The handle http://hdl.handle.net/1887/20949 holds various files of this Leiden University dissertation.

**Author:** Javan Peykar, Ariyan  
**Title:** Arakelov invariants of Belyi curves  
**Issue Date:** 2013-06-11
In [23] Faltings proved the Shafarevich conjecture. That is, for a number field $K$, finite set $S$ of finite places of $K$, and integer $g \geq 2$, there are only finitely many $K$-isomorphism classes of curves over $K$ of genus $g$ with good reduction outside $S$. This is a qualitative statement, i.e., this statement does not give an explicit bound on the “complexity” of such a curve.

In this chapter we are interested in quantitative versions of the Shafarevich conjecture, e.g., the effective Shafarevich conjecture and Szpiro’s small points conjecture.

Our main result (joint with Rafael von Känel) is a proof of Szpiro’s small points conjecture for cyclic covers of the projective line of prime degree; see Theorem 4.4.1. To explain a part of our proof, we have also found it fit to discuss the proof of the effective Shafarevich conjecture for cyclic covers of the projective line of prime degree due to de Jong-Rémond and von Känel in Section 4.2.1. We finish this chapter with a discussion of a result of Levin which gives some hope for obtaining applications of the results in this chapter to long-standing conjectures in Diophantine geometry.

The results of this chapter form only a small part of our article with von Känel [31]. In loc. cit we also discuss the optimality of the constant, and we give better bounds than those presented here.

4.1. The effective Shafarevich conjecture

In this section we follow Rémond ([51]). Firstly, we recall Faltings’ finiteness theorem for abelian varieties.

**Theorem 4.1.1. (Faltings [23])** Let $K$ be a number field, $S$ a finite set of finite places of $K$ and $g$ an integer. Then there are only finitely many $K$-isomorphism classes of $g$-dimensional abelian varieties over $K$ with good reduction outside $S$. 

57
An application of Torelli’s theorem allows one to deduce the following finiteness theorem for curves from Theorem 4.1.1.

**Theorem 4.1.2.** Let $K$ be a number field, $S$ a finite set of finite places of $K$ and $g \geq 2$ an integer. Then there are only finitely many $K$-isomorphism classes of genus $g$ curves over $K$ with good reduction outside $S$.

We are interested in an effective version of Faltings’ finiteness theorem for curves. Let us consider the “effective Shafarevich” conjecture as stated in [51].

**Conjecture 4.1.3. (Effective Shafarevich for curves)** Let $K$ be a number field, $S$ a finite set of finite places of $K$ and $g \geq 2$ an integer. Then, there exists an explicit real number $c$ (depending only on $K$, $S$ and $g$) such that, for a smooth projective geometrically connected curve $X$ of genus $g$ over $K$ with good reduction outside $S$,

$$h_{\text{Fal,stable}}(X) \leq c.$$ 

**Remark 4.1.4.** Removing the word “explicit” from Conjecture 4.1.3 gives a statement equivalent to Faltings’ finiteness theorem for curves (Theorem 4.1.2). In fact, it is clear that such a statement follows from Faltings’ finiteness theorem. Conversely, the above conjecture (with or without the word “explicit”) implies that, for any number field $K$, finite set of finite places $S$ of $K$ and integer $g \geq 2$, there are only finitely many $K$-isomorphism classes of genus $g$ curves over $K$ with semi-stable reduction over $O_K$ and good reduction outside $S$. Here we use the “Northcott property” of the Faltings height (Theorem 1.6.5). To obtain Theorem 4.1.2, we argue as follows. For a curve $X$ over $K$ of genus $g \geq 2$ with good reduction outside $S$, there exists a field extension $L/K$ of bounded degree in $g$ and ramified only over $S$ such that $X_L$ has semi-stable reduction over $O_L$. Thus, by the Hermite-Minkowski theorem, it suffices to show that, for a finite Galois extension $L/K$ and smooth projective geometrically connected curve $X$ of genus at least two over $K$, there are only finitely many curves $X'$ over $K$ such that $X'_L$ is isomorphic to $X_L$. Note that the set of such $X'$ is in one-to-one correspondence with $H^1(\text{Gal}(L/K), \text{Aut}_K(X_K))$. Since $\text{Aut}_K(X_K)$ is finite, the cohomology set

$$H^1(\text{Gal}(L/K), \text{Aut}_K(X_K))$$

is finite. This proves Theorem 4.1.2.

### 4.2. The effective Shafarevich conjecture for cyclic covers

In this section we follow de Jong-Rémond ([17]).
For a number field $K$, let $\Delta = |\Delta_{K/Q}|$ be its absolute discriminant. For a finite set of finite places $S$ of a number field $K$, let

$$\Delta_S = \Delta \exp \left( \sum_{p \in S} \log N_{K/Q}(p) + [K : Q] \log 4 \right)^2.$$  

The following theorem is the main result of *loc. cit.* and proves Conjecture 4.1.3 for cyclic covers of the projective line of prime degree.

**Theorem 4.2.1. (de Jong-Rémond)** Let $K$ be a number field, $S$ a finite set of finite places of $K$ and $g$ an integer. Let $X$ be a smooth projective geometrically connected curve of genus $g$ over $K$ with good reduction outside $S$. Suppose that there exists a finite morphism $X \to \mathbb{P}^1_K$ such that $X_K \to \mathbb{P}^1_K$ is a cyclic cover of prime degree for some (hence any) algebraic closure $K \to \overline{K}$. Then

$$h_{\text{Fal,stable}}(X) \leq 2^{22g^2} \Delta_S^{215g^5}.$$  

In this section we aim at explaining the main ingredients of the proof of Theorem 4.2.1. The proof of de Jong-Rémond is obtained in five steps which we will give below. We will give the proof of Theorem 4.2.1 at the end of this section. The first step is to replace the Faltings height of $X$ by the theta height $h_\theta(X)$ of the Jacobian of $X$ with respect to its principal polarization induced by the theta divisor; see [50, Definition 2.6] or [51, Section 4.a].

**Lemma 4.2.2. (Pazuki)** Let $g \geq 1$ be an integer. Then, for a smooth projective geometrically connected genus $g$ curve $X$ over $\overline{Q}$, the inequality

$$h_{\text{Fal}}(X) \leq 2h_\theta(X) + 2^{5g+1} (2 + \max(1, h_\theta(X)))$$  

holds.

**Proof.** This follows from [50, Corollary 1.3]. (Note that we are working with $r = 4$ here in the notation of *loc. cit.*.) \qed

The second step consists of invoking an explicit upper bound for the theta height due to Rémond ([52]). Let $K$ be a number field, $K \to \overline{K}$ an algebraic closure of $K$, $S$ a finite set of finite places and $g$ an integer. Let $X$ be a smooth projective geometrically connected curve over $K$. Let $X \to \mathbb{P}^1_K$ be a finite morphism such that $X_K \to \mathbb{P}^1_K$ is a cyclic cover of prime degree. Let $H$ be the height of the finite set of cross-ratios associated to the branch points of $X_K \to \mathbb{P}^1_K$; see Section 3.3 for the definition of the height of a finite set of algebraic numbers and [17] for the definition of the set of cross-ratios.
Lemma 4.2.3. We have

$$h_\theta(X_{\overline{K}}) \leq 2^{3360 \cdot g^{38g}} H.$$ 

Proof. The computation can be found in [17, p. 1141-1142].

Thus, to prove Theorem 4.2.1, it suffices to bound $H$ explicitly in terms of $K$, $S$ and $g$. The idea is to show that every cross-ratio satisfies a well-studied Diophantine equation.

Lemma 4.2.4. (de Jong-Rémond) Let $b$ be a cross-ratio of the branch locus of $X_{\overline{K}} \to \mathbb{P}^1_{\overline{K}}$. Then, if $L = K(b)$ and $S' = S_L$, we have that $b$ and $1 - b$ are $S_L$-units in $L$.

Proof. By applying [17, Proposition 2.1] to $b$, $1 - b$, $b - 1$ and $(1 - b)^{-1}$, it follows that $b$, $1 - b$, $b^{-1}$ and $(1 - b)^{-1}$ are $S_L$-integers in $L$. This implies that $b$ and $1 - b$ are $S_L$-units in $L$.

The fourth step consists of applying the well-established theory of logarithmic forms ([4]).

Lemma 4.2.5. (Baker-Győry-Yu) Let $L$ be a number field and $S_L$ a finite set of finite places of $L$. Let $d$, $R$ and $P$ be the degree of $L$ over $\mathbb{Q}$, the regulator of $L$ over $\mathbb{Q}$ and the maximum of $|N_{L/\mathbb{Q}}(p)|$ as $p$ runs over $S_L$. Let $s = \#S_L + d$. Then, if $b$ and $1 - b$ are $S_L$-units in $L$, the inequality

$$h(b) \leq 2^{15(16sd)^2 + 4} PR \left(1 + \frac{\max(1, \log R)}{\max(1, \log P)}\right)$$

holds.

Proof. This is an application of the main result of [28] to $b$. In fact, the pair $(b, 1 - b)$ is a solution of the equation $x + y = 1$ with $(x, y) \in O_{S_L}^X \times O_{S_L}^X$. (See the proof of [15, Lemme 3.1] for details.)

The preceding two lemmata can be combined into giving an explicit upper bound for $H$.

Lemma 4.2.6. We have

$$H \leq \Delta_S^{(8g)^5}.$$ 

Proof. Every cross-ratio is an $S_L$-unit, and by Lemma 4.2.5, the height of such an algebraic number can explicitly bounded in terms of the degree $[L : \mathbb{Q}]$, the regulator of $L$ over $\mathbb{Q}$ and the maximum of $|N_{L/\mathbb{Q}}(p)|$ as $p$ runs over $S_L$. This explicit bound implies an explicit upper bound in terms of $K$, $S$ and $g$. This computation requires some results from algebraic number theory; see [17, p. 1139-1140] for the proof.

Proof of Theorem 4.2.1. By Lemma 4.2.2, it suffices to bound the theta height $h_\theta(X)$ explicitly (in terms of $K$, $S$ and $g$). By Lemma 4.2.3, it suffices to bound $H$ explicitly. This is precisely the content of Lemma 4.2.6.
4.3. Szpiro’s small points conjecture

We consider Szpiro’s small points conjecture; see [60], [61], [63], [64], [59].

**Conjecture 4.3.1. (Szpiro’s small points conjecture)** Let $K$ be a number field, $K \to \overline{K}$ an algebraic closure of $K$, $S$ a finite set of finite places of $K$ and $g \geq 2$ an integer. Then, there exists an explicit real number $c$ such that, for a smooth projective geometrically connected curve $X$ of genus $g$ over $K$ with good reduction outside $S$, there is a point $a$ in $X(\overline{K})$ with

$$h(a) \leq c.$$ 

A point $a$ satisfying the conclusion of Conjecture 4.3.1 is called a “small point”. Roughly speaking, the following theorem shows that the existence of a small point on $X$ is equivalent to an explicit upper bound for $e(X)$.

**Theorem 4.3.2.** Let $X$ be a smooth projective connected curve over $\mathbb{Q}$ of genus $g \geq 2$. Then, for all $a$ in $X(\overline{\mathbb{Q}})$, the inequality

$$e(X) \leq 4g(g-1)h(a)$$

holds. Moreover, for any $\epsilon > 0$, there exists a in $X(\overline{\mathbb{Q}})$ such that

$$h(a) \leq \frac{e(X)}{4(g-1)} + \epsilon.$$

**Proof.** The first statement is due to Faltings; see Theorem 2.2.1. The second statement follows from Faltings’ Riemann-Roch theorem (Section 1.2) and is due to Moret-Bailly; see the proof of [48, Proposition 3.4].

**Remark 4.3.3.** Removing the word “explicit” from Conjecture 4.3.1 gives a statement equivalent to Faltings’ finiteness theorem for curves (Theorem 4.1.2). In fact, the Arakelov invariant $e(X)$ satisfies the following Northcott property. Let $C$ be a real number, and let $g \geq 2$ be an integer. For a number field $K$, there are only finitely many $K$-isomorphism classes of smooth projective connected curves $X$ over $K$ of genus $g$ with semi-stable reduction over $O_K$ and $e_{\text{stable}}(X) \leq C$. Thus, since $e(X) \leq 4g(g-1)h(b)$ for any $b$ in $X(\overline{K})$, to deduce Faltings’ finiteness theorem for curves from Conjecture 4.3.1, we can argue as in Remark 4.1.4.

4.4. Szpiro’s small points conjecture for cyclic covers

The following theorem proves Szpiro’s small points conjecture (Conjecture 4.3.1) for cyclic covers of the projective line of prime degree.
Theorem 4.4.1. ([31, Theorem 3.1]) Let $K$ be a number field of degree $d$ over $\mathbb{Q}$, $S$ a finite set of finite places of $K$ and $g$ an integer. Let $X$ be a smooth projective geometrically connected curve of genus $g$ over $K$ with good reduction outside $S$. Suppose that there exists a finite morphism $\pi : X \to \mathbb{P}^1_K$ such that $\pi|_{\mathbb{P}^1_K} : X_{\mathbb{P}^1_K} \to \mathbb{P}^1_{\overline{K}}$ is a cyclic cover of prime degree for some algebraic closure $K \to \overline{K}$. Then there exists $a$ in $X(\mathbb{Q})$ such that

$$h(a) \leq \frac{10^7}{g} \left(4d!(2g+2)\Delta_S^{(8g)^5} \right)^{45(d!(2g+2))^32d^{(2g+1)-2}(d!(2g+1))!} (2g+1)^5.$$  

Proof. We may and do assume that $0$, $1$, and $\infty$ are branch points of the finite morphism $\pi : X \to \mathbb{P}^1_K$. Now, by Corollary 2.5.3, there exists $a$ in $X(\mathbb{Q})$ such that

$$h(a) \leq 10^7 \deg_B(X)^5.$$

To bound $\deg_B(X)$, we argue as in the proof Theorem 3.3.3. In fact, by Khadjavi’s effective version of Belyi’s theorem ([35, Theorem 1.1.c]), the inequality

$$\deg_B(X) \leq (4NH_B)^{9N^32^N-2N!} \deg \pi$$

holds, where $B$ is the branch locus of $\pi_{\overline{K}}$, $H_B$ is the height of the set $B$, and $N$ is the number of elements in the orbit of $B$ under the action of $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Let $H$ be the height of the finite set of cross-ratios associated to $B$. Note that

$$N \leq [K : \mathbb{Q}]! \#B, \quad \#B \leq 2g + 2, \quad \deg \pi \leq 2g + 1, \quad H_B \leq H,$$

where the first inequality is clear, the second inequality and third inequality follow from Riemann-Hurwitz, and the last inequality follows from the fact that every algebraic number $\alpha$ different from $0$ and $1$ equals the cross ratio of $0$, $1$, $\infty$ and $\alpha$. By Lemma 4.2.6, $H \leq \Delta_S^{(8g)^5}$, where $\Delta_S$ is as in Section 4.2.1. Putting these inequalities together implies the theorem. 

Remark 4.4.2. The above proof of Theorem 4.4.1 gives a very large upper bound on $h(a)$. We actually give a much better upper bound for $h(a)$ in our article [31]. In fact, we prove that

$$h(a) \leq \exp \left( \mu^{d}\mu (N_S \Delta)^{\mu} \right),$$

where we let $d = [K : \mathbb{Q}]$, $\Delta$ the absolute discriminant of $K$ over $\mathbb{Q}$, $N_S = \prod_{v \in S} N_v$, and $\mu = d(5g)^5$. In loc. cit. we also study the optimality of the upper bound, we study points with small Néron-Tate height, and we improve its value under further restrictive assumptions on $X$.

4.5. Zhang’s lower bound for $e(X)$

In this section we prove a slightly stronger version of Szpiro’s small points conjecture for cyclic covers of prime degree of the projective line.
Theorem 4.5.1. ([31, Theorem 3.1]) Let $K$ be a number field, $S$ a finite set of finite places of $K$ and $g$ an integer. Let $X$ be a smooth projective geometrically connected curve of genus $g$ over $K$ with good reduction outside $S$. Suppose that there exists a finite morphism $X \to \mathbb{P}^1_K$ such that $X_K \to \mathbb{P}^1_K$ is a cyclic cover of prime degree. Then there are infinitely many $a$ in $X(K)$ with
\[ h(a) \leq 2 \cdot 10^7 \left( 4d!(2g + 2)\Delta_S^{(8g)^5} \right)^{45(d!(2g+2))^{2d!(2g+1)} (2g+1)^5}. \]

To prove Theorem 4.5.1, we will apply the following result of Zhang.

Theorem 4.5.2. There are infinitely many points $a$ in $X(\mathbb{Q})$ such that
\[ h(a) \leq \frac{e(X)}{2(g - 1)}. \]

Proof. This follows from [69, Theorem 6.3]. \qed

Proof of Theorem 4.5.1. Theorem 4.5.1 is a consequence of Theorem 4.4.1 and the above result of Zhang. In fact, by Zhang’s result and Faltings’ inequality ([24, Theorem 5]), there are infinitely many points $a$ in $X(\mathbb{Q})$ such that, for all $b$ in $X(\mathbb{Q})$, the inequality
\[ h(a) \leq 4g(g-1)e(X) \leq 2gh(b) \]
holds. \qed

4.6. Diophantine applications of the effective Shafarevich conjecture (after Levin)

In this section we follow Levin ([39]). Faltings proved the Mordell conjecture via the Shafarevich conjecture. In fact, in [49] Parshin famously proved that the Shafarevich conjecture for curves (Theorem 4.1.2) implies Mordell’s conjecture.

Theorem 4.6.1. (Faltings) For a number field $K$ and smooth projective geometrically connected curve $X$ over $K$ of genus at least two, the set $X(K)$ of $K$-rational points on $X$ is finite.

Rémond proved that the effective Shafarevich conjecture (Conjecture 4.1.3) implies an “effective version of the Mordell conjecture”. His proof relies on Kodaira’s construction. For the sake of brevity, we only state a consequence of Rémond’s result. We refer the reader to [51, Théorème 5.3] for a more precise statement.

Theorem 4.6.2. ([51, Théorème 5.3]) Assume Conjecture 4.1.3. Let $K$ be a number field and $X$ a smooth projective geometrically connected curve over $K$ of genus $g \geq 2$. Then there exists an explicit real number $c$ such that, for all $a \in X(K)$, we have
\[ h(a) \leq c. \]
Remark 4.6.3. An explicit expression for $c$ is given in [51, Théorème 5.3].

It is natural to ask whether “weak versions” of the effective Shafarevich conjecture have Diophantine applications. For instance, one could ask whether Theorem 4.2.1 implies “a weak effective version of the Mordell conjecture”. Currently, no such implication is known. Nevertheless, it seems reasonable to suspect that some “weak version” of the effective Shafarevich conjecture implies some version of Siegel’s theorem.

Theorem 4.6.4. (Siegel) Let $X$ be a smooth quasi-projective curve over a number field $K$, $S$ a finite set of places of $K$ containing the archimedean places, $O_{K,S}$ the ring of $S$-integers, and $f \in K(X)$. If $X$ is a rational curve, then we assume further that $f$ has at least three distinct poles. Then the set of $S$-integral points of $X$ with respect to $f$,

$$X(f, K, S) = \{ a \in X(K) \mid f(a) \in O_{K,S} \}$$

is finite.

In general, there is no quantitative version of Siegel’s theorem known, i.e., there is no known algorithm for explicitly computing the set $X(f, K, S)$. Of course, in some special cases there are known techniques for effectively computing $X(f, K, S)$; see [39, Section 1]. This ineffectivity arises in the classical proofs of Siegel’s theorem from the use of Roth’s theorem.

Theorem 4.6.5. (Roth [53]) Let $\theta$ be a real algebraic number of degree $d \geq 2$. For all $\epsilon > 0$, there are only finitely many rational numbers $p/q$, with $p, q \in \mathbb{Z}$ coprime, such that

$$|\theta - \frac{p}{q}| \leq \frac{1}{|q|^{2+\epsilon}}.$$

Currently, Roth’s theorem remains ineffective. That is, if $\theta$ is a real algebraic number of degree $d \geq 2$, there is no known algorithm (in general!) for explicitly computing the set of rational numbers $p/q$ such that $|\theta - p/q| \leq \frac{1}{|q|^{2+\epsilon}}$.

An interesting result of Levin shows that an effective version of the Shafarevich conjecture for hyperelliptic Jacobians has Diophantine applications. In fact, Levin proves that an effective Shafarevich conjecture for hyperelliptic Jacobians implies an effective version of Siegel’s theorem for integral points on hyperelliptic curves. We interpret his result as to give some hope for obtaining applications of the results in this chapter to effective Diophantine conjectures such as Siegel’s theorem.

Theorem 4.6.6. ([39, Theorem 3]) Let $g \geq 2$ be an integer. Suppose that, for any number field $K$ and finite set of finite places $S$ of $K$ the set of $K$-isomorphism classes of hyperelliptic curves $C$ over $K$ of genus $g$ with good reduction outside $S$ is effectively computable (e.g., an explicit
hyperelliptic Weierstrass equation for each such curve is given). Then for any number field $K$, any finite set of places $S$ of $K$, any hyperelliptic curve $X$ over $K$ of genus $g$, and any rational function $f$ in $K(X)$, the set of $S$-integral points with respect to $f$,

$$X(f, K, S) = \{ a \in X(K) \mid f(a) \in O_{K,S} \}$$

is effectively computable.

Levin’s proof uses a slight variation on Parshin’s proof of the well-known implication mentioned before “Shafarevich implies Mordell”. It remains to be seen whether one can use Parshin-type constructions to obtain applications of the results in this chapter to effective Diophantine conjectures.