SOME CONSEQUENCES OF MASSER'S COUNTING THEOREM ON ELLIPTIC CURVES

A. GALATEAU, V. MAHÉ

Abstract. We use Masser's counting theorem to prove a lower bound for the canonical height in powers of elliptic curves. We also prove the Galois case of the elliptic Lehmer problem, combining Kummer theory and Masser's result with bounds on the rank and torsion of some groups of rational points on an elliptic curve.

1. Introduction

The classical Lehmer problem. This article is dedicated to the study of the Néron-Tate height on elliptic curves (and their products). The problem of understanding how small the height of a non-torsion point can be finds its origin in a question raised by Lehmer (see [20], §13, page 476), which turned out with time to be formulated as a conjecture. If x is a non-zero algebraic number, we let $h(x)$ be its (absolute logarithmic) Weil height.

Conjecture 1.1 (Lehmer)**.** *For all $x \in \bar{\mathbb{Q}}^*$ not a root of unity:*

$$h(x) \gg \frac{1}{[\mathbb{Q}(x) : \mathbb{Q}]}.$$

The notation $\gg$ means that the inequality is true up to some positive constant. Many particular cases of this conjecture have been solved, for instance if the minimal polynomial of x is non-reciprocal (see Smyth [35]) or has odd coefficients (see Borwein, Dobrowolski and Mossinghoff [5], or Dubickas and Mossinghoff [10] for further results).

There can even be an absolute lower bound for the height if x belongs to some specific infinite extension of $\mathbb{Q}$ (see Amoroso and Dvornicich [2] for the abelian closure $\mathbb{Q}^{\mathrm{ab}}$ of $\mathbb{Q}$, Schinzel [29] for the field $\mathbb{Q}^{\mathrm{tr}}$ of totally real numbers, or Habegger [13] for the field generated by torsion points of an elliptic curve defined over $\mathbb{Q}$). The best general estimate so far is due to Dobrowolski ([9], see [36] for an effective version).

Theorem 1.2 (Dobrowolski)**.** *For all $x \in \bar{\mathbb{Q}}^*$ of degree $D := [\mathbb{Q}(x) : \mathbb{Q}]$ not a root of unity:*

$$h(x) \gg \frac{1}{D}\left(\frac{\log\log(3D)}{\log(2D)}\right)^3.$$

Date: July 14, 2016.

This theorem has been extended in greater dimension by Amoroso and David ([1], or [3] for sharper estimates). As a consequence, they proved the following special case of the Lehmer conjecture.

Theorem 1.3 (Amoroso, David)**.** *For all $x \in \bar{\mathbb{Q}}^*$, not a root of unity, with $\mathbb{Q}(x)/\mathbb{Q}$ Galois:*

$$h(x) \gg \frac{1}{[\mathbb{Q}(x) : \mathbb{Q}]}.$$

Their theorem also covers the case where the degree of the Galois closure of $\mathbb{Q}(x)$ over $\mathbb{Q}$ is bounded by a fixed power of $[\mathbb{Q}(x) : \mathbb{Q}]$.

Points of small height in elliptic curves and abelian varieties. For E an elliptic curve defined over a number field k, Néron and Tate constructed a "canonical" height function

$$\hat{h} : E(\bar{k}) \to \mathbb{R}_+$$

which vanishes exactly on the torsion subgroup of $E(\bar{k})$. Like in the classical case, the height $\hat{h}(P)$ of a point $P \in E(\bar{k})$ is conjectured to be bounded from below in terms of the degree $D := [k(P) : k]$ of P as follows.

Conjecture 1.4 (elliptic Lehmer)**.** *If $P \in E(\bar{k})$ has degree D and infinite order:*

$$\hat{h}(P) \gg_E \frac{1}{D}.$$

The notation $\gg_E$ means that the inequality is true up to a positive number depending on E. The best general bound is a theorem of Masser ([25]).

Theorem 1.5 (Masser)**.** *For all $P \in E(\bar{k})$ of degree D and not torsion:*

$$\hat{h}(P) \gg_E \frac{1}{D^3\big(\log(2D)\big)^2}.$$

Masser's estimate can be improved in several special cases. In the CM case, for instance, we recover the analog of Dobrowolski's theorem (see [19]).

Theorem 1.6 (Laurent)**.** *If E has CM, for all $P \in E(\bar{k})$ of degree D and not torsion:*

$$\hat{h}(P) \gg_E \frac{1}{D}\left(\frac{\log\log(3D)}{\log(2D)}\right)^3.$$

If the j-invariant of E is not an algebraic integer (which implies that E has no CM), David proved that for all $P \in E(\bar{k})$ of infinite order and degree D (see [7]):

$$\hat{h}(P) \gg_E \frac{1}{D^{\frac{15}{8}}\big(\log(2D)\big)^2}.$$

Again, the Lehmer bound can be improved to a "positive constant" depending on E but *not* on D if the point P belongs to some specific infinite extension K of k (see [34] for $K = k^{\mathrm{ab}}$ or [13] for $K = k(E_{\mathrm{tors}})$).

Let A be an abelian variety of dimension g, defined over k, and $\mathcal{L}$ an ample and symmetric line bundle on A. There is associated with $\mathcal{L}$ a Néron-Tate height $\hat{h}_{\mathcal{L}}$ defined on the $\bar{k}$-points of A. This height can also be bounded from below away from the torsion subgroup of A (see [24], or [23] for an earlier and weaker estimate).

Theorem 1.7 (Masser)**.** *For all $P \in A(\bar{k})$ of degree D and not torsion:*

$$\hat{h}_{\mathcal{L}}(P) \gg_{A,\mathcal{L}} \frac{1}{D^{2g+1}\big(\log(2D)\big)^{2g}}.$$

Remark. This theorem has been used recently by Habegger and Pila to prove the Zilber-Pink conjecture for curves in abelian varieties (see [14], §9.1).

In fact, the dimension of A can be replaced by the maximum of the dimensions of the simple factors of A (if we fix an ample line bundle for each factor and consider the corresponding Segre embedding on A). It is conjectured that we should have:

$$\hat{h}_{\mathcal{L}}(P) \gg_{A,\mathcal{L}} D^{-\frac{1}{g}}$$

if P has infinite order modulo every abelian subvariety of A. Again, better results are known in the CM case (see [8], or [6] for a refined version).

Theorem 1.8 (David, Hindry)**.** *Suppose that A has CM and let $\kappa(g) = (2g(g+1)!)^{g+2}$. Then for all $P \in A(\bar{k})$ of degree D and infinite order modulo every abelian subvariety:*

$$\hat{h}(P) \gg_{A,\mathcal{L}} \frac{1}{D^{\frac{1}{g}}\big(\log(2D)\big)^{\kappa(g)}}.$$

This article shows some applications of Masser's counting theorem on elliptic curves. The first one concerns points of small height in powers of elliptic curves. Recall that E is an elliptic curve defined over a number field k, and let g be a positive integer. We show the following bound, which improves Theorem 1.7 in this particular case (see Corollary 2.4 below).

Theorem 1.9. *For all $P \in E^g(\bar{k})$ of degree D and infinite order modulo every abelian subvariety of E^g:*

$$\hat{h}(P) \gg_{E,g} \frac{1}{D^{1+\frac{2}{g}}\log(D)^{\frac{2}{g}}}.$$

The bound that we give here is effective. Remark that in the CM case, a stronger and effective bound follows from the effective version of Laurent's theorem given in [37].

The elliptic Lehmer problem in the Galois case. Another application concerns the Galois case of the elliptic Lehmer problem.

Theorem 1.10. *For all $P \in E(\bar{k})$ of infinite order such that $k(P)/k$ is Galois of degree D:*

$$\hat{h}(P) \gg_E \frac{1}{D}.$$

Remark. The theorem actually holds in slightly greater generality; for any $1 \leq M < 2$ and $P \in E(\bar{k})$ of infinite order and degree D such that the Galois closure of $k(P)$ over k has degree at most D^M:

$$\hat{h}(P) \gg_{E,M} \frac{1}{D}.$$

Moreover, this is true for any $M \geq 1$ if E has CM.

In the CM case, we can get an even better bound:

Theorem 1.11. *Suppose that E has CM and let $\epsilon > 0$. For all P in $E(\bar{k})$ of infinite order such that $k(P)/k$ is Galois of degree D:*

$$\hat{h}(P) \gg_{E,\epsilon} \frac{1}{D^{\frac{1}{2}+\epsilon}}.$$

We get an effective version of Theorem 1.10 in the non-CM case for D large enough, and the bound for D can be explicited using [22]. In the CM case, the proof of Theorem 1.11 (and Theorem 1.10) relies on Theorem 1.8 and the main result of [26], which might both be made effective using tools from Arakelov geometry (see [37] for an effective version of Theorem 1.8 in dimension one).

We will start by proving our lower bound for the height in powers of elliptic curves, which happens to be a natural angle when tackling the Galois case of the Lehmer problem. We will then give lower bounds for the rank of the $\mathbb{Z}$-module generated by a set of conjugates. In the last section, we will study the Lehmer problem in Kummer extensions by using Serre's open image theorem and a classical result on complex multiplication. Combined with our lower bound on the rank, this tool will be sufficient to tackle the CM case. In order to prove Theorem 1.10, we will make a final construction using a bound on the torsion and Masser's counting theorem.

Acknowledgments. The authors would like to warmly thank Gaël Rémond as well as the referee for their precise reading and helpful comments on this article.

2. Points of small height in powers of elliptic curves

We start by recalling the central tool of this article, Masser's counting result on elliptic curves, and we apply this theorem to the study of points of small height on powers of elliptic curves. This approach naturally produces results towards the Galois case of the elliptic Lehmer problem, but we only get the expected bound up to a logarithmic factor in the degree.

2.1. **Preliminaries.** From here on, we let E be an elliptic curve defined over a number field k. It is the projective curve associated with an equation:

$$y^2 = x^3 + ax + b,$$

where $a, b \in k$ are such that $4a^3 + 27b^2 \neq 0$. If K is an extension of k, we will denote by $E(K)$ the group of points of E with coordinates in K. If $P \in E(\bar{k}) \subset \mathbb{P}^2(\bar{k})$, we let $h(P)$ be the (absolute logarithmic) Weil height of P. The Néron-Tate (or canonical) height of P is defined by the following limit process:

$$\hat{h}(P) := \lim_{n\to+\infty} \frac{h(nP)}{n^2}.$$

The Néron-Tate height has several nice properties. It is quadratic and vanishes exactly on the torsion subgroup of $E(\bar{k})$. Furthermore, the difference $|h - \hat{h}|$ is bounded on $E(\bar{k})$.

2.2. **Masser's counting theorem.** This is a remarkably ubiquitous result with many immediate corollaries, such as a lower bound for the Néron-Tate height of non-torsion points, a lower bound for the degree of the field generated by the n-torsion (where n is a positive integer), and an upper bound for the order of K-rational torsion groups (where K is a number field containing k). We refer to the main theorem of [25] for a more precise statement.

Theorem 2.1 (Masser)**.** *There is a positive number c_1 depending on E such that for any $D \geq 2$ and any extension K of k of relative degree at most D, the cardinality of $\left\{P \in E(K), \hat{h}(P) \leq \frac{1}{c_1 D}\right\}$ is at most $c_1 D \log(D)$.*

Remarks. (i) The constant c_1 can be effectively computed in terms of the degree of k.

(ii) The theorem remains true if we replace c_1 by any constant greater than c_1. For the remaining of this paragraph, we will thus assume that $c_1 \geq 10^5$, so that:

$$c_1^{3/2} \log(2) \log\log(4) \geq 39 \quad \text{and} \quad \sqrt{c_1} > 12 \log(c_1).$$

We derive a lower bound for the height in the Galois case, which is optimal up to the log factor.

Corollary 2.2. *Let P be a non-torsion point of $E(\bar{k})$ such that $k(P)/k$ is Galois and let $D := [k(P) : k] \geq 2$. Then:*

$$\hat{h}(P) \geq \frac{1}{c_1^4 D \log(D)^3}.$$

Proof. Let $K := k(P)$. We proceed by contradiction and assume that:

$$\hat{h}(P) < \frac{1}{c_1^4 D \log(D)^3}.$$

Consider the set:

$$S(P) := \big\{pP^\sigma, \sigma \in \mathrm{Gal}(K/k), 1 \leq p \leq q := c_1^{3/2}\log(D)\mathrm{loglog}(2D)\big\},$$

where we restrict ourselves to prime multiples of the P^σ's. Because K/k is Galois and the Néron-Tate height is quadratic, we get:

$$S(P) \subset \Big\{Q \in E(K), \hat{h}(Q) \leq \frac{1}{c_1 D}\Big\},$$

so that, by Theorem 2.1:

$$|S(P)| \leq c_1 D\log(D).$$

Now, we want to show that the set $S(P)$ has a large cardinality. Suppose that there are two primes p, p' and $\sigma, \tau \in \mathrm{Gal}(K/k)$ such that:

$$pP^\sigma = p'P^\tau.$$

The Néron-Tate heights of P^σ and P^τ are non-zero and equal. Therefore, we get: $p = p'$ and: $(pP)^\sigma = (pP)^\tau$. By a classical combinatorial computation (see [9], Lemma 3), the prime number p belongs to a set of cardinality at most

$$\frac{\log(q)}{\log(2)}.$$

But bounding from below the number of primes $\leq q$ yields (see [28], Corollary 1 and remark that $q \geq 39$):

$$\pi(q) \geq \frac{q}{\log(q)} \geq 2\frac{\log(q)}{\log(2)}.$$

Thus, we get:

$$\begin{aligned} |S(P)| &\geq D\left(\pi(q) - \frac{\log(q)}{\log(2)}\right) \geq D\frac{\pi(q)}{2} \\ &\geq D\frac{q}{2\log(q)} \geq D\log(D)\frac{c_1^{3/2}}{12\log(c_1)}. \end{aligned}$$

Since $D \geq 2$, we derive: $\sqrt{c_1} \leq 12\log(c_1)$, which is a contradiction. □

2.3. **The elliptic Lehmer problem in greater dimension.** Amoroso and David have shown how the Galois case of the classical Lehmer problem follows from a Dobrowolski-type bound in greater dimension (see [1]). In the elliptic or multi-elliptic setting, such a bound is still far from reach, but we can substantially improve Masser's general bound.

Proposition 2.3. *Let $P_1, \ldots, P_n$ be $\mathbb{Z}$-linearly independent points of $E(\bar{k})$, all defined over a field K of degree $D \geq 2$. We have:*

$$\sum_{i=1}^{n} \hat{h}(P_i) \geq \frac{1}{n(c_1 D)^{1+\frac{2}{n}}\log(D)^{\frac{2}{n}}}.$$

Proof. We consider:

$$S := \Big\{ Q = \sum_{i=1}^{n} r_i P_i, \hat{h}(Q) \leq \frac{1}{c_1 D} \Big\},$$

where $r_1, \ldots, r_n$ run in $\mathbb{Z}$. The set S is finite, and by Theorem 2.1:

$$|S| \leq c_1 D \log(D).$$

Let:

$$\Lambda := \bigoplus_{i=1}^{n} \mathbb{Z} P_i.$$

This is a lattice of rank n in the vector space $V := \Lambda \otimes_{\mathbb{Z}} \mathbb{R}$, which is equipped with an euclidean norm: $||.||$ induced by the Néron-Tate height. If $Q \in \Lambda$, we have: $||Q|| = \hat{h}(Q)^{1/2}$, so $Q \in S$ if and only if its image in V belongs to the euclidean ball $B(0, r)$ of V with radius

$$r := \frac{1}{\sqrt{c_1 D}}.$$

We thus need to estimate the number of points $A(r)$ in Λ with euclidean norm at most r. For each point Q of Λ, let

$$\Lambda(Q) := \Big\{ Q + \sum_{i=1}^{n} t_i P_i \mid \forall i : -1/2 \leq t_i \leq 1/2 \Big\},$$

and let $v > 0$ be its volume; it is the covolume of Λ and it does not depend on Q. We consider two cases.

Suppose first that the $\Lambda(Q)$, for $Q \in \Lambda$ and $||Q|| \leq r$, do not cover $B(0, r/2)$. This ball is contained in the union of all the $\Lambda(Q)$ for $Q \in \Lambda$, so we can find two points Q, R such that $R \in \Lambda(Q)$ with: $||R|| \leq r/2$ and $||Q|| > r$. By the triangle inequality, we get:

$$||R - Q|| \geq ||Q|| - ||R|| > \frac{r}{2}.$$

Since R belongs to $\Lambda(Q)$, we can apply the Cauchy-Schwarz inequality to

$$||R - Q|| = ||\sum_{i=1}^{n} t_i P_i||,$$

which yields:

$$\sum_{i=1}^{n} \hat{h}(P_i) > \frac{r^2}{n} = \frac{1}{c_1 n D},$$

and the inequality of the proposition holds in this case.

Otherwise, by comparing volumes:

$$V_n \left(\frac{r}{2}\right)^n \leq A(r) v \leq |S| v \leq c_1 D \log(D) v,$$

where V_n is the volume of the unit ball in the n-dimensional euclidean space. By Hadamard's inequality:

$$\prod_{i=1}^{n} \hat{h}(P_i) \geq v^2 \geq \frac{V_n^2}{4^n (c_1 D)^{n+2} \log(D)^2}.$$

Using the inequality of arithmetic and geometric means, we finally get:

$$\sum_{i=1}^{n} \hat{h}(P_i) \geq n \left(\prod_{i=1}^{n} \hat{h}(P_i) \right)^{1/n} \geq \frac{n V_n^{\frac{2}{n}}}{4 (c_1 D)^{1+\frac{2}{n}} \log(D)^{\frac{2}{n}}}.$$

Recall that:

$$V_n = \frac{\pi^{n/2}}{\Gamma(1 + n/2)},$$

where Γ is the Euler Gamma function. For $x \geq 2$, by a crude estimation of the error in Stirling's formula, we find:

$$\Gamma(x) \leq 2\sqrt{\pi} x^{x-1/2} e^{-x},$$

so that, for $n \geq 2$:

$$\begin{aligned} V_n &\geq \left(\frac{2\pi e}{2+n} \right)^{n/2} \cdot \frac{e}{\sqrt{2\pi(2+n)}} \geq \left(\frac{8}{n} \right)^{n/2} \cdot \frac{e}{\sqrt{2\pi(2+n)}} \\ &\geq \left(\frac{4}{n} \right)^{n/2} \cdot \sqrt{\frac{2^{n-1} e^2}{\pi(2+n)}} \geq \left(\frac{4}{n} \right)^{n/2}. \end{aligned}$$

This lower bound for V_n still holds for $n = 1$ (both terms are in fact equal) and we finally derive:

$$\sum_{i=1}^{n} \hat{h}(P_i) \geq \frac{1}{(c_1 D)^{1+\frac{2}{n}} \log(D)^{\frac{2}{n}}}.$$

□

Remark. If P is a point of infinite order and degree D generating a Galois extension, this estimate and a direct imitation of Amoroso and David's strategy (from the number field case) yields:

$$\hat{h}(P) \gg_{E,\epsilon} \frac{1}{D^{1+\epsilon}}.$$

This does not improve the lower bound found in Corollary 2.2. In order to get a result of Lehmer strength, we would need a Dobrowolski-type result on powers of elliptic curves, which is still far from reach in general.

As an immediate corollary, we can now prove Theorem 1.9. Let g be a positive integer and $\hat{h}$ the canonical height on E^g associated with the g-power polarization associated with our Weierstrass embedding on E.

Corollary 2.4. *There is a constant c_2 depending on E and g such that for all $P \in E^g(\bar{k})$ of degree $D \geq 2$ and infinite order modulo every abelian subvariety of E^g:*

$$\hat{h}(P) \geq \frac{c_2}{D^{1+\frac{2}{g}} \log(D)^{\frac{2}{g}}}.$$

Proof. If E has CM, we can use Theorem 1.8 which provides an even stronger bound. If E has no CM, the corollary is a straightforward consequence of Proposition 2.3. □

In comparison, we get a weaker estimate if $A = E_1 \times \cdots \times E_g$ is a product of elliptic curves defined over k. Again, we fix a Weierstrass embedding for each E_i $(1 \leq i \leq g)$ and let $\hat{h}$ be the canonical height on A associated with the resulting Segre embedding of A.

Proposition 2.5. *For all $P \in A(\bar{k})$ with degree $D \geq 2$ and infinite order:*

$$\hat{h}(P) \gg_A \frac{1}{D^3 \log(D)^2}.$$

Proof. We let $P := (P_1, \ldots, P_g)$ not torsion of degree D; there is $1 \leq i \leq g$ such that P_i has infinite order. By [25], Corollary 1, there exists $c(E_i) > 0$ such that:

$$\hat{h}(P) \geq \frac{c(E_i)}{D_i^3 \log(D_i)^2},$$

where $D_i := [k(P_i) : k] \leq D$. The Proposition follows immediately with $c(A) := \min\{c(E_i) \mid 1 \leq i \leq g\}$. □

Remark. When the bound for the height does not increase with g, there is no point in making the extra hypothesis that P has infinite order *modulo every abelian subvariety.*

3. The rank of the group generated by a set of conjugates

We get back to the one-dimensional case. We are going to give lower bounds for the rank of the $\mathbb{Z}$-module generated by all the conjugates of a point of $E(\bar{k})$ under suitable conditions. For the whole section, we let L be a fixed *Galois extension* of k of relative degree $D := [L : k] \geq 2$. If $Q \in E(L)$, the conjugates of Q will be the images of Q by the elements of $\mathrm{Gal}(L/k)$.

3.1. The group theoretical approach.

The first bound uses classical results on finite subgroups of linear groups, following an idea of Amoroso and David (see [1], Corollaire 6.1). We make the following hypothesis on a point Q in $E(L)$.

Assumption 1. For any positive integer m, the field generated over k by the conjugates of mQ is L.

Remark. The Assumption 1 holds if the $\mathbb{Z}$-module H generated by the conjugates of Q is free. Indeed, if the conjugates of some multiple mQ of Q

are defined over a strict subfield of L, there is a non-trivial $\sigma \in \mathrm{Gal}(L/k)$ which fixes all the conjugates of mQ, and the m-torsion subgroup of H is not zero. This stronger hypothesis will be satisfied in the application we have in mind.

Lemma 3.1. *Let Q be as in the Assumption 1 and let H be the $\mathbb{Z}$-module generated by the conjugates of Q. The rank r of H satisfies:*

$$r \geq \sqrt{\frac{\log(D)}{\log(3)}}$$

Proof. By the Mordell-Weil theorem, the torsion subgroup of H is finite. Let n be its exponent. The $\mathbb{Z}$-module nH is free of rank r. The Galois group $\mathrm{Gal}(L/k)$ acts on nH, and this action induces a morphism:

$$\phi : \mathrm{Gal}(L/k) \to GL_r(\mathbb{Z}).$$

If an element $\sigma \in \mathrm{Gal}(L/k)$ acts trivially on nH, the conjugates of nQ belong to the fixed field of σ. So the morphism ϕ is injective because of Assumption 1. By a classical theorem of Minkowksi, reduction modulo 3 is injective on the finite subgroups of $GL_r(\mathbb{Z})$ (see [30]); we thus have:

$$D = |\mathrm{Gal}(L/k)| \leq 3^{r^2},$$

and the lemma follows. □

Remark. Our estimate on the order of finite subgroups of $GL_r(\mathbb{Z})$ can be sharpened. For $r > 10$, Feit (using unpublished results of Weisfeiler) proved that they have order at most $2^r r!$; this bound is optimal. See [11], or [12], which gives a simpler proof for $r \gg 1$. This estimate gives the following bound, for $D \gg 1$:

$$r \geq \frac{\log(D)}{\log\log(D)}.$$

3.2. **An euclidean argument.** Our second bound uses volume computations on euclidean spaces. It gives better results under stronger hypotheses, and it will not be used in the sequel.

Definition 3.2. Let K be a finite extension of k. There are finitely many points of $E(K)$ with bounded height, and we define $h(K)$ as the minimum of the height of non-torsion points of $E(K)$.

Now, we consider the following hypotheses on a point $P \in E(L)$:

Assumption 2.
(i) The Néron-Tate height of P is minimal among non-torsion points:

$$\hat{h}(P) = h(L).$$

(ii) No multiple of P is defined over a strict subfield of L.

Remark. The fact that P is not torsion is also a consequence of (ii), because the field L is a strict extension of k and the origin of E is in $E(k)$.

Lemma 3.3. *Let P be as in the Assumption 2 and let M be the $\mathbb{Z}$-module generated by the conjugates of P. The rank r of M satisfies the following:*

$$r \geq \frac{\log(D)}{\log(3)}.$$

Proof. Again, we consider the $\mathbb{Q}$-vector space $V := M \otimes_{\mathbb{Z}} \mathbb{Q}$. It has dimension r and is equipped with an euclidean structure induced by the Néron-Tate height. We claim that the conjugates P^σ of P, for $\sigma \in \mathrm{Gal}(L/k)$, are pairwise distinct in V. If not, there exist $\sigma \neq \tau$ in $\mathrm{Gal}(L/k)$ such that $P^\sigma - P^\tau$ is torsion. But this contradicts (ii) of the Assumption 2.

The P^σ, for $\sigma \in \mathrm{Gal}(L/k)$, thus define D distinct points of V and they all belong to the same euclidean sphere of radius:

$$\rho := \hat{h}(P)^{1/2} \neq 0.$$

For each $\sigma \in \mathrm{Gal}(L/k)$, let S_σ be the open sphere with center P^σ and radius $\rho/2$. Now, the S_σ's are pairwise disjoint; if not, there would be $\sigma \neq \tau$ in $\mathrm{Gal}(L/k)$ such that:

$$\hat{h}(P^\sigma - P^\tau) < \rho^2 = \hat{h}(P).$$

By the minimality condition (i), the point $Q := P^\sigma - P^\tau$ should be torsion. Once again, this would contradict (ii).

The S_σ's are pairwise disjoint and all belong to the ball of radius $3\rho/2$. A volume comparison immediately yields: $D \leq 3^r$, and:

$$r \geq \frac{\log(D)}{\log(3)}.$$

□

Remark. This computation can be slightly refined by considering the "hyperspherical cap" H_σ obtained by intersecting the sphere S_σ with the sphere S of center 0 and radius ρ (note that this intersection is not empty because the center P^σ of S_σ belongs to S). We denote by $A_r(\rho)$ the area of S, which is given by:

$$A_r(\rho) = \frac{2\pi^{r/2}}{\Gamma(r/2)}\rho^{r-1}.$$

The area of H_σ is:

$$\frac{1}{2}A_r(\rho)I_{\sin(\phi)^2}\left(\frac{r-1}{2}, \frac{1}{2}\right)$$

where the function I is the so-called "incomplete Beta function" (see for instance [21], Formula (1) page 68) and $\phi = 2\arcsin(1/4)$ is the angle of the cone with center 0 and section H_σ. By comparing areas, we find that there exists a positive number c such that:

$$r \geq \frac{2\log(D)}{\log(64/15)} - c\log\log(2D).$$

4. The elliptic Lehmer problem in the Galois case

We can now proceed to prove our theorems on the elliptic Lehmer problem in the Galois case. The first step is to give bounds on the size of the torsion in a Galois number field. For the remaining, we suppose that K is a finite *Galois extension* of k with degree D.

4.1. **Bounding the torsion.** We first give a bound on the size of the torsion inside K in terms of D, when E has no CM. This is done by using Serre's open image theorem. For the remaining, if $n \geq 1$ is an integer, we let E_n be the n-torsion subgroup of $E(\bar{k})$ and $G(n) := \mathrm{Gal}(k(E_n)/k)$.

Lemma 4.1. *Suppose that $End(E) = \mathbb{Z}$ and that there is a point of finite order $n \geq 1$ defined over K. Then:*

$$n \ll_E D^{\frac{1}{4}} |\log\log(D)|.$$

Proof. Let ξ be a point of order n defined over K. Serre's open image theorem (see the main result of [31]) shows that there is $m \gg_E n$ such that the orbit of ξ under the action of $G(n)$ contains all non-zero elements in E_m. Since K is a Galois extension of k, the group E_m belongs to $E(K)$, and by Serre's theorem again:

$$D \geq |G(m)| \gg_E |GL_2(\mathbb{Z}/m\mathbb{Z})|.$$

There remains to estimate the order of this linear group in terms of m, which is classical. We have:

$$|GL_2(\mathbb{Z}/m\mathbb{Z})| = \phi(m) \cdot |SL_2(\mathbb{Z}/m\mathbb{Z})| = \phi(m)m^3 \cdot \prod_{p|m} \left(1 - \frac{1}{p^2}\right),$$

where the last equality is obtained by combining the chinese remainder theorem and an easy inductive computation for prime powers. The product on primes is bounded from below by $\zeta(2)^{-1}$. We thus obtain (see for instance [15], XVIII, 4, Theorem 326):

$$|GL_2(\mathbb{Z}/m\mathbb{Z})| \gg \frac{m^4}{\log\log(m)} \gg_E \frac{n^4}{\log\log(n)},$$

and the lemma follows. □

We suppose now that E has CM by an order $\mathcal{O}$ of an imaginary quadratic field F and that $F \subset k$. Remark that we can take k to be the Hilbert class field of F. For $n \geq 1$ an integer, we let $\mathcal{O}(n) := \mathcal{O}/n\mathcal{O}$. The group $G(n)$ is a subgroup of $\mathcal{O}(n)^\times$. We will use the following estimate for the degree of the field generated by $G(n)$ and its subgroups.

Lemma 4.2. *Let $H \subset E_{\mathrm{tors}}$. Then:*

$$[k(H) : k] \gg_E \frac{|H|}{\log(|H|)}.$$

Proof. This is an immediate consequence of Theorem 2.1. □

Remark. Let $H := E_n$ in the previous lemma. Since $k(E_n)/k$ is Galois, we get:

$$|G(n)| \gg_E \frac{n^2}{\log(n)}.$$

There is a slightly weaker lower bound if E is replaced by a CM abelian variety (see [27], Theorem 1.1 and below, where the value of ν is explicited). By the theory of complex multiplication ([31], §4.5, Corollaire), it can be proved that: $G(n) = \mathcal{O}(n)^\times$ as soon as n is coprime to an integer that depends solely on E.

4.2. **Descent in Kummer extensions.** As the Assumption 1 of the previous section already suggests it, if we are to bound from below the height of a point P, the case where a multiple of P belongs to a strict subfield of $k(P)$ might be of special interest.

We let $P \in E(\bar{k})$ of infinite order and $K := k(P)$ a Galois extension of k with degree D. The following lemma is reminiscent of Amoroso and David's result on Kummer extensions (see [1], Lemme 6.2).

Lemma 4.3. *Suppose that a multiple of P is defined over a field L of degree d. Then:*

$$\hat{h}(P) \gg_{E,d} \frac{1}{D^{\frac{1}{2}} \log(D)}.$$

Proof. Let n be the exponent of the torsion subgroup of $E(K)$. The point $Q := nP$ is defined over L and has infinite order. We assume first that E does not have CM. By Theorem 1.5 and Lemma 4.1:

$$\hat{h}(P) = \frac{\hat{h}(nP)}{n^2} \gg_E \frac{h(L)}{D^{\frac{1}{2}} (\log\log D)^2} \gg_{E,d} \frac{1}{D^{\frac{1}{2}} \log\log(D)^2},$$

and this inequality implies the one stated in the lemma.

We suppose now that E has CM by an order $\mathcal{O}$ of a quadratic imaginary field $F \subset k$. Let us consider the "Kummer" group homomorphism ϕ_P :

$$\begin{array}{ccc} \mathrm{Gal}(K(E_n)/L(E_n)) & \longrightarrow & E_n \\ \sigma & \mapsto & \sigma(P) - P. \end{array}$$

The image of ϕ_P is a subgroup H of E_n and all the elements of H have their coordinates in K (because all the conjugates of P have coordinates in K). Let $m \leq n^2$ be the order of H. The extension $K(E_n)/L(E_n)$ is Galois and we have:

$$[K : L(H)] = [K(H) : L(H)] \geq [K(E_n) : L(E_n)] \geq |H| = m.$$

Using Lemma 4.2, we derive:

$$D \geq m \cdot [k(H) : k] \gg_E \frac{m^2}{\log(m)}.$$

Let us consider the following ideal of $\mathcal{O}$:

$$\mathcal{I} := \{\alpha \in \mathcal{O} : \forall h \in H, \alpha h = 0\}$$

The theory of complex multiplication (see [33], II, Proposition 1.4 and Corollary 1.5 for the case of maximal orders, [18], 8, §1 for the general case) yields an isogeny of degree m defined over k:

$$\alpha_H : E \longrightarrow E' := \bar{\mathcal{I}} * E$$

such that $H = \mathrm{Ker}(\alpha_H)$. The elliptic curve E' has CM by an order in F, and we can assume that it has the same field of definition. The "Kummer" morphism $\phi_{\alpha_H(P)}$ is trivial by construction of α_H, so $\alpha_H(P)$ is defined over $L(E_n)$. Ratazzi's theorem ([26], Theorem 1.1 and the remark following Conjecture 1.3) yields:

$$\hat{h}(P) = \frac{\hat{h}\big(\alpha_H(P)\big)}{m} \gg_{E',d} \frac{1}{D^{\frac{1}{2}}\log(D)}.$$

Up to isomorphism, which does not change the height, there is a finite number of possible curves E' ([33], II, Proposition 2.1, or [18], 10, §2). Therefore, we can choose the constant to depend only on E in the above inequality. □

Remarks. (i) One can do without Ratazzi's relative estimate and use Bashmakov's theorem (see [17], V, §5, Theorem 5.1, or [4]), so that after multiplying $\alpha_H(P)$ by a well chosen $\beta \in \mathcal{O}(n)$, we get a point defined over L. It is the case if the number β is any difference of two distinct elements of $G(n) \subset \mathcal{O}(n)^\times$, so that multiplication by β kills the first cohomology group. A little bit of combinatorics (together with the remark following Lemma 4.2) shows that β can be chosen to have norm $\ll_E \log(D)$, and this costs an extra $\log(D)$ factor in the height lower bound.

(ii) Our approach involving Kummer extensions does not work very well in the non-CM case, where there is no good bound for the degree d of the field L (following from a sharp multidimensional height estimate).

4.3. **The CM case.** We are now in a position to settle the CM case rapidly. We suppose here that E has CM and prove a slightly more precise version of Theorem 1.11.

Proposition 4.4. *Let $P \in E(K)$ of infinite order and degree D such that the extension $k(P)/k$ is Galois. Then:*

$$\hat{h}(P) \gg_E \frac{1}{D^{\frac{1}{2}}\log(D)}.$$

Proof. Suppose first that there exist three conjugates P_1, P_2, P_3 of P that are linearly independent over $\mathrm{End}(E)$. The abelian variety E^3 is of CM type and the point $(P_1, P_2, P_3) \in E^3$ has infinite order modulo any abelian

subvariety, so we can apply David and Hindry's estimate (see Theorem 1.8). It yields:

$$3\hat{h}(P) \gg_E \frac{1}{D^{\frac{1}{3}}(\log 2D)^{\kappa(3)}},$$

and this is stronger than the bound stated in the proposition.

Suppose on the other hand that there are at most two conjugates of P that are linearly independent over $\mathrm{End}(E)$, and let r be the rank of the $\mathbb{Z}$-module G generated by the conjugates of P. Since the endomorphism ring $\mathrm{End}(E)$ has rank 2 over $\mathbb{Z}$, this implies that $r \leq 4$. We let n be the exponent of the torsion subgroup of $E(K)$ and L be the field generated over k by the conjugates of nP. The subgroup H of G generated by the conjugates of nP has rank r over $\mathbb{Z}$ and is free, so the Assumption 1 with $Q = nP$ and the field L is valid. Therefore, Lemma 3.1 yields:

$$[L : k] \leq 3^{16}.$$

We can use Lemma 4.3 to obtain:

$$\hat{h}(P) \gg_E \frac{1}{D^{\frac{1}{2}}\log(D)},$$

and the proposition follows. □

Remark. If the degree of the Galois closure of $k(P)$ over k has cardinality at most D^M, for any $M \geq 1$, the same method yields a bound of Lehmer strength.

4.4. **The non-CM case.** We can now give an explicit lower bound for the height in the non-CM and Galois case. The Lemma 4.1 controls the Kummer piece of the extension that we consider. The remaining piece happens to be small by another application of Masser's counting theorem. We let:

$$c_5 := 3^{-14}c_1^{-1}.$$

Proposition 4.5. *For D large enough and any $P \in E(K)$ of infinite order such that $k(P)/k$ is Galois:*

$$\hat{h}(P) \geq \frac{c_5}{D}.$$

Proof. We suppose by contradiction that there exists $Q \in E(K)$ of infinite order such that:

$$\hat{h}(Q) < \frac{c_5}{D}.$$

The set of points defined over K with positive height $< \frac{c_5}{D}$ is not empty, and it is finite by the Northcott theorem. We let P of minimal height $h > 0$ among these. Let n be the exponent of the torsion subgroup of $E(K)$ and

$$d := [k(nP) : k].$$

We are going to bound d in terms of D. We fix d conjugates $P^{\sigma_1}, \ldots, P^{\sigma_d}$ of P such that:

$$\forall i \neq j : \quad nP^{\sigma_i} \neq nP^{\sigma_j},$$

and let $\mathcal{D} := \{P^{\sigma_1}, \dots, P^{\sigma_d}\}$. We claim that for any $j \geq 0$, the map ψ_j:

$$\begin{aligned} \mathcal{D}^{j+1} &\longrightarrow E(K) \\ (P_0, \dots, P_j) &\longrightarrow \sum_{i=0}^{j} 3^i P_i \end{aligned}$$

is injective. Suppose that there are two $j+1$-tuples $(P_0, \dots, P_j)$ and $(Q_0, \dots, Q_j)$ in $\mathcal{D}^{j+1}$ such that: $\sum_{i=0}^{j} 3^i(P_i - Q_i) = 0$. For any $0 \leq k \leq j$, define:

$$A_k := \sum_{i=0}^{k} 3^i (P_i - Q_i)$$

By the triangle inequality applied to the norm associated with the Néron-Tate height (see for instance [32], VIII, Theorem 9.3):

$$\hat{h}(A_k)^{\frac{1}{2}} \leq 2h^{\frac{1}{2}} \sum_{i=0}^{k} 3^i = (3^{k+1} - 1)h^{\frac{1}{2}},$$

so that:

$$\hat{h}(A_k) < 3^{2(k+1)} h.$$

Since $A_j = 0$, we see that:

$$\hat{h}(P_j - Q_j) = 3^{-2j} \hat{h}(A_j - A_{j-1}) = 3^{-2j} \hat{h}(A_{j-1}) < h.$$

By minimality of h and because the difference between two distinct points of $\mathcal{D}$ is never a torsion point, we have: $P_j = Q_j$. We can iterate this process to get:

$$\forall\ 0 \leq k \leq j : \quad P_k = Q_k,$$

and our claim holds. Another application of the triangle inequality shows that, for all $Q \in \mathrm{Im}(\psi_6)$:

$$\hat{h}(Q) \leq 3^{14} h \leq \frac{1}{c_1 D}.$$

Combining the injectivity of ψ_6 with Theorem 2.1, we find:

$$d^7 \leq c_1 D \log(D).$$

The point nP has degree d and infinite order, so Theorem 1.5 gives the following bound:

$$\hat{h}(nP) \gg_E \frac{1}{d^3 \log(2d)^2} \gg_E \frac{1}{D^{\frac{3}{7}} \log(D)^3}.$$

By the properties of finite abelian groups, there is a K-rational torsion point with order n, so we can apply Lemma 4.1 and we get:

$$\frac{c_5}{D} > \hat{h}(P) = \frac{\hat{h}(nP)}{n^2} \gg_E \frac{1}{D^{\frac{13}{14}} \log(D)^4}.$$

This is a contradiction for D large enough. □

Remarks. (i) This method can be extended to the case where the degree of the Galois closure of $k(P)$ over k has cardinality at most D^M, for any $M < 2$. If M is bigger, the bound on the torsion becomes too weak, but we can still get a Lehmer bound "up to an ε".

(ii) For a general elliptic curve E, one could hope for a stronger bound in the Galois case, namely:

$$\hat{h}(P) \gg_{E,\epsilon} \frac{1}{D^{\frac{1}{2}+\epsilon}},$$

for all $\epsilon > 0$. This estimate would follow from a Dobrowolsky-type bound for powers of elliptic curves (which is a hard open problem in the non-CM case) and arguments from Kummer theory.

(iii) Using the main result of [24], this strategy could yield an estimate of the same strength for an abelian variety A defined over a number field k together with a line bundle $\mathcal{L}$, namely:

$$\hat{h}_{\mathcal{L}}(P) \gg_{A,\mathcal{L}} \frac{1}{[k(P) : k]}$$

for a point $P \in A(\bar{k})$ of infinite order such that $k(P)/k$ is Galois. This would follow from a good bound for the order n of a torsion point defined over a Galois extension of k with degree D:

$$n \ll_A D^{\alpha},$$

where $\alpha < 1/2$. For related results concerning Galois properties of torsion points on abelian varieties, see for instance [16].

References

[1] F. Amoroso and S. David, *Le problème de Lehmer en dimension supérieure.* J. Reine Angew. Math. 513 (1999), 145-179.

[2] F. Amoroso and R. Dvornicich, *A lower bound for the height in abelian extensions.* J. Number Theory 80 (2000), 260-272.

[3] F. Amoroso and E. Viada, *Small points on rational subvarieties of tori.* Comment. Math. Helv. 87 (2012), no. 2, 355-383.

[4] M. Bashmakov, *Cohomology of abelian varieties over a number field.* Russ. Math. Surv. 27 (6) (1972), 25-70.

[5] P. Borwein, E. Dobrowolski and M. Mossinghoff, *Lehmer's problem for polynomials with odd coefficients.* Ann. Math. 166 (2007), 347-366.

[6] M. Carrizosa, *Petits points et multiplication complexe.* Int. Math. Res. Not. (2009), 3016-3097.

[7] S. David, *Points de petite hauteur sur les courbes elliptiques.* J. Number Theory 64 (1997), no. 1, 104-129.

[8] S. David and M. Hindry, *Minoration de la hauteur de Néron-Tate sur les variétés abéliennes de type C.M.* J. Reine Angew. Math. 529 (2000), 1-74.

[9] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial.* Acta Arith. 34 (1979), 391-401.

[10] A. Dubickas and M. J. Mossinghoff, *Auxiliary polynomials for some problems regarding Mahler's measure.* Acta Arith. 119 (2005), no. 1, 65-79.

[11] W. Feit, *The orders of finite linear groups.* Preprint (1995).

[12] S. Friedland, *The maximal orders of finite subgroups in $GL_n(\mathbb{Q})$.* Proc. Amer. Math. Soc. 125 (1997), no. 12, 3519-3526.
[13] P. Habegger, *Small height and infinite non-abelian extensions.* Duke Math. J. 162 (2013), no. 11, 1895-2076.
[14] P. Habegger and J. Pila, *O-minimality and certain atypical intersections.* Preprint (2014).
[15] G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers.* Oxford Science Publications, 1979.
[16] M. Hindry and N. Ratazzi, *Points de torsion sur les variétés abéliennes de type GSp* J. Inst. Math. Jussieu 11 (2012), no. 1, 27-65.
[17] S. Lang, *Elliptic curves: diophantine analysis.* Grundlehren der mathematischen Wissenschaften, vol. 231. Springer-Verlag, Berlin, 1978.
[18] S. Lang, *Elliptic functions.* Graduate Texts in Mathematics, 112. Springer Verlag, New-York, 1987.
[19] M. Laurent, *Minoration de la hauteur de Néron-Tate.* Séminaire de théorie des nombres de Paris, 1981-82, M. J. Bertin éd. Progr. Math. 38 (1983), 137-152.
[20] H. Lehmer, *Factorisation of certain cyclotomic functions.* Ann. Math. (2) 34 (1933), no. 3, 461-479.
[21] S. Li, *Concise formulas for the area and volume of a hyperspherical cap.* Asian J. of Math. and Stat. 4 (2011), 66-70.
[22] D. Lombardo, *Bounds for Serre's open image theorem for elliptic curves over number fields.* Algebra Number Theory 9 (2015), no. 10, 2347-2395.
[23] D. Masser, *Small values of the quadratic part of the Néron-Tate height on an abelian variety.* Compos. Math. 53 (1984), 153-170.
[24] D. Masser, *Letter to D. Bertrand.* Nov. 17th 1986.
[25] D. Masser, *Counting points of small height on elliptic curves.* Bull. Soc. Math. Fr. 117 (1989), 247-265.
[26] N. Ratazzi, *Théorème de Dobrowolski-Laurent pour les extensions abéliennes sur une courbe elliptique à multiplication complexe.* Int. Math. Res. Not. 58 (2004), 3121-3152.
[27] K. Ribet, *Division fields of abelian varieties with complex multiplication* Mém. Soc. Math. Fr. 2 (1980), 75-94.
[28] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers.* Illinois J. Math. 6 (1962), no. 1, 64-94.
[29] A. Schinzel, *On the product of the conjugates outside the unit circle of an algebraic number.* Acta Arith. 24 (1973), 385-399.
[30] J.-P. Serre, *Rigidité du foncteur de Jacobi d'échelon $n \geq 3$.* Appendice à l'exposé 17 du séminaire Cartan, 1960-1961.
[31] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques.* Invent. Math. 15 (1972), 259-331.
[32] J. Silverman, *The arithmetic of elliptic curves.* Graduate Texts in Mathematics, 106. Springer-Verlag, Berlin, 1986.
[33] J. Silverman, *Advanced topics in the arithmetic of elliptic curves.* Graduate Texts in Mathematics, 151. Springer-Verlag, Berlin, 1994.
[34] J. Silverman, *A lower bound for the canonical height on elliptic curves over abelian extensions.* J. Number Theory 104 (2004), no. 2, 353-372.
[35] C. J. Smyth, *On the product of the conjugates outside the unit circle of an algebraic integer.* Bull. London Math. Soc. 3. (1971), 169-175.
[36] P. Voutier, *An effective lower bound for the height of algebraic numbers.* Acta Arith. 74 (1996), 81-95.
[37] B. Winckler, *Intersection arithmétique et problème de Lehmer elliptique.* Thèse de doctorat, Université de Bordeaux (2015).