Regulators of Elliptic Curves

Autissier, Pascal; Hindry, Marc; Pazuki, Fabien

Published in:
International Mathematics Research Notices

DOI:
10.1093/imrn/rny285

Publication date:
2021

Document version
Peer reviewed version

Document license:
Other

Citation for published version (APA):
REGULATORS OF ELLIPTIC CURVES

PASCAL AUTISSIER, MARC HINDRY AND FABIEN PAZUKI

Abstract. We study the regulator of the Mordell-Weil group of elliptic curves over number fields, functions fields of characteristic zero or function fields of characteristic $p > 0$. We prove a new Northcott property for the regulator of elliptic curves of rank at least 4 defined over a number field. In the function field case, we obtain that non-trivial families of elliptic curves with bounded regulators and bounded ranks are limited families. We conclude by asking new questions.

Keywords: Heights, abelian varieties, regulators, Mordell-Weil.

Mathematics Subject Classification: 11G50, 14G40.

1. Introduction

Let $K$ be a number field or a function field of transcendence degree one over its field of constants $k$. Let $A$ be an abelian variety over $K$, where we assume $\text{Tr}_{K/k}(A) = 0$ in the case of function fields. Then the group of $K$-rational points $A(K)$ is finitely generated by Néron’s thesis, generalizing the Mordell-Weil Theorem. For a modern exposition of the Lang-Néron results, we refer to [Con06]. Giving more arithmetic information about the Mordell-Weil group is a difficult problem in general, as explained for instance in [Hin07]. A central notion attached to the group of $K$-rational points is the regulator. Its appearance in the strong form of the Birch and Swinnerton-Dyer conjecture, or in statements à la Brauer-Siegel given in [HiPa16] stresses the importance of it when studying the arithmetic of elliptic curves and of abelian varieties in general. We refer to [Paz14] [Paz16] for the proof of a Northcott property of regulators of number fields, and for a conjectural similar statement for abelian varieties.

The three authors are supported by ANR-17-CE40-0012 Flair. The first and third authors are supported by ANR-14-CE25-0015 Gardio. The third author is supported by the DNRF Niels Bohr Professorship of Lars Hesselholt. The authors would like to thank Gaël Rémond for his remarks, and the referee for his work and his helpful comments.
The main result obtained here concerns the regulator of elliptic curves over number fields. We use $h(.)$ for the Weil height of algebraic numbers.

**Theorem 1.1.** Let $E$ be an elliptic curve defined over the number field $K$. Let $d = [K : \mathbb{Q}]$ and $m$ be the Mordell-Weil rank of $E(K)$. Assume $m \geq 1$. Denote $h = \max\{1, h(j_E)\}$. Then there is a $c(d, m) > 0$ depending at most on $d$ and on $m$, such that

$$\frac{\text{Reg}(E/K)}{\left(\text{Card} \ E(K)_{\text{tors}}\right)^2} \geq c(d, m) h^{\frac{m-4}{3}} \left(\log(3h)\right)^\frac{2m+2}{3},$$

and one may take $c(d, m) = \frac{c^m}{m^m d^{m+2} (\log(3d))^{m+1}}$, where $c > 0$ is an absolute constant.

It implies immediately the following corollary.

**Corollary 1.2.** Let $K$ be a number field and $m \geq 4$ be an integer. There are at most finitely many $\overline{K}$-isomorphism classes of elliptic curves over $K$ with rank $m$ and bounded regulator.

Theorem 1.1 has other interesting consequences. For instance, combining with classical estimates on the asymptotic of the number of points of bounded height on elliptic curves (see for instance [Lan83] Theorem 7.4 page 126 and Theorem 7.5 page 127), one remarks the following.

**Remark 1.3.** Pick an elliptic curve $E$ of rank $m \geq 1$ over the number field $K$ of degree $d$ and let $\hat{h}_E$ be the Néron-Tate height on $E$. Then

$$\text{Card}\{P \in E(K) \mid \hat{h}_E(P) \leq T\} \sim c_E T^{m/2},$$

where $T \to +\infty$ is a real number, and

$$c_E = \frac{\pi^{m/2}}{\Gamma\left(\frac{m}{2} + 1\right)} \text{ Card} \ E(K)_{\text{tors}} \sqrt{\text{Reg}(E/K)},$$

$\Gamma$ being the gamma function. One sees here that $c_E$ is essentially the inverse of the square root of the quotient studied in Theorem 1.1 which implies the estimate

$$c_E \leq c'(d, m) h^{-\frac{m-4}{6}} \left(\log(3h)\right)^{-\frac{m+1}{3}},$$

where $c'(d, m)$ is a positive real number depending at most on $d$ and $m$.

The proof of Theorem 1.1 relies on a general approach to bound the regulator from below using counting arguments of points of small height and explained in Lemmas 3.1 and 3.2. Direct application of counting results of David [Dav97] would then give 16 instead of 4 in Corollary 1.2. To be able to go down to 4, we combine the counting results of David [Dav97] and of Petsche [Pet06], the Lemma 3.4 and provide a non-trivial optimization of parameters.

We also obtain similar statements in the function field case, with the natural restrictions inherent to this other context (non-isotriviality, bounded inseparability degree, limited families).

The article starts by recalling the relevant definitions in Section 2. In Section 3 we give the general approach to obtain lower bounds on the regulator of an abelian variety in any dimension. In Section 4 we focus on elliptic curves defined over a number field and we prove Theorem 1.1. In Sections 5 and 6 we give the counterparts respectively for elliptic curves over function fields in characteristic zero and characteristic $p > 0$. In Section 7 we propose new questions about the growth of regulators of elliptic curves and abelian varieties.

Throughout the text, we use the logarithm $\log$ normalized by $\log(e) = 1$. 

2. Definitions

2.1. Number fields. Let $K$ be a number field of degree $d$. Let $M_K$ be a complete set of inequivalent absolute values $|.|_v$ on $K$, given local degrees $n_v$ and normalized by $|p|_v = 1/p$ for any $v|p$, for the underlying rational prime $p$. Hence the product formula holds:

$$\forall x \in K - \{0\}, \sum_{v \in M_K} n_v \log |x|_v = 0.$$ 

The height on $K$ is defined by the formula

$$h(x) = \frac{1}{d} \sum_{v \in M_K} n_v \log \max\{1, |x|_v\}.$$ 

Let $E$ be an elliptic curve defined over the number field $K$, with neutral element $O$. We define the Néron-Tate height on the group of rational points $E(K)$ with respect to $(O)$ by

$$\hat{h}_E(P) = \frac{1}{2} \lim_{n \to \infty} \frac{1}{n^2} h(x([n]P)).$$

2.2. Function fields. Let $K = k(C)$ be the function field of a smooth projective and geometrically connected curve $C$ defined over $k$ and of genus $g$. We denote by $M_K$ a complete set of inequivalent valuations $v(.)$ and given with local degrees $n_v$ (from each point $a \in C$ one has a valuation given for $x \in K$ by $a(x) = \text{ord}_a(x)$, and $n_v = [k(a) : k]$), which gives a normalization such that for any non-zero element $x \in K$, the product formula holds:

$$\sum_{v \in M_K} n_v v(x) = 0.$$ 

The height on $K$ is then defined as $h(0) = 0$ and for any $x \in K - \{0\}$, we pose

$$h(x) = \sum_{v \in M_K} n_v \max\{0, -v(x)\}.$$ 

Let $E$ be an elliptic curve defined over the function field $K$. We define the Néron-Tate height on the group of rational points $E(K)$ with respect to $(O)$ by

$$\hat{h}_E(P) = \frac{1}{2} \lim_{n \to \infty} \frac{1}{n^2} h(x([n]P)).$$

A divisor $I$ on $K$ is a formal sum $\sum_{v \in M_K} a_v \cdot v$ where $a_v \in \mathbb{Z}$ is zero for all but finitely many places $v$. The divisor is effective if for all $v$, $a_v \geq 0$. In that case we pose

$$h(I) = \sum_{v \in M_K} n_v a_v = \deg(I).$$
2.3. **Regulators of abelian varieties.** Let $K$ be a number field or a function field of transcendence degree one over its field of constants $k$. Let $A/K$ be an abelian variety over the field $K$ polarized by an ample and symmetric line bundle $L$. We assume that $A$ has trace zero if $K$ is a function field. Let $m_K$ be the Mordell-Weil rank of $A(K)$. Let $\hat{h}_{A,L}$ be the Néron-Tate height associated with the pair $(A, L)$. We assume that $A$ has trace zero if $K$ is a function field. Let $m_K$ be the Mordell-Weil rank of $A(K)$. Let $\hat{h}_{A,L}$ be the Néron-Tate height associated with the pair $(A, L)$. Let $< ., . >_L$ be the associated bilinear form, given by

$$< P, Q >_L = \frac{1}{2} \left( \hat{h}_{A,L}(P + Q) - \hat{h}_{A,L}(P) - \hat{h}_{A,L}(Q) \right)$$

for any $P, Q \in A(K)$. This pairing on $A \times A$ depends on the choice of $L$.

**Definition 2.1.** Let $P_1, ..., P_{m_K}$ be a basis of the lattice $A(K)/A(K)_{\text{tors}}$, where $A(K)$ is the Mordell-Weil group. The regulator of $A/K$ is defined by

$$\text{Reg}_L(A/K) = \det(< P_i, P_j >_{1 \leq i, j \leq m_K}),$$

where by convention an empty determinant is equal to 1.

As for the height, the regulator from Definition 2.1 depends on the choice of an ample and symmetric line bundle $L$ on $A$.

One usually defines the regulator in a more intrinsic way, that doesn’t depend on the choice of $L$. Start with the natural pairing on the product of $A$ with its dual abelian variety $\hat{A}$ given by the Poincaré line bundle $P$: for any $P \in A(K)$ and any $Q \in \hat{A}(K)$, define $< P, Q >= \hat{h}_{A,\hat{A},P}(P, Q)$. Next choose a base $P_1, ..., P_{m_K}$ of $A(K)$ modulo torsion and a base $Q_1, ..., Q_{m_K}$ of $\hat{A}(K)$ modulo torsion. Then define

$$\text{Reg}(A/K) = |\det(< P_i, Q_j >_{1 \leq i, j \leq m_K})|.$$

Let us recall how these two regulators are linked (see for instance [Hin07]). Let $\Phi_L : A \to \hat{A}$ be the isogeny given by $\Phi_L(P) = t_\mathcal{P}^* L \otimes L^{-1}$. By Proposition 9.3.6 page 291 of [BoGu06], one has the formula

$$< P, Q >_L = \frac{1}{2} < P, \Phi_L(Q) >.$$

Hence if $u$ is the index of the subgroup $\Phi_L(\mathbb{Z}P_1 \oplus ... \oplus \mathbb{Z}P_{m_K})$ in $\hat{A}(K)$ modulo torsion, one has

$$\text{Reg}_L(A/K) = u 2^{-m_K} \text{Reg}(A/K).$$

Let us remark that when $L$ induces a principal polarization, the index $u$ is equal to 1. Hence in the case of elliptic curves, we have $L = (O)$ and

$$\text{Reg}_L(E/K) = 2^{-m_K} \text{Reg}(E/K).$$

3. **Lower bounds for regulators of abelian varieties**

3.1. **Minkowski and regulators.** A natural idea is to apply Minkowski’s successive minima inequality to the Mordell-Weil lattice, we give it here as a lemma.

**Lemma 3.1.** Let $K$ be a number field or a function field of transcendence degree one over its field of constants $k$. Let $A$ be an abelian variety over the field $K$, let $L$ be an ample and symmetric line bundle on $A$. We assume that $A$ has trace zero if $K$ is a function field. Let $m$
be the Mordell-Weil rank of $A(K)$. Assume $m \geq 1$. Let $\Lambda = A(K)/A(K)_{\text{tors}}$. Then for any $i \in \{1, \ldots, m\}$, let us denote the Minkowski $i$th-minimum of $(\Lambda, \sqrt{\hat{h}_{A,L}})$ by $\lambda_i$. We have
\begin{equation}
\lambda_1 \cdots \lambda_m \leq m^{m/2}(\text{Reg}_L(A/K))^{1/2}.
\end{equation}

Proof. Minkowski’s successive minima inequality reads
\begin{equation}
\lambda_1 \cdots \lambda_m \leq \frac{2^m \text{vol}((\Lambda \otimes \mathbb{R})/\Lambda)}{\text{vol}(B(0,1))}.
\end{equation}

As the volume of a Euclidean unit ball in $\Lambda \otimes \mathbb{R} \simeq \mathbb{R}^m$ is $\frac{\pi^{m/2}}{\Gamma(\frac{m}{2}+1)}$, and as $\text{vol}((\Lambda \otimes \mathbb{R})/\Lambda) = (\text{Reg}_L(A/K))^{1/2}$ we obtain
\begin{equation}
\lambda_1 \cdots \lambda_m \leq \frac{2^m \Gamma(\frac{m}{2}+1)}{\pi^{m/2}}(\text{Reg}_L(A/K))^{1/2}.
\end{equation}
Now for any $m \geq 1$, one gets easily $2^m \Gamma(\frac{m}{2}+1) \leq (\pi m)^{\frac{m}{2}}$, it leads to the result. □

Lemma 3.2. Let $A$ be an abelian variety over a number field $K$, let $L$ be an ample and symmetric line bundle on $A$. Let $m$ be the Mordell-Weil rank of $A(K)$. Let $\Lambda = A(K)/A(K)_{\text{tors}}$. Assume $m \geq 1$. Assume one has
\begin{equation}
\text{Card}\{P \in \Lambda \mid \hat{h}_{A,L}(P) \leq H\} \leq C,
\end{equation}
for $H,C$ two fixed positive real numbers. Then for any $1 \leq i \leq m$, the $i$-th successive minimum of $\Lambda$ satisfies
\begin{equation}
\lambda_i^2 \geq \frac{H}{i^2 C^{2/i}}.
\end{equation}

Proof. Let $P_1, \ldots, P_m$ be linearly independent points of $\Lambda$ satisfying $\lambda_i^2 = \hat{h}_{A,L}(P_i)$ for any $1 \leq i \leq m$. Consider the set of all sums $a_1 P_1 + \cdots + a_i P_i$ where for any index $j \in \{1, \ldots, i\}$ the integral coefficient $a_j$ satisfies $0 \leq a_j \leq C^{1/i}$. It contains more than $C$ points, hence (by the assumption) at least one of them has height greater than $H$. This point can be written as $P = a_1 P_1 + \cdots + a_i P_i$, and $\hat{h}_{A,L}(P) \leq i^2 \max\{\hat{h}_{A,L}(a_j P_j) \mid 1 \leq j \leq i\}$ by the triangular inequality for the norm $\sqrt{\hat{h}_{A,L}(\cdot)}$, hence
\begin{equation}
H \leq \hat{h}_{A,L}(P) \leq i^2 C^{2/i} \lambda_i^2.
\end{equation}
□

Lemma 3.1 and Lemma 3.2 combine to give the following.

Corollary 3.3. Let $A$ be an abelian variety over a number field $K$, let $L$ be an ample and symmetric line bundle on $A$. Let $m$ be the Mordell-Weil rank of $A(K)$. Assume $m \geq 1$. Assume one has
\begin{equation}
\text{Card}\{P \in A(K)/A(K)_{\text{tors}} \mid \hat{h}_{A,L}(P) \leq H\} \leq C,
\end{equation}
for $H,C$ two fixed positive real numbers. Then
\begin{equation}
\text{Reg}_L(A/K) \geq \frac{H^m}{m^m (m!)^2} \prod_{i=1}^m \frac{1}{C^{2/i}}.
\end{equation}
3.2. **Regulators and van der Corput.** We show how to improve on Corollary 3.3 by invoking van der Corput.

**Lemma 3.4.** Let $A$ be an abelian variety over a number field $K$, let $L$ be an ample and symmetric line bundle on $A$. Let $m$ be the Mordell-Weil rank of $A(K)$. Assume $m \geq 1$. Assume one has

$$\text{Card}\{P \in A(K)/A(K)_{\text{tors}} \mid \hat{h}_{A,L}(P) \leq H\} \leq C,$$

for $H, C$ two fixed positive real numbers. Then

$$\text{Reg}_L(A/K) \geq \frac{H^m}{m^m C^2}.$$

**Proof.** Consider $K = \{P \in A(K) \otimes \mathbb{R} \mid \hat{h}_{A,L}(P) \leq H\}$. It is a compact symmetric convex set (hence with finite volume) in $A(K) \otimes \mathbb{R} \simeq \mathbb{R}^m$. We apply van der Corput’s result [1], see for instance Theorem 7.1 in [GrLe87], to the lattice $\Lambda = A(K)/A(K)_{\text{tors}}$ to obtain

$$\text{Card}(K \cap \Lambda) \geq \frac{\text{Vol}(K)}{2^m \text{Covol}(\Lambda)} = \frac{H^{m/2}}{2^m (\text{Reg}_L(A/K))^{1/2} \pi^{m/2} \Gamma(\frac{m}{2} + 1)}.$$

This gives directly $\frac{H^{m/2}}{m^m (\text{Reg}_L(A/K))^{1/2}} \leq C$, hence the claim. \qed

**Remark 3.5.** Lemma 3.4 implies directly (with the same notation) that if

$$\text{Card}\{P \in A(K) \mid \hat{h}_{A,L}(P) \leq H\} \leq C,$$

then one has

$$\text{Reg}_L(A/K) \geq \frac{H^m}{m^m C^2 (\text{Card} A(K)_{\text{tors}})^2}.$$

4. **Regulators of elliptic curves over number fields**

To warm up, we will first combine Lemma 3.3 with various height lower bounds.

4.1. **Szpiro and finiteness.** Let us first extract Corollary 4.2 page 430 from [HiSi88].

**Theorem 4.1.** (Hindry-Silverman) Let $K$ be a number field of degree $d$. Let $E/K$ be an elliptic curve and let $P \in E(K)$ be a non-torsion point. Then

$$\hat{h}_E(P) \geq (20 \sigma_{E/K})^{-8d} 10^{-4 \sigma_{E/K}} h(E),$$

where $h(E) = \frac{1}{12} \max\{h(\Delta(E/K)), h(j_E)\}$, with $\Delta(E/K)$ the minimal discriminant of $E/K$ and $j_E$ its $j$-invariant.

Note that [Dav97] or Theorem 2 page 259 of [Pet06] give an inverse polynomial dependence in the Szpiro quotient and in the degree of the number field.

We get the following corollary.

**Corollary 4.2.** Let $K$ be a number field of degree $d$. There are at most finitely many $K$-isomorphism classes of elliptic curves over $K$ with non-trivial bounded rank, bounded regulator and bounded Szpiro quotient.

---

1In the spirit of Blichfeldt’s principle.
Proof. Combine Theorem 4.1 and (3) to get the inequality
\[ \text{Reg}_L(E/K) \geq \frac{1}{m^m} \left( (20 \sigma_{E/K})^{-8d} 10^{-4 \sigma_{E/K} h(E)} \right)^m. \]

As soon as the rank \( m \) is positive and bounded, and as long as \( \sigma_{E/K} \) is bounded, a bounded regulator implies a bounded height. Finiteness of the set of \( K \)-isomorphism classes follows, see Corollary 2.5 of [CoSi86] page 259 for instance. Note that our height is equivalent to Faltings’s height \( h_F(E) \) used by Silverman in the aforementioned corollary, one easily gets \( h_F(E) \ll h(E) \) from the explicit formula for \( h_F(E) \) given in the same reference. \( \square \)

4.2. Big ranks and finiteness. Another approach is based on Corollaire 1.6 page 111 of [Dav97], which we recall here.

**Proposition 4.3.** (David) Let \( K \) be a number field of degree \( d \). Let \( E \) be an elliptic curve defined over \( K \) of rank \( m \geq 1 \). Let \( \Lambda = E(K)/E(K)_{\text{tors}} \). Let \( i \) be an integer such that \( 1 \leq i \leq m \) and \( \lambda_i \) the \( i \)-th successive minimum. Let \( h_i \) be \( \max\{1, h_i(E)\} \). Then
\[ \lambda_i^2 \geq c_{16}(i) h_i(i^2 - 4i - 4)/(i(i^2 + 4i) d^{(i+2)/i}) \left( 1 + \frac{\log(d)}{h} \right)^{-2/i}, \]
and in particular
\[ \lambda_5^2 \geq c_{17} h_1^{1/120} d^{-7/5} \left( 1 + \frac{\log(d)}{h} \right)^{-2/5}. \]

We deduce the following unconditional statement.

**Corollary 4.4.** Let \( K \) be a number field. There are at most finitely many \( \overline{K} \)-isomorphism classes of elliptic curves over \( K \) of fixed rank \( m \geq 16 \) with bounded regulator.

**Proof.** By combining Proposition 4.3 with (3) one obtains
\[
\text{Reg}_L(E/K) \geq \frac{1}{m^m} \prod_{i=1}^{m} c_{16}(i) h_i(i^2 - 4i - 4)/(i(i^2 + 4i) d^{(i+2)/i}) \left( 1 + \frac{\log(d)}{h} \right)^{-2/i}.
\]

A direct computation shows that
\[
\sum_{i=1}^{16} \frac{i^2 - 4i - 4}{4i^2 + 4i} \geq 0.009 \quad \text{and} \quad \sum_{i=1}^{15} \frac{i^2 - 4i - 4}{4i^2 + 4i} \leq -0.16.
\]

Hence as soon as \( m \geq 16 \), if \( m \) and \( d \) are fixed, a bounded regulator implies a bounded \( j \)-invariant, which implies the finiteness of the set of \( \overline{K} \)-isomorphism classes for a fixed base field \( K \). \( \square \)

We will now show how to improve on this corollary using counting results from [Dav97, Pet06] and our Lemma 3.4. We start with a small technical lemma that will help later on.

**Lemma 4.5.** Let \( K \) be a number field of degree \( d \) and let \( I \) be a non-zero integral ideal in \( \mathcal{O}_K \). Let \( S \) be the number of prime ideals dividing \( I \). There is an absolute constant \( c_0 > 0 \) such that
\[
\log N(I) \geq c_0 S \log \left( \frac{S}{d} + 2 \right),
\]
where \( N(I) \) stands for the norm of the ideal \( I \).
Proof. Above each rational prime number $p$, there are at most $d$ prime ideals in $\mathcal{O}_K$. Let us write $S = dq + r$ the Euclidean division of $S$ by $d$, where $0 \leq r < d$. Then one has

\[
\log N(I) \geq d\log p_1 + \ldots + d\log p_q + r\log p_{q+1},
\]

where $p_i$ denotes the $i$-th rational prime number. An easy bound from below is $\log p_i \geq \log(i+1)$ for any integer $i \geq 1$, hence

\[
\log N(I) \geq d\log(q+1)! + r\log(q+2) \geq c_0dq\log(q+3) + c_0r\log(q+3) \geq c_0S\log\left(\frac{S}{d} + 2\right).
\]

We now give the proof of Theorem 1.1.

Proof. (of Theorem 1.1 and Corollary 1.2) By Theorem 1.2 of [Dav97] and Proposition 8 of [Pet06], one has two independent upper bounds, with $c_1, c_2, c_3, c_4$ positive absolute constants:

(a) Card$\{P \in E(K) \mid \hat{h}_E(P) \leq c_1\frac{h_v(E)}{d}\} \leq c_2\frac{d^{m+2}}{h_v(E)}(1 + \log d)$, where one defines $h_v(E) = \max\{n_v\log |E|_v, \rho_v\}$, with $\rho_v = 0$ if $v$ is a finite place of multiplicative reduction and $\rho_v = \sqrt{3}/2$ if $v$ is archimedean.

(b) Card$\{P \in E(K) \mid \hat{h}_E(P) \leq c_3\frac{h(\Delta(E/K))}{\sigma^2}\} \leq c_4d\sigma^2\log(c_4d\sigma^2)$, where $\sigma = \sigma_{E/K}$ is the Szpiro quotient.

First case: if one considers an elliptic curve $E/K$ with $h(j_E) < 1$, one obtains by (a), as $h = 1$ in this case, for the choice $v$ archimedean and Lemma 3.4 (or Remark 3.3):

\[
\frac{\text{Reg}(E/K)}{(\text{Card } E(K)_{\text{tors}})^2} \geq \frac{\text{Reg}_{\text{L}}(E/K)}{(\text{Card } E(K)_{\text{tors}})^2} \geq c_1^m\frac{h_v(E)^{m+2}}{c_3^2d^{m+2}} \frac{1}{m^m(1 + \log d)^2} \geq \frac{c_1^m\sqrt{3}^{m+2}}{c_3^2(2d)^{m+2}m^m(1 + \log d)^2},
\]

which is the claimed lower bound in this case.

Thus we may assume from now on that $h(j_E) \geq 1$. Let us denote $K' = K[\sqrt{E[12]}]$. The elliptic curve $E$ is semi-stable over $K'$ and the degree $d' = [K' : \mathbb{Q}] \leq [K : \mathbb{Q}]\text{Card }GL_2(\mathbb{Z}/12\mathbb{Z}) = 4608d$. Note that for any place $v$ of $K'$ one has

\[
\text{Card}\left\{P \in E(K) \mid \hat{h}_E(P) \leq c_1\frac{h_v(E)}{d'}\right\} \leq \text{Card}\left\{P \in E(K') \mid \hat{h}_E(P) \leq c_1\frac{h_v(E)}{d}\right\}.
\]

Similarly, with $\sigma = \sigma_{E/K'}$ and $\Delta = \Delta(E/K')$, one has

\[
\text{Card}\left\{P \in E(K) \mid \hat{h}_E(P) \leq c_3\frac{h(\Delta)}{\sigma^2}\right\} \leq \text{Card}\left\{P \in E(K') \mid \hat{h}_E(P) \leq c_3\frac{h(\Delta)}{\sigma^2}\right\}.
\]

Both $h$ and $\hat{h}_E(P)$ are invariant by field extension, so (a), (b) and Lemma 3.4 (or Remark 3.3) with $H = c_1h_v(E)/d'$ and $C = c_2d'h(1 + (\log d')/h)/h_v(E)$ for the first inequality and $H = c_3h(\Delta)/\sigma^2$ and $C = c_4d'\sigma^2\log(c_4d'\sigma^2)$ for the second inequality) imply that for any elliptic curve $E/K$ with $h(j_E) \geq 1$, and keeping $m$ the rank of $E$ over $K$, for any place $v$ of $K'$ of multiplicative reduction or archimedean,

\[
\frac{\text{Reg}(E/K)}{(\text{Card } E(K)_{\text{tors}})^2} \geq \max\left\{\frac{c_1^m\frac{h_v(E)^{m+2}}{c_3^2d^{m+2}}\frac{1}{\sigma^{2m}(c_4d'\sigma^2)^{2m}}}{m^m}, \frac{c_3^m\frac{h(\Delta)^m}{\sigma^{2m}(c_4d'\sigma^2)^{2m}}}{m^m}\right\}
\]
This implies

$$\frac{\text{Reg}(E/K)}{\text{Card } E(K)_{\text{tors}}}^2 \geq \max \left\{ \frac{c_1^m h_v(E)^{m+2}}{h^2}, \frac{c_2^m h(\Delta)^m}{(c_4 d')^2 \sigma^{2m+4}(\log(c_4 d' \sigma^2))^2} \right\} \frac{1}{m^m(1 + \log d')^2}. $$

Now using $d' \leq 4608d$ and $\log(c_4 d' \sigma^2) \ll \log(3h(\Delta))$ with an implied constant depending at most on $d$, and let $c(d, m) > 0$ stand for a quantity depending at most on $d$ and $m$ and that may slightly change along the way, we get

$$\frac{\text{Reg}(E/K)}{\text{Card } E(K)_{\text{tors}}}^2 \geq \max \left\{ \frac{h_v(E)^{m+2}}{h^2}, \frac{h(\Delta)^m}{\sigma^{2m+4}(\log(3h(\Delta)))^2} \right\} c(d, m).$$

Second case: assume $h(\Delta) \leq \frac{h}{2}$. As one has

$$h = h(j_E) = h(\Delta) + \frac{1}{d'} \sum_{v \in M_{K'}} n_v \log \max \{|j_E|_v, 1\},$$

there exists an archimedean place $v$ such that $\log \max \{|j_E|_v, 1\} \geq \frac{h}{2}$, hence one deduces $h_v(E) \geq \frac{h}{2}$. So (12) implies

$$\frac{\text{Reg}(E/K)}{\text{Card } E(K)_{\text{tors}}}^2 \geq c(d, m) \frac{(h/2)^{m+2}}{h^2} \geq c(d, m) h^m,$$

which is a better lower bound than the one claimed.

Third case: assume $h(\Delta) \geq \frac{h}{2}$. Let $S'$ stand for the number of places in $K'$ where $E$ has multiplicative reduction. We have in particular $S' \neq 0$ and by considering $v$ the finite place of $K'$ with maximal $h_v(E)$, one gets by the semi-stability assumption

$$h_v(E) \geq \frac{h(\Delta)d'}{S'},$$

and by Lemma 4.5 there is an absolute $c_0 > 0$ such that

$$\frac{h(\Delta)d'}{\sigma} = \log N(F(E/K')) \geq c_0 S' \log \left( \frac{S'}{d'} + 2 \right),$$

hence

$$\frac{h(\Delta)d'}{c_0 S' \log \left( \frac{S'}{d'} + 2 \right)} \geq \sigma,$$

inject (14) and (16) in (12), and get:

$$\frac{\text{Reg}(E/K)}{\text{Card } E(K)_{\text{tors}}}^2 \geq c(d, m) \max \left\{ \frac{h(\Delta)^m}{(S')^{m+2}}, \frac{h(\Delta)^m}{S' \log \left( \frac{S'}{d'} + 2 \right)} \right\}.$$
\[
\frac{\text{Reg}(E/K)}{(\text{Card } E(K)_{\text{tors}})}^2 \geq c(d, m) h(E) (\log(3h(E)))^{\frac{(2m+2)(m+2)}{3m+4}},
\]
which gives directly
\[
\frac{\text{Reg}(E/K)}{(\text{Card } E(K)_{\text{tors}})}^2 \geq c(d, m) h(E)^{\frac{m-4}{3}} (\log(3h(E)))^{\frac{2m+2}{3}},
\]
as claimed.

Subcase (ii): assume \(S' > d' h(E)^{\frac{2}{3}} (\log(3h(E)))^{-\frac{2m+2}{3m+4}}\). Then the second part of (17) implies
\[
\frac{\text{Reg}(E/K)}{(\text{Card } E(K)_{\text{tors}})}^2 \geq c(d, m) h(E) (\log(3h(E)))^{\frac{(2m+2)(m+2)}{3m+4}},
\]
which ends the analysis of this last case with
\[
\frac{\text{Reg}(E/K)}{(\text{Card } E(K)_{\text{tors}})}^2 \geq c(d, m) h(E)^{\frac{m-4}{3}} (\log(3h(E)))^{\frac{2m+2}{3}}.
\]
A careful study of the different cases gives the claim for \(c(d, m)\) and this concludes the whole proof of Theorem 1.1.

To obtain Corollary 1.2 note that a bounded regulator and a fixed rank \(m \geq 4\) implies a bounded \(j\)-invariant, hence the claimed finiteness.

\[\square\]

Remark 4.6. There exists infinitely many elliptic curves over \(\mathbb{Q}\) with rank at least 19, we refer to the work of Elkies [Elk08]. They are obtained by specialization of an elliptic curve with rank at least 19 over \(\mathbb{Q}(T)\).

Remark 4.7. It is easier to produce elliptic curves of rank at least 5 over \(\mathbb{Q}(T)\), and we thank Jean-François Mestre for pointing this out. Pick a generic long Weierstrass equation \((W)\) : \(y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6\). We have five parameters \((a_1, a_3, a_2, a_4, a_6)\). Choose the points \((0, 0), (1, 1), (2, 3), (3, -1), (T, 2)\). There exists a unique non-constant set of parameters \((a_1, a_3, a_2, a_4, a_6) \in \mathbb{Q}(T)^5\) such that \((W)\) passes through these five points. These points are generically independent on the curve defined by \((W)\). See also [Mes91] for explicit examples with rank bigger than 11 over \(\mathbb{Q}(T)\). Then use specialization to obtain families over \(\mathbb{Q}\) with big ranks.

5. Regulators of elliptic curves over function fields of characteristic zero

We will combine lemma 3.1 with the following theorem.

Theorem 5.1. (Hindry-Silverman [HiSi88], Theorem 6.1 page 436) Let \(K\) be a function field of characteristic zero and genus \(g\). Let \(E/K\) be an elliptic curve of discriminant \(\Delta(E/K)\) and let \(P \in E(K)\) be a non-torsion point. Then
\[
\hat{h}_E(P) \geq 10^{15.5-23g} h(E),
\]
where \(h(E) = \frac{1}{2} \deg \Delta(E/K)\). The same inequality is valid for elliptic curves over function fields in characteristic \(p > 0\) if the \(j\)-map has inseparable degree 1.
We can now deduce the following statement by looking at Moret-Bailly’s results on families of abelian varieties with bounded height. We first recall the definition of a limited family.

**Definition 5.2.** Let $\mathcal{A}_1$ be the coarse moduli space of elliptic curves over $K$ (i.e. the affine line of $j$-invariants). Let $\mathcal{E}$ be a set of elliptic curves defined over $K$. The set $\mathcal{E}$ is limited if there exists a variety $T$ over the field of constants $k \subseteq K$, an open set $U \subseteq T_K$ surjective on $T$ and a $k$-morphism $f : U \to \mathcal{A}_1$ such that for any $E \in \mathcal{E}$, there is an $x \in T(k)$ with $f(x_K)$ being the image of $E$ in $\mathcal{A}_1(K)$.

**Corollary 5.3.** Let $K$ be a function field of characteristic zero and genus $g$. The set of elliptic curves of trace zero over $K$, with non-trivial bounded rank and bounded regulator is limited.

**Proof.** Apply Theorem 5.1 and (3) to get the inequality

$$\text{Reg}_L(E/K) \geq \frac{1}{m^m} \left( 10^{-15.5-23gh(E)} \right)^m.$$ 

As soon as one fixes $m > 0$, a bounded regulator implies a bounded height. Then apply [MB85] Théorème 4.6 page 236.

2 Confer Définition 1.1 page 212 of [MB85] for limited families in more general settings.

6. Regulators of elliptic curves over function fields of positive characteristic

We will combine lemma 3.1 with the following consequence of [HiSi88], which improves on Lemma 6.6 page 998 of [Nas16].

**Theorem 6.1.** (based on Hindry-Silverman [HiSi88], see also [Nas16]) Let $P$ be a point of infinite order on $E$ over $k(C)$ of positive characteristic $p$ and genus $g$, and assume that the $j$-map of $E$ has inseparable degree $p^e$. Then one has

$$\hat{h}_E(P) \geq p^{-2e}10^{-15.5-23gh(E)}.$$ 

**Proof.** There exists a curve $E_0$ of inseparable degree 1 such that $\phi^e : E_0 \to E = E_0^{(p^e)}$ is the $e$-th Frobenius isogeny. Denote the dual isogeny by $\hat{\phi}^e$. We compute

$$\hat{h}_E(P) = p^{-e}\hat{h}_{E_0}(\hat{\phi}^e(P)) \geq p^{-e}10^{-15.5-23gh(E_0)},$$

where this last inequality comes from the separable case (see Theorem 5.1) and since $h(E) = p^e h(E_0)$, we are done.

In link with this Theorem 6.1, the interested reader should note that the remark page 434 of [HiSi88] is inaccurate. Moreover, in Theorem 7 of [GoSz95] one should assume $e = 0$.

**Corollary 6.2.** Let $K$ be a function field of characteristic $p > 0$ and genus $g$. The set of elliptic curves of trace zero over $K$, with non-trivial bounded rank, bounded inseparability degree and bounded regulator is limited, and finite when $K$ has finite constant field.

**Proof.** Apply Theorem 6.1 and (3) to get the inequality

$$\text{Reg}_L(E/K) \geq \frac{1}{m^m} \left( p^{-2e}10^{-15.5-23gh(E)} \right)^m.$$ 

As soon as the rank $m$ is positive and bounded, and as long as $e$ is bounded, a bounded regulator implies a bounded height. Then apply [MB85] Théorème 4.6 page 236.
7. Questions

7.1. Regulator and rank.

**Question 7.1.** Let $E$ be an elliptic curve over a number field $K$. Let $m_K$ be its Mordell-Weil rank. Can one prove

$$\text{Reg}(E/K) \geq c_0 m_K,$$

where $c_0 > 0$ is a constant depending at most on $K$?

The case of rank zero is trivial. Already in rank one, it would imply a non-trivial lower bound on the height of a generator of $E(K)$.

7.2. Small points on an elliptic curve. A weaker version of Lang’s conjectural inequality would already provide new insights.

**Question 7.2.** Let $E$ be an elliptic curve over a number field $K$. Let $P$ be a $K$-rational point of infinite order. Can one prove

$$\hat{h}_E(P) \geq f(h(E)),$$

where $f$ is a function tending to infinity when $h(E)$ tends to infinity?

The interest here comes from the following remark: if one combines (22) with inequality (3), this would imply a big improvement on Corollary 1.2 by replacing the condition $m \geq 4$ by $m \geq 1$. Note that the inequality $\hat{h}_E(P) \geq c_0 > 0$, where $c_0$ depends at most on $K$, is already an open and interesting problem though.

7.3. Regulator and injectivity volume. The Lang-Silverman conjecture in dimension $g \geq 1$, or the ABC conjecture in dimension 1, imply that on a simple principally polarized abelian variety $(A, L)$ of dimension $g$ over a number field $K$, when the rank is non-zero we have $\lambda_1^2 \gg h(A)$.

Let $\rho_\sigma(A, L)$ be the injectivity diameter of $A_\sigma(\mathbb{C})$ and $V_\sigma(A, L)$ be the injectivity volume, as described in [Aut16]. We would thus get by the Matrix Lemma

$$m \text{Reg}_L(A/K)^{1/m} \gg \lambda_1^2 \gg h(A) \gg \sum_{\sigma: K \to \mathbb{C}} \frac{1}{\rho_\sigma(A, L)^2} \gg \sum_{\sigma: K \to \mathbb{C}} \frac{1}{V_\sigma(A, L)^{1/g}},$$

where all the implied constants are positive and may depend on $K$ and $g$.

**Question 7.3.** Can one prove independently

$$\text{Reg}_L(A/K) \gg \left( \sum_{\sigma: K \to \mathbb{C}} \frac{1}{V_\sigma(A, L)^{1/g}} \right)^{c_0 m},$$

for a universal $c_0 > 0$? For elliptic curve with $m \geq 5$, the value $c_0 = \frac{1}{10}$ is valid from Theorem 1.1 with an implied constant depending on $K$ and on $m$.

**References**


Regulators of elliptic curves

13


Institut de Mathématiques de Bordeaux, Université de Bordeaux, 351, cours de la Libération, 33405 Talence, France.

E-mail address: pascal.autissier@math.u-bordeaux.fr

Institut de Mathématiques de Jussieu-PRG, UFR mathématiques de l’Université Paris 7 Denis Diderot, Bâtiment Sophie Germain, 5 rue Thomas Mann, F-75205 Paris CEDEX 13.

E-mail address: marc.hindry@imj-prg.fr

Department of Mathematical Sciences, University of Copenhagen, Universitetsparken 5, 2100 Copenhagen Ø, Denmark.

E-mail address: fpazuki@math.ku.dk