SMALL HEIGHT IN FIELDS GENERATED BY SINGULAR MODULI

AURÉLIEN GALATEAU

Abstract. We prove that some fields generated by j-invariants of CM elliptic curves (of infinite dimension over $\mathbb{Q}$) satisfy the Property (B). The singular moduli are chosen so as to have supersingular reduction simultaneously above a fixed prime q, which provides strong q-adic estimates leading to an explicit lower bound for the height.

1. Introduction

Algebraic numbers with small height. This article is dedicated to algebraic extensions of the field of rational numbers that satisfy the so-called Property (B). This problem finds its origin in a famous question raised by Lehmer (see [17], §13, p. 476), now considered as a conjecture. Let h be the (logarithmic, absolute) Weil height on $\bar{\mathbb{Q}}^*$.

Conjecture 1.1 (Lehmer)**.** *There is $c > 0$ such that for all $x \in \bar{\mathbb{Q}}^*$ not a root of unity :*

$$h(x) \geq \frac{c}{[\mathbb{Q}(x) : \mathbb{Q}]}.$$

The Lehmer conjecture is still unsolved, although it is known to hold in many particular cases. The best general result in this direction is due to Dobrowolski, who proved the expected lower bound for the height up to a logarithmic factor in the degree (see [8]).

In some special cases, it is even possible to find a lower bound which is independent of the degree. This happens for instance if we consider a sequence of algebraic numbers with Galois orbit not equidistributed. An interesting example is that of totally real number fields ([24]).

Theorem 1.2 (Schinzel)**.** *Let K be a totally real number field. For all $x \in K^*$ not a root of unity:*

$$h(x) \geq \frac{1}{2}\log\Big(\frac{1+\sqrt{5}}{2}\Big).$$

An other example of this phenomenon was later given by Amoroso and Dvornicich (see [2]), who settled the case of $\mathbb{Q}^{\mathrm{ab}}$, the abelian closure of $\mathbb{Q}$.

Theorem 1.3 (Amoroso, Dvornicich)**.** *Let $x \in \mathbb{Q}^{\mathrm{ab}}$ not zero or a root of unity. Then :*

$$h(x) \geq \frac{\log(5)}{12}.$$

Date: June 3, 2015.

1991 *Mathematics Subject Classification.* Primary 11G50; Secondary 11G05, 14H52, 14G40.

This theorem was soon generalized to the abelian closure K^{ab} of any number field K by Amoroso and Zannier (see [3]), who shaded a new light on the Lehmer conjecture by suggesting a *relative Lehmer conjecture*, with the degree of an algebraic number replaced by its degree over $\mathbb{Q}^{\mathrm{ab}}$.

The Bogomolov Property. Inspired by these results, Bombieri and Zannier introduced the following properties (see [4]).

Definition 1.4. *Let $\mathcal{A}$ be a subset of $\bar{\mathbb{Q}}^*$.*

(i) We say that $\mathcal{A}$ has the Bogomolov Property (B) if there exists $c(\mathcal{A}) > 0$ such that, for all $x \in \mathcal{A}$ not zero or a root of unity : $h(x) \geq c(\mathcal{A})$.

(ii) We say that $\mathcal{A}$ has the Northcott Property (N) if for any $H > 0$, the set of elements in $\mathcal{A}$ with height at most H is finite.

The "Northcott theorem" asserts that any number field has the Property (N), and it is straightforward to see that Property (N) is stronger than Property (B). Thus, as far as these properties are concerned, the relevant fields are infinite extensions of $\mathbb{Q}$.

In the same article, Bombieri and Zannier provided new examples of fields satisfying the Property (B). If K is a number field and L/K is an infinite extension, we say that L/K has bounded local degree at a finite place v of K if there exists $D > 0$ such that for all place $w|v$ of L, we have :

$$[L_w : K_v] \leq D.$$

They proved the following result, which can be seen as a non-archimedean analogue of Schinzel's theorem (with the convention that an extension $L/\mathbb{Q}$ has bounded degree at ∞ if it is totally real).

Theorem 1.5 (Bombieri, Zannier)**.** *Suppose that $L/\mathbb{Q}$ has bounded local degree at some rational prime. Then L satisfies the Property (B).*

Checcoli later found a sufficient condition for this theorem to apply, formulated in Galois theoretic terms. Namely, she proved that the extension L/K has uniformly bounded local degree at every finite place of K if and only if its Galois group has finite exponent (see [5]).

Another example was recently given by Habegger, who considered the field generated by the torsion group E_{tors} of an elliptic curve E defined over $\mathbb{Q}$ ([11]).

Theorem 1.6 (Habegger)**.** *The field $\mathbb{Q}(E_{\mathrm{tors}})$ satisfies the Property (B).*

If E has CM, class field theory of quadratic imaginary fields shows that this result follows from the theorem of Amoroso and Zannier on K^{ab}, where K is the CM field. But if E is not of CM type, Habegger shows that his result goes beyond the abelian case or the bounded local degree case. The restriction on the field of definition of E comes from the theorem of Elkies on supersingular primes ([9]).

Amoroso, David and Zannier have recently tried to unify some of these results in a Galois theoretic point of view. Among other results, they prove the following ([1]).

Theorem 1.7 (Amoroso, David, Zannier)**.** *Let K be a number field and L/K an infinite Galois extension. If the quotient of $\mathrm{Gal}(L/K)$ over its center has finite exponent, the field L has the Property (B).*

They also prove that the height is bounded uniformly in the degree of K and the exponent. We also refer to [6] for another generalization of the bounded local degree case.

Remark. A link has been pointed out by Rosenbloom and Tsfasman between the Property (B) and sphere packing. They contructed families of "asymptotically good" lattices (with rank going to infinity and density exponent explicitly bounded) by using Schinzel's estimate for the height on totally real number fields. Apart from the lower bound for the height on a subfield K of $\bar{\mathbb{Q}}$, an important ingredient is the existence of a subfield of K which is an infinite unramified extension over a number field of small discriminant (see [22]).

The Bogomolov Property in fields generated by j-invariants. A way to look for other examples of fields with the Property (B) is to consider the following case. Let $(K_n)_{n\in\mathbb{N}}$ be a sequence of (pairwise distinct) quadratic fields, and for all $n \in \mathbb{N}$, let L_n be an abelian extension of K_n. We denote by L the compositum of all the L_n's, for $n \in \mathbb{N}$.

Question 1.8. *Does the field L satisfy the Property (B)?*

For each n, the Galois group of L_n over $\mathbb{Q}$ is an extension of an abelian group by $\mathbb{Z}/2\mathbb{Z}$, hence it is "almost" abelian (if not abelian). Furthermore, we know by the work of Bombieri and Zannier ([4]) that the compositum of the K_n's, for $n \in \mathbb{N}$, satisfies the Property (N), hence the Property (B).

Everything becomes much more explicit when we consider a sequence of imaginary quadratic fields and their Hilbert class fields. Let p be a prime and let $K_p := \mathbb{Q}(\sqrt{-p})$. The Hilbert class field L_p (i.e. unramified abelian closure) of K_p is generated over K_p by the j-invariant j_p of an elliptic curve with endomorphism ring the ring of integers of K_p. For any subset $\mathcal{Q}$ of the set $\mathcal{P}$ of prime numbers, we let $K_\mathcal{Q}$ (resp. $L_\mathcal{Q}$) be the compositum of the K_p's (resp. L_p's), for $p \in \mathcal{Q}$. We prove the following theorem, which gives a lower bound for the height on some infinite dimensional subfields of the field $L_\mathcal{P}$.

Theorem 1.9. *Let $q \geq 3$ be a prime. There exists a set $\mathcal{P}_q \subset \mathcal{P}$ of Dirichlet density $\frac{1}{4}$ such that $L_{\mathcal{P}_q}$ satisfies the Property (B).*

We will see while constructing the $\mathcal{P}_q$'s that they are rather distinct one from another. More precisely, for $q \neq q'$, the set $\mathcal{P}_q \cap \mathcal{P}_{q'}$ has Dirichlet density $\frac{1}{8}$.

The main ingredient in the proof of this theorem is a q-adic estimate (q a prime) that expresses an important property of the class field theory of an imaginary quadratic field K. We will start by recalling a classical criterion for the j-invariant of an elliptic curve which is supersingular at a prime above q, and we will review some well-known facts about complex multiplication related to the Hilbert class field H of K. The most useful result for us will concern the splitting of principal prime ideals of K in H.

In the CM case, it is also rather easy to describe the primes of supersingular reduction, and we will use this description to construct the set $\mathcal{P}_q$. We will study the Galois properties of the fields involved and see how they compare to others known to satisfy the Property (B).

We will then recall the basic properties of the Weil height, and prove an explicit version of our theorem. In the last section, we will discuss further examples of families of Hilbert class fields for which the same techniques apply.

2. Supersingular primes and complex multiplication

In this section, we recall some classical facts about supersingular primes for elliptic curves with complex multiplication (CM). We first give a $\mathfrak{p}$-adic property for the j-invariant of an elliptic curve that is supersingular at a prime ideal $\mathfrak{p}$ in a field of definition. This estimate will be sufficient to treat a significant particular case in the proof of our theorem. We explain the role of singular j-invariants in the class field theory of imaginary quadratic fields, and the distribution of supersingular primes for CM elliptic curves.

2.1. **Supersingularity.** Let E be an elliptic curve defined over a number field L. The curve E is given by a Weierstrass equation :

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

with $a, b \in L$ and discriminant $\Delta := -16(4a^3 + 27b^2) \neq 0$. We let $\mathfrak{p}$ a prime ideal of $\mathcal{O}_L$, and we suppose that E has good reduction at $\mathfrak{p}$, i.e. the reduction $\tilde{E}$ of E mod $\mathfrak{p}$ is smooth. Let p be the characteristic of the residue field $k := \mathcal{O}_L/\mathfrak{p}$, and $\tilde{E}[p]$ the p-torsion subgroup of $\tilde{E}(\bar{k})$.

Definition 2.1. *We say that E has supersingular reduction at $\mathfrak{p}$ if $\tilde{E}[p] = 0$.*

If the reduction is not supersingular, the p-torsion subgroup has order p and the reduction is said to be ordinary. Supersingularity can be translated $\mathfrak{p}$-adically on the j-invariant of E.

Lemma 2.2. *If E has supersingular reduction at $\mathfrak{p}$ and $j(E) \in \mathcal{O}_L$:*

$$j(E)^{p^2} \equiv j(E) \pmod{\mathfrak{p}}.$$

Proof. If $\mathfrak{p}$ is a supersingular prime for E, the isogeny $[p]$ is purely inseparable of degree p^2 on $\tilde{E}$. For q a power of p, let $\tilde{E}^{(q)}$ be the elliptic curve obtained by raising all the coefficients to the power q in a Weierstrass equation of $\tilde{E}$. By [28] II.2.12, we have a factorization : $[p] = \hat{\phi} \circ \phi$, where ϕ is the p-power Frobenius :

$$\tilde{E} \longrightarrow \tilde{E}^{(p)}$$

and $\hat{\phi}$ is its dual isogeny, the so-called Verschiebung :

$$\tilde{E}^{(p)} \longrightarrow \tilde{E}.$$

The isogeny $\hat{\phi}$ is purely inseparable of degree p. Again, there is a factorization : $\hat{\phi} = \psi \circ \phi'$, where ϕ' :

$$\tilde{E}^{(p)} \longrightarrow \tilde{E}^{(p^2)}$$

is the p-power Frobenius and ψ :

$$\tilde{E}^{(p^2)} \longrightarrow \tilde{E}$$

is an isogeny of degree 1 (by a straightforward comparison of degrees). This means that ψ is an isomorphism. From the definition of the j-invariant and the fact that $\mathcal{O}_L/\mathfrak{p}$ has characteristic p, we deduce the following equalities in the residue field $\mathcal{O}_L/\mathfrak{p}$:

$$j(\tilde{E}) = j\big(\tilde{E}^{(p^2)}\big) = j(\tilde{E})^{p^2}.$$

Since $j(E)$ is an algebraic integer, its reduction mod $\mathfrak{p}$ is well-defined as an element of $\mathcal{O}_L/\mathfrak{p}$. Furthermore, it is equal to $j(\tilde{E})$ by a straightforward computation in an integral model, and the lemma follows immediately. □

2.2. **Complex multiplication.** The ring $\mathrm{End}(E)$ of endomorphisms of E is the ring of isogenies from E to E (defined over $\bar{L}$). Since L has characteristic 0, it is a free $\mathbb{Z}$-module of rank 1 or 2. The "quantity" of primes at which E has supersingular reduction is closely related to $\mathrm{End}(E)$.

Definition 2.3. *We say that E has complex multiplication (CM) if $\mathrm{End}(E) \neq \mathbb{Z}$. In this case, $\mathrm{End}(E)$ is an order in a quadratic imaginary field.*

We suppose from now on that *E has CM*. We let:

$$K := \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$$

be the imaginary quadratic field of complex multiplication. We also suppose that $\mathrm{End}(E)$ is the ring of integers $\mathcal{O}_K$ of K. The set of primes of $\mathcal{O}_K$ at which E has supersingular reduction is well-understood and can be explicited rather easily.

Proposition 2.4 (Deuring)**.** *Let $\mathfrak{p}$ be a prime of $\mathcal{O}_L$ and let p be the characteristic of $\mathcal{O}_L/\mathfrak{p}$. The prime $\mathfrak{p}$ is supersingular if and only if p is inert in $\mathcal{O}_K$.*

Proof. See [29], II, Exercise 2.30 or [15], p. 182. □

Remark. In the general case, the distribution of supersingular primes is still mysterious. On the one hand, Serre proved that supersingular primes have density zero (after possibly extending the ground field, so as to include the CM field, see [25]). On the other hand, if E is defined over $\mathbb{Q}$, Elkies showed that there are infinitely many supersingular primes ([9]). Lang and Trotter ([16]) conjectured that there is $c(E) > 0$ such that :

$$|\{p \leq x, p \text{ is supersingular}\}| \sim_{x\to\infty} c(E)\frac{\sqrt{x}}{\log(x)}.$$

This conjecture can be extended to general number fields and also covers the CM case, provided that the ground field be extended so as to contain the field of CM.

2.3. **Singular moduli.** Singular moduli are j-invariants of elliptic curves with CM, which can be seen as special points on the classical modular curve. They play a central part in the class field theory of imaginary quadratic fields.

Our congruence property on singular moduli needs an integrality result on the j-invariant of a CM elliptic curve. Since there is only a finite number of (isomorphism classes) of CM elliptic curves with given endomorphism ring (due to the finiteness of its ideal class group), this j-invariant is an algebraic number. But more can be said.

Theorem 2.5 (Weber, Fueter)**.** *If E has CM, then $j(E)$ is an algebraic integer.*

Proof. There are several proofs of this result. See for instance [29], II, Theorem 6.1. □

The modular invariant of a CM elliptic curve plays an important role for the field of CM. For the remaining of this section, we change our point of view and let K be an imaginary quadratic field with ring of integers $\mathcal{O}_K$. This ring is a free $\mathbb{Z}$-module of rank 2, hence a lattice in $\mathbb{C}$.

We let $E_K := \mathbb{C}/\mathcal{O}_K$. This is a complex elliptic curve with CM by $\mathcal{O}_K$, so its j-invariant is algebraic. In fact, the curve E_K is defined over $\bar{\mathbb{Q}}$ ([29], II, Proposition 2.1). The j-invariant of E_K helps to describe the unramified abelian closure of K.

Theorem 2.6 (Weber, Fueter)**.** *The field generated by $j(E_K)$ over K is the maximal unramified abelian extension of K. The degree of this extension is the class number of K, and its Galois group is the class group of K.*

Proof. See [29], II, Theorem 4.1. □

Remark. In fact, the field $K\big(j(E_K)\big)$ is the *minimal* field of definition for E_K. The ramified part of the maximal abelian extension of K is given by the torsion points of E_K, via the so-called "Weber functions".

A direct consequence of this theorem concerns the decomposition of rational primes producing supersingularity in the Hilbert class field $K\big(j(E_K)\big)$.

Corollary 2.7. *Let p be a rational prime which is inert in $\mathcal{O}_K$. Then $p\mathcal{O}_K$ splits completely in $K\big(j(E_K)\big)$.*

Proof. By class field theory, the prime ideals of $\mathcal{O}_K$ that split completely in the Hilbert class field of K are exactly those that are principal ([29], II, Theorem 3.2 and Example 3.3). □

3. Selection of j-invariants and Galois properties

Thanks to Dirichlet's theorem on arithmetic progressions, we show how to find a large number of primes that are simultaneously supersingular for a large number of CM elliptic curves. We then give some Galois properties of the fields $L_{\mathcal{P}_q}$ and compare them to those studied in [1] and [11].

3.1. Simultaneous supersingularity.

Our criterion for supersingularity in the CM case can be explicited using some basic arithmetic properties of quadratic fields. By Dirichlet's theorem on arithmetic progressions, we can find primes that are simultaneously supersingular for CM elliptic curves associated to a positive density of primes.

For any prime number $p \geq 3$, we let $K_p := \mathbb{Q}(\sqrt{-p})$ and $E_p := \mathbb{C}/\mathcal{O}_{K_p}$. This is an elliptic curve with CM and endomorphism ring $\mathcal{O}_{K_p}$. The field L_p generated over K_p by $j(E_p)$ is a field of definition for E_p.

Lemma 3.1. *Let $q \geq 3$ be a rational prime and $\mathcal{P}_q$ be the set of (rational) primes $p \equiv 1 \pmod 4$ such that E_p has supersingular reduction at all primes of $\mathcal{O}_{L_p}$ above q. The set $\mathcal{P}_q$ has Dirichlet density $\frac{1}{4}$.*

Proof. Let $p \geq 3$ and Δ_p be the discriminant of K_p. We have ([14], Ch. 13, §1) :

$$\Delta_p = p \quad \text{if} \quad p \equiv 1 \pmod 4,$$

and :

$$\Delta_p = 4p \quad \text{if} \quad p \equiv 3 \pmod 4.$$

By Proposition 2.4, the curve E_p is supersingular above q if q is inert in $\mathcal{O}_{K_p}$. Furthermore, this condition holds if and only if $q \nmid \Delta_p$ and Δ_p is not a square mod q. Since $q \geq 3$, this is equivalent to the condition that p not be a square mod q. There are $\frac{q-1}{2}$ classes mod q that are not quadratic residues.

By the strong version of Dirichlet's theorem (see [14], Ch. 16, §1), the set of primes in each class has Dirichlet density $\frac{1}{q-1}$, so the set of primes p such that E_p is supersingular above q has Dirichlet density $\frac{1}{2}$. The same holds for the set of primes that are congruent to 1 (mod 4), and since q and 4 are coprime, the lemma follows immediately from the chinese remainder theorem. □

Remarks. The chinese remainder theorem also shows that if q and q' are two distinct primes, the set $\mathcal{P}_q \cap \mathcal{P}_{q'}$ has Dirichlet density $\frac{1}{8}$. Up to the congruence (mod 4), these sets are thus "independant" in a probabilistic point of view. It is also worth mentioning for the sequel that $q \notin \mathcal{P}_q$, since the class 0 (mod q) is excluded in the construction of $\mathcal{P}_q$.

3.2. **Galois properties of fields generated by singular moduli.** In this subsection, we fix q a prime number. We are going to investigate the group:

$$G_q := \mathrm{Gal}(L_{\mathcal{P}_q}/\mathbb{Q}),$$

and show that it is far from being abelian. Since the extension $K_{\mathcal{P}_q}/\mathbb{Q}$ is the compositum of pairwise linearly disjoint quadratic fields, we have:

$$\mathrm{Gal}(K_{\mathcal{P}_q}/\mathbb{Q}) = \prod_{p \in \mathcal{P}_q} \mathbb{Z}/2\mathbb{Z}.$$

The following proposition shows that the structure of G_q is more complicated.

Proposition 3.2. *The group $G_q/Z(G_q)$ has infinite exponent.*

Proof. The Galois extensions $L_p/\mathbb{Q}$, for $p \in \mathcal{P}_q$, are pairwise linearly disjoint because each L_p is only ramified at p. Thus, the Galois group of $L_{\mathcal{P}_q}/\mathbb{Q}$ is the product of the Galois groups of the $L_p/\mathbb{Q}$, for $p \in \mathcal{P}_q$.

By Theorem 1.2 of [21] and a quick computation, we see that the exponent of the ideal class group of $\mathbb{Q}(\sqrt{-p})$ goes to infinity outside of a set of primes of density zero. Let $d \geq 1$, and let $p \in \mathcal{P}_q$ such that the Galois group H_p of L_p/K_p has exponent $\geq d$.

If C is a subgroup of H_p corresponding to an extension M/K_p, the extension $M/\mathbb{Q}$ has Galois group $C \rtimes \mathbb{Z}/2\mathbb{Z}$. If the product is direct, the Kronecker-Weber theorem shows that the field M belongs to a cyclotomic extension. But the extension $M/\mathbb{Q}$ is ramified only at p, with ramification index 2, so it has degree 2 and C is trivial.

Applying this to a cyclic group $C \subset H_p$ of order $\geq d$ and to all its subgroups, we see that $C \cap Z(G_q) = \{1\}$, and $G_q/Z(G_q)$ has exponent $\geq d$. This holds for all $d \geq 1$, and the proposition follows. □

This proposition shows that the condition of Theorem 1.7 does not hold in our case. We can also compare the field $L_{\mathcal{P}_q}$ to the fields studied by Habegger in [11]. These fields are very ramified and built out of one elliptic curve, whereas $L_{\mathcal{P}_q}$ is the compositum of scarcely ramified fields built out of many different elliptic curves with CM.

Proposition 3.3. *If E is an elliptic curve defined over a number field K:*

$$L_{\mathcal{P}_q} \not\subset K(E_{\mathrm{tors}}).$$

Proof. We proceed by contradiction. We can suppose that K is Galois over $\mathbb{Q}$, and that $\mathrm{End}(E) = \mathbb{Z}$ by the previous proposition. Let $p \geq 5 \in \mathcal{P}_q$ large enough, such that p does not ramify in K, the elliptic curve E has good reduction at all primes dividing p, and such that Serre's "open image" theorem applies ([26]):

$$\mathrm{Gal}(K(E[p])/K) = \mathrm{GL}_2(\mathbb{F}_p).$$

The field L_p is tamely ramified at p and unramified at other primes so $L_p \subset K(E[p])$. Again, we can choose p so that

$$\mathrm{Gal}(L_p/\mathbb{Q}) = H_p \rtimes \mathbb{Z}/2\mathbb{Z}$$

is a non trivial product. This Galois group can be embedded as a normal subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ which is not contained in its center. By simplicity of $\mathrm{PSL}_2(\mathbb{F}_p)$, we get:

$$|H_p| \geq p(p^2 - 1).$$

This contradicts the classical upper bound given by Dirichlet's analytic class number formula (see for instance [18], 1):

$$|H_p| \leq \frac{6}{\pi}\sqrt{p}\log(p).$$

□

Remark. By Weil's pairing, the field $K(E_{\mathrm{tors}})$ contains $\mathbb{Q}^{\mathrm{ab}}$, hence $K_{\mathcal{P}_q}$ which is abelian over $\mathbb{Q}$.

4. Heights and fields generated by j-invariants

Let $q \geq 3$ a prime. We are going to give an explicit lower bound for the height on the field $L_{\mathcal{P}_q}$ outside of the roots of unity. We will first treat a significant special case by using the $\mathfrak{q}$-adic estimate on j-invariants for a simultaneously supersingular prime $\mathfrak{q}|q$. We will finally treat the general case by using the decomposition properties of primes in the Hilbert class fields.

4.1. Preliminaries on heights.

Let K be a number field. A place v of K is (the equivalence class of) an absolute value : $K \to \mathbb{R}_+$. Its restriction w to $\mathbb{Q}$ is either the standard archimedean absolute value (we say that v is infinite and write $v|\infty$) or a p-adic absolute value, for p a prime number (we say that v is finite and write $v|p$). Let K_v be the completion of K with respect to v and $d_v := [K_v : \mathbb{Q}_w]$ the local degree of v. We have the following "degree formula", which relates the local and global degrees of K :

$$\sum_{v|w} d_v = [K : \mathbb{Q}].$$

The infinite places of K correspond to field embeddings : $K \hookrightarrow \mathbb{C}$ modulo complex conjugation. The finite places of K are in bijection with the non-zero prime ideals of K. If v is a finite place of K, we can thus define its ramification index e_v and its residual degree f_v, and we have the equality : $d_v = e_v f_v$.

Let x be a non-zero algebraic number. It satisfies the well-known "product formula" :

$$\sum_{v \in M(K)} d_v \log|x|_v = 0.$$

We define the (absolute, logarithmic) Weil height of x by :

$$h(x) = \frac{1}{[K:\mathbb{Q}]} \sum_{v \in M(K)} d_v \log \max\{1, |x|_v\},$$

where K is any number field containing x, and $M(K)$ is the set of places of K. For $x, y \in \bar{\mathbb{Q}}^*$ $(x + y \neq 0)$, we have the following inequalities :

$$h(xy) \leq h(x) + h(y) \quad \text{and :} \quad h(x+y) \leq h(x) + h(y) + \log(2).$$

4.2. **A particular case.** We start by proving a lower bound for a large subring of the algebraic integers of the field $L_{\mathcal{P}_q}$. This is done by using the $\mathfrak{q}$-adic estimate on singular moduli at a supersingular prime $\mathfrak{q}|q$. This also paves the way for the general case, for which we will follow the same approach with some extra information on the decomposition of primes in Hilbert class fields.

Proposition 4.1. *Let $x \in \mathbb{Z}[j_p, p \in \mathcal{P}_q]$ of infinite order. Then:*

$$h(x) \geq \frac{\log(q/2)}{q^2+1}.$$

Proof. Let $\mathcal{Q}$ be a finite subset of $\mathcal{P}_q$ such that $x \in L_{\mathcal{Q}}$. Since x is not a root of unity, we have :

$$y := x^{q^2} - x \neq 0.$$

We can therefore apply the product formula to y. By construction, the prime q does not ramify in $L_{\mathcal{Q}}$. Now, Lemma 2.2 and Theorem 2.5 show that if $v|q$ is a finite place of $L_{\mathcal{Q}}$, for each $p \in \mathcal{Q}$:

$$|j_p^{q^2} - j_p|_v \leq q^{-1},$$

and the properties of binomial coefficients imply: $|y|_v \leq q^{-1}$.

The product formula reads:

$$\begin{aligned} 0 &= \sum_{v \in M(L_{\mathcal{Q}})} \frac{d_v}{[L_{\mathcal{Q}}:\mathbb{Q}]} \log |y|_v \\ &\leq \sum_{v \nmid q} \frac{d_v}{[L_{\mathcal{Q}}:\mathbb{Q}]} \log \max\{1, |y|_v\} - \sum_{v|q} \frac{d_v}{[L_{\mathcal{Q}}:\mathbb{Q}]} \log(q). \end{aligned}$$

Using the basic inequalities recalled earlier in this section yields :

$$\begin{aligned} 0 &\leq h(y) - \log(q) \\ &\leq (q^2+1)h(x) + \log(2) - \log(q), \end{aligned}$$

and the proposition follows. □

4.3. **Local analysis.** We concentrate here on local estimates above q. We let $\mathcal{Q} \subset \mathcal{P}_q$ be a finite set of primes and take $v|q$ a place of $L_{\mathcal{Q}}$. The first lemma focuses on algebraic integers and contains the key argument.

Lemma 4.2. *For all $x \in \mathcal{O}_{L_{\mathcal{Q}}}$:*

$$|x^{q^2} - x|_v \leq q^{-1}.$$

Proof. Let us start with $y \in \mathcal{O}_{L_p}$, where $p \in \mathcal{Q}$. The prime number q is inert in K_p, and the prime ideal $p\mathcal{O}_{K_p}$ splits completely in L_p by Corollary 2.7. We deduce that the residue field of L_p at v is $\mathbb{F}_{q^2}$, and because q is unramified:

$$\left|y^{q^2} - y\right|_v \leq q^{-1}. \tag{1}$$

The extension $L_{\mathcal{Q}}/\mathbb{Q}$ is the compositum of the Galois extensions $L_p/\mathbb{Q}$, for $p \in \mathcal{Q}$, which are linearly disjoint (with coprime discriminants). This implies that:

$$\mathcal{O}_{L_{\mathcal{Q}}} = \otimes_{p\in\mathcal{Q}}\mathcal{O}_{L_p},$$

where the tensor product is over $\mathbb{Z}$ (see for instance [27], Lemma 1.3). If $x \in \mathcal{O}_{L_{\mathcal{Q}}}$, we take a decomposition in the tensor product. By (1), the properties of the binomial coefficients and the ultrametric inequality, we get:

$$\left|x^{q^2} - x\right|_v \leq q^{-1}.$$

□

The next stage is classical. It prepares a reduction to algebraic integers and is based on the "strong approximation theorem".

Lemma 4.3. *For any $x \in L^*_{\mathcal{Q}}$, there is $\beta \in \mathcal{O}_{L_{\mathcal{Q}}}$ such that $\beta x \in \mathcal{O}_{L_{\mathcal{Q}}}$ and:*

$$|\beta|_v = \max\{1, |x|_v\}^{-1}.$$

Proof. See [2], Lemma 1. □

We can now give a final estimate for the v-adic norm.

Corollary 4.4. *For all $x \in L_{\mathcal{Q}}$:*

$$\left|x^{q^2} - x\right|_v \leq q^{-1}\max\{1, |x|_v\}^{q^2+1}.$$

Proof. We can suppose that $x \neq 0$. Let β like in the former lemma. We apply Lemma 4.2 to β and βx:

$$\left|\beta^{q^2} - \beta\right|_v \leq q^{-1} \text{ and: } \left|(\beta x)^{q^2} - \beta x\right|_v \leq q^{-1}.$$

By the ultrametric inequality, we get:

$$\begin{aligned}
\left|x^{q^2} - x\right|_v &= \left|\beta^{-q^2}\right|_v \left|(\beta x)^{q^2} - \beta^{q^2} x\right|_v \\
&= \left|\beta^{-q^2}\right|_v \left|(\beta x)^{q^2} - \beta x + (\beta - \beta^{q^2})x\right|_v \\
&\leq \left|\beta^{-q^2}\right|_v \max\left\{\left|(\beta x)^{q^2} - \beta x\right|_v, \left|\beta - \beta^{q^2}\right|_v |x|_v\right\} \\
&\leq q^{-1}\max\{1, |x|_v\}^{q^2+1},
\end{aligned}$$

which is the expected inequality. □

4.4. **Proof of the theorem.** Let $x \in L^*_{\mathcal{Q}}$ of infinite order. Because x is neither zero nor a root of unity:

$$y := x^{q^2} - x \neq 0.$$

Again, we apply the product formula to y:

$$\begin{aligned}
0 &= \sum_{v\in M(L_{\mathcal{Q}})} \frac{d_v}{[L_{\mathcal{Q}} : \mathbb{Q}]} \log\left|y\right|_v \\
&\leq (q^2+1) \sum_{v\in M(L_{\mathcal{Q}})} \frac{d_v}{[L_{\mathcal{Q}} : \mathbb{Q}]} \log\max\{1, |x|_v\} + \log(2) - \sum_{v|q} \frac{d_v}{[L_{\mathcal{Q}} : \mathbb{Q}]} \log(q),
\end{aligned}$$

where the log(2) comes from the triangle inequality at all archimedian places. We thus find:

$$\log(q/2) \quad \leq \quad (q^2+1)h(x),$$

and like in the special case studied earlier, we get the following lower bound:

$$h(x) \quad \geq \quad \frac{\log(q/2)}{q^2+1}.$$

This finishes the proof of Theorem 1.9. □

Remarks. Our method does not extend to the field generated by the compositum of all $K_p(j_p)$, for $p \in \mathcal{P}$, the set of primes (or a subset of density 1). If q is a prime of ordinary reduction for E_p, we have a decomposition $q := \mathfrak{q}\mathfrak{q}'$ in K_p. In this case, class field theory only gives a relation between the two Frobenius elements $\sigma_{\mathfrak{q}}, \sigma_{\mathfrak{q}'} \in \mathrm{Gal}(L_p/K_p)$, namely: $\sigma_{\mathfrak{q}}\sigma_{\mathfrak{q}'} = 1$.

By the Chebotarev density theorem, the set of primes of K_p that split completely in L_p has density $\frac{1}{[L_p:K_p]}$, and we can't expect to bound the degree of the residue fields for all $q \in \mathcal{P}$ (or a subset of density 1). An interesting phenomenon, which has been exploited implicitly here, is that the inert primes in K_p have density $\frac{1}{2}$ as rational primes and density 0 in K_p.

The classical strategy used for instance in [2] or [11] - with a $\mathfrak{q}$-adic estimate involving some Frobenius element at $\mathfrak{q}|q$ - does not work very well either, because the centraliser of the Frobenius element can have large index in the Galois group as soon as many L_p's are involved.

5. Further examples

We indicate here how to generalize our method to other families of Galois number fields, including real quadratic fields and simplest cubic fields. We finally make some remarks about properties of cyclotomic fields related to our work.

5.1. **Generalization to families of Galois fields.** For $n \in \mathbb{N}$, let K_n be a number field such that $K_n/\mathbb{Q}$ is Galois, and let L_n be its Hilbert class field. A look at the proof of our theorem shows that the compositum L of the L_n's satisfies the Property (B) if:
-the degree $[K_n : \mathbb{Q}]$ is bounded independently of n;
-there is a prime p which is simultaneously inert in K_n for all n;
-the discriminants of the K_n's are pairwise coprime.

In this case, we can get an explicit lower bound for the height. The only difference with the bound obtained above is the power of p, which can expressed in terms of the finite number of values taken by $[K_n : \mathbb{Q}]$. The second condition implies that p is unramified in the compositum of the K_n's. By class field theory, the ideal $p\mathcal{O}_{K_n}$ splits completely in L_n for all n. The coprimality condition on the discriminants might be removed by working with local fields in Lemma 4.2.

Because of the third hypothesis, the extensions $L_n/\mathbb{Q}$ are pairwise linearly disjoint and $\mathrm{Gal}(L/\mathbb{Q}) = \prod_{n\in\mathbb{N}} \mathrm{Gal}(L_n/\mathbb{Q})$. This field is all the more interesting for us as $\mathrm{Gal}(L_n/K_n)$, the ideal class group of K_n, has big order or exponent.

We start with families of real quadratic fields. For p a prime, we let here $K_p := \mathbb{Q}[\sqrt{p}]$ and L_p its Hilbert class field. For a set $\mathcal{Q} \subset \mathcal{P}$, let $L_{\mathcal{Q}}$ be the compositum of the L_p's, for $p \in \mathcal{Q}$.

Proposition 5.1. *For all $q \geq 3$ prime, there is a set $\mathcal{P}_q \subset \mathcal{P}$ of Dirichlet density $\frac{1}{4}$ such that $L_{\mathcal{P}_q}$ has the Property (B).*

Proof. Identical to that of Theorem 1.9. □

Remark. We could also consider the compositum of a mixed family of real and quadratic fields of prime discriminant. A specificity of real quadratic fields compared to imaginary ones is that much less is known on the class group. The Cohen-Lenstra heuristics predict that the class number is statistically very small ([7]). This example might thus be less interesting in our setting.

5.2. **Simplest cubic fields.** We now look for a family of cubic fields that satisfies our criteria. The most simple example to investigate is that of the so-called "simplest cubic" fields.

Let $m \in \mathbb{N}$ and let K_m be the splitting field of the polynomial:

$$P_m(X) := X^3 - mX^2 - (m+3)X - 1,$$

with discriminant:

$$d_m := f_m^2 = (m^2 + 3m + 9)^2.$$

We can check that if $x_m > 0$ is a root of P_m, the other roots are $-\frac{1}{1+x_m} < 0$ and $-1 - \frac{1}{x_m} < 0$. Thus, the extension $K_m/\mathbb{Q}$ is normal with Galois group $\mathbb{Z}/3\mathbb{Z}$. Let L_m be the Hilbert class field of K_m.

Definition 5.2. *The field K_m is a simplest cubic field if its ring of integers is $\mathbb{Z}[x_m]$.*

The field K_m is a simplest cubic field if and only if $m \not\equiv 0 \pmod 3$ and f_m is square free, or if $m \equiv 0, 6 \pmod 9$ and $f_m/9$ is square free ([31], Proposition 1 and Corollary). In this case, the number d_m is the discriminant of K_m.

We can go further about the arithmetic properties of the f_m's. According to Hardy and Littlewood's 'Conjecture F", there should be infinitely many $m \in \mathbb{N}$ such that f_m is prime. One can prove (see [19], Proposition 1) that if $N(x)$ is the number of $0 \leq m \leq x$ such that K_m is a simplest cubic field:

$$\frac{N(x)}{x} \longrightarrow_{x \to +\infty} \frac{8}{9} \prod_{p \equiv 1 \pmod 6} \left(1 - \frac{2}{p^2}\right) \approx 0.83.$$

We will use an infinite sequence of square free and pairwise coprime discriminants.

Lemma 5.3. *There exists an infinite set $\mathcal{N} \subset \mathbb{N}$ such that:*

$$\forall m \neq n \in \mathcal{N},\ f_m \text{ and } f_n \text{ are square free and coprime.}$$

Proof. We construct the set $\mathcal{N} = \{m_k, k \geq 1\}$ by induction. Since $f_1 = 13$, we start with $m_1 = 1$. Let $k \geq 2$ and suppose that we have found $m_1, \ldots, m_{k-1}$ with the required properties.

We denote by $P \geq 13$ the greatest prime factor of $m_1 \cdots m_{k-1}$. Since f_m is always odd, it is sufficient to find an integer m such that:

$$\forall p \in \mathcal{P} \quad : \quad p \nmid f_m \text{ if } 3 \leq p \leq P, \text{ and } p^2 \nmid f_m \text{ otherwise.} \tag{2}$$

For $x \geq 1$, let $A(x)$ be the set of $1 \leq m \leq x$ with these properties. Let $q \geq 1$ be an integer and suppose that there is $m \geq 1$ such that $q|f_m$. For any other n with $q|f_n$, we immediately check that:

$$(2m+3)^2 \equiv (2n+3)^2 \pmod{q}.$$

Thus, if $q = p$ is a prime ≥ 3, there are at most two classes mod p that may contain an m such that $p|f_m$. If $q = p^2$ and $p \geq 5$, we rapidly see that there are at most two classes mod p^2 that may contain an m with $p^2|f_m$.

Now, let N be the product of all primes $3 \leq p \leq P$, and suppose that $x \geq N^2$. By the chinese remainder theorem, there are at least $\prod_{3\leq p\leq P}(p-2)$ classes mod N such that for each m in one of these classes, $\gcd(f_m, N) = 1$. Let $A_1(x)$ be the set of $1 \leq m \leq x$ such that the first pack of conditions in (2) is realized. Since $x \geq N$, we have:

$$|A_1(x)| \geq \frac{1}{2} \prod_{3\leq p\leq P} \left(1 - \frac{2}{p}\right) x := cx.$$

For $p \in \mathcal{P}$, let:

$$A_p(x) := \{m \in A_1(x), p^2|f_m\}.$$

This set is empty for $p \leq P$. If $P < p \leq \sqrt{\frac{x}{N}}$, we can use the chinese remainder theorem because p^2 and N are coprime, and we find that:

$$|A_p(x)| \leq \frac{4}{p^2} cx.$$

For a "big" prime $p > \sqrt{\frac{x}{N}}$, we get the weaker estimate:

$$|A_p(x)| \leq 2\Big(1 + \Big\lfloor \frac{x}{p^2} \Big\rfloor\Big) \leq 2(N+1)$$

We now give a lower bound for $|A(x)|$. For $x \geq 3$, we see that: $f_x \leq (2x)^2$, so we can restrict ourselves to primes $p \leq 2x$:

$$\begin{aligned} |A(x)| &\geq |A_1(x)| - \sum_{P<p\leq 2x} |A_p(x)| \\ &\geq cx - cx \sum_{P<p} \frac{4}{p^2} - \sum_{p\leq 2x} 2(N+1) \\ &\geq c\Big(1 - \sum_{P<p} \frac{4}{p^2}\Big)x - \frac{4(N+1)}{\log(x)} x, \end{aligned}$$

where the last inequality comes from a classical upper bound on the number of primes at most x ([23], Theorem 1). We remark that:

$$4 \sum_{P<p} \frac{1}{p^2} \leq 4 \sum_{13<p} \frac{1}{p^2} \leq 4 \sum_{17\leq n} \Big(\frac{1}{n-1} - \frac{1}{n}\Big) \leq \frac{1}{4},$$

and for x large enough, we finally get: $|A(x)| \geq 1$. □

An interesting property of simplest cubic fields for our purpose is that they have a common inert prime.

Lemma 5.4. *If K_m is a simplest cubic field, the ideal $(2)\mathbb{Z}[x_m]$ is prime.*

Proof. Let $\tilde{P}_m$ be the reduction of P_m mod 2. We have: $\tilde{P}_m = X^3 + X + 1$ if m is even, and $\tilde{P}_m = X^3 + X^2 + 1$ if m is odd. In each case, $\tilde{P}_m$ has no root so it is irreducible. By Dedekind's criterion ([20], I, Proposition 8.3), it follows that 2 remains prime in K_m. □

Let $L_{\mathcal{N}}$ be the compositum of the Hilbert class fields L_m, for $m \in \mathcal{N}$. We are in a position to prove that this field has the Property (B).

Proposition 5.5. *For all $x \in L_{\mathcal{N}}^*$ of infinite order:*

$$h(x) \geq \frac{\log(2)}{18}.$$

Proof. The proof is very close to that of Theorem 1.9, and we will not enter in all the details. Let x of infinite order in a finite compositum $L_{\mathcal{N}(x)}$, and $v|2$ in $M(L_{\mathcal{N}(x)})$. Let $m \in \mathcal{N}(x)$ and $y \in \mathcal{O}_{L_m}$. Since 2 is inert in K_m, it splits completely in L_m so that the residue field at v is $\mathbb{F}_{2^3}$ and:

$$\left|y^8 - y\right|_v \leq 2^{-1}.$$

By construction of $\mathcal{N}$, the fields L_m, for $m \in \mathcal{N}(x)$, have pairwise coprime discriminants. Suppose first that x is an algebraic integer. Exactly like in Lemma 4.2, we get:

$$\left|x^8 - x\right|_v \leq 2^{-1}.$$

We now apply a 2-adic acceleration trick:

$$\left|x^{16} - x^2\right|_v = \left|(x^8 - x)^2 + 2x(x^8 - x)\right|_v \leq 2^{-2}.$$

If x is no longer an algebraic integer, we use strong approximation and imitate the proof of Corollary 4.4, which yields:

$$\left|x^{16} - x^2\right|_v \leq 2^{-2} \max\{1, |x|_v\}^{18}.$$

We can now apply the product formula to $x^{16} - x^2$, which is not zero by the hypothesis on x, with trivial estimates at places not above 2. We find the expected bound:

$$h(x) \geq \frac{\log(4) - \log(2)}{18} = \frac{\log(2)}{18}.$$

□

Remark. The field $L_{\mathcal{N}}$ also has a rather complicated Galois structure. For each $m \in \mathcal{N}$, one can prove that:

$$[L_m : K_m] \geq \frac{f_m}{e \log(f_m)^3};$$

and under the assumption of GRH, the abelian group $\mathrm{Gal}(L_m/K_m)$ has exponent $\gg \frac{\log(m)}{\log\log(m)}$, where $\gg$ means that the stated inequality is true up to a positive constant ([19], Theorem 4 and Proposition 9).

5.3. **Inert primes in cyclotomic fields.** For an infinite compositum of cyclotomic fields, the first condition is not realized. However, we remark that there is a good criterion to identify inert primes in this case. For $p \in \mathcal{P}$ a prime, let $\mathbb{Q}(\xi_p)$ be the field generated by a primitive p-th root of unity.

Lemma 5.6. *A prime $q \neq p$ is inert in $\mathbb{Q}(\xi_p)$ if and only if the image of q in $(\mathbb{Z}/p\mathbb{Z})^*$ is a generator.*

Proof. See [30], Theorem 2.13. □

The existence of infinitely many p's such that q is a generator of $(\mathbb{Z}/p\mathbb{Z})^*$ is the object of Artin's conjecture on primitive roots. A special case is the following.

Conjecture 5.7 (Artin)**.** *The set $\mathcal{P}_q$ of primes p such that q is a generator of $(\mathbb{Z}/p\mathbb{Z})^*$ has density $c_A := \prod_{p\in\mathcal{P}} \left(1 - \frac{1}{p(p-1)}\right) > 0$.*

The real number $c_A \approx 0.37$ is supposed to be independent of q. Artin's conjecture holds under the assumption of GRH ([13]). Furthermore, Heath-Brown proved (see [12], or the earlier version [10]) that for all primes q but at most two, the set $\mathcal{P}_q$ is infinite and:

$$|\mathcal{P}_q \cap [1, x]| \gg \frac{x}{\log(x)^2}.$$

It is also possible to bound from below the exponent of the class group of $\mathbb{Q}(\xi_p)$ explicitly in terms of p (see for instance [2], Corollary 2).

References

[1] F. Amoroso, S. David, and U. Zannier. On fields with the Property (B). *Proc. Amer. Math. Soc.*, 142(6):1893–1910, 2014.

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

[3] F. Amoroso and U. Zannier. A relative Dobrowolski lower bound over abelian extensions. *Ann. Scuola Norm. Sup. Pisa*, 29(4):711–727, 2000.

[4] E. Bombieri and U. Zannier. A note on heights in certain infinite extensions of $\mathbb{Q}$. *Rend. Mat. Acc. Lincei*, 12(9):5–14, 2001.

[5] S. Checcoli. Fields of algebraic numbers with bounded local degrees and their properties. *Trans. Amer. Math. Soc.*, (365):2223–2240, 2013.

[6] S. Checcoli and M. Widmer. On the Northcott property and other properties related to polynomial mappings. *Math. Proc. Camb. Philos. Soc.*, 4(155):1–12, 2013.

[7] H. Cohen and H.W. Lenstra. Heuristics on class groups of number fields. *Lecture Notes in Math.*, 1068:33–62, 1984.

[8] E. Dobrowolski. On a question of Lehmer and the number of irreducible factors of a polynomial. *Acta Arith.*, 34:391–401, 1979.

[9] N. Elkies. The existence of infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$. *Invent. Math.*, 89:561–567, 1987.

[10] R. Gupta and M. Ram Murty. A remark on Artin's conjecture. *Invent. Math.*, 78:127–130, 1984.

[11] P. Habegger. Small height and infinite nonabelian extensions. *Duke Math. J.*, 162(11):2027–2076, 2013.

[12] D. Heath-Brown. Artin's conjecture for primitive roots. *Quart. J. Math. Oxford*, 37:27–38, 1986.

[13] C. Hooley. On Artin's conjecture. *J. Reine Angew. Math.*, 225:209–220, 1967.

[14] K. Ireland and M. Rosen. *A classical introduction to modern number theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1980.

[15] S. Lang. *Elliptic functions*, volume 112 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1987.

[16] S. Lang and H. Trotter. Frobenius distributions in GL_2-extensions. *Lecture Notes in Math.*, 504, 1976.
[17] D. H. Lehmer. Factorization of certain cyclotomic functions. *Ann. of Math.*, 34:461–479, 1933.
[18] S. Louboutin. L-functions and class numbers of imaginary quadratic fields and of quadratic extensions of an imaginary quadratic field. *Math. Comp.*, 59(199):213–230, 1992.
[19] S. Louboutin. The exponent three class group problem for some real cyclic cubic number fields. *Proc. Amer. Math. Soc.*, 130(2):353–361, 2001.
[20] J. Neukirch. *Algebraic number theory*, volume 322 of *Grund. Math. Wissenschaft.* Springer-Verlag, 1999.
[21] F. Pappalardi. On the exponent of the ideal class group of $\mathbb{Q}(\sqrt{-d})$. *Proc. Amer. Math. Soc.*, 123(3):663–671, 1995.
[22] M. Rosenbloom and M. Tsfasman. Multiplicative lattices in global fields. *Invent. Math.*, 101:687–696, 1990.
[23] G. Rosser and L. Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois J. Math.*, 6(1):64–94, 1962.
[24] A. Schinzel. On the product of the conjugates outside the unit circle of an algebraic number. *Acta Arith.*, 24:385–399, 1973.
[25] J. P. Serre. Groupes de Lie l-adiques attachés aux courbes elliptiques. *Colloque de Clermont-Ferrand, IHES*, 1964.
[26] J. P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15:259–331, 1972.
[27] G. Shimura. Construction of class fields and zeta functions of algebraic curves. *Ann. of Math.*, 85:58–159, 1967.
[28] J. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.
[29] J. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.
[30] L. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New-York, 1982.
[31] L. Washington. Class numbers of the simplest cubic fields. *Math. Comp.*, 48:371–384, 1987.

Aurélien Galateau, Université de Franche-Comté
E-mail address: aurelien.galateau@univ-fcomte.fr