Why is it difficult to compute the Mordell-Weil group ?[1]

Marc Hindry

To the memory of Serge Lang

1. Introduction.

The Mordell-Weil group is the group of rational points of an abelian variety A defined over a number field K, it is classical (see for example [Lang2], [HS2]) that this group is finitely generated and can therefore be written as

$$A(K) = \mathbf{Z}P_1 \oplus \ldots \oplus \mathbf{Z}P_r \oplus A(K)_{\mathrm{tor}}$$

where the torsion group $A(K)_{\mathrm{tor}}$ is finite and r is called the *rank* of A over K. Computing the torsion part is comparatively easy and we have also good theoretical results for elliptic curves i.e. abelian varieties of dimension 1 (see paragraph 5). Computing generators of the infinite part of $A(K)$ is notoriously difficult even if this has been achieved for (finitely) many examples; see Cremona [Cr] for a precise description of the procedure `mwrank`. We present a heuristic, largely based on the Birch & Swinnerton-Dyer conjecture, which partly explains this experimental phenomenon.

The proof of the Mordell-Weil theorem involves an exact sequence of the type

$$0 \to A(K)/mA(K) \to \mathrm{Sel}^{(m)}(A/K) \to \text{Ш}(A/K)[m] \to 0$$

where $m \geq 2$, and the middle group (the Selmer group) is effectively computable but the last group, the m-part of the Tate-Shafarevic group provides trouble; indeed the Tate-Shafarevic group, which can be described as the group measuring the failure of the Hasse principle for curves of genus 1 or principal homogeneous spaces of abelian varieties and can be defined as

$$\text{Ш}(A/K) := \mathrm{Ker}\left\{ H^1(\mathrm{Gal}(\bar{K}/K), A_K) \to \prod_v H^1(\mathrm{Gal}(\bar{K}_v/K_v), A_{K_v}) \right\},$$

is not even known to be finite except in few cases.

The Mordell-Weil group $A(K)$ can be equipped with a canonical quadratic form, the Néron-Tate height $\hat{h} : A(K) \to \mathbf{R}$ which, after tensoring with $\mathbf{R}$, provides $A(K) \otimes \mathbf{R}$ with an Euclidean structure

$$\langle P, Q \rangle := \frac{1}{2}\left(\hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)\right).$$

We wish to find bounds for the height of the (appropriately selected) generators P_i. Classical considerations for a lattice in an Euclidean space show that it is sufficient to obtain :

(a) Lower bounds for the minimum of $\hat{h}(P)$ for non torsion points;

(b) Upper bounds for the volume of the lattice, that is, equivalently, upper bound for the regulator

$$\mathrm{Reg}(A/K) := \left|\det\left(\langle P_i, P_j \rangle\right)\right|.$$

[1] *This is an expanded version of my talk at Centro Ennio de Giorgi; Pisa, 22th June 2005. Version, 12 december 2005.*

Indeed Hadamard's inequality and a theorem of Hermite show that there exists a basis $P_1, \ldots, P_r$ of $A(K)$ modulo torsion such that :

$$\mathrm{Reg}(A/K) \leq \hat{h}(P_1) \ldots \hat{h}(P_r) \leq c^{r^2} \mathrm{Reg}(A/K)$$

with $\hat{h}(P_1) = \min_P \hat{h}(P)$ (the minimum being for non torsion points in $A(K)$). Hence, if say we order the P_i's so that $\hat{h}(P_1) \leq \ldots \leq \hat{h}(P_r)$, we get $\hat{h}(P_r) \leq c^{r^2} \mathrm{Reg}(A/K)/(\min_P \hat{h}(P))^{r-1}$.

The first problem is computable for each example and there are a few theoretical results, mainly for elliptic curves, whereas the second problem has proved rather intractable and the only known approach relies on the famous Birch & Swinnerton-Dyer conjecture as initiated by Manin [Man] and pursued by Lang [Lang3].

Apart from section 5 and perhaps some of the lemmas in section 3 this text is mainly a survey. We view the very speculative approach provided as a motivation for conjecture 5.5 which can be viewed as a Brauer-Siegel formula for abelian varieties and refines the conjectural upper bound proposed by Serge Lang [Lang3].

2. The classical case of the regulator and class number of a number field.

The natural invariant to label, count or describe number fields K is their discriminants denoted Δ_K (considering the degree $d_K := [K : \mathbf{Q}]$ as a trivial invariant that is anyway bounded by a constant times $\log \Delta_K$). Especially, by another classical theorem of Hermite, there is only a finite number of number fields of discriminant less than X. The more mysterious invariants are the *class number* denoted h_K and the *regulator* of the units denoted R_K . These quantities are related via the Dedekind zeta function

$$\zeta_K(s) := \prod_{\wp} \left(1 - \mathrm{N}\,\wp^{-s}\right)^{-1} = \sum_{n=1} a_n(K) n^{-s}$$

where the product is over all non zero prime ideals of the ring of integers $\mathcal{O}_K$ and $a_n(K)$ is the number of ideals of norm n. The product and series converge for $\Re(s) > 1$ and the function $\zeta_K(s)$ extends to a meromorphic function on the entire complex plane, holomorphic except for a simple pole at $s = 1$ whose residue is given by

$$\operatorname*{Res}_{s=1} \zeta_K(s) = \frac{2^{r_1} (2\pi)^{r_2} h_K R_K}{w_K \sqrt{\Delta_K}}. \tag{2.1}$$

Here w_K is the number of root of unity contained into K or, for future comparisons, the cardinality of the torsion subgroup of the units group $\mathcal{O}_K^*$; the integers r_1 (resp. r_2) are the number of real embeddings (resp. pairs of complex embeddings) of K. Further the zeta function satisfies the following functional equation : set $\Gamma_{\mathbf{R}}(s) = \pi^{-s/2}\Gamma(s/2)$ and $\Gamma_{\mathbf{C}}(s) = (2\pi)^{-s}\Gamma(s)$ and $\xi_K(s) = \Delta_K^{s/2} \Gamma_{\mathbf{R}}(s)^{r_1} \Gamma_{\mathbf{C}}(s)^{r_2} \zeta_K(s)$, then

$$\xi_K(s) = \xi_K(1 - s).$$

Notice that $\mathrm{Res}_{s=1} \xi_K(s) = 2^{r_1} h_K R_K / w_K$.

Theorem 2.1. (Brauer-Siegel) *Consider the family of all number fields of degree less than d_0, then as Δ_K goes to infinity we have, for any $\epsilon > 0$, the inequalities*

$$\Delta_K^{1/2-\epsilon} \ll h_K R_K \ll \Delta_K^{1/2+\epsilon}. \tag{2.2}$$

Remark. The implied constants depend on d_0 and ϵ. Also the statement is slightly weaker than the general Brauer-Siegel theorem which allows the degree d_K to go to infinity, providing that $\log \Delta_K / d_K$ goes to infinity.

Since $h_K \geq 1$ (trivial) and $R_K \geq c_1$ (non trivial) we obtain the two bounds

$$h_K \ll \Delta_K^{1/2+\epsilon} \qquad \text{and} \qquad R_K \ll \Delta_K^{1/2+\epsilon}. \tag{2.3}$$

It is also possible to construct fields for which the regulator is "small" and hence the class number is large, i.e. of order roughly $\Delta_K^{1/2}$ (see [ABC]).

For later comparisons we recall a very brief sketch. Let λ_K be the residue of $\xi_K(s)$ at $s = 1$, then the following representation immediately leads to the analytical continuation and functional equation :

$$\xi_K(s) = \frac{\lambda_K}{s(s-1)} + f_K(s),$$

where $f_K(s)$ is an entire function, such that $f_K(s) = f_K(1-s)$ and $f_K(s) \geq 0$ for real s and even $f_K(s) \gg \Delta_K^{s/2}$ (see [Lang1]). Picking $\sigma > 1$ we write $\lambda_K \leq \sigma(\sigma-1)\xi_K(\sigma)$. Using easy bounds for the gamma factors and

$$\zeta_K(\sigma) \leq \zeta(\sigma)^{d_K} \leq \left(1 + \frac{1}{\sigma - 1}\right)^{d_K},$$

we obtain for $\sigma \in]1,2]$: $\xi_K(\sigma) \ll \Delta_K^{\sigma/2}(1+(\sigma-1)^{-1})^{d_K}$ Finally selecting $\sigma := 1 + 1/\log \Delta_K$ yields

$$h_K R_K \ll \sqrt{\Delta_K}\,(\log \Delta_K)^{d_K - 1}$$

The lower bound is much harder. The starting point is to select $\sigma < 1$ such that $\zeta_K(\sigma) < 0$; in particular, granting (a small part of) Riemann's hypothesis, any $\sigma \in]1/2, 1[$ would be admissible. One then writes $\lambda_K > \sigma(1-\sigma)f_K(\sigma)$ and obtains

$$h_K R_K \gg \sigma(1-\sigma)\Delta_K^{\frac{1}{2} - \frac{1-\sigma}{2}}.$$

If one can pick $\sigma = 1 - c/\log \Delta_K$, that is if the function $\zeta_K(s)$ has no zero on the segment $[1 - c/\log \Delta_K, 1[$ then

$$h_K R_K \gg \frac{\sqrt{\Delta_K}}{\log \Delta_K}.$$

A large part of Brauer and Siegel's work is aimed at avoiding Riemann's hypothesis and reaching a slightly weaker (and ineffective) lower bound for the residue.

Convention. We will write "as usual" $F \ll G^\epsilon$ instead of: for all $\epsilon > 0$ there exists a constant C_ϵ such that when G is sufficiently large, $F \leq C_\epsilon G^\epsilon$.

3. The invariants of abelian varieties.

Let A be an abelian variety defined over K a number field, we can associate various objects to it.

The *dual abelian variety* $\check{A}$ represents the connected component of the Picard group of A; it is defined over K and isogenous to A, specifically, if $\mathcal{L}$ is an ample line bundle, the map $\phi_{\mathcal{L}} : A \to \check{A}$ given by $\phi_{\mathcal{L}}(a) = t_a^*\mathcal{L} \otimes \mathcal{L}^{-1}$ is an isogeny; the product $A \times \check{A}$ carries the *Poincaré bundle* denoted

$\mathcal{P}$. An ample line bundle $\mathcal{L}$ defines a *principal polarisation* if $\phi_{\mathcal{L}}$ is an isomorphism; a trick due to Zahrin shows that the abelian variey $A^4 \times \check{A}^4$ carries a principal polarisation and therefore often allows to assume the existence of such a polarisation.

If L/K is a finite extension, we may extend scalars and define A_L, the "same" abelian variety viewed over L. There is a subtler adjoint construction, starting with an abelian variety B defined over K, the *restriction of scalars* denoted $R_K^L B$; it is an abelian variety of dimension $[L : K] \dim(B)$, defined over K such that $(R_K^L B)_L$ is isomorphic to the product $\prod_\sigma B_\sigma$ where σ runs over the embeddings $L \hookrightarrow \bar{K}$; the arithmetic behaviour is well documented in [Mil], in particular it follows from the construction that $(R_K^L B)(K) \cong B(L)$. This device often enables one to reduce, at least theoretically, to abelian varieties defined over $\mathbf{Q}$.

The abelian variety A/K has a nice canonical model called the *Néron model* $\pi : \mathcal{A} \to R = \mathrm{Spec}(\mathcal{O}_K)$ (see [BLR] and Artin's paper [Ar] in [Co-Si]), it is a group scheme such that any rational map from a smooth R-scheme S to $\mathcal{A}$ extends to a morphism; in particular it comes equipped with the neutral section $e : R \to \mathcal{A}$ and any point $P \in A(K)$ gives rise to a section $\bar{P} : R \to \mathcal{A}$. The special fibre $\mathcal{A}_v$ is an abelian variety for almost all $v \in R$; the abelian variety is said to have *good reduction* (resp. *semistable reduction*) if $\mathcal{A}_v$ is an abelian variety (resp. the connected component of $\mathcal{A}_v$ is a semi-abelian variety); we denote $c_v := (\mathcal{A}_v/\mathcal{A}_v^0)(\mathbf{F}_v)$ the number of components of the special fibre that are rational over $\mathbf{F}_v$. Equivalently we may define $c_v := (A(K_v) : A^0(K_v))$ where K_v is the completion of K and $A^0(K_v)$ is the subgroup of K_v-rational points which extends to the connected component in the Néron model.

Classically one defines *Weil heights* as follows (see [HS2] or [Lang2]): one defines a height function $h : \mathbf{P}^n(\bar{\mathbf{Q}}) \to \mathbf{R}$ and then for any very ample line bundle L on a variety X one chooses an embedding $i : X \hookrightarrow \mathbf{P}^n$ associated to L and put $h_L(P) := h \circ i(P)$, the latter being only defined up to $O(1)$. On abelian varieties the situation is better since if L is a line bundle on A, there is a quadratic form q_L and a linear form ℓ_L such that $h_L(P) = q_L(P) + \ell_L(P) + O(1)$; the function $\hat{h}_L(P) := q_L(P) + \ell_L(P)$ is canonical and called the *Néron-Tate height* associated to L. The pairing associated to L is defined as

$$\langle P, Q\rangle_L := \frac{1}{2}\left(\hat{h}_L(P+Q) - \hat{h}_L(P) - \hat{h}_L(Q)\right). \tag{3.1}$$

If L is ample and symmetric the quadratic form $\hat{h}_L$ is positive definite on $A(K) \otimes \mathbf{R}$ and $\langle \cdot, \cdot \rangle_L$ provides an Euclidean structure.

We also have a natural pairing $\langle \cdot, \cdot \rangle : A(\bar{K}) \times \check{A}(\bar{K}) \to \mathbf{R}$ associate with the Poincaré line bundle, defined by :

$$\langle P, \check{P}\rangle := \hat{h}_{\mathcal{P}}(P, \check{P}). \tag{3.2}$$

Further the functorial properties of the construction tell us that all heights on A can be recovered from this pairing :

$$\hat{h}_L(P) = \langle P, \phi_L(P)\rangle. \tag{3.3}$$

We can therefore define the canonical *regulator* of A/K by choosing a basis $P_1, \ldots, P_r$ of $A(K)$ modulo torsion and a basis $\check{P}_1, \ldots, \check{P}_r$ of $\check{A}(K)$ modulo torsion, and setting :

$$\mathrm{Reg}(A/K) := \left|\det\left(\langle P_i, \check{P}_j\rangle\right)\right|. \tag{3.4}$$

Note that if L is ample and m is the index of the subgroup $\phi_L(\mathbf{Z}P_1 \oplus \ldots \mathbf{Z}P_r)$ in $\check{A}(K)$ modulo torsion, we have

$$\mathrm{Reg}_L(A/K) := |\det\left(\langle P_i, P_j\rangle_L\right)| = m\,\mathrm{Reg}(A/K). \tag{3.5}$$

A *Metrised line bundle* on $\mathrm{Spec}(\mathcal{O}_K)$ is a projective $\mathcal{O}_K$-module M of rank one with v-adic norms $\|\cdot\|_v$ such that for $\alpha \in \mathcal{O}_K$ and $m \in M$ we have $\|\alpha m\|_v = |\alpha|_v \|m\|_v$ and also $\|\cdot\|_v = 1$ for almost all v. The *Arakelov degree* is defined as :

$$\deg_{\mathrm{Ar}}\left(M, \|\cdot\|_v\right) := -\log \prod_v \|m\|_v = \log \mathrm{Card}\left(M/m\mathcal{O}_K\right) - \sum_{v \mid \infty} \log \|m\|_v, \tag{3.6}$$

where the right hand side is independent of $m \in M \setminus \{0\}$ by the product formula. One way to construct such hermitian module is to consider a (line) bundle $\mathcal{L}$ on a $\mathrm{Spec}(\mathcal{O}_K)$-scheme $\mathcal{X}$, put metrics on $\mathcal{L} \otimes_\sigma \mathbf{C}$ for each embedding $\sigma : K \to \mathbf{C}$ and pull back the (line) bundle and metrics via a section $P : \mathrm{Spec}(\mathcal{O}_K) \to \mathcal{X}$; one can therefore define

$$h_{\mathcal{X},\mathcal{L},\|\cdot\|_v}(P) := \frac{1}{[K:\mathbf{Q}]} \deg_{\mathrm{Ar}}\left(P^*\mathcal{L}, \|\cdot\|_v\right), \tag{3.7}$$

and check that this is a Weil height h_L on the generic fibre X with line bundle L.

There are two ways to associate a height to an abelian variety A/K, one may consider the moduli space $\mathrm{A}_{g,S}$ of abelian varieties of dimension g with appropriate additional structure "S" (polarisation and level structure say) embed it into a projective space $j : \mathrm{A}_{g,S} \hookrightarrow \mathbf{P}^N$ and define the naive height of A as $h(j([A]))$ where $[A]$ is the isomorphism class of A. Restricting for simplicity to principally polarised abelian varieties we have a classical model over $\mathbf{C}$. Define the *Siegel space* $\mathcal{H}_g$ as the set of $g \times g$ symmetric matrix τ (i.e. ${}^t\tau = \tau$) with positive definite imaginary part ($\mathrm{im}\,\tau > 0$) and put $\Gamma := \mathrm{Sp}(2g, \mathbf{Z})$ then $\mathrm{A}_{g,S}(\mathbf{C}) \cong \mathcal{H}_g/\Gamma$, the abelian variety corresponding to $\tau \in \mathcal{H}_g$ being $A_\tau := \mathbf{C}^g/\mathbf{Z}^g + \tau\mathbf{Z}^g$. It is often useful to restrict τ to a fundamental domain (modulo Γ) where for example $\mathrm{im}(\tau_{i,i}) \geq \sqrt{3}/2$, $|\mathrm{im}(\tau_{i,j})| \leq \mathrm{im}(\tau_{i,i})/2$ and $\mathrm{im}(\tau_{1,1}) \leq \ldots \leq \mathrm{im}(\tau_{g,g})$.

A more canonical way to construct a height was used by Faltings in his celebrated paper [Fal2]. One considers the line bundle of relative g-differentials on the Néron model $\Omega^g_{\mathcal{A}/\mathrm{Spec}(\mathcal{O}_K)}$ and pull it back via the neutral section to obtain a line bundle on $\mathrm{Spec}(\mathcal{O}_K)$:

$$\omega_A := e^*\Omega^g_{\mathcal{A}/\mathrm{Spec}(\mathcal{O}_K)} \tag{3.8}$$

which can be metrised by defining the norm of a g-differential as

$$\|\alpha\|^2 = (2\pi)^{-g} \int_{A(\mathbf{C})} |\alpha \wedge \bar{\alpha}|\,. \tag{3.9}$$

One then defines the *Faltings height* as :

$$h_{\mathrm{Falt}}(A/K) := \frac{1}{[K:\mathbf{Q}]} \deg_{\mathrm{Ar}}(\omega_A, \|\cdot\|). \tag{3.10}$$

The Faltings height is invariant by extension of scalars if A/K has semi-stable reduction and we may therefore define the *stable Faltings height* as the height obtained over an extension where A has semi-stable reduction, we denote it $h_{\mathrm{st}}(A)$. It is easy to see that $h_{\mathrm{st}}(A) \leq h_{\mathrm{Falt}}(A/K)$. To be "concrete", consider $A/\mathbf{Q}$, its Néron model $\mathcal{A}/\mathrm{Spec}(\mathbf{Z})$ and η a generator over $\mathbf{Z}$ of $\Omega^g_{\mathcal{A}/\mathrm{Spec}(\mathbf{Z})}$ then

$$h_{\mathrm{Falt}}(A/\mathbf{Q}) = -\log\|\eta\| = -\frac{1}{2}\log\left\{\left(\frac{1}{2\pi}\right)^g \int_{A(\mathbf{C})} |\eta \wedge \bar{\eta}|\right\}. \tag{3.11}$$

The two height theories are comparable in the sense that there is a line bundle λ on $M_{g,S}$ and a rational number r such that

$$|h_{\rm st}(A) - rh_\lambda([A])| \ll \log\max(2, h_{\rm st}(A)).$$

We also have nice formulas as $h_{\rm Falt}(\check{A}/K) = h_{\rm Falt}(A/K)$ and $h_{\rm Falt}((A\times B)/K) = h_{\rm Falt}(A/K) + h_{\rm Falt}(B/K)$.

Suppose A is principally polarised and that for each archimedean place v of K (we'll just write $v\,|\,\infty$) we select an element τ_v (usually chosen in Siegel's fundamental domain) such that $A(\bar{K}_v) \cong \mathbf{C}^g/(\mathbf{Z}^g + \tau_v\mathbf{Z}^g)$, then one can show (see the *Matrix lemma* in [Mas] or [Bost]):

$$\frac{1}{[K:\mathbf{Q}]}\sum_{v\,|\,\infty}\|\operatorname{im}\tau_v\| \ll h_{\rm Falt}(A/K). \tag{3.12}$$

For E/K an elliptic curve, the Faltings height can be expressed in term of more classical invariant (see for example [Fal1] or Silverman's paper in [Co-Si]) :

$$h_{\rm Falt}(E/K) = \frac{1}{12[K:\mathbf{Q}]}\left\{\log \mathrm{N}\,\Delta_{E/K} - \sum_{v\,|\,\infty}[K_v:\mathbf{R}]\log\left|\Delta(\tau_v)(\operatorname{im}\tau_v)^6\right|\right\} \tag{3.13}$$

where $\Delta_{E/K}$ is the *minimal discriminant* of E/K and $\Delta(\tau)$ the usual modular form (see [Sil1]) and $E(\bar{K}_v) \cong \mathbf{C}/\mathbf{Z} + \tau_v\mathbf{Z}$. In particular one gets $\left|h_{\rm st}(A/K) - \frac{1}{12}h(j_E)\right| \ll \log\max(2, h(j_E))$. When $K = \mathbf{Q}$, one can usually replace the Faltings height by the “naïve” height $h^*(E) := \log\max\left\{|c_4|^{1/4}, |c_6|^{1/6}\right\}$, since $h_{\rm Falt}(E/\mathbf{Q}) - c_1 \le h^*(E) \le h_{\rm Falt}(E/\mathbf{Q}) + O(\log h_{\rm Falt}(E/\mathbf{Q}))$.

For A the jacobian of a curve C of genus 2, the Faltings height can also be expressed in terms of more classical invariant (see [Ue]) :

$$h_{\rm Falt}(A/K) = \frac{6}{5[K:\mathbf{Q}]}\left\{\sum_{\wp}\operatorname{ord}_\wp(\Delta_\wp)\log\mathrm{N}\,\wp - \sum_{v\,|\,\infty}\log\left|J_{10}(\tau_v)\,(\det\operatorname{im}\tau_v)^5\right|\right\} \tag{3.14}$$

where $\Delta_\wp$ is the minimal $\wp$-discriminant of the curve and J_{10} the Igusa invariant (Cf loc. cit.). Finally in the case where $A = J_X$ is the Jacobian of a curve X/K, we have the arithmetic Noether formula ([M-B] and [Fal1]) which we write in the semistable case.

$$h_{\rm Falt}(J_X/K) = \frac{1}{12[K:\mathbf{Q}]}\left\{\omega_{X/\mathcal{O}_K}\cdot\omega_{X/\mathcal{O}_K} + \sum_{\wp}\delta(X_\wp)\log\mathrm{N}\,\wp + \sum_{\sigma:K\to\mathbf{C}}\delta(X_\sigma(\mathbf{C}))\right\},$$

where $\delta(X_\wp)$ is the number of singular points on the special fibre at $\wp$ of the regular minimal model $\mathcal{X}/\mathcal{O}_K$ and $\delta(X_\sigma(\mathbf{C}))$ is the invariant of the Riemann surface $X_\sigma(\mathbf{C})$ defined by Faltings (see [Fal1]) and finally the only thing we need to know about the arithmetic intersection number $\omega_{X/\mathcal{O}_K}\cdot\omega_{X/\mathcal{O}_K}$ is that it is positive. Since $\delta : \mathcal{M}_g(\mathbf{C}) \to \mathbf{R}$ has a lower bound, we deduce that

$$\frac{1}{[K:\mathbf{Q}]}\sum_{\wp\,|\,\mathcal{F}_{A/K}}\delta(X_\wp)\log\mathrm{N}\,\wp \ll h_{\rm Falt}(A/K).$$

Further, studying the relationship between the geometry of the special fibre $X_\wp$ and the group of components of the special fibre of the Néron model of J_X (see [BLR], chapter 9.6 or [Ar]), one deduces relatively easily that $c_\wp \ll \delta(X_\wp)^g$.

The two examples (3.13) and (3.14) suggest the existence of a decomposition of the Faltings height in terms of local terms with contributions from the places of bad reduction and archimedean places. In particular it suggests that the following type of inequality, analogous to the archimedean inequality above (3.12), should be true for a general abelian variety, although we proved it only for jacobian varieties.

$$\frac{1}{[K:\mathbf{Q}]}\sum_{\wp\,|\,\mathcal{F}_{A/K}} c_\wp^{1/g}\log \mathrm{N}\,\wp \ll h_{\mathrm{Falt}}(A/K). \tag{3.15}$$

The real period. To simplify, we assume here $K=\mathbf{Q}\subset\mathbf{R}\subset\mathbf{C}$. Select η a Néron differential i.e. a generator over $\mathbf{Z}$ of $\Omega^g_{\mathcal{A}/\,\mathrm{Spec}(\mathbf{Z})}$; we define

$$\Omega_A := \int_{A(\mathbf{R})} |\eta|\,. \tag{3.16}$$

For future reference notice that if, say, $\eta=\omega_1\wedge\ldots\wedge\omega_g$, this integral can be written as follows. The homology group $H_1(A(\mathbf{C}),\mathbf{Z})$ has rank $2g$ and $H_1(A(\mathbf{C}),\mathbf{Z})^+$, the part fixed under the action of complex conjugation, has rank g and basis, say, $\delta_1,\ldots,\delta_g$; then

$$\Omega_A = 2^f\left|\det\left(\int_{\delta_i}\omega_j\right)\right|,$$

where $2^f := (A(\mathbf{R}):A(\mathbf{R})^0)$.

The ℓ-adic representation is obtained from the Tate module

$$V_\ell(A/K)=\left(\lim_{\leftarrow} A[\ell^n]\right)\otimes\mathbf{Q}_\ell$$

on which $\mathrm{Gal}(\bar K/K)$ acts. Since $V_\ell(A/K)\cong\mathbf{Q}_\ell^{2g}$ we may view this as a representation $\rho_\ell:\mathrm{Gal}(\bar K/K)\to\mathrm{GL}_{2g}(\mathbf{Q}_\ell)$.

The *conductor* $\mathcal{F}_{A/K}$ is defined as follows. Let $\wp$ be a prime in $\mathcal{O}_K$, choose a prime above $\wp$ in the algebraic closure and denote by G_i the ramification groups (starting with G_0 the *inertia group*) and look at the action on $V=V_\ell(A/K)$ then

$$\mathcal{F}_{A/K}:=\prod_\wp \wp^{f(A,\wp)} \qquad \text{with} \qquad f(A,\wp):=\sum_{i=0}^{\infty}\frac{|G_i|}{|G_0|}\,\mathrm{codim}\,V^{G_i} \tag{3.17}$$

Notice the sum is actually finite and, by non trivial results, the result is indeed an integer independent of the choices made. Further $f(A,\wp)=0$ if A has good reduction at $\wp$ and, writing $f(A,\wp)=\mathrm{codim}\,V^{G_0}+f_1(A,\wp)$, the term $f_1(A,\wp)$ comes from wild ramification and therefore only occurs for small primes, thus most of the time $f(A,\wp)\le 2g$. If $B=R^K_{\mathbf{Q}}A$, we have $\mathcal{F}_{B/\mathbf{Q}}=\mathrm{N}^K_{\mathbf{Q}}\,\mathcal{F}_{A/K}\Delta_K^{2\dim A}$ (see [Mil]).

Conjecture 3.1. (Szpiro) *The discriminant and conductor of an elliptic curve E/K satisfy the following inequality :*

$$\log \mathrm{N}^K_{\mathbf{Q}}\,\Delta_{E/K}\le(6+\epsilon)\log\mathrm{N}^K_{\mathbf{Q}}\,\mathcal{F}_{E/K}+C_\epsilon \tag{3.18}$$

Via this conjecture, it is natural to define the *Szpiro's ratio* as $\sigma_{E/K} := \log \mathrm{N}\,\Delta_{E/K} / \log \mathrm{N}\,\mathcal{F}_{E/K}$ (see [HS1]); the conjecture then says that the Szpiro's ratio is bounded and more precisely is smaller than $6+\epsilon$ except for finitely many elliptic curves. It is quite natural to slightly generalise the statement by including the term $\max\{h(j_E), \log \mathrm{N}_{\mathbf{Q}}^{K}\,\Delta_{E/K}\}$ on the left and one obtains a conjecture proposed by Frey; in terms of the Faltings height it can be stated as

Conjecture 3.2. (Szpiro, Frey) *The height and conductor of an elliptic curve E/K satisfy the following inequality :*

$$h_{\mathrm{Falt}}(E/K) \leq \left(\frac{1}{2}+\epsilon\right) \log \mathrm{N}_{\mathbf{Q}}^{K}\,\mathcal{F}_{E/K} + C_\epsilon. \tag{3.19}$$

Over $\mathbf{Q}$, this conjecture is equivalent to the ABC conjecture. Looking at the function field analog for abelian varieties we have the following theorem [Del1, lemme 3.2] :

Theorem 3.3. (Deligne) *Let $\pi : \mathcal{A} \to C$ be a semiabelian scheme over a smooth projective curve C of genus g_0, defined over an algebraically closed field of characteristic 0, and assume that there is a finite set S of closed points of C such that the scheme $\mathcal{A}$ is abelian over $C \setminus S$ then*

$$\deg \omega \leq \frac{g}{2}\left(2g_0 - 2 + |S|\right). \tag{3.20}$$

where $\omega := e^*\Omega^g_{\mathcal{A}/C}$.

This suggest that the correct generalisation of Szpiro's conjecture to higher dimensional abelian varieties (where we drop the semi-stability assumption) should be :

Conjecture 3.4. (Generalised Szpiro conjecture) *The height and conductor of an abelian variety A/K of dimension g satisfy the following inequality :*

$$h_{\mathrm{Falt}}(A/K) \leq \left(\frac{g}{2}+\epsilon\right) \log \mathrm{N}_{\mathbf{Q}}^{K}\,\mathcal{F}_{E/K} + C_\epsilon \tag{3.21}$$

Remark. Playing with restriction of scalars, we note that, if the latter conjecture is true in all dimensions over $\mathbf{Q}$, we would obtain

$$h_{\mathrm{Falt}}(A/K) \leq \left(\frac{g}{2}+\epsilon\right) \log \mathrm{N}_{\mathbf{Q}}^{K}\,\mathcal{F}_{E/K} + (g^2+\epsilon)\log \Delta_K + C_\epsilon$$

with the constant C_ϵ depending on $[K:\mathbf{Q}]$ and ϵ.

For the rest of this section we assume for simplicity (see the remark at the end) that $K = \mathbf{Q}$ and to ease notation we set $N_A := \mathrm{N}_{\mathbf{Q}}^{K}\,\mathcal{F}_{A/K}$.

Lemma 3.5. *Assume Szpiro's conjecture, then for all $\epsilon > 0$ we have :*

$$\prod_p c_p \ll N_A^\epsilon. \tag{3.22}$$

Proof. Assume first that $g = 1$. In view of (3.15) we interpret Szpiro's conjecture as meaning the existence of a constant σ such that $\sum_{p \mid N} c_p \log p \leq \sigma \log N$. We also know that $\log N \gg\ll$

$\sum_{p\,|\,N} \log p$; the proof is then elementary. Notice $\sum_{p\,|\,N} c_p \leq \sum_{p\,|\,N} c_p \log p/\log 2 \leq \sigma \log N/\log 2$, hence the arithmetic-geometric inequality gives

$$\sum_{p\,|\,N} \log c_p \leq \omega(N) \log\left(\frac{\sum_{p\,|\,N} c_p}{\omega(N)}\right) \leq \omega(N) \log\left(\frac{\sigma \log N}{\omega(N)\log 2}\right).$$

Select a small η (say $\eta = \epsilon/2$). If $\omega(N) \leq \eta \log N/\log\log N$ then

$$\sum_{p\,|\,N} \log c_p \leq \eta \log N \log(\sigma \log N)/\log\log N \leq 2\eta \log N \leq \epsilon \log N;$$

else, recall $\omega(N) \leq c_1 \log N/\log\log N$, hence

$$\sum_{p\,|\,N} \log c_p \leq \frac{c_1 \log N}{\log\log N} \log\left(\frac{\sigma}{\eta} \log\log N\right) \leq \epsilon \log N.$$

In the general case we replace c_p by $c_p^{1/g}$ and argue the same way, invoking (3.15). □

In the same vein, we note the following easy lemma.

Lemma 3.6. *For all $\epsilon > 0$ we have :*

$$\left|A(\mathbf{Q})_{\rm tor} \times \check{A}(\mathbf{Q})_{\rm tor}\right| \ll (\log N_A)^{4g} \ll N_A^{\epsilon}. \tag{3.22}$$

Proof. Using (a weak form of) the prime number theorem, we may select two distinct primes p_1, p_2 coprime with N_A and $\ll \log N_A$. Since it is well known then that $A(\mathbf{Q})_{\rm tor}$ injects into $\tilde{A}_{p_1}(\mathbf{F}_{p_1}) \times \tilde{A}_{p_2}(\mathbf{F}_{p_2})$ we see that

$$|A(\mathbf{Q})_{\rm tor}| \ll (p_1 p_2)^g \ll (\log N_A)^{2g}.$$

Applying the same argument to $\check{A}$ gives the lemma. □

Lemma 3.7. *The height and real period of an abelian variety $A/\mathbf{Q}$ are related by the following inequality :*

$$H(A) \ll \Omega_A^{-1} \ll H(A) \log H(A)^{g/2} \ll H(A)^{1+\epsilon}. \tag{3.23}$$

Proof. The argument (at least for $g = 1$) can be found in [Del2]. To compute $H(A)$ and compare it to Ω_A we choose a Néron differential $\eta = \omega_1 \wedge \ldots \omega_g$ and a basis $\gamma_1, \ldots, \gamma_{2g}$ of $H_1(A(\mathbf{C}), \mathbf{Z})$, such that $\gamma_1, \ldots, \gamma_g$ form a basis of $H_1(A(\mathbf{C}), \mathbf{Z})^+$ and the lattice associated is $\Lambda = \Omega_1 (\mathbf{Z}^g + \tau \mathbf{Z}^g)$. We have $\Omega_A = |\det \Omega_1|$ and $H(A) = \|\eta\|^{-1}$ and

$$\begin{aligned}\|\eta\|^2 &= \left(\frac{1}{2\pi}\right)^g \int_{A(\mathbf{C})} |\eta \wedge \bar{\eta}| = \left(\frac{1}{2\pi}\right)^g \int_{\mathbf{C}^g/\Omega_1(\mathbf{Z}^g+\tau\mathbf{Z}^g)} |dz \wedge d\bar{z}| \\ &= |\det \Omega_1|^2 \left(\frac{1}{2\pi}\right)^g \int_{\mathbf{C}^g/\mathbf{Z}^g+\tau\mathbf{Z}^g} |dz' \wedge d\bar{z}'| = \frac{|\det \Omega_1|^2}{(2\pi)^g} \det(\operatorname{im} \tau).\end{aligned}$$

Hence

$$H(A) = \frac{\Omega_A^{-1} (2\pi)^{g/2}}{\sqrt{\det(\operatorname{im} \tau)}}.$$

By the minimality of the volume of Ω_1 and the matrix lemma (see [Mas], [Bost]), we have:

$$1 \ll \det \operatorname{im} \tau \ll \| \operatorname{im} \tau \|^g \ll h(A)^g,$$

which achieves the proof of the lemma. □

The L-function. Recall the ℓ-adic representation $\rho : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}(V_\ell(A))$; choosing a prime above p defines a decomposition group and an inertia group which, up to conjugation, depends only on p, hence we denote them abusively by D_p and I_p, we denote also by Frob_p the canonical generator of D_p/I_p, thus Frob_p is defined only modulo I_p and up to conjugation; the following definition then makes sense :

$$L(A/\mathbf{Q}, s) := \prod_p \det \left(1 - \rho(\mathrm{Frob}_p) p^{-s} \mid V_\ell(A)^{I_p}\right)^{-1} = \sum_{n=1}^{\infty} a_n(A) n^{-s} \tag{3.24}$$

The Euler product and Dirichlet series converges for $\Re(s) > 3/2$. It is a classical generalisation of conjectures of Hasse-Weil and Riemann that, if we define

$$\Lambda(A, s) := N_A^{s/2} \Gamma_{\mathbf{C}}(s)^g L(A, s) \tag{3.25}$$

then we have :

Conjecture 3.8.
(a) (Hasse-Weil conjecture for $A/\mathbf{Q}$) The function $L(A, s)$, originally defined for $\Re(s) > 3/2$ extends to an entire function and satisfies the functional equation

$$\Lambda(A, s) = \epsilon_{A/\mathbf{Q}} \Lambda(A, 2 - s) \tag{3.26}$$

(with $\epsilon_{A/\mathbf{Q}} = \pm 1$).
(b) (Riemann's hypothesis for $A/\mathbf{Q}$) The function $L(A, s)$ has no zeroes with $\Re(s) > 1$.

The first part, though a major challenge in the general case, is now known for CM abelian varieties (Shimura-Taniyama), some modular abelian varieties as $J_0(N)$ (Shimura) and elliptic curves over $\mathbf{Q}$ (Wiles). The Riemann hypothesis remains unproven in any single case. Notice also that the sign of the functional equation determines the parity of the order of vanishing at $s = 1$.

Let A/K be an abelian variety, we may construct in the same way a function $L(A/K, s)$ which we may recover or define (see [Mil]) introducing the restriction of scalars $R_{\mathbf{Q}}^K A$ and setting :

$$L(A/K, s) := L(R_{\mathbf{Q}}^K A/\mathbf{Q}, s).$$

4. The Birch & Swinnerton-Dyer and Lang's conjectures.

The behaviour at the centre of symmetry of the functional equation of $L(A, s)$ has been the object of many investigations.

Conjecture 4.1. (Birch & Swinnerton-Dyer) *The L-function of an abelian variety $A/\mathbf{Q}$ has a zero of order $r := \operatorname{rk} A(\mathbf{Q})$ at $s = 1$ and leading term :*

$$L^*(A, 1) := \lim_{s \to 1} \frac{L(A, s)}{(s-1)^r} = \frac{|\text{Ш}(A/\mathbf{Q})| \operatorname{Reg}(A/\mathbf{Q})}{|A(\mathbf{Q})_{\mathrm{tor}}| \left|\check{A}(\mathbf{Q})_{\mathrm{tor}}\right|} \Omega_A \prod_p c_p. \tag{4.1}$$

Remark. One can formulate this conjecture for abelian varieties A/K, but it is known by Milne [Mil] that the BSD conjecture for A/K is equivalent to the BSD conjecture for $R_{\mathbf{Q}}^{K}A/\mathbf{Q}$.

The statement implicitely assumes analytic continuation (to a neighbourhood of 1) and finiteness of the Tate-Shafarevic group. The evidence includes deep work by Coates-Wiles [CW], Gross-Zagier [GZ], Rubin [Rub] and Kolyvagin [Kol]. We now note that the predicted formula has a similar shape as the formula giving the residue of Dedekind zeta function, roughly speaking the terms correspond as follows

Number Field K		Abelian variety A/K
$\zeta_K(s)$	$\leftrightarrow$	$L(A,s)$
h_K	$\leftrightarrow$	$\lvert\mathit{III}(A/K)\rvert$
R_K	$\leftrightarrow$	$\mathrm{Reg}(A/K)$
$(\mathcal{O}_K^*)_{\mathrm{tor}}$	$\leftrightarrow$	$A(K)_{\mathrm{tor}} \times \check{A}(K)_{\mathrm{tor}}$
$\sqrt{\Delta_K}$	$\leftrightarrow$	Ω_A^{-1} or $H(A)$

Just as the residue formula provides analytic estimates for the regulator of units of a number field, the hope is that the Birch & Swinnerton-Dyer conjecture will provide analytic estimates for the regulator of $A/\mathbf{Q}$. For a comparison with an earlier guess from Birch & Swinnerton-Dyer, stating that $\prod_{p\leq X} \mathrm{Card}\, A(\mathbf{F}_p)/p^g \sim C_{A/\mathbf{Q}}(\log X)^r$, see [Gold].

Concerning the minimal non zero height we have the following conjecture.

Conjecture 4.2.

(a) *(Lang) Let E/K be a elliptic curve then for all non torsion point in $E(K)$ we have*

$$\hat{h}(P) \geq c_K \log \mathrm{N}_{\mathbf{Q}}^{K} \Delta_{E/K}. \tag{4.2}$$

(b) *(Lang, Silverman) Let A/K be an abelian variety of dimension g, then, for all point $P \in A(K)$ generating A, we have*

$$\hat{h}(P) \geq c_{K,g} h_{\mathrm{Falt}}(A/K). \tag{4.3}$$

The hypothesis "P generates A" means that A is the smallest algebraic subgroup containing P; such a condition is necessary to avoid trivial counter examples where $A = A_1 \times A_2$ and $P = (P_1, 0)$ since $h_{\mathrm{Falt}}(A) = h_{\mathrm{Falt}}(A_1) + h_{\mathrm{Falt}}(A_2)$. The following results are known

Theorem 4.3.

(a) (Hindry-Silverman [HS1]) *Let E/K be an elliptic curve with Szpiro's ratio $\sigma_{E/K}$ and let P be a non torsion point in $E(K)$, then*

$$\hat{h}(P) \geq c(\sigma_{E/K}) \log \mathrm{N}_{\mathbf{Q}}^{K} \Delta_{E/K}.$$

(a) (David [Dav]) *Let A/K be an abelian variety such that $h_{\mathrm{Falt}}(A/K) \leq \rho \max_{v|\infty} \|\operatorname{im} \tau_v\|$, and let P be a point in $A(K)$ generating A, then*

$$\hat{h}(P) \geq c(\rho) h_{\mathrm{Falt}}(A/K).$$

Thus for example the first result says that Szpiro's conjecture implies Lang's conjecture for elliptic curves, whereas the second says that Lang-Silverman's conjecture is true for abelian varieties such that the following inequality holds: $h_{\mathrm{Falt}}(A/K) \gg\ll \frac{1}{[K:\mathbf{Q}]}\sum_{v\mid\infty}\|\operatorname{im}\tau_v\|$.

The regulator and minimal non zero height also have an impact on the number of points of given height in $A(K)$ (see for example [HS2]).

Lemma 4.4. *Let L be an ample line bundle on A/K, put $M_{A,L}(X) := \operatorname{Card}\{x \in A(K) \mid \hat{h}_L(x) \le X\}$, then :*

$$M_{A,L}(X) \quad \textit{is} \quad \begin{cases} = & a(A,L,K)X^{r/2} + O(X^{(r-1)/2}) \\ \le & |A(K)_{\mathrm{tor}}|\left(2\sqrt{\frac{X}{\hat{h}_{\min}}}+1\right)^r \end{cases}$$

where $a(A,L,K) = v_r|A(K)_{\mathrm{tor}}|/\sqrt{\operatorname{Reg}(A/K)}$ with $v_r = \pi^{r/2}\Gamma(1+r/2)$, the volume of the unit ball in $\mathbf{R}^r$.

This lemma, combined with Lang's conjecture and a uniform proof of Faltings theorem (Mordell conjecture) yields uniform bounds for the number of points on a curve C/K of genus g of the type (see [DeD]) :

$$\operatorname{Card} C(K) \le |J_C(K)_{\mathrm{tor}}|\, c^{\operatorname{rank} J_C(K)+1}.$$

5. The size of generators of the Mordell-Weil group.

Concerning the torsion part of the group of rational points we have the following theorem which completes earlier work of Mazur and Kamienny.

Theorem 5.1. (Merel) *The cardinality of the group of torsion points of an elliptic curve E/K is bounded uniformly in terms of $[K:\mathbf{Q}]$.*

Even if the evidence for it is scarce, the following conjecture is folklore.

Conjecture 5.2. *The cardinality of the group of torsion points of an abelian variety A/K is bounded uniformly in terms of $g = \dim A$ and K.*

Remark. Playing with restriction of scalars, one sees easily that, if the conjecture is true in all dimensions over $\mathbf{Q}$, then it is true with a bound depending only on g and $[K:\mathbf{Q}]$; indeed $A(K)_{\mathrm{tor}} = \left(R^K_{\mathbf{Q}}A\right)(\mathbf{Q})_{\mathrm{tor}}$. Notice also that lemma 3.6 provides a weak substitute which in fact will be sufficient for our purposes.

Estimates for $L^*(A,1)$. We start with upper bounds :

Lemma 5.3.

(i) Assume analytic continuation and functional equation for $L(A,s)$ as in (3.26) then

$$|L^*(A,1)| \le 2^r N_A^{1/4}(\log N_A)^{2g}. \tag{5.1}$$

(ii) Assume further Riemann's hypothesis for $L(A,s)$ then

$$|L^*(A,1)| \ll N_A^{\epsilon}. \tag{5.2}$$

Sketch of proof (see for example [Lang1] for an analogous treatment of $\zeta_K(s)$). Observing that $|L(A,s)| \le \zeta(\sigma - 1/2)^{2g}$ we can bound $L(A,s)$ in say $\Re(s) \ge \frac{3}{2}+\eta$ and using the functional equation we also get bounds for $\Re(s) \leq \frac{1}{2} - \eta$; applying the Pragmen-Lindelöf principle provides bounds in the critical strip of the type $|L(A, \sigma + it)| \ll N_A^{a(\sigma)}(1 + |t|)^{b(\sigma)}$ and working out details (i) follows out of the use of Cauchy's inequality; this is the so-called convexity bound. For the proof of (ii), one applies first the Borel-Carathéodory lemma to the function $\log L(A, s)$ to find that $|\log L(A, 1+\delta+it)| \ll \log(N|t|)/\delta$; one then applies Hadamard three circles lemma to obtain $|\log L(A, 1+\delta+it)| \ll (\log(N|t|))^{1-\delta+\epsilon}/\delta$ and hence $|L(A, 1+\delta+it)| \ll (N|t|)^{\epsilon}$. Applying once again the functional equation and Phragmen-Lindelöf principle and Cauchy's inequality yields (ii). □

Based on analogy with Siegel's theorem – giving lower bounds for the value at $s = 1$ of Dirichlet L-functions or the residue of Dedekind zeta function – and results of Hoffstein-Lockhart [HL] – giving lower bounds for the value of the residue at $s = 1$ of the convolution series associated to an elliptic curve or a modular form f – which can be rephrased respectively as

$$\Delta_K^{-\epsilon} \ll \mathrm{Res}_{s=1}\,\zeta_K(s) \ll \Delta_K^{\epsilon} \quad \text{and} \quad N^{-\epsilon} \ll \mathrm{Res}_{s=1}\,L(s, f \times f) \ll N^{\epsilon}, \tag{5.3}$$

it seems not absurd to conjecture the following (even if I have to admit it is the one for which there is less evidence) :

Conjecture 5.4.

$$N_A^{-\epsilon} \ll |L^*(A, 1)| \ll N_A^{\epsilon}. \tag{5.4}$$

We have seen that the upper bound would follow from the generalised Riemann Hypothesis; a necessary condition for the validity of the lower bound is that the function $L(A, s)$ shouldn't have a zero too close to 1; indeed one can show that the lower bound in conjecture 5.4 implies that the zero of $L(s)$ which is closest to 1 is at a distance $\gg N^{-\epsilon}$. In fact Mestre [Mes] has observed experimentally for elliptic curves over $\mathbf{Q}$ that the closest zero seemed to be at a distance $\gg 1/\log N_A$ which is a good sign. To be more precise, writing $\Lambda(A, s)$ as an Hadamard product and using the functional equation, one gets

$$\Lambda(A, s) = \Lambda(2)e^{\left(-\frac{\Lambda'}{\Lambda}(2)+r\right)s}(s-1)^r \prod_{\rho \neq 1}\left(1 - \frac{s}{\rho}\right)\exp\frac{s}{\rho},$$

hence after some algebra:

$$L^*(A, 1) = L(2)e^{-\frac{L'}{L}(2)+r-g\frac{\Gamma'}{\Gamma}(2)} \prod_{\rho \neq 1}\left(1 - \frac{1}{\rho}\right)\exp\frac{1}{\rho}.$$

So the behaviour of $L^*(A, 1)$ depends essentially on the product

$$B_A := \prod_{\rho \neq 1}\left(1 - \frac{1}{\rho}\right)\exp\frac{1}{\rho}$$

where the product is taken over all zeroes of $L(A, s)$ in the critical strip, different from 1. The influence of the zeroes closest to 1 is thus made visible.

Finally we observe that the natural analog for abelian varieties over function fields with finite characteristic is an easy corollary of Liouville's inequality (see [HP]).

Putting everything together we arrive at the following conjecture, which we view as an analog of the Brauer-Siegel theorem.

Conjecture 5.5. *For all* $\epsilon > 0$ *and abelian variety* A/K, *we have*

$$H(A)^{1-\epsilon} \ll |\text{Ш}(A/K)| \operatorname{Reg}(A/K) \ll H(A)^{1+\epsilon}. \tag{5.5}$$

The implicit constants depend on K, g, ϵ and, albeit slightly[2], on r. Of course one may rephrase the conjecture as saying that

$$\log\left(|\text{Ш}(A/K)| \operatorname{Reg}(A/K)\right) \sim h(A).$$

In the case of elliptic curve, we may rephrase this in term of the "naïve" height $H^*(E) = \max\left\{|c_4|^{1/4}, |c_6|^{1/6}\right\}$ and get then (conjecturally):

$$\log\left(|\text{Ш}(E/K)| \operatorname{Reg}(E/K)\right) \sim h^*(E).$$

We record the now obvious :

Proposition 5.6. *Assuming Birch & Swinnerton-Dyer's conjecture and conjectures* 3.2 *and* 5.4, *the previous conjecture follows.*

Comments. 1) Looking at the function field case in positive characteristic, Szpiro's conjecture is known and the Birch & Swinnerton-Dyer "almost proven" (i.e. true provided one assumes that the ℓ-part of the Tate-Shafarevic is finite for some ℓ) one can show that a suitable analog of conjecture 5.5 is true under the same hypothesis (see [HP]).

2) This should of course be compared with Lang's conjecture [Lang3] which asserts that

$$|\text{Ш}(A/\mathbf{Q})| \operatorname{Reg}(A/\mathbf{Q}) \ll H(E) N^{\epsilon(N)} c^r (\log N)^r \tag{5.6}$$

Since $\log N \ll h(A)$, we see that the upper bounds of (5.5) and (5.6) are the same, except perhaps the term $(\log N)^r$ which is $O(H(E)^\epsilon)$ only if $r = o(\log N/\log\log N)$. Thus, apart from a simplification of the upper bound, the conjectural insight we add is that the upper bound is almost an equivalent and should yield a "Brauer-Siegel type" formula (note also that Lang's "$H(E)$" is $H(E)^{12}$ in our notation).

3) We have obviously $1 \leq |\text{Ш}(A/K)|$, also according to Lang's conjecture 4.2 we should have $1 \ll \operatorname{Reg}(A/K)$ hence the previous conjectures provide bounds for the Tate-Shafarevic group and the regulator of the shape

$$|\text{Ш}(A/K)| \ll H(A)^{1+\epsilon} \qquad \text{and} \qquad \operatorname{Reg}(A/K) \ll H(A)^{1+\epsilon} \tag{5.7}$$

and in particular, granting many conjectures, we obtain generators for the Mordell-Weil group with height $O\left(H(A)^{1+\epsilon}\right)$. Using the generalised Szpiro conjecture we may reformulate these bounds in terms of the conductor, obtaining :

$$|\text{Ш}(A/\mathbf{Q})| \ll N_A^{\frac{g}{2}+\epsilon} \qquad \text{and} \qquad \operatorname{Reg}(A/\mathbf{Q}) \ll N_A^{\frac{g}{2}+\epsilon}. \tag{5.8}$$

[2] Notice than the rank will appear through terms of the shape c^r which are $\ll N^\epsilon$ as soon as $r = o(\log N)$. The latter is not known in general but would follow from BSD and GRH (see [Mes]).

4) The bound thus predicted for the Tate-Shafarevic group is compatible with the bounds proposed by Mai-Murty [MaMu] and Goldfeld-Szpiro [Gold-Sz] for elliptic curves.

5) Obviously, if the rank is zero the regulator is just 1 and we also obtain

$$H(A)^{1-\epsilon} \ll |\text{Ш}(A/K)| \ll H(A)^{1+\epsilon}$$

implying that the Tate-Shafarevic group can be very large (see Mai-Murty for a precise statement, depending of course on the Birch & Swinnerton-Dyer conjecture). We can propose another type of example. Consider an abelian variety A defined over $\mathbf{Q}(T)$, assume for simplicity that the Chow trace is zero and put $r = \operatorname{rk} A(\mathbf{Q}(T))$; then by a theorem of Silverman (see [Sil2]), almost all fibres A_t have rank at least r over $\mathbf{Q}$ and more precisely the points $P_i(t)$ are independent and satisfy

$$\det\left(\langle P_i(t), P_j(t)\rangle_{A_t}\right) \sim \det\left(\langle P_i, P_j\rangle_A\right) h(t)^r$$

therefore one can show that, for fibres of rank exactly r we have $\operatorname{Reg}(A_t/\mathbf{Q}) \ll h(t)^r$ (if we assume further Lang's conjecture we even have $h(t)^r \ll \operatorname{Reg}(A_t/\mathbf{Q}) \ll h(t)^r$). Now $h(A_t) \sim \lambda h(t)$, therefore, for the fibres with rank r we would obtain again $H(A_t)^{1-\epsilon} \ll |\text{Ш}(A_t/\mathbf{Q})|$.

6) Finally we observe that, if true, conjecture (5.5) explains, at least partially, the difficulty of computing the Mordell-Weil group since it predicts that either the regulator is huge (i.e. exponential in the input measured by $h(A)$) and hence finding generators will be difficult because of the mere size of them, or the Tate-Shafarevic group is huge, and thereby provides a very large obstruction in the descent computations relating the Selmer group to the Mordell-Weil group. As was commented to me by Henri Cohen and Jan Nekovář, there are at least two instances which escape this rough analysis : the case where we have some transcendental construction of rational points (e.g. when the rank is one, Heegner points) and the case where the generators are small and the Tate-Shafarevic group, though very large, has odd order (resp. order not divisible by a small prime ℓ) because the 2-descent (resp. the ℓ-descent) will then be very efficient.

Bibliography.

[ABC] Ankeny, N.; Brauer, R.; Chowla, S. *A note on the class-numbers of algebraic number fields.* Amer. J. Math. 78 (1956), 51–61.

[Ar] Artin M.. *Néron Models*, in *Arithmetic Geometry* (Ed. Cornell-Silverman), Springer 1986, 213–230.

[BLR] Bosch S.; Lütkebohmert W.; Raynaud M., *Néron models.* Ergebnisse der Mathematik und ihrer Grenzgebiete, 21. Springer-Verlag, Berlin, 1990.

[Bost] Bost J-B., *Périodes et isogenies des variétés abéliennes sur les corps de nombres (d'après D. Masser et G. Wüstholz).* Séminaire Bourbaki, Vol. 1994/95. Astérisque No. 237 (1996), Exp. No. 795, 4, 115–161.

[CW] Coates, J.; Wiles, A., *On the conjecture of Birch and Swinnerton-Dyer.* Invent. Math. 39 (1977), no. 3, 223–251.

[Co-Si] Cornell G., Silverman J. (ed), *Arithmetic geometry.* Storrs conference, 1984. Springer-Verlag, New York, 1986.

[Cr] Cremona, J. ; *Algorithms for modular elliptic curves.* Cambridge University Press, 1992 (2nd edition 1997).

[Dav] David S., *Minorations de hauteurs sur les variétés abéliennes.* Bull. Soc. Math. France 121 (1993), no. 4, 509–544.

[DeD] De Diego T., *Points rationnels sur les familles de courbes de genre au moins 2.* J. Number Theory 67 (1997), no. 1, 85–114.

[Del1] Deligne P., *Un théorème de finitude pour la monodromie.* In Discrete groups in geometry and analysis, 1–19, Progr. Math., 67, Birkhäuser, Boston, 1987.

[Del2] Deligne, P., Preuve des conjectures de Tate et de Shafarevitch (d'après G. Faltings). Séminaire Bourbaki, Vol. 1983/84. Astrisque No. 121-122, (1985), 25–41.

[Fal1] Faltings G., *Calculus on arithmetic surfaces.* Annals of Math. 119 (1984), 387–424.

[Fal2] Faltings G., *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern.* Invent. Math. 73 (1983), no. 3, 349–366.

[Gold] Goldfeld D., *Sur les produits partiels eulériens attachés aux courbes elliptiques.* C. R. Acad. Sci. Paris Sér. I Math. 294 (1982), no. 14, 471–474.

[Gold-Sz] Goldfeld D.; Szpiro L., *Bounds for the order of the Tate-Shafarevich group.* Compositio Math. 97 (1995), no. 1-2, 71–87.

[GZ] Gross B.; Zagier D., *Heegner points and derivatives of L-series.* Invent. Math. 84 (1986), no. 2, 225–320.

[HP] Hindry M.; Pacheco A., *Sur un analogue du théorème de Brauer-Siegel pour les variétés abéliennes sur les corps de fonctions en caractéristique p.* In preparation.

[HS1] Hindry M.; Silverman J., *The canonical height and integral points on elliptic curves.* Invent. Math. 93 (1988), no. 2, 419–450.

[HS2] Hindry M.; Silverman J., *Diophantine geometry. An introduction.* Graduate Texts in Mathematics, 201. Springer-Verlag, New York, 2000.

[HL] Hoffstein J.; Lockhart P., *Coefficients of Maass forms and the Siegel zero.* With an appendix by Dorian Goldfeld, Hoffstein and Daniel Lieman. Ann. of Math. (2) 140 (1994), no. 1, 161–181.

[Kol] Kolyvagin, V., *Finiteness of $E(Q)$ and $III(E, Q)$ for a subclass of Weil curves.* (Russian) Izv. Akad. Nauk SSSR Ser. Mat. 52 (1988), no. 3, 522–540, 670–671; translation in Math. USSR-Izv. 32 (1989), no. 3, 523–541.

[Lang1] Lang S., *Algebraic number theory.* Second edition. Graduate Texts in Mathematics, 110. Springer-Verlag, New York, 1994.

[Lang2] Lang S., *Fundamentals of Diophantine geometry.* Springer-Verlag, New York, 1983.

[Lang3] Lang S., *Conjectured Diophantine estimates on elliptic curves.* Arithmetic and geometry, Vol. I, 155–171, Progr. Math., 35, Birkhäuser Boston, 1983.

[MaMu] Mai L.; Murty R., *A note on quadratic twists of an elliptic curve.* Elliptic curves and related topics, 121–124, CRM Proc. Lecture Notes, 4, Amer. Math. Soc., Providence, 1994.

[Man] Manin Y., *Cyclotomic fields and modular curves.* Uspehi Mat. Nauk 26 (1971), no. 6(162), 7–71.

[Mas] Masser D., *Small values of heights on families of abelian varieties.* Diophantine approximation and transcendence theory (Bonn, 1985), 109–148, Lecture Notes in Math., 1290, Springer, Berlin, 1987.

[Mes] Mestre J-F., *Courbes elliptiques et formules explicites.* Séminaire de théorie des nombres, Paris 1981-82, 179-187. Birkhäuser PM 38, 1983.

[Mil] Milne J., *On the arithmetic of abelian varieties.* Invent. Math. 17 (1972), 177–190.

[M-B] Moret-Bailly L., *La formule de Noether pour les surfaces arithmétiques.* Inventiones Math. 98 (1989), 491–498.

[Rub] Rubin, K., *Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication.* Invent. Math. 89 (1987), no. 3, 527–559.

[Sil1] Silverman J., *The arithmetic of elliptic curves.* Graduate Texts in Mathematics, 106. Springer-Verlag, New York, 1986.

[Sil2] Silverman J., *Heights and the specialization map for families of abelian varieties.* J. Reine Angew. Math. 342 (1983), 197–211.

[Ue] Ueno K., *Discriminants of curves of genus* 2 *and arithmetic surfaces.* Algebraic geometry and commutative algebra, Vol. II, 749–770, 1988.

Marc Hindry
U.F.R. Mathématiques, case 7012
Université Paris 7 Denis Diderot
2 Place Jussieu
F-75251 Paris cedex 05
FRANCE

E-mail : hindry@math.jussieu.fr