Conjectural estimates on the Mordell-Weil and Tate-Shafarevich groups of an abelian variety

Andrea Surroca Ortiz∗

January 15, 2020

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 conditional bounds for the Néron-Tate height of generators of its Mordell-Weil group. The bounds are implied by strong but, henceforth, classical conjectures, such as the Birch and Swinnerton-Dyer conjecture and the functional equation of the $L$-series. In particular, we improve and generalise a result by D. Goldfeld and L. Szpiro on the order of the Tate-Shafarevich group, and extend a conjecture of S. Lang on the canonical height of a system of generators of the torsion-free part of the Mordell-Weil 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: 11G40, 11G50, 11G10, 11G05, 14G05, 11H50, 14G40.

Keywords: Abelian variety, $L$-functions, heights, Birch–Swinnerton-Dyer conjecture, Mordell-Weil group, Tate-Shafarevich group.

1 Introduction

The Mordell-Weil theorem states that the group of rational points on an abelian variety $A/K$ defined over a number field is finitely generated, and can thus be written as

$$A(K) \simeq A(K)_{\text{tors}} \oplus \mathbb{Z} P_1 \oplus \ldots \oplus \mathbb{Z} P_r,$$

where $r = \text{rk}(A(K))$ is called its rank, and $A(K)_{\text{tors}}$ is the finite group of its torsion points.

While there exist results on the torsion part, the torsion-free part remains less tractable. Even in the particular case of an elliptic curve, there is no way, in general, to compute the rank or a set of generators of this group.

The proof of the Mordell-Weil theorem involves the Tate-Shafarevich group $\Sha(A/K)$ of $A/K$, which measures the obstruction to the Hasse principle. In fact, a non-trivial element of

∗The first version of this paper was partially supported by the Marie Curie IEF 025499 fellowship of the European Community and the second one by the Ambizione fund PZ00P2_121962 of the Swiss National Science Foundation. This last version is partially supported by the EPSRC EP/N007956/1 grant at the University of Manchester.
III(A/K) corresponds to a homogenous space, which has \(K_v\)-rational points for every place \(v\), but no \(K\)-rational points. Even if it is not easy to construct such a variety, it is still unknown, in the general case, if III(A/K) is finite.

For some applications, it would be sufficient to bound the size (e.g. cardinality, height, volume) of the invariants related to the variety.

In this article, we explore how the canonical height of a well-chosen system of generators (which provides arithmetic information) could be bounded, as well as the order of the Tate-Shafarevich group of \(A(K)\). The bounds given here are not conjectured, but implied, by strong but classical conjectures. We follow the approach of Manin, who proposed a conditional algorithm for finding a basis for the non-torsion rational points of an elliptic curve over \(\mathbb{Q}\). The method is based on the hypothesis that the \(L\)-series of the elliptic curve satisfies a functional equation and the celebrated conjecture of Birch and Swinnerton-Dyer [BSD65] (BSD-conjecture for short), which translates analytic information into algebraic and arithmetic information.

We extend Manin’s method to an abelian variety \(A\) of arbitrary dimension, defined over an arbitrary number field \(K\). The bounds are given in terms of more tractable objects associated to the variety and the number field. Precisely, our bounds depends on the Faltings’ height \(h = h_{\text{Fal}}(A/K)\) of \(A/K\) (which measures the arithmetic complexity of the variety), the absolute value \(F = |N_{K/Q} F_{A/K}|\) of the norm of the conductor (which gives information about the places of bad reduction), the dimension \(g\) of \(A\), the Mordell-Weil rank \(r = \text{rk}(A(K))\), the degree \(d = [K : \mathbb{Q}]\), and the absolute value \(D_K\) of the discriminant of \(K\). Moreover, the dependence of the bounds is explicit in all the parameters.

Suppose that \(A\) carries a polarisation \(\phi_L : A \to \bar{A}\). The associated Néron-Tate height on \(A(\mathbb{R})\),

\[ h_L = h_{A,L} : A(\mathbb{K}) \to \mathbb{R}, \]

extends to a positive definite quadratic form on \(A(K) \otimes \mathbb{R} \simeq \mathbb{R}^r\). The associated pairing \(\langle , \rangle_L\) endows \(A(K) \otimes \mathbb{Z} \mathbb{R} \simeq \mathbb{R}^r\) with a structure of a euclidean space, and we can view \(A(K)/A(K)_{\text{tors}}\) as a lattice sitting inside this \(\mathbb{R}^r\). The regulator \(\text{Reg}_L(A/K) := \det(\langle P_i, P_j \rangle_L)_{1 \leq i,j \leq r} \geq 0\) of \(A/K\) relative to \(L\), where \(\{P_i\}_{1 \leq i \leq r}\) is a basis for \(A(K)/A(K)_{\text{tors}}\), is the square of the volume of the fundamental domain for the lattice. Furthermore, we can define a canonical regulator \(\text{Reg}(A/K)\), independent of \(L\).

From Manin’s algorithm one could deduce a bound for the product of the canonical regulator and the Tate-Shafarevich group of \(A(K)\). On this topic, a beautiful analogy with the classical Brauer-Siegel’s formula (relating the discriminant, the regulator and the class number of a number field) is developed by Hindry in [Hin07]. He formulates the following conjecture: For all \(\epsilon > 0\),

\[ |\text{III}(A/K)| \cdot \text{Reg}(A/K) \ll H_{\text{Fal}}(A/K)^{1+\epsilon}, \tag{1} \]

where \(H_{\text{Fal}}(A/K) = e^{H_{\text{Fal}}(A/K)}\) and the implicit constants in the \(\ll\) symbol depend on \(K, g, \epsilon\) and \(\text{rk}(A(K))\). This extends a conjecture of Lang [Lan91, p. 99] for elliptic curves over the field of the rational numbers: Let \(E\) be an elliptic curve defined over \(\mathbb{Q}\), with minimal equation over \(\mathbb{Z}\) given by \(y^2 = x^3 - \gamma_2 x - \gamma_3\), and \(H(E) = \max\{|\gamma_2|^3, |\gamma_3|^2\}\). Then

\[ |\text{III}(E/\mathbb{Q})| \cdot \text{Reg}(E/\mathbb{Q}) \leq b_1 H(E)^{1/12} \cdot F(E)^{r/2} \cdot (\log F)^r, \tag{2} \]

\(^1\)See [HP16] for an unconditional function field analogue, and [Gri18] for an upper and a lower similar bounds for a family of elliptic curves over \(\mathbb{F}_q(t)\).
for $b_1$ and $b_2$ absolute constants and $\epsilon(F)$ tends to 0, when $F$ tends to $\infty$.

Lang modified the heuristic approach of Manin and also proposed the following conjecture [Lan83 Conjecture 3]: Let $E$ be an elliptic curve defined over $\mathbb{Q}$. We can find a basis $\{P_1, \ldots, P_r\}$ for the torsion-free part of $E(\mathbb{Q})$ satisfying

$$\max_{1 \leq i \leq r} \hat{h}(P_i) \ll c \rk(E(\mathbb{Q}))^2 \cdot F_{E/\mathbb{Q}}^{\rk(E(\mathbb{Q}))} \cdot (\log F_{E/\mathbb{Q}})^{\rk(E(\mathbb{Q}))} \cdot e^{F_{\text{alt}}(\mathbb{Q})},$$

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

Furthermore, 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]). Goldfeld and 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 $\epsilon > 0$,

$$|\text{III}(E/K)| = O(F_{E/K}^{1/2+\epsilon}),$$

where the implicit constant in the $O$ depends on $\epsilon$, $K$ and $\rk(E(K))$. In the same article, they announced that this conjecture holds for elliptic curves defined over function fields provided the Tate-Shafarevich group of the function field is finite. Independently, Rajan [Raj97] proved this result. Goldfeld and Lieman [GL96] proved that for a CM elliptic curve defined over $\mathbb{Q}$ with Mordell-Weil rank 0, we have $|\text{III}(E/\mathbb{Q})| < k(\epsilon)F_{E/\mathbb{Q}}^{3/4+\epsilon}$, with $\delta = \frac{59}{120}$ if $j \neq 0, 1728$, $\delta = \frac{37}{70}$ 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 predicts a bound for the discriminant in terms of the conductor), then

$$|\text{III}(E/\mathbb{Q})| = O(F_{E/\mathbb{Q}}^{7/4+\epsilon(F_{E/\mathbb{Q}})}),$$

where $\epsilon(F)$ tends to 0 when $F$ tends to infinity.

We give here bounds in these three directions, that is, for the product $|\text{III}(A/K)|\text{Reg}(A/K)$, the generators $\{P_i\}$ of the Mordell-Weil group, and the group $|\text{III}(A/K)|$. Ours bounds are deduced from the following assumptions.

**Hypothesis 1.1** Let $A$ be an abelian variety of dimension $g$ defined over a number field $K$. Suppose that $A$ carries a principal polarisation $\mathcal{L}$. Suppose that the Tate-Shafarevich group $\text{III}(A/K)$ is finite, the $L$-series of $A/K$ satisfies a condition on the order of growth (Hypothesis 3.5), a functional equation (Conjecture 3.1) and the BSD-conjecture (Conjecture 3.3).

**Remark on the hypothesis.** The assumption that $A$ carries a principal polarisation appears in Section 3.2 (in Lemma 3.11 where it is purely technical and unnecessary, and further in Lemma 3.14) to make evident the $\Im \tau_v$ and link the local periods appearing in the BSD-formula with the Faltings’ height). Using Zarhin’s trick, this hypothesis could be removed, up to modifying the constants in the last statements. For this, one considers the variety $A^4 \times \tilde{A}^4$, which carries a principal polarisation. See, e.g. [LMvdG19, Chap. XI (11.29)] for an explicit construction.
Hypothesis 3.5 is less stringent than being of finite order, which is satisfied in the modular case. In fact, in each case that Conjectures 3.1 and 3.2 are proven, Hypothesis 3.5 is also proven (even if it doesn’t formally follow from Conjectures 3.1 and 3.2). See Remark 3.6 which however is satisfied in the modular case. (See Remark 3.6.)

The core of our work is the next result, which goes in direction of Lang’s conjecture (2). The bound of our proposition refines the conjectural bound (1) of Hindry and extends Rémond’s result [Rém97, Proposition A.2.3, Annexe A], valid for \( g = 1 \) and \( K = \mathbb{Q} \). In what follows, we will state our results in a simplified form, which holds for \( F \neq 1 \). See Section 3.4 for more detailed bounds.

**Proposition 1.2** Suppose that \( A/K \) satisfies Hypothesis 1.1. Then, with the above notations, when \( F \neq 1 \),

\[
|\mathfrak{W}(A/K)| \times \text{Reg}(A(K)) \leq (2^{16} g^2 d)^{4a} \cdot 2^r \cdot D_K^0 \cdot F^{4+\epsilon(F)} \cdot e^{dh} \cdot \max\{1, h\}^{\frac{4a}{F}},
\]

where \( \epsilon(F) = 4gd\log\log F + 2gd\log(\log F) \).

Using classical results on geometry of numbers on the euclidean structure provided by the Néron-Tate height, and lower bounds for non-torsion points, we deduce our other results.

On one hand, we deduce a conditional upper bound for the Néron-Tate height of the elements of a suitable basis of the Mordell-Weil group \( A(K) \) modulo torsion.

**Theorem 1.3** Suppose that \( A/K \) satisfies Hypothesis 1.1. Then we can choose a system \( \{P_1, \ldots, P_r\} \) of generators for the torsion-free part of the Mordell-Weil group \( A(K) \) such that \( \hat{h}_L(P_1) \leq \ldots \leq \hat{h}_L(P_r) \) and, when \( F \neq 1 \),

\[
\hat{h}_L(P_r) \leq (2^{16} g^2 d)^{4a} \cdot (r!)^4 \cdot D_K^0 \cdot F^{4+\epsilon(F)} \cdot e^{dh} \cdot \max\{d + g^2, h\}^{6074g(r-1)+\frac{4a}{F}},
\]

where \( \epsilon(F) = 4gd\log\log F + 2gd\log(\log F) \).

See Section 5 for more detailed bounds, and Remark 5.2 for a comparison of our bound with Lang’s conjecture (3) when \( g = 1 \) and \( K = \mathbb{Q} \).

On the other hand, we extend Theorem 1 of [GS95], the formula is (5), to principally polarised abelian varieties of arbitrary dimension, defined over an arbitrary number field. When the dimension equals 1 and the number field is \( \mathbb{Q} \), our bound improves (5). See Remark 5.6 and, for detailed bounds, see Proposition 5.4.

**Theorem 1.4** Suppose that \( A/K \) satisfies Hypothesis 1.1. Furthermore, suppose that \( A/K \) satisfies Szpiro’s Conjecture (Conjecture 5.3). Then, for every \( \epsilon > 0 \),

\[
|\mathfrak{W}(A/K)| = O((F_{A/K})^{\frac{1}{2}+\frac{1}{2}dg+\epsilon+\delta(F_{A/K})}),
\]

where \( \epsilon > 0 \) and the implicit constant in the \( O \) depends on \( \epsilon, g, K \) and \( r \), and \( \delta(F) \) tends to 0 when \( F \) tends to \( \infty \).

Ours results are stated with the Faltings’ height of \( A/K \), instead of the stable one, \( h_{\text{Stab}}(A) \). In fact, when estimating the local periods, this height appears naturally (see Section 3.2). However, if the number field \( K \) is large enough to contain the points of order 12, that is
$A[12] \subset A(K)$, then we have equality, $h_{\text{Stab}}(A) = h_{\text{Falh}}(A/K)$ (see [sem81, Exposé n.1, Corollaire 5.18]).

In [Man71], [Lan83], and [GS95] the argument is developed when the dimension is 1 and the number field is $\mathbb{Q}$, while in [Hin07] the dependence of the bounds on the number field is not the main interest and is not always made explicit. As pointed out in our joint work with Bosser [BS14], this dependence could play an important role. For example, the discriminant of the number field appears in the rank of the variety. In fact, following the proof of the weak Mordell-Weil theorem, the latter can be bounded in terms of the logarithm of the discriminant of $K$ ([OT89]). Therefore, we consider here abelian varieties of arbitrary dimension over arbitrary number fields, and make this dependence explicit. Furthermore, contrary to [Lan83] and [Hin07] the bounds given here are not conjectured, but implied, by strong but, henceforth, classical conjectures.

As said before, the method is an extension of the one proposed by 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 arithmetic invariants of 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 1.2). In order to achieve this bound, we estimate the remaining 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 3.7). We then relate the local periods to the Faltings’ height of $A/K$ (Lemma 3.17). We also give a bound for the torsion part of the Mordell-Weil group (Lemma 3.20). In Section 4 we recall some classical results on the geometry of numbers, and comment on lower bounds for the Néron-Tate height of non-torsion points. In Section 5 we deduce from the BSD-conjecture the bounds for the highest Néron-Tate height of a set of generators for $A(K)/A(K)_{\text{tors}}$ (Theorem 1.3) and an upper bound for the order of $\text{III}(A(K))$ (Theorem 1.4). We also give particular bounds in the one-dimensional case.

In fact, we apply these results in [BS14] to an elliptic curve to show that, using the elliptic analogue of Baker’s method in linear forms in logarithms, the BSD-conjecture for any single elliptic curve implies an inequality in the direction of the $abc$-conjecture over number fields.

Let’s give a remark on the history of this paper. To deduce Theorem 1.3 and Theorem 1.4 from Proposition 1.2 we use a lower bound for the non-torsion points of the variety (see Section 4). A first version of this work, appearing in Arxiv in 2008, uses a Masser’s lower bound for the non-torsion points on a family of abelian varieties. Since the use of this bound was not appropriate in this context, we wrote a second version, using David’s lower bound, together with the isogenies theorems of Masser-Whüstholz, for a simple principally polarised abelian variety. We then replaced it with a third version, using new isogenies theorems by Gaudron-Rémond. Finally, the lower bound used in this fourth version is the one by Bosser-Gaudron, which is completely explicit, and avoids the use of the isogenies theorems, simplifying the exposition. Some other sections where substantially modified, mostly Sections 3.1 and 3.2.
2 Notations

Throughout the text, we will consider an abelian variety $A$ of dimension $g$ defined over a number field $K$. We denote $d = [K : \mathbb{Q}]$ the degree and $D_K$ the absolute value of the discriminant of the field $K$. To $A$ one can associate different objects: the canonical regulator, the Tate-Shafarevich group, the conductor, the $L$-function, the Faltings’ height.

2.1. The Néron-Tate height and the regulators.

Let’s denote $\hat{A}$ the dual abelian variety of $A$, that is, the connected component of the Picard group of $A$, denoted by $\text{Pic}^0(A)$, which is also defined over $K$, and isogenous to $A$ (see [Mumford1970]). In particular

$$\dim(A) = \dim(\hat{A}), \quad \text{rk}(A(K)) = \text{rk}(\hat{A}(K)), \quad \mathcal{F}_{A/K} = \mathcal{F}_{\hat{A}/K}, \quad h_{\text{Falt}}(A/K) = h_{\text{Falt}}(\hat{A}/K). \quad (8)$$

For the two last equalities see, respectively, [ST68 Corollary 2] and, [Ray85 Corollaire 2.1.3].

Let $\mathcal{L}$ be an invertible sheaf on $A$ and let $\tau_x : A \to A$ be the translation by $x \in A$. We define a morphism $\phi_\mathcal{L} : A \to \hat{A}$ by $\phi_\mathcal{L}(x) = \tau_x^* \mathcal{L} \otimes \mathcal{L}^{-1}$. The morphism $\phi_\mathcal{L}$ is an isogeny (i.e., is surjective and has finite kernel) if and only if $\mathcal{L}$ is ample. In this case, we call it a polarisation and $\deg(\phi_\mathcal{L}) := |\ker \phi_\mathcal{L}| = h^0(A, \mathcal{L})^2$. The polarisation is called principal if its degree is 1.

Let us fix such an ample line bundle $\mathcal{L}$ on $A$, which is identified with an ample symmetric divisor. The associated Néron-Tate height on $A(K)$ (see, e.g. [HS00 Section B.5]),

$$\hat{h}_\mathcal{L} := h_{A,\mathcal{L}} : A(K) \to \mathbb{R},$$

is a positive quadratic form. Since $\hat{h}_\mathcal{L}(P) = 0$ if and only if $P$ is a torsion point, $\hat{h}_\mathcal{L}$ is a positive definite quadratic form on $A(K)/A(K)_{\text{tors}}$, and one could prove that $\hat{h}_\mathcal{L}$ extends to a positive definite quadratic form on $A(K) \otimes_{\mathbb{Z}} \mathbb{R}$. The associated bilinear pairing

$$< P, P' >_{\mathcal{L}} := \frac{1}{2}(\hat{h}_\mathcal{L}(P + P') - \hat{h}_\mathcal{L}(P) - \hat{h}_\mathcal{L}(P')),$$

which satisfies $< P, P >_{\mathcal{L}} = \hat{h}_\mathcal{L}(P)$, endows $A(K) \otimes_{\mathbb{Z}} \mathbb{R} \simeq \mathbb{R}^r$ with a structure of a euclidean space, and we can view $A(K)/A(K)_{\text{tors}}$ as a lattice sitting inside this space. The regulator

$$\text{Reg}_{\mathcal{L}}(A/K) := \det(< P_i, P_j >_{\mathcal{L}})_{1 \leq i,j \leq r} \geq 0,$$

where $\{P_1, \ldots, P_r\}$ is a basis for $A(K)/A(K)_{\text{tors}}$, is the square of the volume of the fundamental domain for the lattice.

We will define now a canonical regulator, independent of the choice of the line bundle $\mathcal{L}$.

Let $\mathcal{P}$ be the Poincaré line bundle on $A \times \hat{A}$ and $h_\mathcal{P} := h_{A \times \hat{A}, \mathcal{P}}$ the canonical height on $A \times \hat{A}$ with respect to $\mathcal{P}$. Let’s define a pairing, for $P \in A(K)$ and $Q \in \hat{A}(K)$,

$$< P, Q >_{\mathcal{P}} := \hat{h}_\mathcal{P}(P, Q).$$

Choose a $\mathbb{Z}$-basis $\{P_1, \ldots, P_r\}$, resp. $\{Q_1, \ldots, Q_r\}$, for $A(K)/A(K)_{\text{tors}}$, resp. of $\hat{A}(K)/\hat{A}(K)_{\text{tors}}$. The canonical regulator of $A$ (also called the discriminant of the height pairing) is defined by

$$\text{Reg}(A) := |\det((< P_i, Q_j >_{\mathcal{P}})_{1 \leq i,j \leq r})|.$$
It is a non-zero real number and does not depend on the choice of the basis (see [Tat66]). However, it could be related to $\mathrm{Reg}_L(A/K)$. In fact, we could recover all heights on $A$ from the canonical pairing (see, e.g., [Ser97, Remark p.39] or [Hin07]):

$$\hat{h}_L(P) = -\frac{1}{2} < P, \phi_L(P) >_P .$$

Denotes

$$u = [\hat{A}(K)/\hat{A}(K)_{\text{tors}} : \phi_L(A(K)/A(K)_{\text{tors}})]$$

the index of the subgroup $\phi_L(A(K)/A(K)_{\text{tors}})$ in $\hat{A}(K)/\hat{A}(K)_{\text{tors}}$. The index $u$ equals 1 if the polarisation $L$ is principal, and we can prove that, in general, $u$ divides $\deg(\phi_L)^r$. Using (8) we can prove that

$$\mathrm{Reg}_L(A/K) = u 2^{-r} \mathrm{Reg}(A/K) \leq 2^{-r} \deg(\phi_L)^r \mathrm{Reg}(A/K).$$

2.2. The Tate-Shafarevich group. The Tate-Shafarevich group of $A/K$ is defined by

$$\Sha(A/K) := \ker(H^1(\Gal(\overline{K}/K), A_K) \to \prod_v H^1(\Gal(\overline{K}_v/K_v), A_{K_v})).$$

Rubin [Rub87] gave the first examples of elliptic curves for which it can be proved that the Tate-Shafarevich group is finite for elliptic curves defined over $\mathbb{Q}$. See also the results of Kolyvagin [Kol88]. We suppose throughout that $\Sha(A/K)$ is finite.

2.3. The conductor. Let $v$ be a finite place of $K$, which corresponds to a prime ideal $p$. We will denote $K_v$ or $K_p$ the completion of $K$ at $v$. For any prime ideal $p$ of $K$, fixing a prime in $K_p$ above $p$, gives us a decomposition group $G_p = \Gal(\overline{K}_p/K_p)$ for $p$ in $\Gal(\overline{K}/K)$. Let $I_p$ be the inertia subgroup of $G_p$, inducing the identity on the residue field $k(p)$. Let $\pi_p$ denote the Frobenius, which generates the quotient $G_p/I_p$. Up to conjugation, $G_p, I_p$ and $\pi_p$ depend only on $p$. Let $\ell$ be any prime, $\ell \neq \text{char}(k(p))$. Denote $A[N]$ the $N$-torsion of $A$, for an integer $N$, $T_\ell(A) = \varprojlim_{n} A[\ell^n]$ the $\ell$-adic Tate module, and $V_\ell(A/K) = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ the $\mathbb{Q}_\ell$-vector space associated. Since $\Gal(\overline{K}/K)$ acts on $V_\ell(A/K)$, we have a $\ell$-adic representation $\rho : \Gal(\overline{K}/K) \to GL(V_\ell(A/K))$.

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

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

where the product runs over the prime ideals $p$ of $K$, and $f_p$ is a positive integer, called the exponent of the conductor, which we will define below. The exponent $f_p$ is zero if and only if $A$ has good reduction at $p$. As in [Ser70], we will attach to the representation $\rho$ two positive integers $\varepsilon_p(\ell)$ and $\delta_p(\ell)$, which measure the ramification of $\rho$. We follow the notations of [LRSS93]. Denote $V_\ell(A/K)^{I_p}$ the submodule of elements fixed by $I_p$. Define

$$\varepsilon_p(\ell) = \text{codim}_{\mathbb{Q}_\ell} V_\ell(A/K)^{I_p}.$$

Let $L_p = K_p(A[\ell])$ be the field generated over $K_p$ by the $\ell$-torsion points of $A$. Denote $v_{L_p}$ the normalised valuation on $L_p$. Let $\pi_{L_p}$ be a uniformiser for $L_p$. Denote $\Gamma_i = \{ \sigma \in \mathbb{Q} \}$
\( \Gal(L_p/K_p); \forall \ell \geq i + 1 \) the \( i \)-th inertia group associated to \( L_p/K_p \) and \( g_i = |G_i| \) its order. Write \( g_0 = |\Gal(L_p/K_p)| \). We define

\[
\delta_p(\ell) = \sum_{i \geq 1} \frac{g_i}{g_0} \dim_F \left( \frac{A[\ell]}{A[I^\ell]} \right).
\]

It has been proven (see the references in [LRS93]) that \( \varepsilon_p(\ell) \) and \( \delta_p(\ell) \) are independent of \( \ell \) so we will denote them by \( \varepsilon_p \) and \( \delta_p \). They are called the tame part and the wild part of the conductor, respectively. The exponent of the conductor is given by

\[
f_p = \varepsilon_p + \delta_p.
\]

It is known that if \( p > 2g + 1 \), where \( p \) is the prime number lying below \( p \), then \( f_p \leq 2g \). Furthermore, it is proven in [LRS93] that \( f_p \leq 12g^2v_{K_0}(p) \) unconditionally (see [BK94] for the best possible upper bounds in all cases).

It is also known that for elliptic curves defined over \( \Q \), the conducteur satisfies \( F_{E/\Q} \geq 11 \). In higher dimension, we still have the following lower bound over \( \Q : F_{A/\Q} > 3 \) (see loc. cit.). Inrevanche, there are number fields where the abelian variety have good reduction everywhere (see [Sch03]) and then, \( F_{A/K} = 1 \).

### 2.4. L-series

We now define the \textit{L-series}, also called the \( \zeta \)-function, of the variety \( A \) (see [Ser70 Section 4]). Since the Frobenius is defined up to \( I_p \), it makes sense to define a polynomial \( P_{A,p}(T) = \det(1 - (p\pi_p)|V_\ell(A/K)^{I_p}T) \), where \( \pi_p \) is regarded as acting on the submodule \( V_\ell(A/K)^{I_p} \) of elements fixed by \( I_p \). The polynomial \( P_{A,p}(T) \) has integral coefficients which are independent of \( \ell \) ([ST68 Theorem 3]). Define

\[
L(A/K, s) = \prod_{v_p} P_{A,p}(N(v_p)^{-s})^{-1}
\]

where the product is taken over all non-archimedean places \( v_p \) of \( K \) and \( N(v_p) \) is the norm of the prime ideal \( p \) associated to \( v_p \). Define the \textit{normalised \( \ell \)-function} by

\[
\Lambda(A/K, s) = (N_{K/\Q}(F_{A/K}) \cdot D_R^{2g})^{s/2} \cdot ((2\pi)^{-s} \cdot \Gamma(s))^{g[K:Q]} \cdot L(A/K, s),
\]

where \( \Gamma(z) = \int_0^{+\infty} t^{z-1}e^{-t}dt \) is the classical \( \Gamma \)-function. For the \( \Gamma \)-factors see [Ser70 section 3]. The Euler product converges and gives an analytic function for all \( s \) satisfying \( \Re(s) > \frac{3}{2} \).

### 2.5. The local factor

In order to state the Birch and Swinnerton-Dyer conjecture, we will introduce a \textit{local factor} for \( A \). We follow here the approach of Gross [Gro82], using the theory of Néron models and Tamawaga numbers.

Let \( \mathcal{A} \) denote the Néron model of \( A \) over the ring of integers \( \mathcal{O}_K \) of \( K \) and \( \mathcal{A}^0 \) the largest open subgroup of \( \mathcal{A} \) in which all fibers are connected.

As a first step, to every place \( v \) of \( K \), we will associate a local number \( c_v \).

For a \textit{finite} place \( v \), \( \mathcal{A}(K_v) \) is a commutative group, and \( \mathcal{A}^0(K_v) \) is the subgroup of the \( K_v \)-rational points which reduces to the identity component of the Néron model \( A \). Denote

\[
c_v := \left| \mathcal{A}(K_v) : \mathcal{A}^0(K_v) \right|
\]

\[\text{For a general formulation on BSD, we could see the original formulation of Tate on abelian varieties [Tat66], and also [Miy72], as well as [Blo80] for a volume theoretic formulation.}\]
the index. Since this integer is 1 for almost all $v$ (that is, for the places where $A$ has good reduction), we may define the product

$$c_f(A/K) = \prod_{v \in M_K^0} c_v.$$  (12)

Denote $\Omega^1_{A/K}$ the sheaf of differential 1-forms on $A/K$. Let $\{\omega_1, \ldots, \omega_g\}$ be a $K$-basis of $H^0(A, \Omega^1_{A/K})$. Then $\eta = \omega_1 \wedge \ldots \wedge \omega_g$ is a non-zero differential $g$-form on $A$. Let $\Omega^g_{A/\mathcal{O}_K}$ be the invertible sheaf of the differential $g$-forms on $A$.

The module $H^0(A, \Omega^g_{A/\mathcal{O}_K})$ of global invariant differentials on $A$ is a projective $\mathcal{O}_K$-module of rank 1 and can be written as

$$H^0(A, \Omega^g_{A/\mathcal{O}_K}) = \eta \cdot a,$$

where $a = a_{\eta}$ is a fractional ideal of $K$ (depending on $\eta$). We have

$$a_{\eta} = a_{\eta} \cdot (\alpha) \quad \text{for} \quad \alpha \in K^*.$$

Let $v$ be an archimedean place of $K$ and let's denote $A_v$ the abelian variety obtained from $A$ by the action by $v$. The integral homology $H_1(A_v(\overline{K_v}), \mathbb{Z})$ of $A_v$ is a free $\mathbb{Z}$-module of rank $2g$. Let $(\gamma_{1,v}, \ldots, \gamma_{2g,v})$ be a basis of $H_1(A_v(\overline{K_v}), \mathbb{Z})$.

Let $v$ be a complex place and define, $\omega_{g+j} = \overline{\omega_j}$ for $j \in \{1, \ldots, g\}$, and

$$c_v := c_v(A, \eta) = \left| \det \left( \int_{\gamma_{i,v}} \omega_j \right)_{1 \leq i,j \leq 2g} \right|.$$

Let $v$ be a real place. Choose the basis so that $\gamma_{1,v}, \ldots, \gamma_{g,v}$ generates the part of $H_1(A_v(\overline{K_v}), \mathbb{Z})$ fixed by complex conjugation. Denote $|A_v(\mathbb{R}) : A_v(\mathbb{R})^0|$ the number of real components of the variety $A_v$ and define

$$c_v := c_v(A, \eta) = |A_v(\mathbb{R}) : A_v(\mathbb{R})^0| \cdot \left| \det \left( \int_{\gamma_{i,v}} \omega_j \right)_{1 \leq i,j \leq g} \right|.$$

These two integrals are non-zero and depend only on $A$, the $g$-form $\eta$ and the place $v$.

We also define the archimedean local factor as

$$c_{\infty}(A/K) = N_{K/\mathbb{Q}}(a) \cdot \prod_{v \in M_K^\infty} c_v,$$  (13)

which is independent of the choice of the differential $\eta$ (because of the product formula). Finally, we define the local factor of $A$ as

$$c(A/K) = c_f(A/K)c_{\infty}(A/K),$$  (14)

which is a positive real number.

Manin [Man71] gives another formulation for the local factors (for $g = 1$), in terms of measures. We follow here [Rem97, Chapitre II] (see pages 15 and 18, where he denotes $\omega = \omega_1 \wedge \ldots \wedge \omega_g$ our $\eta$, and $m_v(A, \omega)$ our $c_v = c_v(A, \eta)$). See also [Gro82, p.224] and [Tat66].
Indeed, let $\mu_v$ be an additive Haar measure on $K_v$ such that $\mu_v(O_{K_v}) = 1$ 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. $K_v = \mathbb{C}$). Then, when the differential form $\eta \in H^0(A, \Omega_{A/K}^g)$ is algebraic, it induces an analytic form to which one could associate the module measure $\text{mod}(\eta)$, denoted by $|\eta|/\mu_v^g$ by Gross, and called the associated Haar measure on $A(K_v)$. We then have the following formulas relating the local periods $c_v(A, \eta)$ with the module measure (see [Gro82] p.224 and [Rém97] for further details). For an archimedean place, we have ([Rém97] p.15)

$$c_v(A, \eta) = \int_{A(K_v)} \text{mod}(\eta),$$

and also the formula (see [Rém97] p.18)

$$\int_{A(\mathbb{C})} \text{mod}(\eta) = \int_{A(\mathbb{C})} |\eta \wedge \overline{\eta}|.$$

For a finite place, we have the formula

$$\int_{A(K_v)} \text{mod}(\eta) = N(v)^{\text{ord}_v(a_v) - g} \cdot |A(K_v)|.$$

Since $P_v(N_{K/Q}(p_v)^{-s})^{-1} = N(v)^g \cdot |A^0(K_v)|^{-1}$, we then obtain, for $v$ finite,

$$c_v(A, \eta) = P_v(N_{K/Q}(p_v)^{-s})^{-1} \cdot N(v)^{-\text{ord}_v(a_v)} \int_{A(K_v)} \text{mod}(\eta).$$

### 2.6. The Faltings’ height.

The part of the BSD-formula concerning the local periods $c_v$ can be bounded in terms of the Faltings’ height. We define it in the following way, using Faltings’ normalisation, $\frac{1}{2}$, as in [CS86] Chapter II (where we corrected the typo).

We endowed the line bundle $\Omega_{A/O_K}^g$ with an Hermitian metric by defining, for a section $s$ and for every archimedean place $v$,

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

We also define

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

where $n_v = [K_v : \mathbb{Q}_v]$ equals 1 if $v$ is real and equals 2 if $v$ is complex. We remark that Rémond [Rém97] p.17 have different notations and normalisation than we use here. In fact, he denotes $||s||_v$ the integral $\int_{A(\mathbb{C})} |s \wedge \overline{s}|$ which corresponds to our $2^g \cdot ||s||_v^2$. However, this norm extends the norm on $K_v$ (i.e. $\forall k \in K_v$, $\forall s \in \Omega_{A/O_K}^g \otimes K_v$, $||ks||_v = ||k||_v \cdot ||s||_v$).

Taking the pull-back of $\Omega_{A/O_K}^g$ and metrics via the neutral section $e : \text{Spec}(O_K) \to A$, we obtain a metrised line bundle on $\text{Spec}(O_K)$ (i.e. a projective $O_K$-module of rank 1):

$$\omega_{A/O_K} := e^* \Omega_{A/O_K}^g .$$

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

$$h_{\text{Fal}}(A/K) = \frac{1}{[K : \mathbb{Q}] \deg_{\text{Ar}}(\omega_A/O_K, ||.||)} = -\frac{1}{[K : \mathbb{Q}]} \log \prod_{v \in \mathcal{M}_K} ||s||_v,$$

for any section $s$. The Faltings’ height denoted by Rémond by $h(A)$ corresponds, with our notations, to $h_{\text{Fal}}(A/K) - \log(2^g/2).

It is well known that

$$\deg_{\text{Ar}}(\omega_A/O_K, ||.||) = \log \text{card}(\omega_A/O_K/sO_K) - \sum_{v \mid \infty} \log ||s||_v.$$

The height defined in the same way but, over a number field extension where $A$ has semi-stable reduction, is called stable Faltings’ height. We denote it by $h_{\text{stab}}(A)$. It doesn’t depend on the ground field and it satisfies

$$h_{\text{stab}}(A) \leq h_{\text{Fal}}(A/K),$$

with equality if, and only if, $A/K$ is semi-stable.

3 On the Birch and Swinnerton-Dyer conjecture

We can now give a classical generalisation of a conjecture of Hasse-Weil and state the celebrated conjecture of Birch and Swinnerton-Dyer (see, e.g., [BSD65] for the case of elliptic curves and [Gro82] for a general formulation for an abelian variety defined over an arbitrary number field).

**Conjecture 3.1 (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]). See also [PT15] and [BFTP18] and, for elliptic curves defined over a real quadratic field, [FLHS15].

**Conjecture 3.2 (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 $L^*(A/K, 1) = \lim_{s \to 1} \frac{L(A/K, s)}{(s-1)\zeta(A(K))}$ in the Taylor expansion of $L(A/K, s)$ at $s = 1$ satisfies

$$L^*(A/K, 1) = |\text{III}(A/K)| \cdot \text{Reg}(A(K)) \cdot |A(K)_{\text{tors}}|^{-1} \cdot |\hat{A}(K)_{\text{tors}}|^{-1} \cdot c(A/K) \cdot D_K^{g/2}. \ (18)$$
In the 70’s and 80’s, striking progress was achieved on the BSD-conjecture, providing evidence for its truth ([CW77], [GZ86], [Rub87], [Ko88]). 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., up to some factor term. More recently, more evidence arises from [BS15]. See also the references in [KT03], in particular for the function field case, where much more is known.

In this section we bound the product \( |\text{III}(A/K)| \cdot \text{Reg}(A/K) \) from above. In order to do it, the formula (18) of the BSD-conjecture suggests to bound each one of the remaining terms. This is done in the following lemmas.

### 3.1 Bound for the leading coefficient \( L^*(A/K, 1) \)

For his algorithm, Manin deals with the case when \( A = E \) is an elliptic curve and \( K = \mathbb{Q} \) ([Man71] Theorem 11.1]). Following his notations, let’s consider the Dirichlet expansion of the \( L \)-series \( L(E/\mathbb{Q}, s) = \sum_{n=1}^{\infty} a_n n^{-s} \) and set \( F(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z} \). Then \( F \) is holomorphic in the upper half-plane. He then uses (several times) the Hecke functional equation \( F(z) = \varepsilon N^{-1} z^{-2} F\left(-\frac{1}{N^2}\right) \), where \( N > 0 \) is the conductor of \( E \), and the fact that the sequence \( (a_n) \) does not grow faster than \( O(n^c) \) for some \( c > 0 \). (In fact, in this case, \( |a_n| \leq n^{1/2}\tau(n) \), where \( \tau(n) \) is the number of divisors of \( n \).) See also Theorem 9.3 a), Remarks 9.7 and Section 11.3 of loc. cit.

Classically, when looking forward to bound the leading coefficient of such \( L \)-series, one proceeds in three steps. First, a bound could be easily given for \( |\Lambda(s)| \) in the half-plane defined by \( \Re(s) > 3/2 \), using the Hasse-Weil bound. Second, using the functional equation, one proves that the bound is still valid in the other half-plane defined by \( \Re(s) < 1/2 \). What is missing, is to bound it in the vertical strip defined by \( 1/2 < \Re(s) < 3/2 \). However, in each case when Conjectures 3.1 and 3.2 are proven, it is also proven that \( |\Lambda(s)| \) is bounded in this vertical strip (even if it doesn’t follow formally from Conjectures 3.1 and 3.2 but, e.g. from modularity).

Here we use the Hasse-Weil bound for bounding \( |\Lambda(s)| \) in the right-half-plane \( \Re(s) > 3/2 \), the functional equation for the \( \Lambda \)-series (Conjecture 3.1) to bound it in the left-half-plane \( -1/2 < \Re(s) \), and the classical convexity argument as in the Phragmén-Lindelöf principle (see [PL08] or [Tit75] section 5.61 page 177)) to bound it in the vertical strip \( -1/2 \leq \Re(s) \leq 3/2 \). Nevertheless, in order to apply the Phragmén-Lindelöf principle, we will use a hypothesis on the order of growth of the \( \Lambda \)-series, Hypothesis 3.5 as in (20) below. In some sense, this condition replaces the condition on the growth of the sequence \( (a_n) \) of the coefficients of the \( L \)-series used by Manin. We conclude by applying the Cauchy inequality in two different ways so as to obtain different kinds of bounds for the leading coefficient \( L^*(A/K, 1) \).

**Lemma 3.3 (Phragmén-Lindelöf)** Let \( f(z) \) be an analytic function of \( z = re^{i\theta} \), regular in the region \( D \) between two straight lines making an angle \( \pi/\alpha \) at the origin, and on the lines themselves. Suppose that

\[
f(z) \leq M
\]

on the lines, and that,

\[
f(z) = O(e^{r^\beta}), \text{ as } r \to \infty, \text{ where } \beta < \alpha,
\]

uniformly in the angle. Then actually, the inequality \( f(z) \leq M \) holds throughout the region \( D \).
We will use the above result when the angle is transformed into a strip.

**Lemma 3.4** Let $\varepsilon > 0$ be any positive number. Set $\alpha(\varepsilon) = \frac{\pi}{2} + \varepsilon$. Let $\phi(s)$ be an analytic function, regular in the strip $S$ between the two parallel lines $\sigma = 3/2 + \varepsilon$ and $\sigma = 1/2 - \varepsilon$, and on the lines themselves. Suppose that

$$\phi(s) \leq M$$
onumber

on the lines, and that,

$$\phi(s) = O(e^{\varepsilon|\rho|}), \text{as } \tau = \Im(s) \to \infty, \text{where } \rho < \alpha(\varepsilon),$$

uniformly in the angle. Then actually, the inequality $\phi(s) \leq M$ holds throughout the strip $S$.

**Proof of Lemma 3.4** We use the notation $z = re^{i\theta}$, $r \geq 0$, in the region $D$ of the complex plane defined by $|\theta| \leq \frac{\pi}{2\alpha(\varepsilon)}$. We set $s = i\log z + 1$, and $f(z) = \phi(s)$. In this way, the two straight lines making an angle $\pi/2$ at the origin are transformed into two parallel lines $\sigma = 3/2 + \varepsilon$ and $\sigma = 1/2 - \varepsilon$. The origin is sent to the “infinity” of the negative part of the imaginary axis. The imaginary part of our variable $\sigma$ satisfies the following bounds:

$$\Im(s) = \log |\rho| + 1, \text{uniformly.}$$

Then actually, the inequality $\phi(s) \leq M$ holds throughout the strip $S$. \hfill $\square$

**Hypothesis 3.5** Let $A/K$ be an abelian variety defined over a number field. The $\Lambda$-series of $A/K$ satisfies

$$|\Lambda(A/K, s)| = O(e^{\varepsilon|\rho|}), \text{as } \tau = \Im(s) \to \infty, \text{where } \rho \leq \frac{\pi}{2}, \text{uniformly.}$$

**Remark 3.6** Hypothesis 3.5 is less stringent than being of finite order. One expects that the $\Lambda$-series of an abelian variety is always of finite order. For example, $\Lambda$ is of order 1 in the case of an elliptic curve over $\mathbb{Q}$. Indeed, as soon as the $L$-series $L(s) = \sum_{n=1}^{\infty} a_n n^{-s}$ is the Mellin transform of a function $F(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}$, which is modular, and satisfies $a_n = O(n^\varepsilon)$, one can apply Hecke’s lemma (see [Wei67, Lemma 1], B $\Rightarrow$ A) to bound $|\Lambda(s)|$ in a vertical strip, say $-3 \leq \Re(s) \leq 5$. We then bound $|\Lambda(s)|$ for $\Re(s) \geq 5$. Using again the Hecke functional equation for $F$, the bound also holds in the half plane $\Re(s) \leq -3$. Then, for $|s| = R \gg 1$, $|\Lambda(s)| \ll e^{R\log R}$ and we conclude that the normalised $\Lambda$-series is of order 1.

As it is well known, the further condition (20), and thus Hypothesis 3.5, is required to apply the Phragmén-Lindelöf theorem. Indeed, wild functions such as $e^{\varepsilon^2}$, on the strip $|\Im(z)| < \frac{\pi}{2}$, are not bounded by their maximum on the boundary. This function doesn’t satisfy (20).

**Lemma 3.7** Let $A/K$ be an abelian variety of dimension $g$ satisfying Conjecture 3.1 and Hypothesis 3.5. Let $r = \max_{s=1}^{\infty} L(A/K, s)$ and $F = N_{K/\mathbb{Q}}(F_{A/K})$. Then the leading coefficient of the $L$-series of $A/K$ at $s = 1$ satisfies the following bounds:

$$|L^*(A/K, 1)| \leq (9/2\pi)^g |K:\mathbb{Q}|^{1/2} \cdot D_K^g$$

$$|L^*(A/K, 1)| \leq e \cdot 2^r \cdot (6/5)^g |K:\mathbb{Q}|^{1/2} \cdot F^{1/2} \cdot D_K^g \cdot (\log(F \cdot D_K^g))^{2g |K:\mathbb{Q}|}. \quad (22)$$

---

$^3$The order of the function $f$ is $\inf_{m} \{ f(z) = O(e^{\varepsilon|z|^m}) \}$, as $|z| \to \infty$ = $\lim_{R \to \infty} \frac{\log \log \max_{|z| \leq R} |f(z)|}{\log R}$. 

13
Before proving the lemma, let us explain why we give two different bounds.

**Remark 3.8** The upper bounds (21) and (22) depends on $g$, $[K : \mathbb{Q}]$, $\mathcal{F}$ and $D_K$. The bound (22) also depends on the order of the $L$-series at 1, here denoted by $r$. Conjecturally, $r$ equals the rank of $A(K)$. When $g = 1$ and $K = \mathbb{Q}$, it is expected that $\text{rk}(E(\mathbb{Q})) = 0$ or 1. In this case, the bound (21) is sharper than (22) as soon as $\mathcal{F} \geq 6$. Moreover, as pointed out in [BS14], the dependence of these bounds on the number field could play an important role in some applications. Concerning the rank, Ooe and Top [OT89] proved the following bound:

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

(23)

where $\gamma_1, \gamma_2$ and $\gamma_3$ are positive real numbers depending only on $g$ and $[K : \mathbb{Q}]$ (see [Rém10, Proposition 5.1] for explicit computations of $\gamma_1, \gamma_2$ and $\gamma_3$). Using (23), we deduce from (22) a bound independent of the rank, which growth in $\mathcal{F}$ and $D_K$ is as:

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

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, which is sharper than (21).

**Proof of Lemma 3.7** Let us consider the abelian variety $A' = \text{Res}_KA$ 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 $g' = g[K : \mathbb{Q}]$. Furthermore

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

(24)

The Hasse-Weil bound gives $P_{A', \rho}(T) = \prod_{i=1}^{g'} (1 - \alpha_i T)$, where $\rho = \deg(P_{A', \rho}) \leq 2g'$ 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

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

hence

$$|L(A'/\mathbb{Q}, s)| \leq \zeta(\sigma - \frac{1}{2})^{2g'}.$$
Since $|\zeta(1 + \epsilon)| \leq (1 + \frac{1}{\epsilon})$, for $\epsilon > 0$, it follows that
\[
|\Lambda(A'/Q, \frac{3}{2} + \epsilon + i\tau)| \leq M(\epsilon),
\] (25)
with $M(\epsilon) = \mathcal{F}^{\frac{3}{2} + \frac{1}{2}} \cdot (2\pi)^{-g'(\frac{3}{2} + \epsilon)} \cdot \Gamma\left(\frac{3}{2} + \epsilon\right)^{g'} \cdot (1 + \frac{1}{\epsilon})^{2g'}$.

Using the functional equation, that is, Conjecture 3.1, the same bound (25) is valid for $|\Lambda(A'/Q, \frac{1}{2} - \epsilon - i\tau)|$.

We now apply Lemma 3.4 to the function $\Lambda(A'/Q, s)$, which is regular into the strip between the two parallel lines $\sigma = 3/2 + \epsilon$ and $\sigma = 1/2 - \epsilon$ and satisfies the bound (25) on these lines. Since we supposed that $\Lambda(A'/Q, s) = \Lambda(A/K, s)$ satisfies Hypothesis 3.3, a suitable choice for $\epsilon$ (made at the end of our proof) makes that condition (20) is satisfied. We then conclude that the bound (25) is still valid throughout the strip, that is, 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 $\mathbb{D}(1, \frac{1}{2} + \epsilon)$, we obtain
\[
L^*(A'/Q, 1) = \frac{(2\pi)^{g'} \Lambda(r)(A'/Q, 1)}{\sqrt{\mathcal{F}^r}} \leq \frac{(2\pi)^{g'} \Gamma\left(\frac{3}{2} + \epsilon\right)^{g'} \left(1 + \frac{1}{\epsilon}\right)^{2g'}}{\max_{s \in \mathbb{D}(1, \frac{1}{2} + \epsilon)} \Lambda(A'/Q, s)}.
\]

The upper bound (25) gives
\[
L^*(A'/Q, 1) \leq \frac{1}{(\frac{1}{2} + \epsilon)^{g'}} \cdot (2\pi)^{-g'(\frac{1}{2} + \epsilon)} \cdot \mathcal{F}^{\frac{3}{2} + \frac{1}{2}} \cdot \Gamma\left(\frac{3}{2} + \epsilon\right)^{g'} \cdot \left(1 + \frac{1}{\epsilon}\right)^{2g'}.
\]

To prove (21), we choose $\epsilon = \frac{1}{2}$ and obtain
\[
L^*(A'/Q, 1) \leq \left(\frac{9}{2\pi}\right)^{g'} \cdot \sqrt{\mathcal{F}^{A'/Q}}.
\]

To prove (22), we take $\epsilon = \frac{2}{\log \mathcal{F}}$. (Remark that, since $A'$ is defined over $\mathbb{Q}$, $F_{A'/Q} > 3$ and $\log F_{A'/Q} \neq 0$.) Thus $(\frac{1}{2} + \epsilon)^{-r} \leq 2^r$ and $\mathcal{F}^{\frac{3}{2} + \frac{1}{2}} = e \cdot \mathcal{F}^{\frac{3}{2}}$. Since the abelian variety $A'$ is defined over $\mathbb{Q}$ and satisfies Conjecture 3.1, we have [Mes86, Section 3, Proposition]}

\[
\mathcal{F}^r = F_{A'/Q} > 10^{g'}.
\] (26)

Then, $1 + \frac{1}{\epsilon} \leq \log \mathcal{F}$ and $\frac{1}{\epsilon} + \epsilon \in [\frac{1}{2}, \frac{3}{2}]$, and therefore $\Gamma\left(\frac{3}{2} + \epsilon\right) = (\frac{1}{2} + \epsilon)\Gamma\left(\frac{1}{2} + \epsilon\right) \leq \frac{3}{2}\sqrt{\pi} < 3$.

Moreover $3^{g'} \cdot (2\pi)^{-g'(1/2+\epsilon)} = \left(\frac{3}{(2\pi)^{1/2+\epsilon}}\right)^{g'} \leq \left(\frac{6}{\pi}\right)^{g'}$. This gives
\[
L^*(A'/Q, 1) \leq 2^r \cdot e \cdot (6/5)^{g'} \cdot \mathcal{F}^{\frac{3}{2}} = (\log \mathcal{F}^{A'/Q})^{2g'}.
\]

We conclude both cases by applying (21). It remains to be shown that the hypothesis on the growth of the $\Lambda$-series is satisfied by both choices of $\epsilon$. In fact, for $\epsilon = \frac{1}{2}$, $\alpha(\epsilon) = \frac{\pi}{2}$. For $\epsilon = \frac{2}{\log \mathcal{F}}$, using that $\mathcal{F}^r > 2$, we obtain $\alpha(\epsilon) = \pi \times (\frac{4}{\log 2} + 1)^{-1} \leq \frac{\pi}{2}$. \(\square\)

For avoiding the use of Conjecture 3.1 a second time, instead of (20) we can use $\mathcal{F}^r > 3$ and obtain
\[
L^*(A'/Q, 1) \leq e \cdot 2^r \cdot 5^{g'} \cdot \mathcal{F}^{\frac{3}{2}} \cdot (1 + \frac{1}{2} \log \mathcal{F}^{A'/Q})^{2g'}.
\]
3.2 Bound for the local factor

Is in this section where we assume that $A$ is principally polarised. For Lemma 3.10 this hypothesis is technical. It can be removed from Theorem 3.12 as in the version given in [GR14b Théorème 1.1]. Nevertheless, the exposition is simplified here, and we also use it in order to make evident the $\Im \tau_v$ in the matrix lemma (Theorem 3.12 and Lemma 3.13 and 3.14).

We will bound the local periods $c_v$. For every non-archimedean place $v$, the numbers $c_v$ are non-zero integers and can be bounded from below by 1.

As for the archimedean local periods, in order to relate them to the Faltings’ height, we need some preliminaries.

For $v$ complex, the local period $c_v$ is almost the norm $||\omega||_v$ of $\omega$ (up to the normalisation of the Hermitian metric, see Lemma 3.9), while for $v$ real, it is a little bit more delicate to link the local period $c_v$ with the norm $||\omega||_v$ (see Lemma 3.10).

We fix an archimedean place $v$ of $K$. Recall that $(\gamma_1,v,\ldots,\gamma_{2g},v)$ is a basis of the integral homology $H = H_1(A(\overline{K}_v),\mathbb{Z})$ of $A$, chosen so that $\gamma_1,v,\ldots,\gamma_{2g},v$ generates the part of $H$ fixed by complex conjugation.

Let

$$\Omega_1,v = \left( \int_{\gamma_{i,v}} \omega_j \right)_{1 \leq i \leq g} \quad \text{and} \quad \Omega_2,v = \left( \int_{\gamma_{i,v}} \omega_j \right)_{g+1 \leq i \leq 2g}$$

be the periods matrixes associated to $\gamma_1,v,\ldots,\gamma_{2g},v$, where $j$ runs over $\{1,\ldots,g\}$. Moreover, since $A$ is principally polarised, we can choose $\gamma_1,v,\ldots,\gamma_{2g},v$ such that

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

is a symmetric matrix in the Siegel space, that is, $\Im \tau_v$ is definite positive. Let $\Lambda_v = \Omega_{1,v} \mathbb{Z}^g + \Omega_{2,v} \mathbb{Z}^g$ be the associated lattice. Choose an isomorphism over $\mathbb{C}$

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

such that the inverse function of $\varphi$ maps the invariant differential $\eta = \omega_1 \wedge \ldots \wedge \omega_g$ to $dz$:

$$\varphi^*(\eta) = dz.$$

Let $\Gamma_v = \mathbb{Z}^g + \tau_v \mathbb{Z}^g = \Omega_{1,v}^{-1} \Lambda_v$ and choose also an isomorphism over $\mathbb{C}$

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

such that

$$\psi^*(\eta) = \det \Omega_{1,v} dz.$$

We deduce the next result from Rémond’s work [Rém97].

**Lemma 3.9** For a complex place $v$, we have

$$c_v = 2^g ||\eta||_v.$$  \hfill (28)

**Proof.** We use the module measure of the differential form $\eta$, (15) and (16):

$$c_v := \left| \det \left( \int_{\gamma_i} \omega_j \right)_{1 \leq i,j \leq 2g} \right| = \int_{A(\overline{K}_v)} \mod (v) = \int_{A(\mathbb{C})} |\eta \wedge \overline{\eta}| =: 2^g ||\eta||_v.$$
Lemma 3.10 We suppose that $A$ carries a principal polarisation. For a real place $v$, we have

$$c_v = \frac{|A_v(\mathbb{R}) : A_v(\mathbb{R})^0|}{\sqrt{\det \Im(\tau_v)}} ||\eta||_v.$$

Proof. By definition of $c_v$ and $\Omega_{1,v}$ we have

$$c_v := |A_v(\mathbb{R}) : A_v(\mathbb{R})^0| \cdot \left| \det \left( \int_{\mathcal{C}_v} \omega_j \right) \right|_{1 \leq i, j \leq g} =: |A_v(\mathbb{R}) : A_v(\mathbb{R})^0| \cdot |\det \Omega_{1,v}|.$$

Then, using the definition of the metric for $v$ real and the inverse map of $\psi$ we compute

$$||\eta||_v^2 = ||\eta||_{v'}^2 = \frac{1}{2g} \int_{\mathcal{A}(\mathcal{K}_v)} |\eta \wedge \eta| = \frac{1}{2g} \int_{\mathcal{C}_v} |\det \Omega_{1,v}|^2 \left| dz \wedge \overline{dz} \right|$$

$$= \frac{1}{2g} |\det \Omega_{1,v}|^2 \int_{\mathcal{C}_v/(\mathbb{Z}^g + \tau_v \mathbb{Z}^g)} 2^g \left| dx \wedge dy \right| = |\det \Omega_{1,v}|^2 \det \Im(\tau_v).$$

For the last equality we use that $\int_{\mathcal{C}_v/(\mathbb{Z}^g + \tau_v \mathbb{Z}^g)} \left| dx \wedge dy \right|$ is the area of a fundamental domain for $\mathbb{C}^g/(\mathbb{Z}^g + \tau_v \mathbb{Z}^g)$, which is $\det \Im(\tau_v)$. Then

$$||\eta||_v = \frac{\sqrt{\det \Im(\tau_v)}}{|A_v(\mathbb{R}) : A_v(\mathbb{R})^0|} c_v.$$

We then deduce the following result for $c_\infty(A/K)$.

Lemma 3.11 We assume that $A$ carries a principal polarisation. The archimedean local factor defined in (13) satisfies

$$c_\infty(A/K) = 2^g \prod_{v \text{ real}} \frac{|A_v(\mathbb{R}) : A_v(\mathbb{R})^0|}{\sqrt{\det \Im(\tau_v)}} \cdot e^{-[K:Q]h_{\text{alt}}(A/K)},$$

where $t$ is the number of complex places of $K$.

Proof. Recall that $H^0(A, \Omega_{A/\mathcal{O}_K}^g) = \eta \cdot a_\eta$. Recall also that, by the product formula, $\sum_{v \in \mathcal{M}_K} \log ||\eta||_v = \sum_{v \in \mathcal{M}_K} \log ||k\eta||_v$, for all $k$ in $K$. Then to compute the degree of $\omega_{A/\mathcal{O}_K}$, we choose the invariant differential $\eta$:

$$[K : \mathbb{Q}]h_{\text{alt}}(A/K) = \deg_{A,\mathcal{O}_K}(\omega_{A/\mathcal{O}_K}, ||.||) = \log ||\eta_{a_\eta}/\eta\mathcal{O}_K|| - \sum_{v|\infty} \log ||\eta||_v.$$

On the one hand, $||\eta_{a_\eta}/\eta\mathcal{O}_K|| = |a_\eta/\mathcal{O}_K| = |\mathcal{O}_K/a_\eta^{-1}| = N_{K/\mathbb{Q}}(a_\eta^{-1}).$

On the other hand, from Lemma 3.9 and Lemma 3.10 we deduce that the product of the archimedean local periods satisfies the following equality

$$\prod_{v|\infty} ||\eta||_v = \prod_{v \text{ real}} \frac{\sqrt{\det \Im(\tau_v)}}{|A_v(\mathbb{R}) : A_v(\mathbb{R})^0|} \cdot \prod_{v \text{ complex}} \frac{1}{2g} \prod_{v|\infty} c_v.$$
and then

\[ [K : \mathbb{Q}] h_{\text{Fal}}(A/K) = \log N_{K/\mathbb{Q}}(a_0^{-1}) - \sum_{v | \infty} \log c_v - \sum_{v \text{ real}} \log \frac{\sqrt{\det(\tau_v)}}{|A_v(\mathbb{R}) : A_v(\mathbb{R})^0|} + \sum_{v \text{ complex}} \log(2^g). \]  

(29)

Since, by definition [13], \( c_\infty(A/K) = N_{K/\mathbb{Q}}(a) \cdot \prod_{v \in M_K^\infty} c_v \), we can conclude. \( \square \)

Remark that it is the Faltings’ height on \( K \), instead of the stable one, which appears naturally in the proof.

It is worth noting that Rémond [Rémond97, Lemme II.3.1] proves an analog result to our Lemma 3.10, without the assumption that the polarisation is principal.

Nevertheless, in order to apply the matrix lemma and relate the local periods with the Faltings’ height, we will assume later that \( A \) carries a principal polarisation.

To state his result, let’s fix an archimedean place \( v \) of \( K \). Denote \( \Lambda = H_1(A_v(\mathbb{A}_v), \mathbb{Z}) \) the integral homology of \( A_v \), \( \Lambda^+ \) its sub-module fixed by complex conjugation, and \( \Lambda^- \) the biggest sub-module of \( \Lambda \) in which the complex conjugation induces \( -i \). Let’s fix \((\gamma_1,v,\ldots,\gamma_g,v)\) a basis for \( \Lambda^+ \), and \((\gamma_{g+1},v,\ldots,\gamma_{2g},v)\) a basis for \( \Lambda^- \). Let \( M_v \) be a matrix of \( GL_g(\mathbb{C}) \) such that

\[(\gamma_{g+1},v,\ldots,\gamma_{2g},v) = M_v(\gamma_1,v,\ldots,\gamma_g,v).\]

Since \( M_v \) depends on the choice of the basis up to a multiplication by an element of \( GL_g(\mathbb{Z}) \), its determinant is well defined up to a sign. Let’s choose the basis such that \( \det(\mathcal{M}_v) > 0 \).

Then the transcription of [Rémond97, Lemme II.3.1 p.18] with our notations and normalisations reads as

\[ c_v = 2^g \frac{|A_v(\mathbb{R}) : A_v(\mathbb{R})^0|^{\frac{1}{2}}}{\sqrt{\det(\mathcal{M}_v)}} |\eta_v|, \]  

(30)

for a real place \( v \), and his Corollaire II.3.1 gives

\[ c_\infty(A/K) = \prod_{v \text{ real}} \frac{|A_v(\mathbb{R}) : A_v(\mathbb{R})^0|^{\frac{1}{2}}}{\sqrt{\det(\mathcal{M}_v)}} \cdot 2^{\frac{|\mathbb{K} : \mathbb{Q}|}{2}} \cdot e^{-[K:Q] h_{\text{Fal}}(A/K)}. \]  

(31)

In order to compare our results with Rémond’s ones, recall that, we have chosen \( \tau_v = \Omega_{1,v}^{-1}\Omega_{2,v} \), where \( \Omega_{1,v} \) and \( \Omega_{2,v} \) are the periods matrixes associated to \( \gamma_1,v,\ldots,\gamma_{2g},v \) defined by [27], being a symmetric matrix in a fundamental domain.

We then have an induced isomorphism \( A(\mathbb{K}_v) \simeq \mathbb{C}^g/\Gamma_v \) with \( \Gamma_v = \mathbb{Z}^g + \tau_v \mathbb{Z}^g \) and, with the above notation, \( \Lambda \simeq \Gamma_v = \mathbb{Z}^g + \tau_v \mathbb{Z}^g \). Then \( \Lambda^+ \simeq \mathbb{Z}^g \) and \( \Lambda^- \simeq M_v^c \mathbb{Z}^g \). Moreover \( \Lambda^+ \oplus \Lambda^- = \mathbb{Z}^g + M_v^c \mathbb{Z}^g \subset \Lambda = \mathbb{Z}^g + \tau_v \mathbb{Z}^g \).

On the one hand, the index satisfies the following equalities.

\[ [\Lambda : \Lambda^+ \oplus \Lambda^-] = \frac{\text{Vol}(\Lambda)}{\text{Vol}(\Lambda^+ \oplus \Lambda^-)} = \frac{\text{Covol}(\Lambda^+ \oplus \Lambda^-)}{\text{Covol}(\Lambda)} = \frac{\det(\mathcal{M}_v)}{\det(\mathcal{M}_v)}. \]

On the other hand, we have (see the proof of [Rémond97, Lemme II.3.1]),

\[ [\Lambda : \Lambda^+ \oplus \Lambda^-] = \frac{2^g}{|A_v(\mathbb{R}) : A_v(\mathbb{R})^0|}. \]

This gives

\[ \det(\mathcal{M}_v) = \frac{|A_v(\mathbb{R}) : A_v(\mathbb{R})^0|}{2^g} \det M_v. \]
for all non-zero $\omega$ we denote with a sub-index polarisation $L$.

Theorem 3.12 (Autissier) Suppose that the abelian variety $A$, $L$ carries a principal polarisation. Then $\lambda(A/K) = \frac{1}{3} h(A) + 6g$.

Lemma 3.13 For $L$ a principal polarisation and $v$ an archimedean place, we have

$$\rho(A_v, L_v)^{-2} \geq \frac{1}{g} (\det \mathcal{T}_v)^{1/9}.$$  

Proof. We choose to use the parametrisation $A(K_v) \simeq \mathbb{C}^g / \Gamma_v$, with $\Gamma_v = \mathbb{Z}^g + \tau_v \mathbb{Z}^g$. Then, for $z \in \mathbb{C}^g$, we denote $||z||_{L_v}^2 = ||z||_{\Gamma_v}^2 = H(z, z) = t_z(\mathcal{T}_v)^{-1} t_{\bar{z}}$.

We apply Minkowski’s theorem to the lattice $\Gamma_1 = \mathbb{Z}^g \subset \Gamma_v$, that is, $\lambda_1(\Gamma_1)^g \text{Vol}(\Gamma_1) \leq 2^g$, where $\lambda_1(\Gamma_1)$ is the first minimum of $\Gamma_1$ for the norm $||z||_{\Gamma_v}$. We then have

$$\lambda_1(\Gamma_1)^g \leq 2^g \frac{\text{Covol}(\Gamma_1)}{\text{Vol}(B)},$$

where $B$ is the unit ball. On one hand, for the chosen norm we have $\text{Covol}(\Gamma_1) = (\det \mathcal{T}_v)^{-1/2}$. On the other hand, the unit ball $B$ contains $[-\frac{1}{\sqrt{g}}, \frac{1}{\sqrt{g}}]^g$, and then $\text{Vol}(B) \geq \frac{2^g}{g^{g/2}}$. Hence

$$\lambda_1(\Gamma_1)^g \leq \frac{2^g}{g^{g/2}} \sqrt{\det \mathcal{T}_v}.$$
Since \( \rho(A_v, \mathcal{L}_v) := \lambda_1(\Gamma_v) \leq \lambda_1(\Gamma_1) \), we then have

\[
\rho(A_v, \mathcal{L}_v) \leq \frac{g^{1/2}}{(\det \mathbb{Z}_v)^{1/2}}
\]

and we can conclude. \( \square \)

We then deduce from Theorem 3.12 the next matrix lemma, involving \( \tau_v \).

**Lemma 3.14** Suppose that the abelian variety \((A, \mathcal{L})\) carries a principal polarisation. The sum of the determinants of the matrices \( \mathbb{Z}(\tau_v) \) satisfies

\[
\frac{1}{g[K : \mathbb{Q}]} \sum_{v \in M_K} (\det \mathbb{Z}(\tau_v))^{1/g} \leq 3h_{Stab}(A) + 6g.
\]

Nevertheless, in the case of an elliptic curve, we could work directly with the Faltings' height. In fact, for \( A \) an elliptic curve, we have \((CS86, \text{Prop. 1.1 of Chap. X})\)

\[
12[K : \mathbb{Q}]h_{Falt}(A/K) = \log N_{K/\mathbb{Q}} \Delta_{A/K} - \sum_{v | \infty} n_v \log |\Delta(\tau_v)| - \sum_{v | \infty} 6n_v \log |\mathbb{Z}(\tau_v)|,
\]

(32)

where \( \Delta_{A/K} \) is the minimal discriminant of the elliptic curve, and \( \Delta(\tau) \) is the modular form \((2\pi)^{12}q \prod_{n=1}^{\infty} (1 - q^n)^{24} \), where \( q = e^{2\pi i \tau} \).

It is worth noting that this is an analogous formula to (29). On the right hand term, the first term involves an ideal of \( K \), that is \( a_\ell \), and, resp. \( \Delta_{A/K} \). The second term of (29) involves the uniformization \( \varphi : \mathbb{C}^g/L_v \rightarrow A(K_v) \). In fact, by definition, for the real archimedean places, the \( c_v \) are related to the matrix \( \Omega_{1,v} \) and \( \Lambda_v = \Omega_{1,v}Z^g + \Omega_{0,v}Z^g = \Omega_{1,v}(Z^g + \tau_vZ^g) \).

In formula (32), \( \Delta(\tau_v) \) is the discriminant of the equation of the curve defined by the parametrization \( \mathbb{C}^{g}/(Z + \tau_vZ) \rightarrow A(K_v) \). Both third terms involve \( \mathbb{Z}(\tau_v) \). Observe that, while in (32) all the archimedean places are involved in this third term, in (29), only the real ones appear, and some parts of the \( \tau_v \) are hidden in the second term. This is because, in the second term of (29), for the real places, the \( c_v \) are related to \( \Omega_{1,v} \), and the parametrization is the one related to the lattice \( \Omega_{1,v}(Z^g + \tau_vZ^g) \), while in (32), the lattice is \( Z + \tau_vZ \). (The fourth term is there because the normalisation of the norm that we use to define Faltings' height.) However, the proof of both formulas are close, and they involved the area of the fundamental domain of the lattice.

Moreover, if we work out the third term (the one with the \( \mathbb{Z}(\tau_v) \)), e.g. with a matrix lemma, we could obtain a relation between the height of the variety \( h_{Falt}(A/K) \) and the local numbers \( c_\infty(A/K) \). That is what we will do in Lemma 3.17 in general dimension. In fact, we deduce from Lemma 3.11 a lower bound for \( c_\infty(A/K) \), in terms of the Faltings' height, the degree \( [K : \mathbb{Q}] \) and the dimension \( g \). It is this lower bound, which we will use to prove the main results.

Conversely, we point out that, if we work out the second term (which is \( |\Delta(\tau_v)| \) for (32)), we could obtain a relation between \( h_{Falt}(A/K) \) and the \( \mathbb{Z}(\tau_v) \), that is, a matrix lemma. That is what we will do in Lemma 3.15 where we recover the same kind of result as in Lemma 3.14 in the one-dimensional case.

\[\footnote{Remark that we could relate this with the parametrization we used before, that is \( A(K_v) \simeq \mathbb{C}^g/\Lambda_v \), with \( \Lambda_v = \Omega_{1,v}Z^g + \Omega_{0,v}Z^g \). Indeed, we could define \( ||z||^2_{\Lambda_v} = H'(z, z) = t_z \Omega_1^{-1}(\mathbb{Z}_{\tau_v})^{-1}\Omega_1z \), since \( \mathbb{H}'(\Lambda_v, \Lambda_v) \subset \mathbb{Z} \). Denote \( \lambda_1(\Omega_{1,v}Z^g) \) the first minimum of the lattice \( \Omega_{1,v}Z^g \) for the norm \( ||z||^2_{\Lambda_v} \). We then have \( \lambda_1(Z^g) = \lambda_1(\Omega_{1,v}Z^g) \).} \]
Lemma 3.15 If \( g = 1 \), the following bound also holds
\[
\frac{1}{[K : \mathbb{Q}]} \sum_{v \in M_K} \Im(\tau_v) \leq 3h_{\text{Fal}}(A/K) + \frac{11}{2}.
\]

Proof. We use the formula (32).
We estimate then each of the three terms on the right hand side. First, \( \log N_{K/Q} \Delta_{A/K} \geq 0 \).
Second, \( \log \Im(\tau_v) \leq \frac{1}{6}\Im(\tau_v) \), hence \( -\sum_{v|\infty} 6n_v \log \Im(\tau_v) \geq -\frac{6}{\pi} \sum_{v|\infty} n_v \Im(\tau_v) \).
As for the second term, we use the estimate (see exercise on page 256 of loc. cit., where we corrected the missprint for the modular form),
\[
\log |\Delta(\tau_v)| = \log |(2\pi)^{12}q_r| + A_r, \text{ with } |A_r| \leq \frac{1}{9}.
\]
Thus
\[
\log |\Delta(\tau_v)| \leq -2\pi \Im(\tau_v) + \log \left( (2\pi)^{12} e^{1/9} \right).
\]
We obtain
\[
\frac{1}{[K : \mathbb{Q}]} \sum_{v|\infty} \Im(\tau_v) \leq \frac{1}{[K : \mathbb{Q}]} \sum_{v|\infty} n_v \Im(\tau_v) \leq \frac{12}{2\pi - 6/e} h_{\text{Fal}}(A/K) + \frac{\log \left( (2\pi)^{12} e^{1/9} \right)}{2\pi - 6/e},
\]
what gives the announced bound.

Observe that Proposition 3.2 of [GR14b] (which follows from Autissier’s matrix lemma) with Remarque 3.3 of loc. cit. gives bounds in the case where \( A \) is an elliptic curve. They use Deligne’s normalisation for the stable Faltings’ height, which we denote by \( h_D(A) \), and with our notation this reads as \( h_D(A) = h_{\text{Stab}}(A) + g/2 \log \pi \). Using the fact that \( h_{\text{Stab}}(A) \leq h_{\text{Fal}}(A/K) \), we deduce the following bounds.

Lemma 3.16 If \( g = 1 \), then
\[
[K : \mathbb{Q}]^{-1} \sum_{v|\infty} \Im(\tau_v) \leq 6, 45 \max \{ h_{\text{Fal}}(A/K) + \frac{\log \pi}{2}, 1 \}
\]
and also
\[
[K : \mathbb{Q}]^{-1} \sum_{v|\infty} \Im(\tau_v) \leq 1, 92 \max \{ h_{\text{Fal}}(A/K) + \frac{\log \pi}{2}, 1000 \}.
\]

Observe that for \( h_{\text{Fal}}(A/K) \in [\frac{1}{2}, 638] \), the bound of Lemma 3.15 is sharper than the bounds of Lemma 3.16. In contrast, for \( h > 638 \), the second bound of Lemma 3.16 is of a better quality. In particular for \( h \in [638, 1000 - \frac{\log \pi}{2}] \), where it equals 1920, which is independent of the height. Moreover, for \( h > 1000 - \frac{\log \pi}{2} \), the bound 3,020 is valid too. However, all of these bounds have the shape
\[
\frac{1}{[K : \mathbb{Q}]} \sum_{v \in M_K} \Im(\tau_v) \leq m_1 h_{\text{Fal}}(A/K) + m_2,
\]
with \( m_1 \leq 6, 45 \) and \( m_2 \leq 1920 \). In what follows, to simplify the exposition and because it doesn’t matter for our purpose, we will use \( 3h + 6 \), which always holds.
Lemma 3.17 The archimedean local factor satisfies the following inequality.

\[ c_\infty(A/K)^{-1} \leq (3g[K : \mathbb{Q}]h_{\text{Falt}}(A/K) + 6g^2[K : \mathbb{Q}]) \frac{g[K : \mathbb{Q}]}{2} \cdot e^{[K : \mathbb{Q}]h_{\text{Falt}}(A/K)}. \] (33)

The weaker, but eventually more useful bound also holds.

\[ c_\infty(A/K)^{-1} \leq (6g^2[K : \mathbb{Q}] \max\{1, h_{\text{Falt}}(A/K)\}) \frac{g[K : \mathbb{Q}]}{2} \cdot e^{[K : \mathbb{Q}]h_{\text{Falt}}(A/K)}. \] (34)

Proof.
Let’s denote \( d = [K : \mathbb{Q}] \) and \( t \) the number of complex places of \( K \). Since \(|A_v(\mathbb{R}) : A_v(\mathbb{R})^0| \geq 1\), we deduce from Lemma 3.11

\[ c_\infty(A/K)^{-1} \leq \left( \frac{1}{2} \right)^g t \prod_{v \in M_K^{\text{real}}} \sqrt{\det \mathfrak{Z}(\tau_v)} \cdot e^{dh_{\text{Falt}}(A/K)}. \]

For the complex places, we use that \( \det \mathfrak{Z}(\tau_v) \geq \left( \frac{\sqrt{3}}{2} \right)^g \) (because \( \tau_v \) is a matrix in the Siegel space). Thus

\[ \prod_{v \in M_K^{\text{real}}} \sqrt{\det \mathfrak{Z}(\tau_v)} \leq \left( \frac{2}{\sqrt{3}} \right)^{\frac{g}{2}} \prod_{v \in M_K^{\text{real}}} \sqrt{\det \mathfrak{Z}(\tau_v)}. \]

Using the arithmetic-geometric inequality, we obtain

\[ \prod_{v \in M_K^{\infty}} (\det \mathfrak{Z}(\tau_v))^{1/g} \leq \frac{1}{d} \left( \sum_{v \in M_K^{\infty}} (\det \mathfrak{Z}(\tau_v))^{1/g} \right)^{d}. \]

And then,

\[ c_\infty(A/K)^{-1} \leq \left( \frac{1}{2} \right)^g \left( \frac{2}{\sqrt{3}} \right)^{\frac{g}{2}} \left( \sum_{v \in M_K^{\infty}} (\det \mathfrak{Z}(\tau_v))^{1/g} \right)^{\frac{gd}{2}} \cdot e^{dh_{\text{Falt}}(A/K)}. \]

We conclude with Lemma 3.14. The second inequality is just an easy deduction from the first one. \( \square \)

3.3 Bound for the cardinality of the torsion part
In the one-dimensional case, using the results of Merel [Mer96] and Parent [Par99] we can obtain a uniform bound for the cardinality of the torsion part of the Mordell-Weil group. In fact, Merel’s result tells us which prime numbers could divide \(|E(K)_{\text{tors}}|\) and Parent’s result gives us a bound for the powers of these primes, independent on the power.

Lemma 3.18 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

\[ |E(K)_{\text{tors}}| \leq B(d). \] (35)

On may take \( B(d) = (129(5^d - 1)(3d)^6)^2 \log(1 + 3^{d/2})^{-8} \).
Notice that the dependence on $d$ of $B(d)$ is twice exponential and not only exponential as expected in [Par99]. For the convenience of the reader, we give the details of the proof of Lemma 3.18. Before the proof, we state an analytic lemma, which will be used therein.

**Lemma 3.19** For $n \geq 1$, denote $p_1, p_2, \ldots, p_n$ the $n$ first prime numbers. As usual, denote $\theta(p_n) = \sum_{i=1}^{n} \log p_i$. For every $n \geq 2$, 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 $\sum_{i=1}^{n} \log i \geq \int_{1}^{n} \log xd\!x = n \log n - n + 1$ and $\sum_{i=2}^{n} \log(\log i) > \log 2$. From these remarks we deduce that, for $n \geq 2$,

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

Let $n \geq 4$. Then $\theta(p_n) > \frac{1}{2} n \log n \geq e$ and, since for $x \geq e$, the function $x \mapsto \frac{x}{\log x}$ is increasing, 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 $n \leq 4 \frac{\theta(p_n)}{\log \theta(p_n)}$. \hfill \Box

**Proof of Lemma 3.18** Following a result of Merel, if there is an element in $E(K)_{\text{tors}}$ 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 Oesterl´e (in an unpublished article) by $m(d) = (1 + 3d^2)^2$. We will use here Oesterl´e’s bound. Let us denote $p_1 < \ldots < p_m$ the first $m$ prime numbers, where $m$ satisfies $p_m \leq m(d)$ and $p_{m+1} > m(d)$. Since $m(d) \geq 4, m \geq 4$, and $\theta(p_m) = \log(p_1 \ldots p_m) \geq \log(2 \times 3 \times 5 \times 7) \geq e$. We also have $\theta(p_m) \leq m \log m(d)$. Applying Lemma 3.19 to $m$, we deduce that

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

For $i \in \{1, \ldots, m\}$, there exist some $n_i \geq 0$, such that $|E(K)_{\text{tors}}| \leq p_1^{n_1} \ldots p_m^{n_m}$. From [Par99, Theorem 1.2], we know that, for every $p \in \{p_1, \ldots, p_m\}$ and every non-zero integer $n$,

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

(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

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

\hfill \Box

In the general case, no such uniform bound on torsion of an abelian variety $A/K$, depending only on the dimension and the degree is known, but the following lemma suffice for our purpose.

**Lemma 3.20** Let’s $\mathcal{F} = N_{K/Q}(\mathcal{F}_{A/K})$ denote the norm of the conductor of $A/K$ and $\mathcal{G} = \max\{2, \mathcal{F}\}$. We have

$$|A(K)_{\text{tors}}| \cdot |\hat{A}(K)_{\text{tors}}| \leq \frac{5}{\log 2} \cdot (\log \mathcal{G})^{4g[K:Q]}.$$
Proof. 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 [Dus99], for $X \geq 17$, $\pi(X) \geq \frac{X}{\log X - 1}$. And by [Rob83], for $N \geq 3$, we have $\omega(N) \leq 1,3841 \cdot \frac{\log N}{\log \log N}$.

Set $Y = \log F$ and $C = \frac{5}{\log 2}$. If $F \geq \exp\left(\frac{17 \log 2}{5}\right)$, which is bigger than 10, then $F \geq 3$ and $CY = \frac{5}{\log 2} \log F \geq 17$, and we can apply the two previous results, for $N = F$ and $X = CY$. (In particular, $\log \log F \neq 0$.) We then have

$$
\pi(C \log F) - \omega(F) = \pi(CY) - \omega(e^Y) \geq \frac{CY}{\log(CY) - 1} - 1,3841 \cdot \frac{Y}{\log Y}
$$

Moreover, we could verify (e.g. with GP/Pari), that there is no $F \in [2, 11]$, for which the inverse inequality holds, that is, for all $F \geq 2, \pi(\frac{5}{\log 2} \log F) - \omega(F) \geq 2$.

We can then take two distinct primes numbers, $p$ and $q$, coprime with $\mathcal{G} = \max\{2, F\}$ and $\leq \frac{5}{\log 2} \log \mathcal{G}$. (This is clear for if $\mathcal{G} = F$. Otherwise $\mathcal{F} < 2$ and we have $\{p, q\} \subset \{3, 5\}$.)

Let $p$ and $q$ 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 $\mathcal{G}$, the ideals $p$ and $q$ do not divide the conductor of $A$. (This is clear for if $\mathcal{G} = F$. Otherwise, $\mathcal{F} = 1$, and, if $p$ or $q$ divide $\mathcal{F}_{A/K}$, then $\mathcal{F} \geq N_{K/Q}(p)$ or $\mathcal{F} \geq N_{K/Q}(q)$, which are both greater than 3, and this is not possible.) Hence $A$ has good reduction at $p$ and $q$ ([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

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

we deduce that $|A(K)_{\text{tors}}| \leq (N_{K/Q}(p) \cdot N_{K/Q}(q))^{g} \leq (pq)^g_{[K:Q]} \leq (\frac{5}{\log 2} \log \mathcal{G})^{2g_{[K:Q]}}$. We proceed in the same way for $|\hat{A}(K)_{\text{tors}}|$. Since the conductor of $\hat{A}$ is the same as the conductor of $A$ ([ST68 Corollary 2]), we can conclude. □

3.4 Bound for the product of the order of the Tate-Shafarevic group and the regulator

We first prove Proposition 3.2.

Proof of Proposition 3.2. We start by the formula 18 of Conjecture 3.2. We then bound $|L^*(A/K, 1)|$ using (22) of Lemma 3.7 the local factors using the bound (34) of Lemma 3.17 and the torsion part of $A(K)$ using Lemma 3.20. Thus, the product $|\text{III}(A/K)| \times \text{Reg}(A(K))$ is bounded from above by

$$
(2^{16} \cdot g^2 d) \cdot 2^e \cdot D_K^{\frac{1}{2}} \cdot F^\frac{1}{2} \cdot (\log G)^{4qd} \cdot (\log(F \cdot D_K^{2g}))^{2qd} \cdot e^{dh} \cdot \max\{1, h\}^{\frac{dh}{2} + 1},
$$

which could be written as in the statement of the proposition, when $\mathcal{F} \neq 1$. □

In the one-dimensional case, let’s denote $E$ the abelian variety which is an elliptic curve. Then the following bounds also hold.
Proposition 3.21 Under Hypothesis 1.1, the product of the order of the Tate-Shafarevic group and the regulator of the elliptic curve $E$ satisfy the following bounds

$$||\mathbb{I}(E/K)| \cdot \text{Reg}(E/K) \leq C_d \cdot 2^r \cdot D_K \cdot F^\frac{1}{2} \cdot (\log(F \cdot D_K^2))^{2d} \cdot e^{dh} \cdot h^{d/2},$$  \(37\)

with $C_d = e\left(\frac{\alpha\sqrt{2}}{2\pi}\right)^d \cdot d^d \cdot (129.(5^d - 1)(3d)^6)^{\frac{1+3d/2}{8}}$, and

$$||\mathbb{I}(E/K)| \cdot \text{Reg}(E/K) \leq C'_d \cdot D_K^\frac{3}{2} \cdot F^\frac{1}{2} \cdot e^{dh} \cdot h^{d/2},$$  \(38\)

with $C'_d = \left(\frac{\alpha\sqrt{2}}{2\pi}\right)^d \cdot d^d \cdot (129.(5^d - 1)(3d)^6)^{\frac{1+3d/2}{8}}$.

Proof. We start again from the formula (18) of Conjecture 3.2. To bound the local factor, we use the bound (33) of Lemma 3.17 and to bound the torsion part of the curve, we use Lemma A.2.3, of Annex A reads as follows. Let $E/K$ be an elliptic curve defined over $\mathbb{Q}$. With the same notations as in (2), his Proposition A.2.3., of Annex A reads as follows. Let $E$ be an elliptic curve defined over $\mathbb{Q}$. Suppose that $E$ verifies Conjecture 3.2. Then, for every $\epsilon > 0$, there exists a constant $C_r$, such that

$$||\mathbb{I}(E/Q) | \cdot \text{Reg}(E/Q) \leq C_r F^{\frac{1}{2} + \epsilon} H(E)^{\frac{1}{2} + \epsilon},$$

and there exist an absolute constant $C > 0$ such that

$$||\mathbb{I}(E/Q) | \cdot \text{Reg}(E/Q) \leq C F^{1/2 + \epsilon} H(E)^{1/2} (\log \max \{2, H(E)\})^{1/2}.$$

In [BS14], we use estimate (38), which is independent of the rank. However, estimate (37) gives a better dependence on the conductor, when the rank is neglected.

Remark 3.22 Being inspired by the Brauer-Siegel formula\footnote{Consider the family of all number fields $K$ with degree bounded by, say, $d_0$, when the discriminant $\Delta_K$ goes to infinity. Then $\Delta_K^{1/2+\epsilon} \ll h_K \text{Reg}_K \ll \Delta_K^{1/2+\epsilon}$, where $\text{Reg}_K$ is the regulator and $h_K$ the class number.}, one would like to also have a lower bound for the product of the order of the Tate-Shafarevic group and the canonical regulator, in terms of the height of the variety. Pacheco and Hindry [HP16] explain why the expected lower bound seems not to be the exact translation from the Brauer-Siegel formula $(H_{\text{Fal}}(A/K))^{-\epsilon} \ll ||\mathbb{I}(A/K)| \cdot \text{Reg}(A/K))$. Nevertheless, in [AHP18], an explicit lower bound for the regulator of an elliptic curve $E$ over a number field $K$ is given (and thus holds for the product with the order of the Tate-Shafarevic group), in terms of $[K : \mathbb{Q}], r = \text{rk}(E(K)), |E(K)_\text{tors}|$ and the height of the modular invariant $j_E$. Their bound depends on $j_E$ as $h(j_E)^{\frac{r+1}{3}} \cdot (\log(3h(j_E)))^{\frac{r+1}{3}}$. Notice that $h_{\text{Fal}}(E/K) \gg \max \{h(j_E), \log N_{K/\mathbb{Q}} \Delta_{E/K}\}$.

If one would like to deduce from the BSD-conjecture a lower bound for the product of the order of the Tate-Shafarevic group and the canonical regulator, one would be confronted with

- the problem of estimating 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 \( L^\ast(A/K, 1) \).

For the local numbers \( c_v \), this could be done, when e.g. \( A \) is a jacobian variety, under Szpiro’s conjecture (see [Hin07, Lemma 3.5]). The question for the \( L \)-series also seems difficult (in the case \( g = 1 \) and \( K = \mathbb{Q} \) one could see the proof of Theorem 2 of [GS95]).

4 Geometry of numbers and non-torsion points

We now have a bound for the product of the order of the Tate-Shafarevic group and the regulator. Recall that the regulator is built from the canonical heights of generators of the Mordell-Weil group, and this is what we would like to bound. In order to manage separately these quantities, we use a classical result on geometry of numbers.

Recall that the Néron-Tate height \( \hat{h}_L \) on \( A(K) \) extends to a positive definite quadratic form on \( A(K) \otimes \mathbb{R} \). We will apply Minkowski’s theorem on the successive minima to the lattice \( A(K) / A(K)_{\text{tors}} \), sitting inside the euclidean space \( A(K) \otimes \mathbb{R} \simeq \mathbb{R}^r \), with inner product \( \langle, \rangle_L \) and which satisfies \( \langle P, P \rangle_L = \hat{h}_L(P) \). The symmetric convex distance-function is then \( \sqrt{\hat{h}_L(.)} \), and the regulator \( \text{Reg}_L(A/K) \) is the square of the volume of the fundamental domain for the lattice.

**Lemma 4.1** We can choose a basis \( \{P_1, \ldots, P_r\} \) for the Mordell-Weil group modulo torsion satisfying \( \hat{h}_L(P_1) \leq \ldots \leq \hat{h}_L(P_r) \), and

\[
\prod_{i=1}^{r} \hat{h}_L(P_i) \leq (r!)^2 r^r \text{Reg}_L(A/K) \leq (r!)^2 \left( \frac{r}{2} \right)^r \deg(\phi_L)^r \text{Reg}(A/K).
\]

**Proof.** We proceed as [Rém05, Lemma 5.1]. Let’s denote \( \lambda_1 \leq \ldots \leq \lambda_r \) the successive minima with respect to the lattice \( L = A(K) / A(K)_{\text{tors}} \), and \( B \) the unit ball. Minkowski’s theorem [Cas97, Theorem V, Chapter VIII, section 4.3] gives

\[
\lambda_1 \ldots \lambda_r \cdot \text{Vol}(B) \leq 2^r \text{Vol}((A(K) \otimes \mathbb{R})/L) = 2^r \text{Reg}_L(A/K)^{\frac{1}{2}}.
\]

Lemma 1, page 204 of *loc. cit.* gives us a linear independently family of non-torsion points \( Q_1, \ldots, Q_r \) such that \( \lambda_i = \sqrt{\hat{h}_L(Q_i)} \). Then, by Lemma 8 page 135 of same reference, we know that there is a basis \( P_1, \ldots, P_r \) of the torsion-free part of \( A(K) \) verifying, for any \( j \in \{1, \ldots, k\} \),

\[
\sqrt{\hat{h}_L(P_j)} \leq \max\{\sqrt{\hat{h}_L(Q_j)}, \frac{1}{2} \sum_{l=1}^{j} \sqrt{\hat{h}_L(Q_l)}\} \leq \max\{1, \frac{j}{2}\} \sqrt{\hat{h}_L(Q_j)} \leq j \lambda_j.
\]

We conclude using a previous argument on the volume of the unit ball \( B \) (that is, \( \text{Vol}(B) \geq \frac{2^r}{r^{r/2}} \)). The second inequality comes from inequality (10). \( \square \)

Thus, in order to bound from below the canonical regulator of the variety, it suffices to give a lower bound for the \( \hat{h}_L(P_i)'s \). In the same way, a lower bound for the product \( \prod_{i=1}^{r-1} \hat{h}_L(P_i) \) of the \( (r - 1) \) first heights of the generators together with an upper bound for the canonical regulator gives us an upper bound for the greatest height \( \hat{h}_L(P_r) \). Thus, for both applications, it will be sufficient to bound from below the smallest height \( \hat{h}_L(P_1) \).
We are then interested in lower bounds for the height of the elements of a basis of the Mordell-Weil group modulo torsion and more generally for points of infinite order. We recall that a rational point of an abelian variety has Néron-Tate height zero if and only if it is a torsion point.

There are two different directions on which these kind of lower bounds are studied. Let $A/K$ be an abelian variety defined over a number field. Let $K'/K$ be any finite extension of the ground field $K$ and let $P$ in $A(K')$ be a non-torsion point. In the first case, $A/K$ is fixed and the dependence on the degree $[K' : K]$ is the main interest. This is a Lehmer-type problem. In [BSL14] lower bounds of the first kind are used. This is because $A/K$ is fixed, while the field $K'$, which is the field of rationality of the point $P$ (which comes from a covering of $\mathbb{P}^1 \setminus \{0, 1, \infty\}$), varies. In the second case, the accent relies in the dependence on the variety $A/K$. For the second kind of bounds, there is a conjecture of Lang [Lan78 page 92]: for every elliptic curve $E/K$, there is a positive number $c_{[K:Q]}$ depending only on the degree $[K : Q]$, such that, for all non-torsion points $P$ in $E(K)$,

$$\hat{h}_C(P) \geq c_{[K:Q]} \cdot \log N_{K/Q} \Delta E/K$$  \hspace{1cm} (40)

Silverman [Sil84] proved Lang’s conjecture for elliptic curves with integral $j$-invariant and generalised it to higher dimension [Sil84]: Let $A/K$ be an abelian variety of dimension $g$, then, there exists $c_{K,g}$ depending at most on $K$ and $g$, such that for all point $P$ in $A(K)$ generating $A$, we have

$$\hat{h}_C(P) \geq c_{K,g} h_{\text{Fal}}(A/K).$$

Concerning this problem, Masser [Mas87 Corollary 1] proved that for every $K/K_0$, there exists a real number $c_{[K:Q]}$ depending on $[K : Q]$ such that, for all non-torsion points $P$ in $A(K)$, one has

$$\hat{h}_C(P) \geq c_{[K:Q]} \cdot h_{\text{Fal}}(A/K_0)^{(2g+1)}. \hspace{1cm} (41)$$

We used this bound in a first version of this work. However, Masser’s result holds for an open subset of a family of abelian varieties and the number $c_{[K:Q]}$ is not explicit. In a second version of our work, we used Theorem 1.4 of David [Dav93]. This theorem is stated for $A_\tau$, the abelian variety given by the theta function $\Theta_\tau$ associated to $\tau$ in the Siegel space, is stated with the theta height of $A_\tau$, and gives a lower bound for non-torsion points when the abelian variety is simple. Then, using Masser-Wüstholz isogenies theorems [MW93, Lemma 4.2], we deduced the following corollary of David’s result.

**Proposition 4.2** Let $(A, \mathcal{L})$ be a principally polarised abelian variety of dimension $g$ defined over $K$. Suppose that $A$ is simple and that $A[2] \subset A(K)$. Let $h_F(A) = \max \{1, h_{\text{Stab}}(A)\}$, $d = [K : Q]$ and $D(g, d) = 3^{4g^2} \cdot 32^{4g^2} \cdot d$. Then there exists an explicitly calculable constant $c(g) > 0$ depending at most on $g$ such that for any non-torsion point $P$ in $A(K)$,

$$\hat{h}_C(P) \geq c(g) \cdot (8D(g, d)^2)^{-4g-2} \cdot h_F(A)^{-4g-1} \cdot (\log h_F(A) + 3 \log D(g, d))^{-4g-1}. \hspace{1cm} (42)$$

In a further version of our work, using Rédmond-Gaudron’s isogenies theorems [GR14a Théorème 1.2], we deduced from David’s theorem, a lower bound valid for $A$ not necessarily
simple and not necessarily carrying a principal polarisation (as the one given by the theta function).

Finally, we use in this present version the theorem of Bosser and Gaudron ([BG19 Théorème 1.3 and Proposition 4.4]). In fact, they proved bounds valid for an abelian variety not necessarily simple, and completely explicit in both the abelian variety and the degree of the number field. (See also [Win15] for a result in this direction.)

**Proposition 4.3 (Bosser-Gaudron)** Let \((A, \mathcal{L})\) be a polarised abelian variety of dimension \(g\) defined over a number field \(K\) and let \(P\) in \(A(K)\) be a non-torsion point. If \(g = 1\), then

\[
\hat{h}_\mathcal{L}(P)^{-1} \leq 10^{40}[K : \mathbb{Q}]^7 \max\{1, \log[K : \mathbb{Q}], h_{\text{Stab}}(A)\}^6.
\]

If \(g \geq 2\), then

\[
\hat{h}_\mathcal{L}(P)^{-1} \leq (736g)^{8g^2}[K : \mathbb{Q}]^{4g+3} \deg(\phi_\mathcal{L}) \max\{1, \log[K : \mathbb{Q}], h_{\text{Stab}}(A)\}^{4g+2}.
\]

From these bounds they deduce the following bound, independent of the polarisation \(\mathcal{L}\) and valid for all \(g \geq 1\),

\[
\hat{h}_\mathcal{L}(P)^{-1} \leq \max\{[K : \mathbb{Q}] + g^9, h_{\text{Stab}}(A)\}^{6074g}.
\]

\[\text{(45)}\]

5 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 1.3 and Theorem 1.4 as well as the specific results in the one-dimensional case. We then comment on these results. We prove Theorem 1.3 when proving the following result.

**Proposition 5.1** Suppose that \(A/K\) satisfies Hypothesis 1.1. Then we can choose a system \(\{P_1, \ldots, P_r\}\) of generators for the free-part of \(A(K)\) verifying the following. If \(g = 1\), then

\[
\max_{1 \leq i \leq r} \hat{h}_\mathcal{L}(P_i) \leq C_d \cdot D_K \cdot (r!)^2 r^r (10^{40} d^7)^{r-1} \cdot \mathcal{F}^{\frac{1}{4}} \cdot (\log(\mathcal{F} \cdot D_K^2))^{2d} \cdot e^{\delta h} \cdot \max\{1, \log d, h\}^{6(r-1)},
\]

if \(g \geq 2\), then

\[
\max_{1 \leq i \leq r} \hat{h}_\mathcal{L}(P_i) \leq (2^{16} g^2 d)^{2d} \cdot (r!)^2 r^r \cdot \deg(\phi_\mathcal{L})^{2r-1} \cdot (C_{g,d}')^{r-1} \cdot D_K^9 \cdot \mathcal{F}^{\frac{1}{4}} \cdot (\log(\mathcal{F} D_K^2))^{2gd} \cdot e^{\delta h} \cdot \max\{1, \log d, h\}^{(4g+2)(r-1)},
\]

where \(\mathcal{G} = \max\{2, \mathcal{F}\}\), \(C_d = e \left(\frac{6g^7}{5}\right)^d \cdot \mathcal{F}^{\frac{1}{4}} \cdot (129(5^d - 1)(3d)^6)^{\frac{(14+8d/2)^8}{\log(1+3^{d/2})}}\) and \(C_{g,d}' = (736g)^{8g^2} d^{4g+3}\).

**Proof of Theorem 1.3 and Proposition 5.1** We start from inequality (39), obtained from Minkowski’s theorem on successive minima. We recall that \(\deg(\phi_\mathcal{L}) = 1\) if \(\mathcal{L}\) is principal (e.g. if \(g = 1\)). Remark that \(h_{\text{stab}}(A) \leq h_{\text{alt}}(A/K) =: h(A)\). We then apply the conditional upper bound (36) of Proposition 1.2 for the canonical regulator to obtain the result for \(g \geq 2\), and resp., the conditional upper bound (37) of Proposition 5.2 for \(g = 1\), and remark that
\[ |\text{III}(A/K)| \geq 1. \] We conclude applying Proposition 4.3 to \( \hat{h}_L(P_i) \), for \( i = 1, \ldots, r - 1 \). Indeed, (43) gives the bound valid for \( g = 1 \), (44) gives the bound for \( g \geq 2 \), and (45) gives

\[
\max_{1 \leq i \leq r} \hat{h}_L(P_i) \leq (2^{16} g^2 d)^{\frac{rd^2}{8}} \cdot r^r \cdot \deg(\phi_L)^{2r-1} \cdot (C'_g d)^{r-1} \cdot D_K^{9} \cdot F^{\frac{4}{7}} \cdot (\log G)^{4g} \cdot (\log(FD_K^{2g}))^{2gd}.
\]

which could be written as in Theorem 1.3 when \( F \neq 1 \).

Remark 5.2 For \( K = \mathbb{Q} \), the bound (46) of Proposition 5.1 becomes

\[
\hat{h}(P_r) \leq C_1 \cdot 10^{40(r-1)} \cdot (r!)^2 r^r \cdot F^{1/4} \cdot (\log(F))^2 \cdot e^h \cdot h^{3/2} \cdot \max\{1, h\}^6(r-1),
\]

for an effective absolute constant \( C_1 \). This bound should be compared with Lang’s conjecture (3). Lang obtained a factor \( e^{x^2} \), which he could not reduce to \( e^r \), as he remarked in [Lan83]. Note on p. 170]. Our bound gives a factor which grows with \( r \) as \( e^{3r+1 \log r + 44r} \). This is because we use Minkowski’s theorem, instead of Hermite’s, as Lang do. Concerning the height of the variety, we have a supplementary factor: \( \max\{1, h\}^{1/2 + 6(r-1)} \). The factor \( h^{3/2} \) (as well as \( e^h \)) comes from the local factor \( c_{\infty} \). The factor \( \max\{1, h\}^{6(r-1)} \) comes from the lower bound (43) for non-torsion points. To bound the height of non-torsion points, in the one-dimensional case, Lang used his conjectural bound (40) and compared the discriminant of the curve with its conductor. As for the dependence on the conductor, we obtain \( F^{1/4} \cdot (\log(F))^2 \). Contrary to this, Lang suggested \( \mathcal{F}^{\varepsilon(F)} \cdot (\log(F))^\rho \). This is because, for bounding the leading coefficient of the \( L \)-function, he avoided the use of the functional equation, which he replaced by some hypothetical bound of his own, inspired by the Riemann hypothesis on the zeta function and some analytic estimates. Notice that the bound (23) gives \( r \ll \gamma \log F \) (which is optimal in the function field case). This gives a bound for Lang’s conjecture in terms of the conductor such as \( e^{x^2} \cdot F^{\varepsilon(F)} \cdot (\log(F))^r \ll F^{\varepsilon(F) + \gamma \log \log F + \gamma^2 \log^2 F} \), when our bound reads as \( F^{\varepsilon(F) + 4\gamma \log \log F + \delta} \), with \( \varepsilon(F) = 4^{\log \log F} \) and \( \delta \) independent of \( F \). (Here, \( g = 1 \) and \( K = \mathbb{Q} \), thus \( F \geq 11 \).)

We also remark that we can bound the regulator from below using Minkowski’s inequality (39) and the lower bounds for non-torsion points of Proposition 4.3. This lower bound for \( \text{Reg}(A/K) \), together with the upper bound for the product \( |\text{III}(A/K)| \text{Reg}(A/K) \) obtained in Proposition 1.2, gives an estimate for the order of \( \text{III}(A/K) \), which grows in the conductor and in the height as

\[
|\text{III}(A/K)| \ll F^{\frac{1}{4} + \varepsilon(F)} \cdot e^{dh + e'(h)},
\]

where \( \varepsilon(F) \to 0 \) when \( F \to \infty \), and \( e'(h) \to 0 \) when \( h \to \infty \), and the implied constant in the symbol \( \ll \) depends on \( g, d, D_K, r, \deg(\phi_L) \).

On one hand, even if this is not made explicit here, we would like to point out that there should be an inequality of the form \( F \ll e^{12h} \). For an elliptic curve, this is quite obvious because the Faltings’ height is related to the minimal discriminant ideal, which is divided by the conductor \( (h \gg \max\{h(j_E), \log N_{K/Q}\Delta_{E/K}\} \gg \log F) \). In higher dimension, the implied
constant in \( \ll \) would depend at least on \( g \) and \( K \). With this inequality, we could deduce an upper bound for \( |\text{III}(A/K)| \), which is independent of \( F \) and growths in the height as

\[
|\text{III}(A/K)| \ll e^{(d+3)h+e''(h)}.
\]

On the other hand, an inverse inequality between the height and the conductor would lead to an upper bound as a function in \( F, r, K \) and \( g \). This inequality was predicted in the 80’s by Szpiro [Szp90]: Given \( \epsilon > 0 \), there exists a constant \( c_\epsilon > 0 \) such that for any elliptic curve \( E \) defined over \( \mathbb{Q} \) with minimal discriminant \( \Delta_{E/Q} \), we have

\[
\log \left( |\Delta_{E/Q}|^{\frac{1}{d_2}} \right) \leq \left( \frac{1}{\epsilon} + \epsilon \right) \log F + c_\epsilon.
\]

Over an arbitrary number field, we have Frey’s version (see Conjecture 3.2 of [Hin07]): Given \( \epsilon > 0 \), there exists a constant \( c_\epsilon > 0 \) such that for any elliptic curve \( E \) defined over a number field \( K \), we have

\[
h_{\text{Fal}}(E/K) \leq \left( \frac{1}{2} + \epsilon \right) \log F + c_\epsilon.
\]

In higher dimension, we could expect the following (Hindry Superiority).

**Conjecture 5.3 (Generalised Szpiro’s 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

\[
h_{\text{Fal}}(A/K) \leq c_1 \log F_{A/K} + c_2.
\]

Looking at the function field analog and a theorem of Deligne, Hindry suggest that we may take \( c_1 = (\frac{2}{3} + \epsilon) \), for every \( \epsilon > 0 \). Playing with restriction of scalars, he adds: \( c_2 = (g^2 + \epsilon) \log D_K + c_{\epsilon,d} \), where \( c_{\epsilon,d} \) depends only on \( \epsilon \) and \( d = [K : \mathbb{Q}] \).

We deduce Theorem 5.4 from the following proposition.

**Proposition 5.4** Suppose that \( A/K \) satisfies Hypothesis \( (\mathcal{L}) \). Furthermore, suppose that \( A/K \) satisfies Szpiro’s Conjecture (Conjecture 5.3). Then, for every \( \epsilon > 0 \),

\[
|\text{III}(A/K)| \leq C'_{d,g,\epsilon} \cdot D_K^{d_2+g+\epsilon} \cdot (C_{d,g,\epsilon})^{6075g} \cdot (r!)^2 r^{r} \cdot F^{\frac{1}{2} + \frac{d_2}{2} + \epsilon}.
\]

\[
\cdot \left( \log \mathcal{G} \right)^{4gd} \left( \log (FD_K^{2g}) \right)^{2gd} \left( \log (c_{\epsilon,d}D_K) \right)^{6075g+\frac{d_2}{2}},
\]

where \( \mathcal{G} = \max\{2, F\} \), \( C_{d,g,\epsilon} = (d + g^2)(g^2 + \epsilon) \), and \( C'_{d,g,\epsilon} = c_{\epsilon,d}(2^{16} g^2 d C_{d,g,\epsilon})^{\frac{d_2}{2}} \).

If \( g \geq 2 \), then the following bound also holds

\[
|\text{III}(A/K)| \leq C''_{d,g,\epsilon} \cdot D_K^{d_2+g+\epsilon} \cdot (C''_{d,g,\epsilon})^{3} (r!)^2 r^{r} \cdot F^{\frac{1}{2} + \frac{d_2}{2} + \epsilon}.
\]

\[
\cdot \left( \log \mathcal{G} \right)^{4gd} \left( \log (FD_K^{2g}) \right)^{2gd} \left( \log (c_{\epsilon,d}D_K) \right)^{(4g+2)r+\frac{d_2}{2}},
\]

where \( C''_{d,g,\epsilon} = c'_{\epsilon,d}(2^{16} g^2 d (g^2 + \epsilon))^{\frac{d_2}{2}} \), and \( C''_{d,g,\epsilon} = (736g)^{8g^2 (d(g^2 + \epsilon))^{4g+3}} \).

\(^8\)This inequality is optimal in the function field case.
Furthermore, when $\mathcal{F} \neq 1$, this second bound could be written as

$$|\III(A/K)| \leq C'_{d,g,\epsilon} \cdot D_K^{g^2+g+\epsilon} \cdot (C^{(3)}_{d,g,\epsilon})^2 r^r \cdot \mathcal{F}^{\frac{d}{2}+\epsilon+\gamma(\mathcal{F})},$$

where $\gamma(\mathcal{F}) = 4gd \log \frac{\log G}{\log \mathcal{F}} + 2gd \log \frac{\log G}{\log \mathcal{F}} + ((4g+2)r' + \frac{d_g}{2}) \frac{\log \log (c_{e,d} D_K \mathcal{G})}{\log \mathcal{F}}$ tends to 0 when $\mathcal{F}$ tends to infinity.

**Proof.** With Proposition 1.2 and (39) we obtain the following upper bound

$$|\III(A/K)| \leq (2^{16} g^2 d)^{\frac{d_g}{2}} \cdot D_K^g \cdot \mathcal{F}^\frac{d}{2} \cdot (\log \mathcal{G})^{4gd} \cdot \log (\mathcal{F} D_K^{2g}) \cdot 2^{gd} \cdot e^{dh} \cdot \max \{1, h\}^{\frac{d_g}{2}} \cdot (r!)^2 r^r \prod_{i=1}^r h_i^{-1} (P_i).$$

We now use the different bounds of Proposition 4.3. Using (43) we obtain, for all $g \geq 1$,

$$|\III(A/K)| \leq (2^{16} g^2 d)^{\frac{d_g}{2}} \cdot (r!)^2 r^r \cdot D_K^g \cdot \mathcal{F}^\frac{d}{2} \cdot (\log \mathcal{G})^{4gd} \cdot \log (\mathcal{F} D_K^{2g}) \cdot 2^{gd} \cdot e^{dh} \cdot \max \{d+g^g, h\}^{6075gr+\frac{d_g}{2}}. \quad (50)$$

Applying Conjecture 5.3 with $c_1 = \left(\frac{g}{2} + \epsilon\right)$ and $c_2 = (g^2 + \epsilon) \log D_K + c_{e,d}$, we obtain

$$|\III(A/K)| \leq c'_{e,d} \cdot (2^{16} g^2 d)^{\frac{d_g}{2}} \cdot (r!)^2 r^r \cdot D_K^{g^2+g+\epsilon} \cdot \mathcal{F}^{\frac{d}{2}+\epsilon+\gamma(\mathcal{F})} \cdot (\log \mathcal{G})^{4gd} \cdot \log (\mathcal{F} D_K^{2g}) \cdot 2^{gd} \cdot e^{dh} \cdot \max \{d+g^g, h\}^{6075gr+\frac{d_g}{2}},$$

where $c'_{e,d}$ depends only on $\epsilon$ and $d$.

Remark that $A' = \Res_{K/Q}^A$, and, by (24) and (26), $D_K^{2g} \mathcal{F} = \mathcal{F}_{A'/Q} > 10^{gd}$ and this gives $\log (c_{e,d} \cdot D_K^{g^2+\epsilon} \cdot \mathcal{F}^{g/2+\epsilon}) \geq \log (c_{e,d} \cdot 10^{g^2+\epsilon} + \epsilon)$ (which could be smaller than $d+g^g$). However, this shows that $\log (c_{e,d} \cdot D_K^{g^2+\epsilon} \cdot \mathcal{F}^{g/2+\epsilon}) > 1$ and we could use the (rough) bound

$$\max \{d + g^g, \log (c_{e,d} \cdot D_K^{g^2+\epsilon} \cdot \mathcal{F}^{g/2+\epsilon})\} \leq (d + g^g) \cdot \log (c_{e,d} \cdot D_K^{g^2+\epsilon} \cdot \mathcal{F}^{g/2+\epsilon})$$

$$\leq (d + g^g) \cdot \log (c_{e,d} \cdot D_K \cdot \mathcal{F})^{g^2+\epsilon} \leq (d + g^g) (g^2 + \epsilon) \cdot \log (c_{e,d} \cdot D_K \cdot \mathcal{F}).$$

Hence

$$|\III(A/K)| \leq c'_{e,d} \cdot (2^{16} g^2 d)^{\frac{d_g}{2}} \cdot (d + g^g) (g^2 + \epsilon) \cdot D_K^{g^2+g+\epsilon} \cdot \log (c_{e,d} \cdot D_K \cdot \mathcal{F})^{g^2+\epsilon} \cdot \mathcal{F}^{\frac{d}{2}+\epsilon+\gamma(\mathcal{F})} \cdot (r!)^2 r^r \cdot D_K^g \cdot (\log \mathcal{G})^{4gd} \cdot \log (\mathcal{F} D_K^{2g}) \cdot 2^{gd} \cdot e^{dh} \cdot \max \{1, \log d, h\}^{(4g+2)r+\frac{d_g}{2}}.$$

This proves the first item. Moreover, when $\mathcal{F} \neq 1$, this could be written as Theorem 1.4 where $\delta(\mathcal{F}) = 4gd \log \frac{\log \mathcal{F}}{\log \mathcal{G}} + 2gd \log \frac{\log \mathcal{F}}{\log \mathcal{G}} + (6075gr + \frac{d_g}{2}) \frac{\log \log (c_{e,d} D_K \mathcal{F})}{\log \mathcal{F}}$ tends to 0 when $\mathcal{F}$ tends to infinity.

Otherwise, to prove the second item, for $g \geq 2$, using (44) instead of (45), we obtain

$$|\III(A/K)| \leq (2^{16} g^2 d)^{\frac{d_g}{2}} \cdot D_K^g \cdot (736g)^{8g^2 r (4g+3)^r} \cdot (r!)^2 r^r \cdot \mathcal{F}^{\frac{d}{2}+\epsilon+\gamma(\mathcal{F})} \cdot (\log \mathcal{G})^{4gd} \cdot \log (\mathcal{F} D_K^{2g}) \cdot 2^{gd} \cdot \max \{1, \log d, h\}^{(4g+2)r+\frac{d_g}{2}}.$$

Applying Conjecture 5.3 we have $\log h \leq \log (c_{e,d} D_K^{g^2+\epsilon} \mathcal{F}^{\frac{d}{2}+\epsilon})$. By the same reasoning as previously, we have $\log (c_{e,d} \cdot D_K^{g^2+\epsilon} \cdot \mathcal{F}^{g/2+\epsilon}) \geq \log (c_{e,d} \cdot 10^{g^2+\epsilon})$, which is larger than 1, and we could suppose larger than $\log d$ (by growing $c_{e,d}$ if needed), and then,

$$\max \{1, \log d, h\} \leq \log (c_{e,d} D_K^{g^2+\epsilon} \mathcal{F}^{\frac{d}{2}+\epsilon}) \leq (g^2 + \epsilon) \log (c_{e,d} D_K \mathcal{F}).$$
Finally

$$|\text{III}(A/K)| \leq c'_d \cdot (2^{16} g^2 d(g^2 + \epsilon))^\frac{d_f}{d} \cdot D_K^{d g^2 + g + \epsilon} \cdot (736 g)^8 g^2 r (d(g^2 + \epsilon))^{(4 g + 3) r} \cdot (r!)^2 r^r \cdot \frac{F^\tfrac{1}{2} + d_f + \epsilon}{r^r + \epsilon} \cdot (\log(G))^{4 g d} (\log(D_K^2))^{2 g d} \cdot (\log(c_d D_K F))^{(4 g + 2) r + \frac{d_f}{2}},$$

which achieves the proof of Proposition 5.5.

In the specific case of $g = 1$, we use Proposition 3.21 and, since we are focusing on the dependence on the conductor, and, in particular, we will neglect the dependence in the rank, we choose to use [37].

**Proposition 5.5** Let $E/K$ be an elliptic curve defined over a number field $K$. Suppose that $E/K$ satisfies Hypothesis [37] and Szpiro-Frey’s Conjecture (49). Then, for every $\epsilon > 0$,

$$|\text{III}(E/K)| \leq C_d e^{d c_x} \cdot D_K \cdot (r!)^2 r^r (10^{40} d^{13})^r \cdot \frac{F^\tfrac{1}{2} + d_f + \epsilon}{r^r + \epsilon} \cdot (\log(F D_K^2))^{2 d} (\log(e^{c_x} F_{\frac{1}{2} + \epsilon}))^{6 r + \frac{d_f}{2}},$$

where one could take $C_d = e \left(\frac{6\sqrt{2}}{5}\right)^d \cdot d^\frac{d}{2} \cdot (129 (5^d - 1) (3d)^6)^{(1 + 3d/2)^8}$.

When $F \neq 1$, this bound could be written as

$$|\text{III}(E/K)| \leq C_d e^{d c_x} \cdot D_K \cdot (r!)^2 r^r (10^{40} d^{13})^r \cdot \frac{F^\tfrac{1}{2} + d_f + \epsilon + \gamma'(F)}{r^r + \epsilon},$$

where $\gamma'(F) = 2 d \frac{\log(\log(D_K^2))}{\log(F)} + (6 r + \frac{d_f}{2}) \log\frac{\log(e^{c_x} F_{\frac{1}{2} + \epsilon})}{\log(F)}$ tends to 0 when $F$ tends to infinity.

**Proof.** We start with the bound [37] of Proposition 3.21. Then, we apply Minkowski’s theorem [39], and with [43], we obtain

$$|\text{III}(E/K)| \leq C_d \cdot D_K \cdot (r!)^2 r^r (10^{40} d^{13})^r \cdot \frac{F^\tfrac{1}{2} + d_f}{r^r + \epsilon} \cdot (\log(F D_K^2))^{2 d} \cdot e^{d h} \cdot h^\frac{d}{2} \cdot \max\{1, \log d, h\}^{6 r}, \quad (51)$$

with $C_d = e \left(\frac{6\sqrt{2}}{5}\right)^d \cdot d^\frac{d}{2} \cdot (129 (5^d - 1) (3d)^6)^{(1 + 3d/2)^8}$. Applying (19), we deduce

$$|\text{III}(E/K)| \leq C_d \cdot D_K \cdot (r!)^d \cdot (10^{40} d^{13})^r \cdot \frac{F^\tfrac{1}{2} + d_f}{r^r + \epsilon} \cdot (\log(F D_K^2))^{2 d} \cdot e^{d h} \cdot h^\frac{d}{2} \cdot \max\{1, \log d, \log(e^{c_x} F_{\frac{1}{2} + \epsilon})\}^{6 r}.$$

We then use the following (rough) bounds: log $d \leq d$, which is larger than 1, and since we could enlarge $c_d$ enough till have $\log(e^{c_x} F_{\frac{1}{2} + \epsilon}) > 1$, we could bound the maximum by the product of the two elements, to obtain

$$\max\{1, \log d, \log(e^{c_x} F_{\frac{1}{2} + \epsilon})\} \leq d \log(e^{c_x} F_{\frac{1}{2} + \epsilon}),$$

which achieves the proof of Proposition 5.5.

**Remark 5.6** In order to compare with Goldfeld-Szpiro’s result, let’s write the bound of Proposition 5.5 (for $K = \mathbb{Q}$, and thus $F = F_{E/\mathbb{Q}} \geq 11$) as

$$|\text{III}(E/\mathbb{Q})| = O(F_{\frac{1}{2} + c + \gamma'(F)}^r), \quad \text{with} \quad c = 1/2 + \epsilon,$$
where the implied constant in the $O$, as well as the function $\gamma'$, depend on $r$ and $\epsilon$, and $\gamma'(F)$ tends to 0 when $F$ tends to infinity. (Putting $g = 1$ and $K = \mathbb{Q}$ in Theorem 1.3 also gives $|\text{III}(E/\mathbb{Q})| = O(F^{1/4+c+\delta(F)})$. This is the closest possible bound expected by Goldfeld and Szpiro ($c > 1/2$, in [GS95, page 75]). In Theorem 1 of loc. cit., which we have quoted in the introduction by (5), they obtained $|\text{III}(E/\mathbb{Q})| \ll F^{1/4+c+\gamma(F)}$, with $c = 3/2$ and $\gamma(F)$ tends to 0 when $F$ tends to infinity. As we do, they use a lower bound for non-torsion points, in terms of the height of the variety, which we both then bound in terms of the conductor assuming Szpiro’s conjecture. They deduce their lower bound from Lang’s conjecture, together with Hindry-Silverman result on the ratio $\sigma_{E/K}$. Then, we both use Szpiro’s conjecture a second time, for bounding the period. Indeed, the difference between the numbers $c$ is because they use the lower bound for the period: $\Omega^{-1} \ll \Delta^{1+c} e^{\delta h}$, where $\Delta$ is the minimal discriminant of the curve (see [Gal90, page 168]), while our Lemma 3.17 gives: $c^{-1} \ll h^{2} - e h$, which is sharper.

**Remark 5.7** In the same paper Goldfeld and Szpiro proved [GS95, Theorem 2] a sort of reciprocal statement. Precisely, they proved that if their conjectured bound (4) for $|\text{III}(E/\mathbb{Q})|$ holds for every elliptic curve over $\mathbb{Q}$, then a weak version of Szpiro’s conjecture holds ($|\Delta_{E/\mathbb{Q}}| \leq F^{18+\epsilon}$) for every elliptic curve defined over $\mathbb{Q}$. (The full Szpiro’s conjecture $|\Delta_{E/\mathbb{Q}}| \leq F^{6+\epsilon}$ could be deduced assuming the Riemann hypothesis for the Rankin-Selberg zeta functions associated to modular forms of weight $3/2$.) The proof uses 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 could still be obtained for a fixed elliptic curve, or how this result could be generalised to any number field or to higher dimension.

**Acknowledgements**

It’s my pleasure to thank the colleagues who contributed to this paper (or one of the previous versions). My thanks to Carlo Gasbarri and Henri Darmon for pointing me to some references, to Jean-Benoît Bost, for encouraging me to write my first draft with more clarity, to David Masser, Sinnou David, Gaël Rémond and Pascal Autissier, for sharing discussions on their results, to Samuel Le Fourn, for other interesting discussions, and to Olivier Ramaré, for making explicit the constant of Lemma 3.20. I am further deeply grateful to Daniel Bertrand and Marc Hindry, for encouraging me to bringing to completion this work. Finally, I thank Gareth Jones and the EPSRC for partial support of my research.

**References**

[AHP18] P. Autissier, M. Hindry, and F. Pazuki. Regulators of elliptic curves. arXiv:1805.03484v1, 12 pp., 2018.

[Aut13] P. Autissier. Un lemme matriciel effectif. Math. Z., 273(1-2):355–361, 2013.

[BCDT01] C. Breuil, B. Conrad, F. Diamond, and R. Taylor. On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises. J. Amer. Math. Soc., 14(4):843–939 (electronic), 2001.

[BFTP18] G. Boxer, Calegari F., Gee T., and V. Pilloni. Abelian surfaces over totally real fields are potentially modular. arXiv:1812.09269, page 285, 21 December 2018.
[BG19] V. Bosser and É. Gaudron. Logarithmes des points rationnels des variétés abéliennes. *Canad. J. Math.*, 71(2):247–298, 2019.

[BK94] A. Brumer and K. Kramer. The conductor of an abelian variety. *Compositio Math.*, 92(2):227–248, 1994.

[Blo80] S. Bloch. A note on height pairings, Tamagawa numbers, and the Birch and Swinnerton-Dyer conjecture. *Invent. Math.*, 58(1):65–76, 1980.

[Bos96a] J.-B. Bost. Intrinsic heights of stable varieties and abelian varieties. *Duke Math. J.*, 82(1):21–70, 1996.

[Bos96b] J.-B. Bost. Périodes et isogénies des variétés abéliennes sur les corps de nombres [d’après D. Masser et G. Wüstholz]. In *Séminaire Bourbaki*. Volume 1994/95. *Exposés 790-804*, pages 115–161, ex. Paris: Société Mathématique de France, 1996.

[BS14] V. Bosser and A. Surroca. Elliptic logarithms, diophantine approximation and the Birch and Swinnerton-Dyer conjecture. *Bull. Math. Soc. Brazil, New Series*, 45(1):1–23, 2014.

[BS15] M. Bhargava and A. Shankar. Ternary cubic forms having bounded invariants, and the existence of a positive proportion of elliptic curves having rank 0. *Ann. of Math. (2)*, 181(2):587–621, 2015.

[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] G. Cornell and J. 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] J. Coates and A. Wiles. On the conjecture of Birch and Swinnerton-Dyer. *Invent. Math.*, 39(3):223–251, 1977.

[Dav93] S. David. Minorations de hauteurs sur les variétés abéliennes. *Bull. Soc. Math. France*, 121(4):509–544, 1993.

[DP02] S. David and P. Philippon. Minorations des hauteurs normalisées des sous-variétés de variétés abéliennes. II. *Comment. Math. Helv.*, 77(4):639–700, 2002.

[Dus99] P. Dusart. Inégalités explicites pour $\psi(X)$, $\theta(X)$, $\pi(X)$ et les nombres premiers. *C. R. Math. Acad. Sci. Soc. R. Can.*, 21(2):53–59, 1999.

[Ell75] W. J. 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.
[EMvdG19] B. Edixhoven, B. Moonen, and G. van der Geer. *Abelian varieties.* http://gerard.vdgeer.net/, 2019.

[FLHS15] N. Freitas, B. V. Le Hung, and S. Siksek. Elliptic curves over real quadratic fields are modular. *Invent. Math.*, 201(1):159–206, 2015.

[Gau06] É. Gaudron. Formes linéaires de logarithmes effectives sur les variétés abéliennes. *Ann. Sci. École Norm. Sup. (4)*, 39(5):699–773, 2006.

[GL96] D. Goldfeld and D. Lieman. Effective bounds on the size of the Tate-Shafarevich group. *Math. Res. Lett.*, 3(3):309–318, 1996.

[Gol90] D. Goldfeld. Modular elliptic curves and Diophantine problems. In *Number theory (Banff, AB, 1988)*, pages 157–175. de Gruyter, Berlin, 1990.

[GR14a] É. Gaudron and G. Rémont. Polarisations et isogénies. *Duke Math. J.*, 163(11):2057–2108, 2014.

[GR14b] É. Gaudron and G. Rémont. Théorème des périodes et degrés minimaux d’isogénies. *Comment. Math. Helv.*, 89(2):343–403, 2014.

[Gra01] P. Graftieaux. Formal groups and the isogeny theorem. *Duke Math. J.*, (106(1)):81–121, 2001.

[Gri18] R. Griffon. Analogue of the Brauer-Siegel theorem for Legendre elliptic curves. *J. Number Theory*, 193:189–212, 2018.

[Gro82] B. 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] D. Goldfeld and L. 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] B. H. Gross and D. B. Zagier. Heegner points and derivatives of L-series. *Invent. Math.*, 84(2):225–320, 1986.

[Hin07] M. Hindry. Why is it difficult to compute the Mordell-Weil group? *Proceedings of Diophantine Geometry at Centro Ennio de Giorgi, Pisa June 2005, Ed. Scuola Normale Superiore di Pisa*, pages 197–219, 2007.

[HP16] M. Hindry and A. Pacheco. An analogue of the Brauer-Siegel theorem for abelian varieties in positive characteristic. *Mosc. Math. J.*, 16(1):45–93, 2016.

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

[HS00] M. Hindry and Joseph H. Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. An introduction.

[Kol88] V. A. Kolyvagin. Finiteness of $E(\mathbb{Q})$ and $\text{III}(E, \mathbb{Q})$ for a subclass of Weil curves. *Izv. Akad. Nauk SSSR Ser. Mat.*, 52(3):522–540, 670–671, 1988.
K. Kato and F. Trihan. On the conjectures of Birch and Swinnerton-Dyer in characteristic $p > 0$. *Invent. Math.*, 153(3):537–592, 2003.

S. Lang. *Elliptic curves: Diophantine analysis*, volume 231 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1978.

S. 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.

S. Lang. *Number theory. III*, volume 60 of *Encyclopaedia of Mathematical Sciences*. Springer-Verlag, Berlin, 1991. Diophantine geometry.

P. Lockhart, M. Rosen, and J. H. Silverman. An upper bound for the conductor of an abelian variety. *J. Algebraic Geom.*, 2(4):569–601, 1993.

Juri I. Manin. Cyclotomic fields and modular curves. *Uspeki Mat. Nauk*, 26(6(162)):7–71, 1971.

D. 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.

L. Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Invent. Math.*, 124(1-3):437–449, 1996.

J.-F. Mestre. Formules explicites et minorations de conducteurs de variétés algébriques. *Compositio Math.*, 58(2):209–232, 1986.

J. S. Milne. On the arithmetic of abelian varieties. *Invent. Math.*, 17:177–190, 1972.

D. W. Masser and G. Wüstholz. Periods and minimal abelian subvarieties. *Ann. Math.*, (2, 137(2)):407 – 458, 1993.

T. Ooe and J. Top. On the Mordell-Weil rank of an abelian variety over a number field. *J. Pure Appl. Algebra*, 58(3):261–265, 1989.

P. Parent. Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres. *J. Reine Angew. Math.*, 506:85–116, 1999.

E. Phragmén and E. Lindelöf. Sur une extension d’un principe classique de l’analyse et sur quelques propriétés des fonctions monogènes dans le voisinage d’un point singulier. *Acta Math.*, 31(1):381–406, 1908.

S. Patrikis and R. Taylor. Automorphy and irreducibility of some $l$-adic representations. *Compos. Math.*, 151(2):207–229, 2015.

C.S. Rajan. On the size of the Tate-Shafarevich group of elliptic curves over function fields. *Compositio Math.*, 105(1):29–41, 1997.
[Ray85] M. Raynaud. Hauteurs et isogénies. *Astérisque*, (127):199–234, 1985. Seminar on arithmetic bundles: the Mordell conjecture (Paris, 1983/84).

[Rém97] G. Rémond. Sur des problèmes d’effectivité en géométrie diophantienne. *Thèse de doctorat, Université Paris 6*, https://www-fourier.univ-grenoble-alpes.fr/remond/these.ps, 1997.

[Rém05] G. Rémond. Intersection de sous-groupes et de sous-variétés. I. *Math. Ann.*, 333(3):525–548, 2005.

[Rém10] G. Rémond. Nombre de points rationnels des courbes. *Proc. Lond. Math. Soc. (3)*, 101:759–794, 2010.

[Rob83] G. Robin. Estimation de la fonction de Tchebychef θ sur le k-ième nombre premier et grandes valeurs de la fonction ω(n) nombre de diviseurs premiers de n. *Acta Arith.*, 42(4):367–389, 1983.

[Rub87] K. Rubin. Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication. *Invent. Math.*, 89(3):527–559, 1987.

[Sch03] R. Schoof. Abelian varieties over cyclotomic fields with good reduction everywhere. *Math. Ann.*, 325(3):413–448, 2003.

[sem81] Séminaire sur les Pinceaux de Courbes de Genre au Moins Deux, volume 86 of *Astérisque*. Société Mathématique de France, Paris, 1981.

[Ser70] J.-P. Serre. Séminaire Delange-Pisot-Poitou. 11e année: 1969/70. Théorie des nombres. Fasc. 2: Exposé 19. Secrétariat Mathématique, Paris, 1970. http://www.numdam.org.

[Ser97] J.-P. Serre. *Lectures on the Mordell-Weil theorem*. Aspects of Mathematics. Friedr. Vieweg & Sohn, Braunschweig, third edition, 1997. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt, With a foreword by Brown and Serre.

[Shi94] G. 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] J. H. Silverman. Lower bounds for height functions. *Duke Math. J.*, 51(2):395–403, 1984.

[ST61] G. Shimura and Y. 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] J.-P. Serre and J. Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492–517, 1968.

[Szp90] L. Szpiro. Discriminant et conducteur des courbes elliptiques. Number 183, pages 7–18, 1990. Séminaire sur les Pinceaux de Courbes Elliptiques (Paris, 1988).
[Tat66] J. Tate. On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. In Séminaire Bourbaki, Vol. 9, pages Exp. No. 306, 415–440 (1964–1966). Soc. Math. France, Paris, 1995, 1966.

[Tit75] E.C. Titchmarsh. The theory of functions. 2nd ed. London: Oxford University Press. X, 454 p. 5.00 (1975) ., 1975.

[Wei67] A. Weil. Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen. Math. Ann., 168:149–156, 1967.

[Wil95] A. Wiles. Modular elliptic curves and Fermat’s last theorem. Ann. of Math. (2), 141(3):443–551, 1995.

[Win15] B. Winckler. Intersection arithmétique et problème de Lehmer elliptique. PhD. Thesis Bordeaux, page 120 pages, 2015.

Andrea Surroca Ortiz
andrea.surroca.o@gmail.com
https://sites.google.com/view/andreasurroca