1_K \xrightarrow{\sim} \left(\mathbb{P}^1_{\mathfrak{o}_S}\right)_K$ be an isomorphism (where $\left(\mathbb{P}^1_{\mathfrak{o}_S}\right)_K$ denotes $\mathbb{P}^1_{\mathfrak{o}_S} \times_{\operatorname{Spec} \mathfrak{o}_S} \operatorname{Spec} K$, as usual). One obtains a map $\mathbb{P}^1_K \to \mathbb{P}^1_{\mathfrak{o}_S}$ by composing g with the base extension $\left(\mathbb{P}^1_{\mathfrak{o}_S}\right)_K \to \mathbb{P}^1_{\mathfrak{o}_S}$. For each finite place $v \notin S$, this map gives rise to a reduction map $r_{g,v} : \mathbb{P}^1(K) \longrightarrow \mathbb{P}^1(k_v)$ where k_v is residue field of

$\mathfrak{o}_K$ at v. By extending the place v to a place on $\overline{K}$, one may extend $r_{g,v}$ to a map $r_{g,v} : \mathbb{P}^1(\overline{K}) \longrightarrow \mathbb{P}^1(\overline{k}_v)$. This allows us to make the following definition.

Definition 1.1. *Let $\varphi : \mathbb{P}^1_K \longrightarrow \mathbb{P}^1_K$ be a nonconstant morphism of degree greater than 1, let $g : \mathbb{P}^1_K \tilde{\to} \left(\mathbb{P}^1_{\mathfrak{o}_S}\right)_K$ be an isomorphism, let R_φ denote the ramification divisor of φ over $\overline{K}$, and let $v \notin S$ be a finite place of K that has been extended to $\overline{K}$. We say that φ has* **critically good reduction** *at a finite place $v \notin S$ if the following conditions are met:*

(i) *for any points $P \neq Q$ in $\mathbb{P}^1(\overline{K})$ contained in $\operatorname{Supp} R_\varphi$, we have $r_{g,v}(P) \neq r_{g,v}(Q)$; and*
(ii) *for any points $P \neq Q$ in $\mathbb{P}^1(\overline{K})$ contained in $\varphi(\operatorname{Supp} R_\varphi)$ we have $r_{g,v}(P) \neq r_{g,v}(Q)$.*

The terminology "critically good reduction" was suggested to the authors by Joseph Silverman during the preparation of this paper. Our definition does not depend on how we choose to extend v to all of $\overline{K}$, since if v' is a place of $\overline{K}$ that agrees with v on K, then there is an automorphism $\tau \in \operatorname{Gal}(\overline{K}/K)$ such that $r_{g,v}(P) = r_{g,v'}(\tau P)$ for all $P \in \mathbb{P}^1(\overline{K})$. A simple way of describing this definition is to say that all the distinct $\overline{K}$-points in $\operatorname{Supp} R_\varphi$ remain distinct after reduction at v and all the distinct $\overline{K}$-points in $\varphi(\operatorname{Supp} R_\varphi)$ remain distinct after reduction at v.

The automorphism group $\operatorname{Aut}(\mathbb{P}^1_{\mathfrak{o}_S})$ is isomorphic to $\operatorname{PGL}_2(\mathfrak{o}_S)$ (that is, $\operatorname{GL}_2(\mathfrak{o}_S)$ modulo homotheties in $\operatorname{GL}_2(\mathfrak{o}_S)$). This can be seen by choosing $\mathfrak{o}_S$-coordinates for $\mathbb{P}^1_{\mathfrak{o}_S}$. We say that two morphisms $\varphi : \mathbb{P}^1_K \to \mathbb{P}^1_K$ and $\psi : \mathbb{P}^1_K \to \mathbb{P}^1_K$ are g-equivalent if they are the same up to multiplication by an element of $\operatorname{Aut}(\mathbb{P}^1_{\mathfrak{o}_S})$ on both sides; that is, if there are automorphisms $\gamma, \sigma \in \operatorname{Aut}(\mathbb{P}^1_{\mathfrak{o}_S})$ such that

$$\psi = \sigma_K \varphi \gamma_K,$$

where σ_K and γ_K are the pull-backs of σ and γ to $\mathbb{P}^1_K$ (via the isomorphism $g : \mathbb{P}^1_K \tilde{\to} \left(\mathbb{P}^1_{\mathfrak{o}_S}\right)_K$ and the map $\left(\mathbb{P}^1_{\mathfrak{o}_S}\right)_K \longrightarrow \mathbb{P}^1_{\mathfrak{o}_S}$). With this terminology, the main result of this paper is the following analog of Shafarevich's theorem ([Sha63]) for elliptic curves.

Theorem 1. *Let S be a finite set of finite places of a number field K, let n be an integer greater than one, and let $g : \mathbb{P}^1_K \tilde{\to} \left(\mathbb{P}^1_{\mathfrak{o}_S}\right)_K$ be an isomorphism. There are finitely many g-equivalence classes of nonconstant morphisms $\varphi : \mathbb{P}^1_K \longrightarrow \mathbb{P}^1_K$*

of degree n that ramify at three or more points and have critically good reduction at all finite places outside of S.

Note that if a map φ ramifies at exactly two points, it is easy to see that there are automorphisms σ_L and γ_L, each defined over a quadratic extension L of K, such that $\sigma_L \varphi \gamma_L$ is a map of the form $x \mapsto ax^m$. Thus, the equivalence classes for such maps are even easier to describe, provided that one considers a slightly larger automorphism group.

The proof of Theorem 1 is as follows. In Section 3, we use a result of Birch-Merriman and Evertse-Győry ([BM72, EG91]) to show that there is a finite set $\mathcal{Y}$ such that $\operatorname{Supp} R_\varphi$ and $\varphi(\operatorname{Supp} R_\varphi)$ are both contained in $\mathcal{Y}$ after the application of suitable automorphisms. Then, in Section 4, we apply a result of Grothendieck and Mori ([Gro71, Mor79]) to conclude that this gives us a finite set of equivalence classes of maps.

Acknowledgments. We would like to thank Joseph Silverman for many helpful conversations. We would like to thank Xander Faber for his careful reading of the paper and for his many useful suggestions.

2. Connections with other notions of good reduction

Note that the notion of critically good reduction is in some ways quite similar to the notion of good reduction on an elliptic curve. A model $y^2 = F(x) = x^3 + px + q$ for an elliptic curve E over $\mathfrak{o}_K$ has good reduction at a finite place v not dividing 2 or 3 if and only if F has distinct roots modulo v. This implies that the ramification points of the map obtained by projecting onto the x-coordinate remain distinct after reduction at v. In fact, the multiplication-by-two map on an elliptic curve is associated to a map $\varphi : \mathbb{P}^1_K \longrightarrow \mathbb{P}^1_K$, called a Lattès map, which can be written explicitly as $\varphi(x) = \frac{(F'(x))^2 - 8xF(x)}{4F(x)}$. This map is simply the usual rational function that describes the x-coordinate of 2β in terms of the x-coordinate of β for β a point on E (see [Sil86, Chapter 2], for example). Note that our definition of critically good reduction depends on our choice of an isomorphism $g : \mathbb{P}^1_K \tilde{\to} \left(\mathbb{P}^1_{\mathfrak{o}_S}\right)_K$. Choosing coordinates $[x : y]$ gives rise to a natural isomorphism g, and when a map φ is written explicitly in terms of coordinates we will say that φ has critically good reduction at v if it has critically good reduction

at v in the model these coordinates determine. With this convention, we have the following.

Proposition 2.1. *Let E be an elliptic curve over a number field K and let S be a set of finite places of K containing all places v such that $v|2$. If the model $y^2 = F(x)$ for E over $\mathfrak{o}_S$ has good reduction at all finite places $v \notin S$, then the corresponding Lattès map $\varphi(x) = \frac{(F'(x))^2 - 8xF(x)}{4F(x)}$ has both critically good reduction and simple good reduction at all finite places $v \notin S$.*

Proof. Let $v \notin S$ be a finite place of K and let $\mathfrak{m}$ denote the maximal ideal corresponding to v in $\mathfrak{o}_S$. Since the model $y^2 = F(x)$ has good reduction at v, the leading coefficient of F is a unit at v and the roots of F are distinct at v. Suppose that some α in the algebraic closure of $\mathfrak{o}_S/\mathfrak{m}$ is a root of both $4F(x)$ and $(F'(x))^2 - 8xF(x)$ modulo $\mathfrak{m}$; then it is a multiple root of $F(x)$ modulo $\mathfrak{m}$, which would mean that F does not have distinct roots modulo $\mathfrak{m}$ and that E therefore not have good reduction at v. Thus, there is no such α, so $\varphi(x)$ is well-defined modulo $\mathfrak{m}$ for all x. Since the leading coefficient of $(F'(x))^2 - 8xF(x)$ is the same as the leading coefficient of F (and is thus a unit at v), the map φ is also well-defined at infinity. Hence, φ has simple good reduction at v.

To see that the map $\varphi(x) = \frac{(F'(x))^2 - 8xF(x)}{4F(x)}$ has critically good reduction, we simply note that the ramification points of this map are the x-coordinates of the the points in $E[4] \setminus E[2]$ (i.e., the 4-torsion points of E that are not 2-torsion points) and that their images are the x-coordinates of the points $E[2] \setminus \{0\}$. The reduction map at v is injective on prime-to-p torsion for $v \mid p$ (see [Sil86, Proposition VII.3.1], for example), and $p \neq 2$ by assumption, so all of the points in $E[4]$ are distinct modulo $\mathfrak{m}$. Thus, all of the points in $\operatorname{Supp} R_\varphi$ and $\varphi(\operatorname{Supp} R_\varphi)$ are distinct modulo $\mathfrak{m}$, as desired. □

More generally, it is possible to have simple good reduction without having critically good reduction. This can be seen, for example, by taking any monic polynomial $f(x) \in \mathfrak{o}_K[x]$ such that $f'(x)$ has multiple roots at some place v. It is also possible to have critically good reduction without having simple good reduction; the map $x \mapsto \frac{x^2+p}{p}$ is an example of this. On the other hand, under fairly generic hypotheses, critically good reduction does imply simple good reduction.

Proposition 2.2. *Let $\varphi(x) = P(x)/Q(x)$ be a rational function of degree d with coefficients in $\mathfrak{o}_S$ for S some finite set of finite places of a number field K. Let*

$v \notin S$ be a finite place of K. Suppose that φ has $2d-2$ distinct ramification points and that the leading coefficients of P, Q, and $P'(x)Q(x) - P(x)Q'(x)$ are all v-adic units. Then, if φ has critically good reduction at v, it also has simple good reduction at v.

Proof. Suppose that φ does not have simple good reduction. Then there is a α with $|\alpha|_v \leq 1$ such that $P(\alpha)$ and $Q(\alpha)$ are both zero modulo the maximal ideal at v. Let $\bar{P}$, $\bar{Q}$, and $\bar{\alpha}$ denote the reductions of P, Q, and α, respectively, at v. Then $\bar{P}'(\bar{\alpha})\bar{Q}(\bar{\alpha}) - \bar{P}(\bar{\alpha})\bar{Q}'(\bar{\alpha}) = 0$; taking the derivative again, we find that $\bar{P}''(\bar{\alpha})\bar{Q}(\bar{\alpha}) - \bar{P}(\bar{\alpha})\bar{Q}''(\bar{\alpha}) = 0$. Thus, $\bar{\alpha}$ is a double root of $\bar{P}'\bar{Q} - \bar{P}\bar{Q}'$. It follows that $\bar{P}'\bar{Q} - \bar{P}\bar{Q}'$ has fewer distinct roots than $P'Q - PQ'$. Since $'Q - PQ'$ and $\bar{P}'\bar{Q} - \bar{P}\bar{Q}'$ both have the same degree, it follows that two roots of $P'Q - PQ'$ reduce to the same root of $\bar{P}'\bar{Q} - \bar{P}\bar{Q}'$. Since the roots of $P'Q - PQ'$ are all ramification points of φ, this means that φ does not have critically good reduction at v. □

Shafarevich's theorem ([Sha63]) can be considered a special case of Theorem 1 by taking the map $\psi_E : \mathbb{P}^1_K \longrightarrow \mathbb{P}^1_K$ corresponding to the multiplication-by-4 map on an elliptic curve E (this is simply $\varphi \circ \varphi$ where φ is the Lattès map considered earlier). As noted in [Ser98, IV.1.4], if E has good reduction outside of a finite set of places S that includes the places lying over 2 and 3 and for which $\mathfrak{o}_S$ is a principal ideal domain, then there is a model for E given by an equation $y^2 = F(x)$, where the coefficients of F are in $\mathfrak{o}_S$, the leading coefficient of F is an S-unit, and F does not have multiple roots at any of the finite places outside of S. The map ψ_E ramifies over the points where the projection onto the x-coordinate map from E to $\mathbb{P}^1$ ramifies (note that the Lattès map on $\mathbb{P}^1$ corresponding to multiplication-by-2 fails to ramify at infinity, which is why use multiplication-by-4) and has critically good reduction outside of S, since it ramifies at the x-coordinates of the points in $E[8] \setminus E[2]$ and over the x-coordinates of the points in $E[2]$. Now, let E' be another elliptic curve with good reduction outside S having the property that $\psi_{E'}$ is g-equivalent to ψ_E. Let $y^2 = G(x)$ be a model for E', where G has coefficients in $\mathfrak{o}_S$ and the leading coefficient of G is an S-unit. Since ψ_E and $\psi_{E'}$ are g-equivalent, we have an automorphism $\gamma \in \mathrm{Aut}(\mathbb{P}^1_{\mathfrak{o}_S})$ that takes the x-coordinates of the points in $E[2]$ to the x-coordinates of the points in $E'[2]$. After this automorphism we may suppose that F and G have the same roots (since their roots, along with ∞ are the x-coordinates of the 2-torsion). This

means that $G = uF$ for some S-unit u. Since replacing y with a multiple of y in the Weierstrass equation for an elliptic curve does not change the isomorphism class, we see that the isomorphism class of E' is determined is determined by the coset class of u in $\mathfrak{o}_S^*/(\mathfrak{o}_S^*)^2$. Since $\mathfrak{o}_S^*$ is finitely generated, it follows that there are only finitely many isomorphism classes of elliptic curves E' such that $\psi_{E'}$ is g-equivalent to ψ_E. Hence, Theorem 1 implies Shafarevich's theorem.

3. Finiteness theorems and homogeneous forms

Let K be number field, let S be a finite set of finite places of K, and let $g : \mathbb{P}^1 \longrightarrow (\mathbb{P}_{\mathfrak{o}_S})_K$ be an isomorphism. Let $v \notin S$ be a finite place of K. Let k_v denote the residue field of K at v. The isomorphism g gives us a reduction map

$$r_{g,v} : \mathbb{P}^1(K) \longrightarrow \mathbb{P}^1(k_v),$$

as described in the introduction. We may extend v to all of $\overline{K}$. We then have a reduction map

$$r_{g,v} : \mathbb{P}^1(\overline{K}) \longrightarrow \mathbb{P}^1(\overline{k}_v).$$

Definition 3.1. *Let*

$$\mathcal{U} = \{z_1, \ldots, z_n\},$$

where z_i are distinct elements of $\mathbb{P}^1(\overline{K})$, and let $v \notin S$ be a finite place of K. We say that the set $\mathcal{U}$ is $r_{g,v}$-distinct if $r_{g,v}(z_i) \neq r_{g,v}(z_j)$ for all $i \neq j$.

Using coordinates, we have a very simple criterion for deciding when a set is $r_{g,v}$-distinct. We may choose coordinates for $\mathbb{P}^1_K$ and $\mathbb{P}^1_{\mathfrak{o}_S}$ such that the map $\mathbb{P}^1_K \to \mathbb{P}^1_{\mathfrak{o}_S}$ obtained by composing g with the base extension map is given in coordinates by $[a : b] \mapsto [ca : cb]$ for any $c \in K$ such that $ca, cb \in \mathfrak{o}_S$. For each $z_i \in \mathcal{U}$, we write z_i as $[a_i : b_i]$ where $a_i, b_i \in \overline{K}$ and $\max(|a_i|_v, |b_i|_v) = 1$. Then $\mathcal{U}$ is $r_{g,v}$-distinct if and only if

$$|a_i b_j - a_j b_i|_v = 1 \tag{3.1.1}$$

for all $i \neq j$. This follows from the fact that

$$r_{g,v}([a_i : b_i]) = [a_i \mod \mathfrak{m}_v : b_i \mod \mathfrak{m}_v] \in \mathbb{P}^1(\overline{k}_v)$$

where $\mathfrak{m}_v$ is the maximal ideal corresponding to v in the ring of integers of $\overline{K}$.

Definition 3.2. *Let S be a finite set of finite places of K. We say that a set $\mathcal{U} \subseteq \mathbb{P}^1(\overline{K})$ is S-good if for every finite place $v \notin S$, the set $\mathcal{U}$ is $r_{g,v}$-distinct.*

We will relate the notion of sets being S-good to the discriminant of homogeneous forms that vanish at $\mathcal{U}$. This will allow us to apply a finiteness result due to Birch and Merriman ([BM72]; see also [EG91]). We define

$$\mathfrak{o}_S^* = \{z \in K \quad | \quad |z|_v = 1 \text{ for all } v \notin S\}.$$

The elements of this unit group $\mathfrak{o}_S^*$ are called *S-units*. For any $\delta \in \mathfrak{o}_K$ we define $\delta\mathfrak{o}_S^*$ to be the set of all elements of K of the form δu for $u \in \mathfrak{o}_S^*$.

Let $F(x,y)$ be a homogeneous form of degree n in $\mathfrak{o}_S[x,y]$. Factoring F in $\overline{K}[x,y]$ as

$$F(x,y) = \prod_{i=1}^{n}(\beta_i x - \alpha_i y),$$

we define the discriminant $\Delta(F)$ of F as

$$\Delta(F) = \left(\prod_{i<j}(\alpha_i\beta_j - \beta_i\alpha_j)\right)^2.$$

For $\gamma \in \mathrm{SL}_2(\mathfrak{o}_S)$, with

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

we let

$$\gamma(F(x,y)) = F(ax+by, cx+dy).$$

Let $F(x,y)$ and $G(x,y)$ be homogeneous forms in $\mathfrak{o}_S[x,y]$. We say that F and G are in the same $\mathfrak{o}_S$-equivalence class if there is an element $\gamma \in \mathrm{SL}_2(\mathfrak{o}_S)$ and a $\lambda \in \mathfrak{o}_S^*$ such that $\gamma(F(x,y)) = \lambda G(x,y)$. Birch-Merriman ([BM72, Theorem 1]) and Evertse-Győry ([EG91, Theorem 3]) proved the following theorem about $\mathfrak{o}_S$-equivalence classes of homogeneous forms.

Theorem 3.3. *(*[BM72, Theorem 1], [EG91, Theorem 3]*.) Let δ be any nonzero element of $\mathfrak{o}_S$ and let n be a positive integer. There are finitely many $\mathfrak{o}_S$-equivalence classes of degree n homogeneous forms $F(x,y) \in \mathfrak{o}_S[x,y]$ such that $\Delta(F) \in \delta\mathfrak{o}_S^*$.*

We note that Birch and Merriman only state their result for forms in $\mathfrak{o}_K[x,y]$ and in the case that $\delta = 1$, but one can deduce the statement above for forms in $\mathfrak{o}_S[x,y]$ and arbitrary $\delta \in \mathfrak{o}_K$ from their result ([BM72, Theorem 1]). Evertse and Győry's result ([EG91, Theorem 3]) is an effective version of Theorem 3.3.

Proposition 3.4. *Let n be an integer. Then there is a finite set $\mathcal{Y}$ such that for any S-good $\mathrm{Gal}(\overline{K}/K)$-stable set $\mathcal{U}$ of cardinality n, there is a $\gamma \in \mathrm{Aut}(\mathbb{P}^1_{\mathfrak{o}_S})$ such that $\gamma_K(\mathcal{U}) \subseteq \mathcal{Y}$.*

Proof. We will need a little notation to deal with the fact that $\mathfrak{o}_S$ may not be a unique factorization domain. For any fractional ideal J of $\mathfrak{o}_S$ we let $v(J) = e_{J_v}$ where e_{J_v} is the power of the prime $\mathfrak{p}_v$ corresponding to v in the factorization of J into prime ideals. Let $I_1, \ldots, I_s$ be a set of (integral) ideals in $\mathfrak{o}_S$ representing the ideal classes of $\mathfrak{o}_S$; that is, for any fractional ideal J of $\mathfrak{o}_S$, there is an $\alpha \in K$ such that $\alpha J = I_\ell$ for some ℓ. Then there are finitely many sets of the form $\delta\mathfrak{o}_S^*$ where δ is an element of $\mathfrak{o}_k$ such that $v((\delta)) \leq (2n-2)v(I_j)$ for all I_j. Let $\mathcal{W} = \{\delta_1\mathfrak{o}_S^*, \ldots, \delta_m\mathfrak{o}_S^*\}$ be the set of all such $\delta\mathfrak{o}_S^*$.

By Theorem 3.3, for any $\delta \in \mathfrak{o}_S$, there are at most finitely many $\mathfrak{o}_S$-equivalence classes of forms in $G \in \mathfrak{o}_S[x,y]$ of degree n such that $\Delta(G) \in \beta\mathfrak{o}_S^*$. Thus we may choose a set of forms $G_1, \ldots, G_t$ such that for any form F of degree n with $\Delta(F) \in \delta_j\mathfrak{o}_S^*$, for $\delta_j\mathfrak{o}^* \in \mathcal{W}$, there is some G_i such that F is $\mathfrak{o}_S$-equivalent to G_i. Let

$$\mathcal{Y} = \{[a:b] \in \mathbb{P}^1(\overline{K}) \;\mid\; G_i(a,b) = 0 \text{ for some } G_i\}.$$

Let $\mathcal{U} = \{[a_1 : b_1], \ldots, [a_n : b_n]\}$ be S-good and let H be any homogeneous form of degree n in $\mathfrak{o}_S[x,y]$ that vanishes on $\mathcal{U}$. After multiplying through by a nonzero element $\alpha \in K$, we obtain a form $\alpha H \in \mathfrak{o}_S[x,y]$ such that the coefficients of αH generate one of the ideals I_j above. Write each $[a_i : b_i]$ as $[a_i' : b_i']$ where $\max(|a_i'|_v, |b_i'|_v) = 1$. Then, there is an element $\kappa \in \overline{K}$ such that

$$\alpha H(x,y) = \kappa \prod_{i=1}^{n} (b_i'x - a_i'y).$$

We have

$$|\Delta(\alpha H)|_v = |\kappa|_v^{2n-2} \left| \left(\prod_{i<j} (a_i'b_j' - b_i'a_j') \right)^2 \right|_v = |\kappa|_v^{2n-2}$$

since $|a_i'b_j' - b_i'a_j'|_v = 1$ for all i, j (because $\mathcal{U}$ is S-good) and multiplying a form of degree d through by a constant κ changes the discriminant by a factor of κ^{2n-2}. Now, $v((\kappa)) \geq 0$ by the Gauss lemma for polynomials and $v((\kappa)) \leq v(I_j)$ because of the fact that the coefficients of αH generate I_j. Since $v((\kappa)) \leq v(I_j)$, we see that $\kappa^{2n-2}\mathfrak{o}_S^* = \delta_i\mathfrak{o}_S^*$ for some $\delta_i\mathfrak{o}_S^* \in \mathcal{W}$.

Thus, for some G_ℓ, there is a $\tau \in \mathrm{SL}_2(\mathfrak{o}_S)$ and $\lambda \in \mathfrak{o}_S^*$ such that $\tau(\alpha H) = \lambda G_\ell$. Hence, for each $[a_i : b_i]$, we have $G_\ell(\tau([a_i : b_i])) = 0$. Our choice of coordinates gives an inclusion of $\mathrm{SL}_2(\mathfrak{o}_S)$ into $\mathrm{Aut}(\mathbb{P}^1_{\mathfrak{o}_S})$. Thus, τ corresponds to an element $\gamma \in \mathrm{Aut}(\mathbb{P}^1_{\mathfrak{o}_S})$ such that

$$\gamma_K(\mathcal{U}) \subseteq \mathcal{Y},$$

as desired. □

4. Applying a Result of Grothendieck-Mori

We will now state a result due to Grothendieck and Mori ([Gro71, Mor79]). We note that what Mori proves is much more general than what is required here. Let A and B be schemes of finite type over an algebraically closed field L, and let Z be a closed subscheme of A. Let $p : Z \longrightarrow B$ be an L-morphism. Let $\mathrm{Hom}_L(A, B; p)$ be the set of L-morphisms from A to B that extend p, that is

$$\mathrm{Hom}_L(A, B; p) = \{f : A \longrightarrow B \mid f \text{ is an } L\text{-morphism and } f|_Z = p\}.$$

We let $\mathcal{I}_Z$ denote the ideal sheaf of Z in A and let T_B denote the tangent sheaf of B over L.

Theorem 4.1. *(*[Mor79, Propositions 1 and 3]*.) The set* $\mathrm{Hom}_L(A, B; p)$ *is represented by a closed subscheme of* $\mathrm{Hom}_L(A, B)$ *and for any closed point* f *in* $\mathrm{Hom}_L(A, B; p)$*, we have*

$$T_{f,\mathrm{Hom}_L(A,B;p)} \cong H^0(A, f^*T_B \otimes_{\mathcal{O}_A} \mathcal{I}_Z),$$

where $T_{f,\mathrm{Hom}_L(A,B;p)}$ *is the tangent space of* f *in* $\mathrm{Hom}_L(A, B; p)$ *over* L*.*

Using this theorem, we are able to derive the following proposition.

Proposition 4.2. *Let* $\mathcal{Y}$ *be a finite subset of* $\mathbb{P}^1(L)$ *and let* $n > 1$ *be an integer. Then there are finitely many morphisms* $\varphi : \mathbb{P}^1_L \longrightarrow \mathbb{P}^1_L$ *of degree* n *satisfying all of the following conditions:*

(i) $\mathrm{Supp}\, R_\varphi \subseteq \mathcal{Y}$*;*
(ii) $\varphi(\mathrm{Supp}\, R_\varphi) \subseteq \mathcal{Y}$*; and*
(iii) $|\mathrm{Supp}\, R_\varphi| \geq 3$*.*

Proof. There are at most $|\mathcal{Y}|^n$ possible divisors D with support in $\mathcal{Y}$ that could be ramification divisors of morphisms $\varphi : \mathbb{P}^1_L \to \mathbb{P}^1_L$ of degree n. Furthermore,

the fact that $\mathcal{Y}$ is finite means that there are finitely many possibilities for the image $\varphi(\operatorname{Supp} R_\varphi)$. Thus, it suffices to show that for any divisor $D = \sum_{i=1}^m f_i Q_i$ on $\mathbb{P}^1$ with $|\operatorname{Supp} D| \geq 3$ and any sequence of points $P_1, \ldots, P_m$ (not necessarily distinct) with $P_i \in \mathcal{Y}$, there are at most finitely many morphisms φ of degree n such that $R_\varphi = D$ and $\varphi(Q_i) = P_i$.

Let D be the ramification divisor of a map φ of degree n. We write $D = \sum_{i=1}^m (e_{Q_i} - 1)Q_i$ where e_{Q_i} is the ramification index of φ at Q_i. For each $Q_i \in \operatorname{Supp} D$, let $\mathcal{I}_{Q_i}$ represent the ideal sheaf of Q_i in $\mathbb{P}^1$, and let Z be the subscheme of $\mathbb{P}^1$ with ideal sheaf $\mathcal{I} = \prod_{i=1}^m \mathcal{I}^{e_{Q_i}}$ (note that the correct exponent here is e_{Q_i}, not $(e_{Q_i} - 1)$).

At each P_i we have

$$\varphi^*(\mathcal{I}_{P_i}) = \prod_{\varphi(Q)=P_i} \mathcal{I}_Q^{e_Q}$$

(by the definition of the ramification index.) Thus, at each Q, the map to $P_i \in \mathbb{P}^1_L$ from the scheme defined by $\mathcal{I}_{Q_i}^{e_{Q_i}}$ is induced by the unique nonzero map of L-algebras from L to $L[x]/x^{e_Q}$. These piece together to form a unique map $p : Z \longrightarrow \mathbb{P}^1_L$. Thus, we have $R_\varphi = D$ and $\varphi(Q_i) = P_i$ for $i = 1, \ldots, m$ exactly when φ restricts to p on Z.

Using the Riemann-Hurwitz formula, we see that

$$-\deg \mathcal{I}_Z = \deg R_\varphi + |\operatorname{Supp} D| = (2n-2) + |\operatorname{Supp} D| \geq 2n+1.$$

Since $\deg \varphi^* T_{\mathbb{P}^1_L} = 2n$, we have $\deg(\varphi^* T_{\mathbb{P}^1_L} \otimes \mathcal{I}_Z) < 0$, so

$$\dim_L T_{\varphi, \operatorname{Hom}_L(\mathbb{P}^1_L, \mathbb{P}^1_L; p)} = \dim_L H^0(\varphi^* T_{\mathbb{P}^1_L} \otimes \mathcal{I}_Z) = 0.$$

The scheme $\operatorname{Hom}_L(\mathbb{P}^1_L, \mathbb{P}^1_L; p)$ therefore has dimension zero. Since it is also Noetherian, this means that it is finite. Thus, there are at most finitely many maps φ such that $R_\varphi = D$ and $\varphi(Q_i) = P_i$ for $i = 1, \ldots, m$. This completes our proof. □

We are now ready to prove Theorem 1.

Proof. (*Of Theorem 1.*) Since $\operatorname{Supp} R_\varphi$ and $\operatorname{Supp}(\varphi_* R_\varphi)$ are both S-good, there are $\gamma, \sigma \in \mathrm{SL}_2(\mathfrak{o}_S) \subseteq \operatorname{Aut}(\mathbb{P}^1_{\mathfrak{o}_S})$ such that both $\gamma_K(\operatorname{Supp} R_\varphi)$ and $\sigma_K(\varphi(\operatorname{Supp} R_\varphi))$ are contained in $\mathcal{Y}$. Then the map

$$\psi = \sigma_K \varphi \gamma_K^{-1}$$

satisfies the conditions of Proposition 4.2. □

5. Generalizations of Theorem 1

There are many possible ways in which Theorem 1 might be generalized and strengthened.

5.1. **Effectivity.** As noted earlier, Evertse and Győry ([EG91]) have proved an effective version of Theorem 3.3. More precisely, they are able to produce an explicit constant C (depending only on S and the degree n) such that each $\mathfrak{o}_S$-equivalence class of homogeneous forms contains a form with height less than C. This translates immediately into a bound on the height of points in the set $\mathcal{Y}$ used in Proposition 3.4. While Theorem 4.1 is not effective as stated, it should be possible to derive an effective version of Proposition 4.2 by viewing the conditions placed on φ as hypersurfaces in a suitable space of rational functions and applying an arithmetic Bézout-type theorem such as the one proved by Bost, Gillet, and Soulé in [BGS94]. We plan to treat this question in a later paper. Note that effective versions of the Shafarevich conjecture have been proved in the number field case for elliptic curves by Silverman and Brumer ([BS96]) and for more general curves in the function field case by Caporaso and Heier ([Cap02, Hei04]).

5.2. **Higher dimensions.** It should be possible to formulate a higher-dimensional version of Theorem 1. One might for example impose the condition that all the components of the ramification divisor and its image intersect properly at all primes outside of a finite set S. Mori's results still apply in higher dimensions. What is less clear is how to apply finiteness results about homogeneous forms.

5.3. **Function fields.** It may also be possible to prove an analog of Theorem 1 for maps over function fields over finite fields. Note, however, that since there are maps in characteristic p that ramify over single point, certain classes of maps would probably have to be excluded. Unfortunately, these classes include the maps that correspond to Drinfeld modules. Taguchi ([Tag92]) has also shown that the Shafarevich conjecture with the usual notion of good reduction does not hold for Drinfeld modules. It would be interesting to find a notion of good reduction that gives rise to an analog of the Shafarevich conjecture that *does* hold for Drinfeld modules.

5.4. **An *abc*-conjecture for morphisms of the projective line.** In [Szp90], it is conjectured that the minimal discriminant of an elliptic curve can be bounded explicitly in terms of the conductor of the curve. For a morphism $\varphi : \mathbb{P}^1_K \to \mathbb{P}^1_K$, there is a minimal resultant for polynomials P and Q where φ can be written as P/Q and a "critical conductor" for φ; the latter might be defined as the product of the primes at which the map fails to have critically good reduction. It is natural to ask whether the minimal resultant can be bounded explicitly in terms of the critical conductor.

References

[Ara71] S. Ju. Arakelov. Families of algebraic curves with fixed degeneracies. *Izv. Akad. Nauk SSSR Ser. Mat.*, 35:1269–1293, 1971.

[BGS94] J.-B. Bost, H. Gillet, and C. Soulé. Heights of projective varieties and positive green forms. *J. Amer. Math. Soc.*, 7:903–1027, 1994.

[BKP02] F. Bogomolov, L. Katzarkov, and T. Pantev. Hyperelliptic Szpiro inequality. *J. Differential Geom.*, 61(1):51–80, 2002.

[BM72] B. J. Birch and J. R. Merriman. Finiteness theorems for binary forms with given discriminant. *Proc. London Math. Soc. (3)*, 24:385–394, 1972.

[BS96] A. Brumer and J. H. Silverman. The number of elliptic curves over **Q** with conductor N. *Manuscripta Math.*, 91(1):95–102, 1996.

[Cap02] L. Caporaso. On certain uniformity properties of curves over function fields. *Compositio Math.*, 130(1):1–19, 2002.

[EG91] J.-H. Evertse and K. Győry. Effective finiteness results for binary forms with given discriminant. *Compositio Math.*, 79(2):169–204, 1991.

[Fal83] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[Gro71] A. Grothendieck. *Revêtements étales et groupe fondamental* (SGA 1), volume 224 of *Springer Lecture Notes in Math. Series*. Springer-Verlag, Berlin 1971.

[Har77] R. Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977.

[Hei04] G. Heier. Uniformly effective Shafarevich conjecture on families of hyperbolic curves over a curve with prescribed degeneracy locus. *J. Math. Pures Appl. (9)*, 83(7):845–867, 2004.

[HS88] M. Hindry and J. H. Silverman. The canonical height and integral points on elliptic curves. *Invent. Math.*, 93(2):419–450, 1988.

[Mas84] R. C. Mason. *Diophantine equations over function fields*, volume 96 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1984.

[Mor79] S. Mori. Projective manifolds with ample tangent bundles. *Ann. of Math. (2)*, 110(3):593–606, 1979.

[Par68] A. N. Paršin. Algebraic curves over function fields. I. *Izv. Akad. Nauk SSSR Ser. Mat.*, 32:1191–1219, 1968.

[PS00] J. Pesenti and L. Szpiro. Inégalité du discriminant pour les pinceaux elliptiques à réductions quelconques. *Compositio Math.*, 120(1):83–117, 2000.

[Ser98] J.-P. Serre. *Abelian l-adic representations and elliptic curves*, volume 7 of *Research Notes in Mathematics*. A K Peters Ltd., Wellesley, MA, 1998. With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original.

[Sha63] I. R. Shafarevich. Algebraic number fields. In *Proc. Internat. Congr. Mathematicians (Stockholm, 1962)*, pages 163–176. Inst. Mittag-Leffler, Djursholm, 1963.

[Sil86] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[Szp79] L. Szpiro. Sur le théorème de rigidité de Parsin et Arakelov. In *Journées de Géométrie Algébrique de Rennes (Rennes, 1978), Vol. II*, volume 64 of *Astérisque*, pages 169–202. Soc. Math. France, Paris, 1979.

[Szp90] L. Szpiro. Discriminant et conducteur des courbes elliptiques. *Astérisque*, (183):7–18, 1990. Séminaire sur les Pinceaux de Courbes Elliptiques (Paris, 1988).

[Tag92] Y. Taguchi. Ramifications arising from Drinfel′d modules. In *The arithmetic of function fields (Columbus, OH, 1991)*, volume 2 of *Ohio State Univ. Math. Res. Inst. Publ.*, pages 171–187. de Gruyter, Berlin, 1992.

Lucien Szpiro and Thomas J.Tucker
Department of Mathematics City University of New York
E-mail: lszpiro@gc.cuny.edu
E-mail: ttucker@gc.cuny.edu