

# On some conjectures on the Mordell-Weil and the Tate-Shafarevich groups of an abelian variety

Andrea Surroca Ortiz (ETH Zurich)\*

January 7, 2008

**Abstract.** We consider an abelian variety defined over a number field. We give conditional bounds for the order of its Tate-Shafarevich group, as well as bounds for the Néron-Tate height of generators of its Mordell-Weil group. The bounds are implied by strong but nowadays classical conjectures, such as the Birch and Swinnerton-Dyer conjecture and the functional equation of the  $L$ -series. In particular, we generalise a result by D. Goldfeld and L. Szpiro on the order of the Tate-Shafarevich group. The method is an extension of the algorithm proposed by Yu. Manin for finding a basis for the non-torsion rational points of an elliptic curve defined over the rationals.

2000 Mathematics Subject Classification: 11G10, 11G40, 14G05, 11G50.

## 1 Introduction

The Mordell-Weil theorem says that the group of rational points on an abelian variety  $A/K$  defined over a number field is finitely generated:  $A(K) \simeq A(K)_{tors} \times \mathbb{Z}^{rk(A(K))}$ . Nowadays, even in the case of an elliptic curve, there is no way, in general, to compute the torsion part, the rank or a set of generators of this group. For some applications, it would be sufficient to bound the size of them. There exist bounds for the cardinality of the torsion subgroup, e.g., in the case of elliptic curves, [Mer96]. The proof of the Weak Mordell-Weil theorem gives an upper bound for the rank; such an explicit bound is obtained in [OT89]. As for the generators, Yu. Manin [Man71] proposed an algorithm for finding a basis for the non-torsion rational points of an elliptic curve. From Manin's algorithm one could deduce a bound for the Néron-Tate height of the generators. The approach relies on the conjecture of B. J. Birch and H. P. F. Swinnerton-Dyer [BSD65] (BSD-conjecture for short) and on the hypothesis that the  $L$ -series of the elliptic curve satisfies a functional equation. S. Lang modified the heuristic approach of Yu. Manin and proposed the following conjecture [Lan83, Conjecture 3]: *Let  $E$  be an elliptic curve defined over  $\mathbb{Q}$ . Denote  $\mathcal{F}_{E/\mathbb{Q}}$*

---

\*Supported by a Marie Curie Fellowship of the European Community

the conductor,  $H_{\text{Falt}}(E/\mathbb{Q})$  the exponential Faltings height and  $\text{rk}(E(\mathbb{Q}))$  the Mordell-Weil rank of  $E/\mathbb{Q}$ . We can find a basis  $\{P_1, \dots, P_r\}$  of the free part of  $E(\mathbb{Q})$  satisfying

$$\max_{1 \leq i \leq r} \hat{h}(P_i) \ll c^{\text{rk}(E(\mathbb{Q}))^2} \cdot \mathcal{F}_{E/\mathbb{Q}}^{\epsilon(\mathcal{F}_{E/\mathbb{Q}})} \cdot (\log \mathcal{F}_{E/\mathbb{Q}})^{\text{rk}(E(\mathbb{Q}))} \cdot H_{\text{Falt}}(E/\mathbb{Q}), \quad (1)$$

where  $c$  is an absolute constant and  $\epsilon$  is a function which does not depend on the rank and  $\epsilon(\mathcal{F})$  tends to 0 as  $\mathcal{F}$  tends to infinity.

On the other hand, from the proof of the Weak Mordell-Weil theorem we know that, for all  $n \geq 1$ , the  $n$ -torsion part of the Tate-Shafarevich group is finite. It is conjectured that the whole Tate-Shafarevich group is finite; the conjecture is known for certain elliptic curves with complex multiplication ([Rub87]) and certain modular elliptic curves ([Kol88]). D. Goldfeld and L. Szpiro [GS95] suggested the following bound for the order of the Tate-Shafarevich group  $\text{III}(E/K)$  of an elliptic curve, in terms of the conductor. *Let  $E$  be an elliptic curve defined over a field  $K$ , which can be a number field or a function field. Then, for every  $\epsilon > 0$ ,*

$$|\text{III}(E/K)| = O(N_{K/\mathbb{Q}}(\mathcal{F}_{E/K})^{1/2+\epsilon}), \quad (2)$$

where the implicit constant in the  $O$  depends on  $\epsilon$ ,  $K$  and  $\text{rk}(E(K))$ . In the same article they proved that this conjecture holds for elliptic curves defined over function fields provided the Tate-Shafarevich group of the function field is finite. D. Goldfeld and D. Lieman [GL96] proved that, for a CM elliptic curve defined over  $\mathbb{Q}$  with Mordell-Weil rank 0, we have  $|\text{III}(E/\mathbb{Q})| < k(\epsilon) \mathcal{F}_{E/\mathbb{Q}}^{\delta+\epsilon}$ , with  $\delta = \frac{59}{120}$  if  $j \neq 0, 1728$ ,  $\delta = \frac{37}{60}$  if  $j = 0$  and  $\delta = \frac{79}{120}$  if  $j = 1728$ , where  $k(\epsilon)$  depends only on  $\epsilon$  and is effectively computable. It is also proved in [GS95, Theorem 1] that, if the curve  $E$  is defined over  $\mathbb{Q}$  and satisfies the BSD-conjecture and Szpiro's conjecture (which bounds the discriminant in terms of the conductor), then  $|\text{III}(E/\mathbb{Q})| \ll \mathcal{F}_{E/\mathbb{Q}}^{7/4+\epsilon(\mathcal{F}_{E/\mathbb{Q}})}$ , where  $\epsilon(\mathcal{F})$  tends to 0 when  $\mathcal{F}$  tends to infinity.

In this article, we consider an abelian variety  $A$  defined over a number field  $K$ . We are interested in giving, under the assumption of the BSD-conjecture, bounds for its regulator and the order of its Tate-Shafarevich group, as well as bounds for the Néron-Tate height of the generators of its Mordell-Weil group. The bounds are given in terms of more tractable objects associated to the variety and the number field. Precisely, our bounds depends on the dimension  $g$  of  $A$ , the absolute value  $\mathcal{F} = N_{K/\mathbb{Q}} \mathcal{F}_{A/K}$  of the norm of the conductor, the Faltings' height  $h = h_{\text{Falt}}(A/K)$ , the Mordell-Weil rank  $r = \text{rk}(A(K))$ , the degree  $[K : \mathbb{Q}]$  and the absolute value  $D_K$  of the discriminant of  $K$ . Moreover the dependence is explicit in all the parameters, with the exception of  $g$  and  $[K : \mathbb{Q}]$ . We denote by  $H = \exp\{h\}$  the exponential height.

On one hand we give a conditional upper bound for the Néron-Tate height of the elements of a (particular) basis of the free part of the Mordell-Weil group  $A(K)$ .

**Theorem 1.1** *Let  $A$  be an abelian variety defined over a number field  $K$ . Suppose that the  $L$ -series of  $A/K$  satisfies a functional equation (Conjecture 2.1) and the BSD-conjecture (Conjecture 3.1). Then we can choose a system  $\{P_1, \dots, P_r\}$  of generators for the free part of the Mordell-Weil group  $A(K)$  such that  $\hat{h}(P_1) \leq \dots \leq \hat{h}(P_r)$  and*

$$\hat{h}(P_r) \leq c_{[K:\mathbb{Q}],g} \cdot (r!)^4 \cdot 2^r \cdot (c_{[K:\mathbb{Q}]})^{1-r} \cdot D_K^g \cdot \mathcal{F}^{\frac{1}{4}} \cdot (\log \mathcal{F})^{4g[K:\mathbb{Q}]} \cdot (\log(\mathcal{F} \cdot D_K^{2g}))^{2g[K:\mathbb{Q}]}.$$

$$\cdot H^{[K:\mathbb{Q}]} \cdot h^{(2g+1)(r-1)+g[K:\mathbb{Q}]},$$

where  $c_{[K:\mathbb{Q}],g}$  depends at most on the dimension  $g$  and the degree  $[K:\mathbb{Q}]$ , and  $c_{[K:\mathbb{Q}]}$  depends at most on  $[K:\mathbb{Q}]$ .

Notice that Conjecture 2.1 is known for abelian varieties with complex multiplication ([ST61]) and some modular abelian varieties ([Shi94]). As for Conjecture 3.1, the results of [CW77], [GZ86], [Rub87] and [Kol88] provide evidence for its truth. On the other hand, we extend Theorem 1 of [GS95] to arbitrary abelian varieties defined over number fields. This gives a conditional upper bound for  $|\text{III}(A/K)|$ . When the dimension equals 1 and the number field is  $\mathbb{Q}$ , our bound improves Theorem 1 of [GS95].

**Theorem 1.2** *Let  $A$  be an abelian variety defined over a number field  $K$ . Suppose that the  $L$ -series of  $A/K$  satisfies a functional equation (Conjecture 2.1) and the BSD-conjecture (Conjecture 3.1). Suppose that  $A/K$  satisfies the Szpiro's Conjecture (Conjecture 6.1). Then, for every  $\epsilon > 0$ ,*

$$|\text{III}(A/K)| \leq \delta_{[K:\mathbb{Q}],g}(r) \cdot D_K^{g+(g^2+\epsilon)[K:\mathbb{Q}]} \cdot \mathcal{F}^{\frac{1}{4}+(\frac{g}{2}+\epsilon)[K:\mathbb{Q}]} \cdot (\log \mathcal{F})^{4g[K:\mathbb{Q}]} \cdot (\log(\mathcal{F} \cdot D_K^{2g}))^{2g[K:\mathbb{Q}]} \cdot \left( \left( \frac{g}{2} + \epsilon \right) \log \mathcal{F} + (g^2 + \epsilon) \log D_K + c_{\epsilon,[K:\mathbb{Q}]} \right)^{r(2g+1)+g[K:\mathbb{Q}]},$$

where  $\delta_{[K:\mathbb{Q}],g}(r) = c_{[K:\mathbb{Q}],g} \cdot (r!)^4 \cdot 2^r \cdot (c_{[K:\mathbb{Q}]})^r \cdot e^{[K:\mathbb{Q}]c_{\epsilon,[K:\mathbb{Q}]}}$ ,  $c_{[K:\mathbb{Q}],g}$  depends only on  $g$  and  $[K:\mathbb{Q}]$ ,  $c_{[K:\mathbb{Q}]}$  depends only on  $[K:\mathbb{Q}]$  and  $c_{\epsilon,[K:\mathbb{Q}]}$  depends at most on  $\epsilon$  and  $[K:\mathbb{Q}]$ .

Recently, M. Hindry treated this topic for abelian varieties in [Hin05]. He puts the accent on the analogy with the classical Brauer-Siegel formula for number fields. He formulates a conjecture comparing the product of the Tate-Shafarevich group and the regulator, with the height of the variety: *For all  $\epsilon > 0$ ,  $H_{\text{Falt}}(A/K)^{(1-\epsilon)} \ll |\text{III}(A/K)| \cdot \text{Reg}(A/K) \ll H_{\text{Falt}}(A/K)^{(1+\epsilon)}$ , where the implicit constants depend on  $K, g, \epsilon$  and  $\text{rk}(A(K))$ .* In [Man71], [Lan83] and [GS95] the argument is developed when the dimension is 1 and the number field is  $\mathbb{Q}$ , while in [Hin05] the dependence of the bounds on the number field is not always made explicit. As pointed out in our joint work with V. Bosser [BS07], this dependence could play an important rôle. For example, the discriminant of the number field appears in the rank of the variety. In fact, the latter can be bounded in terms of the logarithm of the discriminant of  $K$  ([OT89]). Therefore, we consider here an arbitrary number field and make explicit the dependence on the number field. Furthermore, contrary to [Lan83] and [Hin05] the bounds given here are not conjectured, but implied, by strong but nowadays classical conjectures.

The method is an extension of the one proposed by Yu. Manin, based on the BSD-conjecture. The BSD-conjecture predicts the behavior of the  $L$ -series of the abelian variety  $A$  at the center of symmetry, that is 1. In fact, it states that the order of vanishing of  $L(A/K, s)$  at  $s = 1$  equals the Mordell-Weil rank of  $A/K$ . Furthermore, it gives a formula which relates the value of the leading coefficient of the Taylor expansion of  $L(A/K, s)$  at  $s = 1$  to the product of the Tate-Shafarevich group, the canonical regulator and some

other objects associated to the variety. The notations and the data concerning the abelian variety can be found in the next section. The core of our results are in section 3, where we bound the product of the Tate-Shafarevich group and the canonical regulator (Proposition 3.11). In order to do it, we bound each one of the other terms of the BSD-formula. To deal with the leading coefficient of the Taylor expansion of the  $L$ -series we use the functional equation (Lemma 3.2). We then relate the local periods to the Faltings' height of  $A/K$  (Lemma 3.5). We also give a bound for the torsion part of the Mordell-Weil group (Lemma 3.10). In section 4 we recall some classical results on the geometry of numbers. We quote, in section 5, some lower bounds for the Néron-Tate height of non-torsion points. In section 6 we deduce from the BSD-conjecture, the bounds for the highest Néron-Tate height of a set of generators of  $A(K)/A(K)_{tors}$  (Theorem 1.1) and an upper bound for the order of  $\text{III}(A(K))$  (Theorem 1.2).

In [BS07], we apply these results, for an elliptic curve, to show that, using the elliptic analogue of Baker's method, the BSD-conjecture for a single elliptic curve implies a result in the direction of the  $abc$ -conjecture over number fields.

## 2 Notations

Throughout the text we will consider an abelian variety  $A$  of dimension  $g$  defined over a number field  $K$ . We denote  $D_K$  the absolute value of the discriminant of the field  $K$ . To  $A$  one can associate different objects, as the conductor, the  $L$ -function, the Faltings height, the Tate-Shafarevich group and the regulator. For the notations we follow [Ser70], [LRS93], [Mil72], [Man71], [Gro82], [Tat95] and [CS86].

Let  $v$  be a finite place of  $K$  which corresponds to a prime ideal  $\mathfrak{p}$ . Denote  $K_v$  or  $K_{\mathfrak{p}}$  the completion of  $K$  at  $v$ . For any prime ideal  $\mathfrak{p}$  of  $K$ , fixing a prime in  $K_{\mathfrak{p}}$  above  $\mathfrak{p}$  gives us a decomposition group  $G_{\mathfrak{p}} = \text{Gal}(\overline{K}_{\mathfrak{p}}/K_{\mathfrak{p}})$  for  $\mathfrak{p}$  in  $\text{Gal}(\overline{K}/K)$ . Let  $I_{\mathfrak{p}}$  be the inertia subgroup of  $G_{\mathfrak{p}}$ , inducing the identity on the residue field  $k(\mathfrak{p})$ . Let  $\pi_{\mathfrak{p}}$  denotes the Frobenius which generates the quotient  $G_{\mathfrak{p}}/I_{\mathfrak{p}}$ . (Up to conjugation,  $G_{\mathfrak{p}}$ ,  $I_{\mathfrak{p}}$  and  $\pi_{\mathfrak{p}}$  depend only on  $\mathfrak{p}$ .) Let  $l$  be any prime,  $l \neq \text{char}(k(\mathfrak{p}))$ . Denotes  $A[N]$  the  $N$ -torsion of  $A$ , for an integer  $N$ ,  $T_l(A) = \varprojlim A[l^n]$  the  $l$ -adic Tate module, and  $V_l(A/K) = T_l(A) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$  the  $\mathbb{Q}_l$ -vector space associated. Since  $\text{Gal}(\overline{K}/K)$  acts on  $V_l(A/K)$ , we have a  $l$ -adic representation  $\rho : \text{Gal}(\overline{K}/K) \rightarrow \text{GL}(V_l(A/K))$ .

The *conductor* of the abelian variety  $A/K$  is the integral ideal of  $K$  defined by

$$\mathcal{F}_{A/K} = \prod \mathfrak{p}^{f_{\mathfrak{p}}},$$

where the product runs over the prime ideals  $\mathfrak{p}$  of  $K$ , and  $f_{\mathfrak{p}}$  is a positive integer, called the *exponent of the conductor*, which we will define below. However, the exponent  $f_{\mathfrak{p}}$  is zero if and only if  $A$  has good reduction at  $\mathfrak{p}$ . So, this product is finite. Let  $p$  be the prime number lying below  $\mathfrak{p}$ . It is known that if  $p > 2g + 1$ , then  $f_{\mathfrak{p}} \leq 2g$ . Unconditionally, it is proven in [LRS93] that  $f_{\mathfrak{p}} \leq 12g^2 v_{K_{\mathfrak{p}}}(p)$  (see [BK94] for best possible upper bounds in all cases).

As in [Ser70], we will attach to  $\rho$  two positive integers  $\varepsilon_{\mathfrak{p}}(l)$  and  $\delta_{\mathfrak{p}}(l)$  which measures the ramification of  $\rho$ . For the notations we follow [LRS93]. Denotes  $V_l(A/K)^{I_{\mathfrak{p}}}$  the submodule of elements fixed by  $I_{\mathfrak{p}}$ . Define

$$\varepsilon_{\mathfrak{p}}(l) = \text{codim}_{\mathbb{Q}_l} V_l(A/K)^{I_{\mathfrak{p}}}.$$

Let  $L_{\mathfrak{p}} = K_{\mathfrak{p}}(A[l])$  be the field generated over  $K_{\mathfrak{p}}$  by the  $l$ -torsion points of  $A$ . Denotes  $v_{L_{\mathfrak{p}}}$  the normalized valuation on  $L_{\mathfrak{p}}$ . Let  $\pi_{L_{\mathfrak{p}}}$  be a uniformizer for  $L_{\mathfrak{p}}$ . Denotes  $G_i = \{\sigma \in \text{Gal}(L_{\mathfrak{p}}/K_{\mathfrak{p}}); v_{L_{\mathfrak{p}}}(\sigma\pi_{L_{\mathfrak{p}}} - \pi_{L_{\mathfrak{p}}}) \geq i + 1\}$  the  $i$ -th inertia group associated to  $L_{\mathfrak{p}}/K_{\mathfrak{p}}$  and  $g_i = |G_i|$  its order. Write  $g_0 = |\text{Gal}(L_{\mathfrak{p}}/K_{\mathfrak{p}})|$ . Define

$$\delta_{\mathfrak{p}}(l) = \sum_{i \geq 1} \frac{g_i}{g_0} \dim_{\mathbb{F}_l} \left( \frac{A[l]}{A[l]^{G_i}} \right).$$

It has being proved (see the references in [LRS93]) that  $\varepsilon_{\mathfrak{p}}(l)$  and  $\delta_{\mathfrak{p}}(l)$  are independents of  $l$  so we will denote them by  $\varepsilon_{\mathfrak{p}}$  and  $\delta_{\mathfrak{p}}$ . They are called the *tame* part and, respectively the *wild* part of the conductor. The exponent of the conductor is given by

$$f_{\mathfrak{p}} = \varepsilon_{\mathfrak{p}} + \delta_{\mathfrak{p}}.$$

Let us define the *L-series*, also called the  $\zeta$ -*function*, of the variety  $A$  (see [Ser70, Section 4]). Since the Frobenius is defined up to  $I_{\mathfrak{p}}$ , it makes sense to define a polynomial  $P_{A,\mathfrak{p}}(T) = \det(1 - (\rho(\pi_{\mathfrak{p}})|V_l(A/K)^{I_{\mathfrak{p}}})T)$ , where  $\pi_{\mathfrak{p}}$  is regarded as acting on the submodule  $V_l(A/K)^{I_{\mathfrak{p}}}$  of elements fixed by  $I_{\mathfrak{p}}$ . The polynomial  $P_{A,\mathfrak{p}}(T)$  has integral coefficients which are independent of  $l$  ([ST68, Theorem 3]). Define

$$L(A/K, s) = \prod_{v_{\mathfrak{p}}} P_{A,\mathfrak{p}}(N(v_{\mathfrak{p}})^{-s})^{-1}$$

where the product is taken over all non-archimedean places  $v_{\mathfrak{p}}$  of  $K$  and  $N(v_{\mathfrak{p}})$  is the norm of the prime ideal  $\mathfrak{p}$  associated to  $v_{\mathfrak{p}}$ . Define the *normalized L-function* by

$$\Lambda(A/K, s) = (N_{K/\mathbb{Q}}(\mathcal{F}_{A/K}) \cdot D_K^{2g})^{s/2} \cdot ((2\pi)^{-s} \cdot \Gamma(s))^{g[K:\mathbb{Q}]} \cdot L(A/K, s).$$

(Observe that the product  $\prod_{v \in M_K^{\infty}} \Gamma_v(s)$  of the  $\Gamma$ -factors equals  $((2\pi)^{-s} \cdot \Gamma(s))^{g[K:\mathbb{Q}]}$ . In fact,  $\Gamma_v(s)$  equals  $\Gamma_{\mathbb{C}}(s)^{2g}$  if  $v$  is complex and,  $\Gamma_{\mathbb{C}}(s)^g$  if  $v$  is real, where  $\Gamma_{\mathbb{C}}(s) = (2\pi)^{-s} \Gamma(s)$  (see [Ser70, section 3]).) The Euler product converges and gives an analytic function for all  $s$  satisfying  $\Re(s) > \frac{3}{2}$ . We have a classical generalisation of a conjecture of Hasse-Weil.

**Conjecture 2.1 (Hasse-Weil)** *Let  $A/K$  be an abelian variety defined over a number field. The L-series and the  $\Lambda$ -series of  $A/K$  have an analytic continuation to the entire complex plane and the  $\Lambda$ -series satisfies the functional equation*

$$\Lambda(A/K, 2 - s) = \varepsilon \Lambda(A/K, s), \text{ for some } \varepsilon = \pm 1.$$

This conjecture is true for abelian varieties with complex multiplication ([ST61]), in some special cases, this conjecture is also true for modular abelian varieties ([Shi94]) and it is true for elliptic curves over  $\mathbb{Q}$  ([Wil95] and [BCDT01]).

Denote  $\Omega_{A/K}^1$  the sheaf of differentials 1-forms on  $A/K$  and let  $\{\omega_1, \dots, \omega_g\}$  be a  $K$ -basis of  $H^0(A, \Omega_{A/K}^1)$ . Let  $\eta = \omega_1 \wedge \dots \wedge \omega_g$  be a non zero differential  $g$ -form on  $A$ . Let  $\mathcal{A}$  denote the Néron model of  $A$  over  $\mathcal{O}_K$ , let  $e : \text{Spec}(\mathcal{O}_K) \rightarrow \mathcal{A}$  be its neutral section and let  $\Omega_{\mathcal{A}/\mathcal{O}_K}^g$  be the invertible sheaf of the differential 1-forms on  $\mathcal{A}$ . The module  $H^0(\mathcal{A}, \Omega_{\mathcal{A}/\mathcal{O}_K}^g)$  of global invariant differentials on  $\mathcal{A}$  is a projective  $\mathcal{O}_K$ -module of rank 1 and can be written as

$$H^0(\mathcal{A}, \Omega_{\mathcal{A}/\mathcal{O}_K}^g) = \eta \mathfrak{a},$$

where  $\mathfrak{a}$  is a fractional ideal of  $K$  (depending on  $\eta$ ).

To every place  $v$  of  $K$ , we will associate a local number  $c_v$ . For a *finite* place  $v$  let  $A^0(K_v)$  be the subgroup of  $K_v$ -rational points which reduces to the identity component of the Néron model  $\mathcal{A}$ . Denotes

$$c_v = (A(K_v) : A^0(K_v))$$

the index of the subgroup of  $K_v$ -rational points which extends to the connected component in  $\mathcal{A}$ . Let  $\mu_v$  be an additive Haar measure on  $K_v$  such that  $\mu_v(\mathcal{O}_{K_v}) = 1$  if  $v$  is finite,  $\mu_v$  is the Lebesgue measure if  $v$  is a real archimedean place (i.e.  $K_v = \mathbb{R}$ ) and twice the Lebesgue measure if  $v$  is complex (i.e.  $K_v = \mathbb{C}$ ). Define, for an *archimedean* place  $v$ , the *local period*

$$c_v = \int_{A(K_v)} |\eta| \mu_v^g.$$

Remark that the integral  $c_v$  is non zero. For a non-archimedean place, Yu. Manin define  $m_v = P_v(N_{K/\mathbb{Q}}(\mathfrak{p}_v)^{-1})^{-1} \int_{A(K_v)} |\eta| \mu_v^g$ , which is equivalent to our  $c_v$  (see, e. g., [Man71, lemma 8.9] when the dimension  $g$  is 1). For the complex places, Yu. Manin choose  $\mu_v$  to be the Lebesgue measure, instead, as we do, twice the Lebesgue measure. So with its definition [Man71, formula (38)],  $c_v = 2^g m_v$ . B. Gross [Gro82] gives another formulation for the archimedean places, which is equivalent (see [Man71, lemma 8.8]). Define also the *archimedean local factor* as

$$c_\infty(A/K) = N_{K/\mathbb{Q}}(\mathfrak{a}) \cdot \prod_{v \in M_K^\infty} c_v,$$

which is independent of the choice of the differential  $\eta$ .

The part concerning the local periods  $c_v$  can be bounded in terms of the *Faltings' height*. We recall here its definition (see [CS86, Chapter II]). We endowed the line bundle  $\Omega_{\mathcal{A}/\mathcal{O}_K}^g$  with an hermitian metric by defining, for a section  $s$  and for every archimedean place  $v$ ,

$$|s|_v = \left( \left( \frac{i}{2} \right)^g \int_{A(\overline{K}_v)} s \wedge \overline{s} \right)^{\frac{1}{2}}.$$

We define also

$$\|s\|_v = |s|_v^{n_v},$$

where  $n_v = 1$  if  $v$  is real and  $n_v = 2$  if  $v$  is complex. This norm extends the norm on  $K_v$  (i.e.  $\forall k \in K_v, \forall s \in \Omega_{\mathcal{A}/\mathcal{O}_K}^g \otimes_{\mathcal{O}_K} K_v, \|ks\|_v = \|k\|_v \cdot \|s\|_v$ ). Taking the pull-back of  $\Omega_{\mathcal{A}/\mathcal{O}_K}^g$  and metrics via the neutral section  $e : \text{Spec}(\mathcal{O}_K) \rightarrow \mathcal{A}$ , we obtain a metrised line bundle on  $\text{Spec}(\mathcal{O}_K)$  (i.e. a projective  $\mathcal{O}_K$ -module of rank 1):

$$\omega_{\mathcal{A}/\mathcal{O}_K} = e^* \Omega_{\mathcal{A}/\mathcal{O}_K}^g.$$

The line bundle  $\omega_{\mathcal{A}/\mathcal{O}_K}$  can be identified with  $H^0(\Omega_{\mathcal{A}/\mathcal{O}_K}^g) = \eta \mathfrak{a}$ . In fact,  $e^* \Omega_{\mathcal{A}/\mathcal{O}_K}^g = \pi_* \Omega_{\mathcal{A}/\mathcal{O}_K}^g$ , where  $\pi : \mathcal{A} \rightarrow \text{Spec}(\mathcal{O}_K)$  is the structural morphism, and since the line bundle is affine, it can be identified with the module of its global sections  $H^0(\Omega_{\mathcal{A}/\mathcal{O}_K}^g)$ . The Faltings' height of  $A$  is the *Arakelov degree* of  $\omega_{\mathcal{A}/\mathcal{O}_K}$  :

$$h_{\text{Falt}}(A/K) = \frac{1}{[K : \mathbb{Q}]} \deg_{\text{Ar}}(\omega_{\mathcal{A}/\mathcal{O}_K}, \|\cdot\|) = -\frac{1}{[K : \mathbb{Q}]} \log \prod_{v \in M_K} \|s\|_v,$$

for any section  $s$ . We will also use the notation  $H_{\text{Falt}} = \exp\{h_{\text{Falt}}\}$ . It is well known that

$$\deg_{\text{Ar}}(\omega_{\mathcal{A}/\mathcal{O}_K}, \|\cdot\|) = \log \text{card}(\omega_{\mathcal{A}/\mathcal{O}_K}/s\mathcal{O}_K) - \sum_{v|\infty} \log \|s\|_v.$$

Denote  $\text{III}(A/K) = \ker(H^1(\text{Gal}(\overline{K}/K), A_K) \rightarrow \prod_v H^1(\text{Gal}(\overline{K}_v/K_v), A_{K_v}))$  the *Tate-Shafarevich group* of  $A/K$ . Recall that  $\text{III}(A/K)$  measures the obstruction to the Hasse principle. In fact, a non trivial element of  $\text{III}(A/K)$  corresponds to a homogenous space which have  $K_v$ -rational points for every place  $v$ , but no  $K$ -rational points. Even if it is not easy to construct such a variety, it is only conjectured that  $\text{III}(A/K)$  is finite. K. Rubin [Rub87] gave the first examples of elliptic curves for which it can be proved that the Tate-Shafarevich group is finite (for example, for elliptic curves defined over  $\mathbb{Q}$ ). See also the results of V. A. Kolyvagin [Kol88]. We will suppose throughout the text that  $\text{III}(A/K)$  is finite.

Denote  $\check{A}$  the dual abelian variety of  $A$ , that is  $\text{Pic}^0(A)$ , which is also defined over  $K$ , and isogenous to  $A$ . Let  $\langle, \rangle : A(K) \times \check{A}(K) \rightarrow \mathbb{R}$  denote the Néron-Tate height pairing corresponding to the *Poincaré* divisor on  $A \times \check{A}$ . Denote  $r = \text{rk}(A(K))$  the rank of  $A(K)$ . Choose a basis  $\{P_1, \dots, P_r\}$  for the torsion free part of  $A(K)$  and a basis  $\{Q_1, \dots, Q_r\}$  for the torsion free part of  $\check{A}(K)$ . The *canonical regulator* of  $A$  is defined by

$$\text{Reg}(A) = \det(\langle P_i, Q_j \rangle)_{1 \leq i \leq r; 1 \leq j \leq r}.$$

It is a non zero real number and does not depend on the choice of the basis.

Denote  $A(K)_{\text{tors}}$  and  $\check{A}(K)_{\text{tors}}$  the torsion subgroups of the Mordell-Weil groups. Remark that  $|A(K)_{\text{tors}}|$  and  $|\check{A}(K)_{\text{tors}}|$  are always non zero.

### 3 On the Birch and Swinnerton-Dyer conjecture

We can now state the celebrated conjecture of B. J. Birch and H. P. F. Swinnerton-Dyer (see [BSD65] for the case of elliptic curves and [Man71] and [Gro82] for a general formulation).

**Conjecture 3.1 (Birch and Swinnerton-Dyer)** *Let  $A$  be an abelian variety defined over a number field  $K$ .*

1. *The  $L$ -series  $L(A/K, s)$  has an analytic continuation to the entire complex plane.*
2.  $\text{ord}_{s=1} L(A/K, s) = \text{rk}(A(K))$ .
3. *The leading coefficient  $L^*(A/K, 1) = \lim_{s \rightarrow 1} \frac{L(A/K, s)}{(s-1)^{\text{rk}(A(K))}}$  in the Taylor expansion of  $L(A/K, s)$  at  $s = 1$  satisfies*

$$L^*(A/K, 1) = |\text{III}(A/K)| \cdot \text{Reg}(A(K)) \cdot |A(K)_{\text{tors}}|^{-1} \cdot |\check{A}(K)_{\text{tors}}|^{-1} \cdot c_\infty(A/K) \cdot \prod_{v \in M_K^0} c_v \cdot D_K^{-g/2}. \quad (3)$$

There is some evidence for the truth of this conjecture. In particular, for an elliptic curve defined over  $\mathbb{Q}$  satisfying  $\text{ord}_{s=1} L(E/\mathbb{Q}, s) = 0$ , the conditions 1. and 2. are proved and also a relation between the value of  $L(E/\mathbb{Q}, 1)$  and the order of  $\text{III}(E/\mathbb{Q})$  similar to condition 3. See the results of [CW77], [GZ86], [Rub87], [Kol88].

In this section we bound the product  $|\text{III}(A/K)| \cdot \text{Reg}(A/K)$ . In order to do it, the formula (3) of the BSD-conjecture suggest to bound each one of the remaining terms. This is done in the following lemmas.

The numbers  $c_v$ , for every non-archimedean place  $v$ , are non zero integers and can be bounded from below by 1.

To bound the leading coefficient  $L^*(A/K, 1)$ , Yu. Manin suggested to use the functional equation and some explicit equation for the derivative [Man71, formula (48)]. Here we use the functional equation and the classical convexity argument as in the Phragmén-Lindelöf principle, as in [GS95]. We conclude applying the Cauchy inequality in two different ways, because we want to obtain different kind of bounds.

**Lemma 3.2** *Let  $A/K$  be an abelian variety of dimension  $g$  satisfying Conjecture 2.1. Let  $r = \text{ord}_{s=1} L(A/K, s)$  and  $\mathcal{F} = N_{K/\mathbb{Q}}(\mathcal{F}_{A/K})$ . Then the leading coefficient of the  $L$ -series of  $A/K$  at  $s = 1$  satisfies the following bounds:*

$$|L^*(A/K, 1)| \leq (9/2\pi)^{g[K:\mathbb{Q}]} \sqrt{\mathcal{F}} \cdot D_K^g \quad (4)$$

$$|L^*(A/K, 1)| \leq 2^r \cdot 4^{g[K:\mathbb{Q}]} \cdot \mathcal{F}^{\frac{1}{4}} \cdot D_K^{\frac{g}{2}} \cdot (\log(\mathcal{F} \cdot D_K^{2g}))^{2g[K:\mathbb{Q}]} \quad (5)$$

**Remark 3.3** Conjecturally, the order of the  $L$ -series at 1, here denoted by  $r$ , equals the rank of  $A(K)$ . The bound (4) is independent of  $r$ , while (5) has a term  $2^r$ . Concerning the rank, T. Ooe and J. Top [OT89] proved the following bound:

$$\mathrm{rk}(A(K)) \leq \gamma_1 \log \mathcal{F} + \gamma_2 \log D_K + \gamma_3, \quad (6)$$

where  $\gamma_1, \gamma_2$  and  $\gamma_3$  are positive real numbers depending only on  $g$  and  $[K : \mathbb{Q}]$  and are explicitly given. Using (6), we deduce from (5) a bound independent of the rank, which growth in  $\mathcal{F}$  and  $D_K$  is as:

$$\mathcal{F}^{\frac{5}{4}} \cdot D_K^{\frac{g}{2}+1} \cdot (\log(\mathcal{F} \cdot D_K^{2g}))^{2g[K:\mathbb{Q}]}.$$

Respect to the conductor, the bound (4) is of better quality than this last one. As for the dependence on the discriminant  $D_K$ , the bound (4) has a better dependence than this last bound if the dimension  $g$  is 1 or 2. In [BS07] we are concerned with elliptic curves and we are interested on the dependence on  $D_K$ : the bound (4) is used therein. (However, it is expected that  $\mathrm{rk}(A(K)) \ll \frac{\log \mathcal{F}}{\log \log \mathcal{F}}$ . This would give, using (5), a bound for the leading coefficient of the order

$$\mathcal{F}^{\frac{1}{4}+\epsilon(\mathcal{F})} \cdot D_K^{\frac{g}{2}+1+\epsilon'(D_K)},$$

where  $\epsilon$  and  $\epsilon'$  depend on  $g$  and  $[K : \mathbb{Q}]$  and tend to 0 when  $\mathcal{F}$  tends to infinity and, respectively, when  $D_K$  tends to infinity.) From now on, we will use the bound (4) in the one-dimensional case and the bound (5) otherwise.

*Proof of Lemma 3.2.* Let us consider the abelian variety  $A' = \mathrm{Res}_{\mathbb{Q}}^K A$  over  $\mathbb{Q}$  which is obtained from  $A$  by restriction of scalars (see [Mil72]). Over  $\mathbb{C}$  we then have the decomposition  $A' \simeq \prod_{\sigma} A_{\sigma}(\mathbb{C})$ , where the product runs over all the embeddings  $\sigma : K \hookrightarrow \mathbb{C}$  and  $A_{\sigma}$  is the abelian variety obtained by action of  $\sigma$  on  $A$ . Then  $A'$  is of dimension  $g' = g[K : \mathbb{Q}]$  and

$$L(A'/\mathbb{Q}, s) = L(A/K, s) \text{ and } \mathcal{F}_{A'/\mathbb{Q}} = N_{K/\mathbb{Q}}(\mathcal{F}_{A/K}) \cdot D_K^{2g}. \quad (7)$$

We will use the fact that, since the abelian variety  $A'$  is defined over  $\mathbb{Q}$ , we have [Fon85]

$$\mathcal{N} = \mathcal{F}_{A'/\mathbb{Q}} > 10^{g'}. \quad (8)$$

The Hasse-Weil bound gives  $P_{A',p}(T) = \prod_{i=1}^{\rho} (1 - \alpha_i T)$ , where  $\rho = \deg(P_{A',p}) \leq 2g'$  and  $|\alpha_i| \leq \sqrt{p}$ . Then, if we write  $s = \sigma + i\tau$ , with  $\sigma = \Re(s) > \frac{3}{2}$ , the local factor of the Eulerian product of the  $L$ -series satisfies

$$|P_{A',p}(p)^{-s}|^{-1} \leq (1 - p^{\frac{1}{2}-\sigma})^{-2g'},$$

and then

$$|L(A'/\mathbb{Q}, s)| \leq \zeta(\sigma - \frac{1}{2})^{2g'}.$$

Let  $\sigma = \frac{3}{2} + \epsilon$ , with  $\epsilon > 0$ . Then

$$|\Lambda(A'/\mathbb{Q}, s)| = |\Lambda(A'/\mathbb{Q}, \frac{3}{2} + \epsilon + i\tau)| \leq \mathcal{N}^{\frac{3}{4}+\frac{\epsilon}{2}} \cdot (2\pi)^{-g'(\frac{3}{2}+\epsilon)} \cdot \Gamma(\frac{3}{2} + \epsilon)^{g'} \cdot |\zeta(1 + \epsilon)|^{2g'}.$$

Since  $|\zeta(1 + \epsilon)| \leq (1 + \frac{1}{\epsilon})$ , for  $\epsilon > 0$ , then

$$|\Lambda(A'/\mathbb{Q}, \frac{3}{2} + \epsilon + i\tau)| \leq \mathcal{N}^{\frac{3}{4} + \frac{\epsilon}{2}} \cdot (2\pi)^{-g'(\frac{3}{2} + \epsilon)} \cdot \Gamma(\frac{3}{2} + \epsilon)^{g'} \cdot (1 + \frac{1}{\epsilon})^{2g'}. \quad (9)$$

Using the functional equation, that is, Conjecture 2.1, the same bound (9) is valid for  $|\Lambda(A'/\mathbb{Q}, \frac{1}{2} - \epsilon - i\tau)|$ . The Phragmén-Lindelöf theorem, implies that the bound (9) is still valid for  $s$  with real part  $\sigma$  satisfying  $\frac{1}{2} - \epsilon \leq \sigma \leq \frac{3}{2} + \epsilon$ . Applying the Cauchy inequality in the disc  $\mathcal{D}(1, \frac{1}{2} + \epsilon)$ , we obtain

$$L^*(A'/\mathbb{Q}, 1) = \frac{(2\pi)^{g'} \Lambda^{(r)}(A'/\mathbb{Q}, 1)}{\sqrt{\mathcal{N}} r!} \leq \frac{(2\pi)^{g'}}{\sqrt{\mathcal{N}}} \frac{1}{(\frac{1}{2} + \epsilon)^r} \max_{s \in \mathcal{D}(1, \frac{1}{2} + \epsilon)} \Lambda(A'/\mathbb{Q}, s).$$

The upper bound (9) gives

$$L^*(A'/\mathbb{Q}, 1) \leq \frac{1}{(\frac{1}{2} + \epsilon)^r} \cdot (2\pi)^{-g'(\frac{1}{2} + \epsilon)} \cdot \mathcal{N}^{\frac{1}{4} + \frac{\epsilon}{2}} \cdot \Gamma\left(\frac{3}{2} + \epsilon\right)^{g'} \cdot \left(1 + \frac{1}{\epsilon}\right)^{2g'}.$$

To prove (4), we choose  $\epsilon = \frac{1}{2}$  and obtain

$$L^*(A'/\mathbb{Q}, 1) \leq \left(\frac{9}{2\pi}\right)^{g'} \cdot \sqrt{\mathcal{F}_{A'/\mathbb{Q}}}.$$

To prove (5), we take  $\epsilon = \frac{2}{\log \mathcal{N}}$ . Thus  $(\frac{1}{2} + \epsilon)^{-r} \leq 2^r$  and  $\mathcal{N}^{\frac{1}{4} + \frac{\epsilon}{2}} = e \cdot \mathcal{N}^{\frac{1}{4}}$ . Using the lower bound (8) for the conductor  $\mathcal{N}$  of  $A'/\mathbb{Q}$ , we obtain  $1 + \frac{1}{\epsilon} \leq \log \mathcal{N}$  and  $\Gamma(\frac{3}{2} + \epsilon) \leq (\frac{3}{2}\sqrt{\pi}) < 3$ . For proving the last inequality, remark that  $\Gamma(\frac{3}{2} + \epsilon) = (\frac{1}{2} + \epsilon)\Gamma(\frac{1}{2} + \epsilon) \leq \frac{3}{2}\sqrt{\pi}$ , because  $\frac{1}{2} + \epsilon \in [\frac{1}{2}, \frac{3}{2}]$  and then  $\Gamma(\frac{1}{2} + \epsilon) \leq \Gamma(\frac{1}{2}) = \sqrt{\pi}$ . Moreover  $e \cdot 3^{g'} \cdot (2\pi)^{-g'(1/2 + \epsilon)} = e \cdot \left(\frac{3}{(2\pi)^{1/2 + \epsilon}}\right)^{g'} \leq e \cdot (\frac{6}{5})^{g'} \leq 4^{g'}$ , because  $\frac{1}{2} < \frac{1}{2} + \epsilon < \frac{3}{2}$ . This gives

$$L^*(A'/\mathbb{Q}, 1) \leq 2^r \cdot 4^{g'} \cdot \mathcal{F}_{A'/\mathbb{Q}}^{\frac{1}{4}} \cdot (\log \mathcal{F}_{A'/\mathbb{Q}})^{2g'}.$$

We conclude in both cases applying (7).  $\square$

In order to relate the Faltings' height with the archimedean local periods, we need some preliminaries. For  $v$  complex, the local period  $c_v$  is almost the norm  $\|\omega\|_v$  of  $\omega$ , while for  $v$  real, it is a little bit more delicate to link the local period  $c_v$  with the norm  $\|\omega\|_v$ . We fix an archimedean place  $v$  of  $K$ . Let  $(\gamma_{1,v}, \dots, \gamma_{2g,v})$  be a basis of the integral homology  $H = H_1(A(\overline{K}_v), \mathbb{Z})$  of  $A$ . Choose  $\gamma_{1,v}, \dots, \gamma_{g,v}$  such that  $\gamma_{1,v}, \dots, \gamma_{g,v}$  generates the part of  $H$  fixed by complex conjugation. Let

$$\Omega_{1,v} = \left( \int_{\gamma_{i,v}} \omega_j \right)_{1 \leq i \leq g} \quad \text{and} \quad \Omega_{2,v} = \left( \int_{\gamma_{i,v}} \omega_j \right)_{g+1 \leq i \leq 2g},$$

where  $j$  runs over  $\{1, \dots, g\}$ , be the periods matrixes associated to  $\gamma_{1,v}, \dots, \gamma_{2g,v}$ . Moreover, choose  $\gamma_{1,v}, \dots, \gamma_{2g,v}$  such that

$$\tau_v = \Omega_{1,v}^{-1} \Omega_{2,v}$$

is a symmetric matrix in a fundamental domain. Then  $\Im(\tau_v)$  is positive definite, and satisfies

$$\Im(\tau_{v1,1}) \leq \dots \leq \Im(\tau_{vg,g}), \quad \Im(\tau_{vi,i}) \geq \frac{\sqrt{3}}{2} \quad \text{and} \quad |\Im(\tau_{vi,j})| \leq \frac{1}{2} \Im(\tau_{vi,i}). \quad (10)$$

Let  $\Lambda_v = \Omega_{1,v} \mathbb{Z}^g + \Omega_{2,v} \mathbb{Z}^g$  be the associated lattice. Choose an isomorphism over  $\mathbb{C}$

$$\phi : \mathbb{C}^g / \Lambda_v \rightarrow A(\overline{K}_v)$$

such that the inverse function of  $\phi$  maps the invariant differential  $\eta$  to  $dz$ :  $\phi^*(\eta) = dz$ .

**Lemma 3.4** *The archimedean local factor satisfies*

$$c_\infty(A/K) = \prod_{v \text{ real}} \frac{2^{\epsilon_v}}{\sqrt{\det \Im(\tau_v)}} \cdot H_{Falt}(A/K)^{-[K:\mathbb{Q}]},$$

where  $2^{\epsilon_v} = \text{card}(A_v(\mathbb{R}) : A_v(\mathbb{R})^0)$  is the number of real components of the variety  $A_v$  obtained from  $A$  by the action of  $v$ .

Before proving Lemma 3.4, we deduce an upper bound and a lower bound for  $c_\infty(A/K)$  in terms of the Faltings' height, the degree  $[K:\mathbb{Q}]$  and the dimension  $g$ .

**Lemma 3.5** *The archimedean local factor satisfies the following inequalities*

$$c_{[K:\mathbb{Q}],g} \cdot h_{Falt}(A/K)^{-g[K:\mathbb{Q}]} \cdot H_{Falt}(A/K)^{-[K:\mathbb{Q}]} \leq c_\infty(A/K) \leq 2^{[K:\mathbb{Q}]} H_{Falt}(A/K)^{-[K:\mathbb{Q}]}, \quad (11)$$

where  $c_{[K:\mathbb{Q}],g}$  depends at most on the degree  $[K:\mathbb{Q}]$  and the dimension  $g$ . When  $g = 1$ , one may take  $c_{[K:\mathbb{Q}],1} = (3[K:\mathbb{Q}]^2)^{-[K:\mathbb{Q}]}$ .

*Proof.* Since  $\epsilon_v$  equals 0 or 1, the product of the number of real components satisfies:  $1 \leq \prod 2^{\epsilon_v} \leq 2^{[K:\mathbb{Q}]}$ . On the other hand,  $\Im(\tau)$  satisfies (10). Then

$$\prod_{v \in M_K^\infty \text{ real}} \frac{1}{\sqrt{\det \Im(\tau_v)}} \cdot H_{Falt}(A/K)^{-[K:\mathbb{Q}]} \leq c_\infty(A/K) \leq 2^{[K:\mathbb{Q}]} H_{Falt}(A/K)^{-[K:\mathbb{Q}]}.$$

For  $g = 2$ , using the Matrix Lemma of [Mas87, p. 126] (see also [DP02, Lemma 6.7]), we obtain

$$c_{[K:\mathbb{Q}],g} \cdot h_{Falt}(A/K)^{-g[K:\mathbb{Q}]} \cdot H_{Falt}(A/K)^{-[K:\mathbb{Q}]} \leq c_\infty(A/K). \quad (12)$$

For  $g = 1$ , using the arithmetic-geometric inequality and the Cauchy-Schwartz lemma, we obtain

$$\prod_{v|\infty} \sqrt{\Im(\tau_v)} \leq \frac{1}{\#\{v|\infty\}} \left( \sum_{v|\infty} \sqrt{\Im(\tau_v)} \right)^{\#\{v|\infty\}} \leq \frac{1}{\#\{v|\infty\}} \left( \#\{v|\infty\} \sum_{v|\infty} \Im(\tau_v) \right)^{\#\{v|\infty\}}$$

$$\leq [K : \mathbb{Q}]^{[K:\mathbb{Q}]} \left( \sum_{v|\infty} \mathfrak{S}(\tau_v) \right)^{[K:\mathbb{Q}]} . \quad (13)$$

We now use the formula for the height  $h = h_{\text{Falt}}(E/K)$  of [CS86, Prop. 1.1 of Chap. X]:

$$12[K : \mathbb{Q}]h = \log N_{K/\mathbb{Q}} \Delta_{E/K} - \sum_{v|\infty} 6n_v \log \mathfrak{S}(\tau_v) - \sum_{v|\infty} n_v \log |\Delta(\tau_v)|$$

and, from the exercise on page 256 of *loc. cit.*, the estimate

$$\log |\Delta(\tau_v)| \leq -2\pi \mathfrak{S}(\tau_v) + \log \frac{e^{1/9}}{(2\pi)^{12}} \leq -2\pi \mathfrak{S}(\tau_v).$$

Since  $\log N_{K/\mathbb{Q}} \Delta_{E/K} \geq 0$  and  $\log \mathfrak{S}(\tau_v) \leq \frac{1}{e} \mathfrak{S}(\tau_v)$ , we obtain

$$\sum_{v|\infty} n_v \mathfrak{S}(\tau_v) \leq \frac{12}{2\pi - 6/e} [K : \mathbb{Q}]h \leq 3[K : \mathbb{Q}]h.$$

Putting this inequality into (13), we obtain  $\prod_{v|\infty} \sqrt{\mathfrak{S}(\tau_v)} \leq (3[K : \mathbb{Q}]^2 h)^{[K:\mathbb{Q}]}$  and we can conclude.  $\square$

For the proof of Lemma 3.4 we use the two following lemmas.

**Lemma 3.6** *For an archimedean place  $v$  we have*

$$|\eta|_v = |\Omega_{1,v}| \sqrt{\det \mathfrak{S}(\tau_v)}. \quad (14)$$

*Proof.* Using the definition of the metric and the inverse map of  $\phi$  we compute

$$\begin{aligned} |\eta|_v^2 &= (i/2)^g \int_{A(\overline{K}_v)} \eta \wedge \bar{\eta} = (i/2)^g \int_{\mathbb{C}^g/\Lambda_v} dz \wedge \bar{dz} = (i/2)^g \int_{\mathbb{C}^g/\Omega_{1,v}(\mathbb{Z}^g + \tau_v \mathbb{Z}^g)} dz \wedge \bar{dz} \\ &= (i/2)^g \int_{\mathbb{C}^g/\mathbb{Z}^g + \tau_v \mathbb{Z}^g} |\det \Omega_{1,v}|^2 dz' \wedge \bar{dz}' = (i/2)^g |\det \Omega_{1,v}|^2 \int_{\mathbb{C}^g/\mathbb{Z}^g + \tau_v \mathbb{Z}^g} (-2idx \wedge dy) \\ &= |\det \Omega_{1,v}|^2 \det \mathfrak{S}(\tau_v). \end{aligned}$$

For the last equality we use that  $\int_{\mathbb{C}^g/\mathbb{Z}^g + \tau_v \mathbb{Z}^g} dx \wedge dy$  is the area of a fundamental domain for  $\mathbb{C}^g/\mathbb{Z}^g + \tau_v \mathbb{Z}^g$ , which is  $(1/2^g) \det |\overline{\tau}_v - \tau_v| = \det \mathfrak{S}(\tau_v)$ .  $\square$

**Lemma 3.7** *The product of the local periods satisfies the following equality*

$$\prod_{v|\infty} c_v = \prod_{v \text{ real}} \frac{2^{\epsilon_v}}{\sqrt{\det \mathfrak{S}(\tau_v)}} \cdot \prod_{v|\infty} \|\eta\|_v. \quad (15)$$

*Proof.* For a real place  $v$  we can prove ([Man71, lemma 8.8]) that

$$c_v = \int_{A(\mathbb{R})} |\eta| \mu_v^g = 2^{\epsilon_v} \cdot \left| \det \left( \int_{\gamma_{1,v}} \omega_j \right)_{1 \leq i, j \leq g} \right| = 2^{\epsilon_v} \cdot |\det \Omega_{1,v}|.$$

From Lemma 3.6 we obtain, for  $v$  real,

$$c_v = \frac{2^{\epsilon_v}}{\sqrt{\det \Im(\tau_v)}} |\eta|_v = \frac{2^{\epsilon_v}}{\sqrt{\det \Im(\tau_v)}} \|\eta\|_v.$$

For  $v$  complex, we have

$$\|\eta\|_v = |\eta|_v^2 = (i/2)^g \int_{A(\mathbb{C})} \eta \wedge \bar{\eta} = (i/2)^g \int_{A(\mathbb{C})} (-2i)^g dx \wedge dy = \int_{A(\mathbb{C})} dx \wedge dy,$$

where  $dx \wedge dy$  is the Lebesgue measure on  $A(\mathbb{C})$ . Since  $|\eta| \mu_v^g$  is also the Lebesgue measure on  $A(\mathbb{C})$ , then

$$\|\eta\|_v = \int_{A(\mathbb{C})} |\eta| \mu_v^g = c_v.$$

□

*Proof of Lemma 3.4.* To compute the degree of  $\omega_{\mathcal{A}/\mathcal{O}_K}$  (which we have identified with  $H^0(\mathcal{A}, \Omega_{\mathcal{A}/\mathcal{O}_K}^g) = \eta \mathfrak{a}$ , and since, by the product formula,  $\sum_{v \in M_K} \log \|\eta\|_v = \sum_{v \in M_K} \log \|k\eta\|_v$ , for all  $k$  in  $K$ ), we choose the invariant differential  $\eta$ :

$$[K : \mathbb{Q}] h_{Falt}(A/K) = \deg_{Ar}(\omega_{\mathcal{A}/\mathcal{O}_K}, \|\cdot\|) = \log |\eta \mathfrak{a} / \eta \mathcal{O}_K| - \sum_{v|\infty} \log \|\eta\|_v.$$

Since  $|\eta \mathfrak{a} / \eta \mathcal{O}_K| = |\mathfrak{a} / \mathcal{O}_K| = |\mathcal{O}_K / \mathfrak{a}^{-1}| = N_{K/\mathbb{Q}}(\mathfrak{a}^{-1})$ , then

$$[K : \mathbb{Q}] h_{Falt}(A/K) = -\log N_{K/\mathbb{Q}}(\mathfrak{a}) - \log \left( \prod_{v|\infty} \|\eta\|_v \right).$$

We conclude applying Lemma 3.7.

□

In the one-dimensional case, using the results of L. Merel [Mer96] and P. Parent [Par99] we can obtain an uniform bound for the cardinality of the torsion part of the Mordell-Weil group. In fact, Merel's result tell us which prime numbers could divide  $|E(K)_{tors}|$  and Parent's result give us a bound for the powers of these primes, independent on the power.

**Lemma 3.8** *For every integral number  $d \geq 1$  there is a positive number  $B(d)$  such that for every number field  $K$  with  $[K : \mathbb{Q}] \leq d$  and every elliptic curve  $E$  defined over  $K$  we have*

$$|E(K)_{tors}| \leq B(d). \tag{16}$$

*One may take  $B(d) = (129 \cdot (5^d - 1) (3d)^6)^{\frac{(1+3^{d/2})^8}{2 \log(1+3^{d/2})}}$ .*

For the convenience of the reader we give the details of the proof of Lemma 3.8. Before the proof, we state an analytic lemma which will be used therein.

**Lemma 3.9** *For  $n \geq 1$ , denote  $p_1, p_2, \dots, p_n$  the  $n$  first prime numbers. As usual, denote  $\theta(p_n) = \sum_{i=1}^n \log p_i$ . For every  $n \geq 1$ , one has*

$$n \leq 4 \frac{\theta(p_n)}{\log \theta(p_n)}.$$

*Proof.* Remark (see, e.g., [Ell75, page 25]) that for every  $n \geq 1$ , one has  $p_n \geq n \log n$ . Furthermore, for  $n \geq 2$ , one has  $\sum_{i=1}^n \log i \geq \int_1^n \log x dx = n \log n - n + 1$  and  $\sum_{i=2}^n \log(\log i) > \log \log 2$ . From these remarks we deduce that, for  $n \geq 2$ ,

$$\theta(p_n) = \log 2 + \sum_{i=2}^n \log p_i > \log 2 + \sum_{i=2}^n \log(i \log i) > \log 2 + n \log n - n + 1 + \log \log 2.$$

Let  $n \geq 4$ . Then  $\theta(p_n) > \frac{1}{2} n \log n \geq e$  and, since for  $x \geq e$ , the function  $x \mapsto \frac{x}{\log x}$  grows, then  $\frac{\theta(p_n)}{\log \theta(p_n)} \geq \frac{\frac{1}{2} n \log n}{\log(\frac{1}{2} n \log n)}$ . Moreover,  $\frac{\log n + \log \log n - \log 2}{\log n} = 1 + \frac{\log \log n}{\log n} - \frac{\log 2}{\log n} \leq 1 + \frac{1}{e}$ . Thus

$$n \leq 2 \left(1 + \frac{1}{e}\right) \frac{\theta(p_n)}{\log \theta(p_n)}.$$

We easily check that for  $n = 1, 2$  and  $3$  one also has  $n \leq 4 \frac{\theta(p_n)}{\log \theta(p_n)}$ . □

*Proof of Lemma 3.8.* Following a result of L. Merel, if there is an element in  $E(K)_{tors}$  of order a prime number  $p$ , then  $p \leq m(d)$ . The theorem of [Mer96] gives  $m(d) = d^{3d^2}$ ; but this bound was improved by J. Oesterlé (in an unpublished article) by  $m(d) = (1 + 3^{d/2})^2$ . We will use here Oesterlé's bound. Let us denote  $p_1 < \dots < p_m$  the first  $m$  prime numbers, where  $m$  satisfies  $p_m \leq m(d)$  and  $p_{m+1} > m(d)$ . Then, for  $i \in \{1, \dots, m\}$ , there exist some  $n_i \geq 0$ , such that  $|E(K)_{tors}| \leq p_1^{n_1} \dots p_m^{n_m}$ . We have  $\theta(p_m) = \log(p_1 \dots p_m) \leq m \log m(d)$ . Applying Lemma 3.9, we deduce that

$$m \leq \frac{m(d)^4}{\log m(d)} = \frac{(1 + 3^{d/2})^8}{2 \log(1 + 3^{d/2})}.$$

From [Par99, Theorem 1.2], we now that, for every  $p \in \{p_1, \dots, p_m\}$  and every non zero integer  $n$ ,

$$p^n \leq c(d) = 129 \cdot (5^d - 1) (3d)^6.$$

(In fact, Parent's result is even more precise; it gave better bounds for  $p^n$  depending if  $p$  equals 2, 3 or not.) We conclude that

$$|E(K)_{tors}| \leq c(d)^m \leq (129 \cdot (5^d - 1) (3d)^6)^{\frac{(1+3^{d/2})^8}{2 \log(1+3^{d/2})}}.$$

□

In higher dimension we do not have anymore such a uniform bound. (It is conjectured a bound  $B(d, g)$  depending on the degree and the dimension.) However we can get the following bound, which is sufficient for our purpose.

**Lemma 3.10** *There exists a positive number  $C_{tors}$  such that for every abelian variety  $A/K$  we have*

$$|A(K)_{tors}| \cdot |\check{A}(K)_{tors}| \leq (C_{tors} \cdot \log N_{K/\mathbb{Q}}(\mathcal{F}_{A/K}))^{4g[K:\mathbb{Q}]}.$$

*Proof.* Put  $N = N_{K/\mathbb{Q}}(\mathcal{F}_{A/K})$  the norm of the conductor of  $A$ . As usual, let us denote  $\omega(N)$  the number of prime numbers dividing  $N$  and  $\pi(X)$  the number of prime numbers  $\leq X$ . By the Prime Number Theorem, there exists some absolute constant  $c_1$  such that, for  $X$  large enough,  $\pi(X) \geq c_1 \frac{X}{\log X}$ . Furthermore, there exists another absolute constant  $c_2$  such that  $\omega(N) \leq c_2 \frac{\log N}{\log \log N}$ . Take  $X = C \log N$ , where  $C$  is a positive number large enough to satisfies  $\pi(C \log N) \geq c_1 \frac{C \log N}{\log(C \log N)}$ . Then  $\pi(X) - \omega(N) \geq c_1 C \frac{\log N}{\log \log N + \log C} - c_2 \frac{\log N}{\log \log N}$ . Since  $\frac{\log N}{\log \log N}$  tends to infinity when  $N$  tends to infinity, we can always choose  $C$  such that  $\pi(C \log N) - \omega(N) \geq 2$ . We can then take two distinct primes numbers,  $p$  and  $q$ , coprime with  $N$  and  $\leq C \log N$ .

Let  $\mathfrak{p}$  and  $\mathfrak{q}$  be ideals of  $K$  lying above  $p$  and  $q$  and denote  $v$  and  $w$  the corresponding places of  $K$ . Since  $p$  and  $q$  are coprime with  $N$ , the ideals  $\mathfrak{p}$  and  $\mathfrak{q}$  do not appear in the conductor of  $A$ . Then  $A$  has good reduction at  $\mathfrak{p}$  and  $\mathfrak{q}$  ([ST68, Theorem 1]). Denote  $A_v$  and  $A_w$  the reduced varieties and  $k_v$  and  $k_w$  the residual fields. Then using the injection

$$A(K)_{tors} \hookrightarrow A_v(k_v) \times A_w(k_w)$$

we deduce that  $|A(K)_{tors}| \leq (N_{K/\mathbb{Q}}(\mathfrak{p}) \cdot N_{K/\mathbb{Q}}(\mathfrak{q}))^g \leq (pq)^{g[K:\mathbb{Q}]} \leq (C \log N)^{2g[K:\mathbb{Q}]}$ . We proceed in the same way for  $|\check{A}(K)_{tors}|$ . Since the conductor of  $\check{A}$  is the same as the conductor of  $A$  ([ST68, Corollary 2]), we can conclude.  $\square$

For an abelian variety  $A/K$ , denotes  $g$  the dimension,  $r = \text{rk}(A(K))$  the Mordell-Weil rank,  $\mathcal{F} = N_{K/\mathbb{Q}}\mathcal{F}_{A/K}$  the absolute value of the norm of the conductor,  $h = h_{\text{Falt}}(A/K)$  the Faltings' height,  $H = \exp\{h\}$  its exponential,  $\text{III} = |\text{III}(A/K)|$  the order of the Tate-Shafarevich group and  $R = \text{Reg}(A/K)$  the canonical regulator.

**Proposition 3.11** *Suppose that Conjecture 2.1 and Conjecture 3.1 hold for the abelian variety  $A/K$ . Then, with the notations above,*

$$\text{III} \cdot R \leq c_{[K:\mathbb{Q}],g} \cdot 2^r \cdot D_K^g \cdot \mathcal{F}^{\frac{1}{4}} \cdot (\log \mathcal{F})^{4g[K:\mathbb{Q}]} \cdot (\log(\mathcal{F} \cdot D_K^{2g}))^{2g[K:\mathbb{Q}]} \cdot (H \cdot h^g)^{[K:\mathbb{Q}]}, \quad (17)$$

where  $c_{[K:\mathbb{Q}],g}$  depends at most on the degree  $[K:\mathbb{Q}]$  and the dimension  $g$ .

*Proof.* Apply to the formula (3) of the BSD-conjecture the bound (5) of Lemma 3.2, Lemma 3.5 and Lemma 3.10.  $\square$

Using the bound (4) of Lemma 3.2, instead of (5), we obtain a bound independent of the rank. This bound is particularly interesting when the dimension  $g$  is 1 or 2 and one is interested on the dependence on the discriminant of the number field (see the Remark 3.3).

**Proposition 3.12** *Suppose that Conjecture 2.1 and Conjecture 3.1 hold for the elliptic curve  $E/K$ . Then*

$$|\text{III}(E/K)| \cdot \text{Reg}(E/K) \leq C_d \cdot D_K^{\frac{3}{2}} \cdot \mathcal{F}^{\frac{1}{2}} \cdot (H \cdot h)^d, \quad (18)$$

where  $d = [K : \mathbb{Q}]$  and  $C_d = \left(\frac{9}{2\pi}\right)^d \cdot (3d^2)^d \cdot (129 \cdot (5^d - 1)(3d)^6)^{\frac{(1+3^{d/2})^8}{\log(1+3^{d/2})}}$ .

A similar result is obtained in [Rém97, Proposition A.2.3, Annexe A], for an elliptic curve in the case  $K = \mathbb{Q}$ .

*Proof of Proposition 3.12.* Apply to the formula (3) of the BSD-conjecture the bound (4) of Lemma 3.2, Lemma 3.5 and Lemma 3.8.  $\square$

**Remark 3.13** Since  $\text{III}(A(K))$  is conjectured to be finite, its order is greater than 1 and the bounds of Propositions 3.11 and 3.12 are still valid for  $\text{Reg}(A(K))$ .

**Remark 3.14** If one would like also to deduce from the BSD-conjecture a lower bound for the product of the order of the Tate-Shafarevich group and the canonical regulator, one would be confronted with the problem of estimate from above the product  $\prod_v c_v$  of the local numbers at the finite places and also with the problem of giving a lower bound for  $L^*(A/K, 1)$ . For the local numbers  $c_v$ , this could be done, under Szpiro's conjecture, when  $A$  is a jacobian variety (see [Hin05, Lemma 3.5]). The question for the  $L$ -series seems also difficult (in the case  $g = 1$  and  $K = \mathbb{Q}$  see the proof of Theorem 2 of [GS95]).

## 4 Geometry of numbers

The Néron-Tate height  $\hat{h}$  on  $A(K)$  extends to a positive definite quadratic form on  $A(K) \otimes_{\mathbb{Z}} \mathbb{R}$ . Thus we have a lattice  $A(K)/A(K)_{tors}$  sitting inside a Euclidean space  $A(K) \otimes_{\mathbb{Z}} \mathbb{R} = \mathbb{R}^r$  with inner product  $\langle, \rangle$ , and the canonical regulator  $\text{Reg}(A(K))$  is the square of the volume of the fundamental domain for the lattice. Putting together Minkowski's theorem on the successive minima [Cas97, Theorem V, Chapter VIII, section 4.3] with Lemma 8 page 135 of [Cas97], as [Rém05, Lemma 5.1], we can choose a basis  $\{P_1, \dots, P_r\}$  for the torsion free part of the Mordell-Weil group satisfying  $\hat{h}(P_1) \leq \dots \leq \hat{h}(P_r)$ , and

$$\prod_{i=1}^r \hat{h}(P_i) \leq (r!)^4 \text{Reg}(A(K)). \quad (19)$$

Thus, in order to bound from below the regulator of the variety it suffices to give a lower bound for the  $\hat{h}(P_i)$ 's. In the same way, a lower bound for the product  $\prod_{i=1}^{r-1} \hat{h}(P_i)$  of the  $(r-1)$  first heights of the generators together with an upper bound for the regulator gives us an upper bound for the greatest height  $\hat{h}(P_r)$ . Thus, it will be sufficient to bound from below the smallest height  $\hat{h}(P_1)$ . In section 5, we quote some results about lower bounds for the height of non-torsion points.

## 5 Lower bounds for the height of non-torsion points

A rational point of the abelian variety has Néron-Tate height zero if and only if it is a torsion point. We are interested in lower bounds for the height of the elements of a basis of the free part of the Mordell-Weil group of the variety and more generally for points of infinite order. There are two different directions on which these kind of lower bounds are studied. Let  $A/K_0$  be an abelian variety defined over a number field. Let  $K/K_0$  be any finite extension of the ground field  $K_0$  and let  $P$  in  $A(K)$  be a non-torsion point. In the first case,  $A/K_0$  is fixed and the dependence on the degree  $[K : K_0]$  is the main interest. This is a Lehmer-type problem. In [BS07] lower bounds of the first kind are used. This is because  $E/K_0$  is fixed, while the field  $K$ , which is the field of rationality of the point  $P$ , varies. In the second case, the accent rely in the dependence on the variety  $A/K_0$ . For this last one, there is a conjecture of S. Lang [Lan78, page 92]: *for every elliptic curve  $E/K$ , there is a positive number  $c_K$  depending only on the degree  $[K : \mathbb{Q}]$ , such that, for all non-torsion points  $P$  in  $E(K)$ ,*

$$\hat{h}(P) \geq c_K \cdot \log N_{K/\mathbb{Q}} \Delta_{E/K}. \quad (20)$$

J. Silverman [Sil84] proved Lang's conjecture for an elliptic curve with integral  $j$ -invariant and generalised it to higher dimension [Sil84]. (M. Hindry and J. Silverman [HS88, Theorem 0.3] proved such a lower bound for all elliptic curves, with the constant  $c_K$  replaced by some function on the Szpiro ratio  $\sigma_{E/K} = \frac{\log N_{K/\mathbb{Q}} \Delta_{E/K}}{\log N_{K/\mathbb{Q}} \mathcal{F}_{E/K}}$ . This function, which is explicit, decreases with  $\sigma_{E/K}$ . This result show that the Szpiro's conjecture implies Lang's conjecture.)

Here we consider the second kind of bounds because we put the accent on the variety. Concerning this problem, D. Masser [Mas87, Corollary 1] proved that *for every  $K/K_0$ , there exists a real number  $c_{[K:\mathbb{Q}]}$  depending on  $[K : \mathbb{Q}]$  such that, for all non-torsion points  $P$  in  $A(K)$ , one has*

$$\hat{h}(P) \geq c_{[K:\mathbb{Q}]} \cdot h_{Falt}(A/K_0)^{-(2g+1)}. \quad (21)$$

In fact, D. Masser proved a more precise bound, which is even more precise than the one obtained replacing here  $h_{Falt}$  by the *stable* Faltings' height. However, this bound is enough for our application. (S. David [Dav93, Theorem 1.4] gives an explicit bound. His bound, valid for certain families of abelian varieties under some hypothesis, could tends to infinity when the height of the variety tends to infinity. See the comments on page 515 of *loc. cit.*)

## 6 On the generators of the Mordell-Weil group and the order of the Tate-Shafarevich group

In this last section, we give the proofs of Theorem 1.1 and Theorem 1.2 and comment on these results.

*Proof of Theorem 1.1.* Applying to the inequality (19), obtained from Minkowski's theorem on successive minima, the lower bound (21) for  $\hat{h}(P_1)$  and the conditional upper bound (17) for the regulator we obtain the theorem.  $\square$

When  $g = 1$  and  $K = \mathbb{Q}$ , the bound of Theorem 1.1 should be compared with Lang's conjecture (1). S. Lang obtained a factor  $e^{r^2}$  and he could not reduced it to  $e^r$ , as remarked by himself in [Lan83, Note on p. 170]. Our bound gives a factor which grows with  $r$  as  $e^{4r \log r + cr}$ . This is because we use Minkowski's theorem, instead of Hermite's one. Concerning the height of the variety, we have a supplementary factor:  $h^{(2g+1)(r-1)} \cdot h^{g[K:\mathbb{Q}]}$ . The factor  $h^{g[K:\mathbb{Q}]}$  comes from the Matrix Lemma. The factor,  $h^{(2g+1)(r-1)}$  comes from the lower bound for non-torsion points. To bound the height of non-torsion points, in the one-dimensional case, S. Lang used his conjectured bound (20) and compared the discriminant of the curve with its conductor. As for the dependence on the conductor, we obtain  $\mathcal{F}^{\frac{1}{4} + \epsilon(\mathcal{F})}$ , where  $\epsilon$  depends only on  $g$  and  $K$  and  $\epsilon(\mathcal{F})$  tends to 0 when  $\mathcal{F}$  tends to infinity. Contrary to this, S. Lang suggested  $\mathcal{F}^{\epsilon(\mathcal{F})} \cdot (\log \mathcal{F})^r$ , where  $\epsilon(\mathcal{F})$  tends to 0 when  $\mathcal{F}$  tends to infinity. This is because, for bounding the leading coefficient of the  $L$ -function, he avoided the use of the functional equation, which he replace by some hypothetical bound of his own, inspired by the Riemann hypothesis on the zeta function and some analytic estimates.

We remark that we can deduce a lower bound for the regulator from inequality (19) and the lower bound (21) for non-torsion points:

$$\text{Reg}(A/K) \geq (r!)^4 \cdot (c_{[K:\mathbb{Q}]})^r \cdot h_{\text{Falt}}(A/K)^{-r(2g+1)}.$$

With Proposition 3.11 we obtain an upper bound for the order of the Tate-Shafarevich group:

$$|\text{III}(A/K)| \leq c_{[K:\mathbb{Q}],g} \cdot (r!)^4 \cdot 2^r \cdot (c_{[K:\mathbb{Q}]})^r \cdot D_K^g \cdot \mathcal{F}^{\frac{1}{4}} \cdot (\log \mathcal{F})^{4g[K:\mathbb{Q}]} \cdot (\log(\mathcal{F} \cdot D_K^{2g}))^{2g[K:\mathbb{Q}]} \cdot H^{[K:\mathbb{Q}]} \cdot h^{g[K:\mathbb{Q}] + r(2g+1)}. \quad (22)$$

Even if this is not made explicitly here, we would like to point out that there should be an inequality of the form  $\mathcal{F} \ll H^{12}$ . For an elliptic curve this is quite obvious because the Faltings' height is linked with the minimal discriminant. In higher dimension, the implied constant in  $\ll$  would depend at least on  $g$  and  $K$ . With this inequality, we could deduce from (22) an upper bound for  $|\text{III}(A/K)|$  which is independent of  $\mathcal{F}$  and grows in the height as

$$H^{3+[K:\mathbb{Q}]} \cdot h^{7g[K:\mathbb{Q}] + r(2g+1)}.$$

On the other hand, an inverse inequality between the height and the conductor would lead to an upper bound as a function in  $\mathcal{F}$ ,  $r$ ,  $K$  and  $g$ . This inequality is predicted by the following conjecture.

**Conjecture 6.1 (Generalised Szpiro conjecture)** *Let  $A$  be an abelian variety of dimension  $g$  defined over a number field  $K$ . There exists real numbers  $c_1$  and  $c_2$  depending at most on  $g$  and  $K$  such that*

$$h_{\text{Falt}}(A/K) \leq c_1 \log N_{K/\mathbb{Q}}(\mathcal{F}_{A/K}) + c_2.$$

Looking at the function field analog and a theorem of P. Deligne, M. Hindry [Hin05] suggest that we may take  $c_1 = (\frac{g}{2} + \epsilon)$ , for every  $\epsilon > 0$ . Playing with restriction of scalars, he adds:  $c_2 = (g^2 + \epsilon) \log D_K + c_{\epsilon, [K:\mathbb{Q}]}$ , where  $c_{\epsilon, [K:\mathbb{Q}]}$  depends only on  $\epsilon$  and  $[K:\mathbb{Q}]$ .

*Proof of Theorem 1.2.* Applying Conjecture 6.1 to (22) and replacing  $c_1$  by  $(\frac{g}{2} + \epsilon)$  and  $c_2$  by  $(g^2 + \epsilon) \log D_K + c_{\epsilon, [K:\mathbb{Q}]}$ , we obtain the theorem.  $\square$

When the dimension of the variety is 1 and the number field is  $\mathbb{Q}$ , Theorem 1.2 gives  $|\text{III}(E/\mathbb{Q})| \ll \mathcal{F}^{1/4+c+\gamma(\mathcal{F})}$ , where  $c = 1/2 + \epsilon$ , the function  $\gamma$  depends on  $r$  and  $\gamma(\mathcal{F})$  tends to 0 when  $\mathcal{F}$  tends to infinity. The bound of Theorem 1 of [GS95], which we have quoted in the introduction, is  $|\text{III}(E/\mathbb{Q})| \ll \mathcal{F}^{1/4+c+\gamma(\mathcal{F})}$ , with  $c = 3/2$  and  $\gamma(\mathcal{F})$  tends to 0 when  $\mathcal{F}$  tends to infinity. They expected ([GS95, page 75])  $c > 1/2$ , as we obtained. The difference between the numbers  $c$  is because they use the lower bound for the period:  $\Omega \gg D^{-4} \gg H^{-3}$ , where  $D$  is the minimal discriminant of the curve (see [Gol90, page 168]), while our Lemma 3.5 gives:  $c_\infty \gg h^{-1} \cdot H^{-1}$ .

In the same paper D. Goldfeld and L. Szpiro proved [GS95, Theorem 2] a sort of reciprocal statement. Precisely, they proved that if their conjectured bound (2) holds for every elliptic curve over  $\mathbb{Q}$ , then a weak version of Szpiro's conjecture holds for every elliptic curve defined over  $\mathbb{Q}$ . The proof use the BSD-conjecture for all elliptic curves over  $\mathbb{Q}$ , but just in the case of rank zero, which is a theorem. It would be interesting to investigate if this result can also be generalized to any number field or to higher dimension.

**Acknowledgments.** I would like to thank Carlo Gasbarri, Marc Hindry and Henri Darmon for some useful references and remarks concerning this work and Jean-Benoît Bost for pushing me to improve the presentation of the results. I would also like to thank the universities of Roma 2 and Roma 3 for the hospitality during my visits to Rome.

## References

- [BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over  $\mathbf{Q}$ : wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939 (electronic), 2001.
- [BK94] Armand Brumer and Kenneth Kramer. The conductor of an abelian variety. *Compositio Math.*, 92(2):227–248, 1994.
- [BS07] Vincent Bosser and Andrea Surroca. Elliptic logarithms, diophantine approximation and the Birch and Swinnerton-Dyer conjecture. *Pre-print*, 2007.
- [BSD65] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves. II. *J. Reine Angew. Math.*, 218:79–108, 1965.
- [Cas97] J. W. S. Cassels. *An introduction to the geometry of numbers*. Classics in Mathematics. Springer-Verlag, Berlin, 1997. Corrected reprint of the 1971 edition.

- [CS86] Gary Cornell and Joseph H. Silverman, editors. *Arithmetic geometry*. Springer-Verlag, New York, 1986. Papers from the conference held at the University of Connecticut, Storrs, Connecticut, July 30–August 10, 1984.
- [CW77] John Coates and Andrew Wiles. On the conjecture of Birch and Swinnerton-Dyer. *Invent. Math.*, 39(3):223–251, 1977.
- [Dav93] Sinnou David. Minorations de hauteurs sur les variétés abéliennes. *Bull. Soc. Math. France*, 121(4):509–544, 1993.
- [DP02] Sinnou David and Patrice Philippon. Minorations des hauteurs normalisées des sous-variétés de variétés abéliennes. II. *Comment. Math. Helv.*, 77(4):639–700, 2002.
- [Ell75] William John Ellison. *Les nombres premiers*. Hermann, Paris, 1975. En collaboration avec Michel Mendès France, Publications de l’Institut de Mathématique de l’Université de Nancago, No. IX, Actualités Scientifiques et Industrielles, No. 1366.
- [Fon85] Jean-Marc Fontaine. Il n’y a pas de variété abélienne sur  $\mathbf{Z}$ . *Invent. Math.*, 81(3):515–538, 1985.
- [GL96] Dorian Goldfeld and Daniel Lieman. Effective bounds on the size of the Tate-Shafarevich group. *Math. Res. Lett.*, 3(3):309–318, 1996.
- [Gol90] Dorian Goldfeld. Modular elliptic curves and Diophantine problems. In *Number theory (Banff, AB, 1988)*, pages 157–175. de Gruyter, Berlin, 1990.
- [Gro82] Benedict H. Gross. On the conjecture of Birch and Swinnerton-Dyer for elliptic curves with complex multiplication. In *Number theory related to Fermat’s last theorem (Cambridge, Mass., 1981)*, volume 26 of *Progr. Math.*, pages 219–236. Birkhäuser Boston, Mass., 1982.
- [GS95] Dorian Goldfeld and Lucien Szpiro. Bounds for the order of the Tate-Shafarevich group. *Compositio Math.*, 97(1-2):71–87, 1995. Special issue in honour of Frans Oort.
- [GZ86] Benedict H. Gross and Don B. Zagier. Heegner points and derivatives of  $L$ -series. *Invent. Math.*, 84(2):225–320, 1986.
- [Hin05] Marc Hindry. Why is it difficult to compute the Mordell-Weil group? *Proceedings of Diophantine Geometry at Centro Ennio de Giorgi, Pisa June 2005, preprint*, pages 1–17, 2005.
- [HS88] Marc Hindry and Joseph H. Silverman. The canonical height and integral points on elliptic curves. *Invent. Math.*, 93(2):419–450, 1988.

- [Kol88] V. A. Kolyvagin. Finiteness of  $E(\mathbf{Q})$  and  $\text{SH}(E, \mathbf{Q})$  for a subclass of Weil curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 52(3):522–540, 670–671, 1988.
- [Lan78] Serge Lang. *Elliptic curves: Diophantine analysis*, volume 231 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1978.
- [Lan83] Serge Lang. Conjectured Diophantine estimates on elliptic curves. In *Arithmetic and geometry, Pap. dedic. I. R. Shafarevich on the occasion of his sixtieth birthday. Edited by Michael Artin and John Tate, Vol. I*, volume 35 of *Progr. Math.*, pages 155–171. Birkhäuser Boston, Boston, MA, 1983.
- [LRS93] Paul Lockhart, Michael Rosen, and Joseph H. Silverman. An upper bound for the conductor of an abelian variety. *J. Algebraic Geom.*, 2(4):569–601, 1993.
- [Man71] Juri I. Manin. Cyclotomic fields and modular curves. *Uspehi Mat. Nauk*, 26(6(162)):7–71, 1971.
- [Mas87] David W. Masser. Small values of heights on families of abelian varieties. In *Diophantine approximation and transcendence theory (Bonn, 1985)*, volume 1290 of *Lecture Notes in Math.*, pages 109–148. Springer, Berlin, 1987.
- [Mer96] Loïc Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.*, 124(1-3):437–449, 1996.
- [Mil72] J. S. Milne. On the arithmetic of abelian varieties. *Invent. Math.*, 17:177–190, 1972.
- [OT89] Takeshi Ooe and Jaap Top. On the Mordell-Weil rank of an abelian variety over a number field. *J. Pure Appl. Algebra*, 58(3):261–265, 1989.
- [Par99] Pierre Parent. Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres. *J. Reine Angew. Math.*, 506:85–116, 1999.
- [Rém97] Gaël Rémond. Sur des problèmes d’effectivité en géométrie diophantienne. *Thèse de doctorat, Université Paris 6*, 1997.
- [Rém05] Gaël Rémond. Intersection de sous-groupes et de sous-variétés. I. *Math. Ann.*, 333(3):525–548, 2005.
- [Rub87] Karl Rubin. Tate-Shafarevich groups and  $L$ -functions of elliptic curves with complex multiplication. *Invent. Math.*, 89(3):527–559, 1987.
- [Ser70] Jean-Pierre Serre. *Séminaire Delange-Pisot-Poitou. 11e année: 1969/70. Théorie des nombres. Fasc. 2: Exposé 19*. Secrétariat Mathématique, Paris, 1970. <http://www.numdam.org>.

- [Shi94] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 11 of *Publications of the Mathematical Society of Japan*. Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kano Memorial Lectures, 1.
- [Sil84] Joseph H. Silverman. Lower bounds for height functions. *Duke Math. J.*, 51(2):395–403, 1984.
- [ST61] Goro Shimura and Yutaka Taniyama. *Complex multiplication of abelian varieties and its applications to number theory*, volume 6 of *Publications of the Mathematical Society of Japan*. The Mathematical Society of Japan, Tokyo, 1961.
- [ST68] Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492–517, 1968.
- [Tat95] John Tate. On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. In *Séminaire Bourbaki, Vol. 9*, pages Exp. No. 306, 415–440. Soc. Math. France, Paris, 1995.
- [Wil95] Andrew Wiles. Modular elliptic curves and Fermat’s last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

Andrea Surroca Ortiz  
ETH Zurich  
surroca@math.ethz.ch