Comment. Math. Helv. 100 (2025), 421–462
DOI 10.4171/CMH/596

Around the support problem for Hilbert class polynomials

Francesco Campagna and Gabriel A. Dill

Abstract. Let $H_D(T)$ denote the Hilbert class polynomial of the imaginary quadratic order of discriminant D. We study the rate of growth of the greatest common divisor of $H_D(a)$ and $H_D(b)$ as $|D| \to \infty$ for a and b belonging to various Dedekind domains. We also study the modular support problem: if for all but finitely many D every prime ideal dividing $H_D(a)$ also divides $H_D(b)$, what can we say about a and b? If we replace $H_D(T)$ by $T^n - 1$ and the Dedekind domain is a ring of S-integers in some number field, then these are classical questions that have been investigated by Bugeaud–Corvaja–Zannier, Corvaja–Zannier, and Corrales-Rodrigáñez–Schoof.

1. Introduction

Some of the recent research in diophantine geometry has been driven by the following guiding philosophy: if an ambient variety X contains two generic subvarieties whose dimensions do not add up to at least the dimension of X, then these two subvarieties should not intersect; and, even if they do, this intersection must be "small" in some sense. This philosophy has been motivated by the pioneering works of Bombieri, Masser, and Zannier [8], Zilber [68], and Pink [54], and such a point of view can also be pushed to the setting of arithmetic varieties, where X is now taken to be a variety over the ring of integers of a number field. The archetypal result in this context of "arithmetic unlikely intersections" is the following theorem of Bugeaud, Corvaja, and Zannier [9].

Theorem 1.1 ([9, Theorem 1]). *Let a, b be multiplicatively independent integers ≥ 2, i.e., such that $a^k b^\ell \neq 1$ for all $(k, \ell) \in \mathbb{Z}^2 \backslash \{(0,0)\}$, and let $\varepsilon > 0$. Then, provided n is sufficiently large, we have*

$$\gcd(a^n - 1, b^n - 1) < \exp(\varepsilon n).$$

Here, the left-hand side measures the size of the intersection of the Zariski closure in the square of the multiplicative group $\mathbb{G}^2_{m,\mathbb{Z}}$ of the singleton $\{(a,b)\} \subseteq \mathbb{G}^2_{m,\mathbb{Q}}(\mathbb{Q})$

Mathematics Subject Classification 2020: 11G18 (primary); 11G15, 14G35 (secondary).
Keywords: complex multiplication, elliptic curve, greatest common divisor, singular modulus.

with the kernel of the raising-to-the-n-th-power morphism. This size is always trivially bounded by $\exp(cn)$ for some constant c. Hence, Theorem 1.1 says that this latter bound is too crude if we pick a and b generic enough, meaning that a and b do not satisfy a relation of multiplicative dependence. The philosophy described above incarnates in the fact that we are intersecting two 1-dimensional schemes inside a 3-dimensional ambient scheme (here, "dimension" always means "absolute Krull dimension"). That Theorem 1.1 is an arithmetical analogue of results about unlikely intersections in characteristic 0 has already been pointed out by Zannier in [66, Chapter 2]. We remark that Theorem 1.1 has later been generalized by Corvaja and Zannier in [15].

In this article, we replace $\mathbb{G}_m$ by the coarse moduli space of elliptic curves $Y(1)$, which is the affine line $\mathbb{A}^1$, and we study the analogue of Theorem 1.1 and related questions in this context. This venture is inspired by the well-known fact that there is a notion of special subvarieties in both the realm of tori and the realm of (powers of) modular curves. Let F be a field. A *special subvariety* of $\mathbb{G}_{m,F}^n$ is an irreducible component of an algebraic subgroup of $\mathbb{G}_{m,F}^n$. On the other hand, if $X_1, \ldots, X_n$ are affine coordinates on $Y(1)_F^n$, then a *special subvariety* of $Y(1)_F^n$ is an irreducible component of the intersection of the zero loci of finitely many modular polynomials $\Phi_{N_k}(X_{i_k}, X_{j_k})$ $(k = 1, \ldots, K)$; see [36, p. 55] for the definition of Φ_{N_k}. In particular, a special point of $\mathbb{G}_{m,\mathbb{C}}$ is a root of unity and a special point of $Y(1)_{\mathbb{C}}$ is a *singular modulus*, i.e., the j-invariant of an elliptic curve with complex multiplication.

Theorem 1.1 is about values of the polynomials $T^n - 1$ $(n \in \mathbb{N} = \{1, 2, \ldots\})$. These have the property that their zeroes are all special points of $\mathbb{G}_{m,\mathbb{C}}$. It then appears more natural to consider the family of cyclotomic polynomials $\Psi_n(T)$ $(n \in \mathbb{N})$, which are precisely the minimal polynomials over $\mathbb{Q}$ of the special points of $\mathbb{G}_{m,\mathbb{C}}$. Using the dictionary above, the analogue of this family in the $Y(1)$ case is precisely the family of *Hilbert class polynomials* $H_D(T)$ with $D \in \mathbb{D}$, where $\mathbb{D} = \{-3, -4, \ldots\}$ is the set of negative integers $\equiv 0, 1 \bmod 4$ and $H_D(T) \in \mathbb{Z}[T]$ is the minimal polynomial over $\mathbb{Q}$ of any j-invariant of an elliptic curve with complex multiplication by the imaginary quadratic order of discriminant D. Thus, we are led to studying how large the greatest common divisor of $H_D(a)$ and $H_D(b)$ can be, where $a, b \in \mathbb{Z}$.

This question, which we study in Section 3, as well as more general divisibility questions also make sense with an arbitrary Dedekind domain R in place of $\mathbb{Z}$. Indeed, for any polynomial with integer coefficients like for example $\Psi_n(T)$, $H_D(T)$, and $\Phi_N(X, Y)$, we obtain an associated polynomial with coefficients in R by applying the unique ring homomorphism $\mathbb{Z} \to R$ to all coefficients. We will always denote this associated polynomial by the same symbol as the original one and also speak of Hilbert class polynomials, cyclotomic polynomials, modular polynomials, etc. with coefficients in R.

To warm up, we begin by studying the case where R is the coordinate ring of a smooth affine irreducible curve $\mathcal{C}$ over an algebraically closed field F of characteristic 0. We prove Theorem 3.1, which is a modular analogue of the first part of [1, Theorem 1] by Ailon and Rudnick: the greatest common divisor of the values of two Hilbert class polynomials at two "generic" elements $A, B \in R$ always divides a fixed non-zero ideal $J = J_{A,B} \subseteq R$. Ailon and Rudnick proved their result using the Manin–Mumford conjecture for plane curves, i.e., the theorem of Ihara, Serre, and Tate [35]. Our result similarly follows from the André–Oort conjecture for plane curves, i.e., from the theorem of André [2], which is the modular counterpart of the theorem of Ihara, Serre, and Tate. Silverman also studied the analogue of this question in the elliptic setting, but managed to obtain a comparable result only if the elliptic curve is isotrivial, see [63, Conjecture 7, Theorem 8, and Remark 5]. His result has recently been extended to the case of a product of two arbitrary elliptic curves by Ghioca, Hsia, and Tucker [26] and to the case of a general split semiabelian variety and F equal to the field of algebraic numbers by Barroero, Capuano, and Turchet [4]. In the proofs of all these results, there are two ingredients: the first one is a (relative) Manin–Mumford result for curves, due in the constant case to Ihara–Serre–Tate [35], Raynaud [55], and Hindry [30], in the non-isotrivial abelian case to Masser and Zannier in a series of articles [44–49], and in the non-isotrivial split semiabelian case to Bertrand–Pillay–Masser–Zannier [5] combined with the aforementioned results. The second ingredient is a multiplicity estimate originating in the work of Silverman, see [63, Lemma 4 and Remark 2], [26, Lemma 4.5], and [4, Lemma 4.1].

One may wonder whether a similar theorem as our Theorem 3.1 also holds if the characteristic of F is positive. Our next result, which we prove using the *abc* theorem for function fields by Mason [42], shows that this is not the case if F is an algebraic closure of a finite field.

Theorem 1.2 (Theorem 3.4). *Let $p \in \mathbb{N}$ be prime and fix an algebraic closure $F = \overline{\mathbb{F}}_p$ of $\mathbb{F}_p$. Let R be the coordinate ring of a smooth affine irreducible curve $\mathcal{C}_{/F}$ and let $A, B \in R \backslash F$. Then*

$$\limsup_{D \in \mathbb{D},\, |D| \to \infty} \frac{\deg(\gcd(H_D(A), H_D(B)))}{\deg H_D} > 0,$$

where $\gcd(H_D(A), H_D(B)) := RH_D(A) + RH_D(B)$ *and the degree* $\deg I$ *of a non-zero ideal I of the Dedekind domain R is the number of maximal ideals appearing in the prime factorization of I, counted with multiplicities.*

In the multiplicative setting, Silverman proved a more precise analogue of Theorem 1.2 as [62, Theorem 4] in the case where $\mathcal{C} = \mathbb{A}^1_F$. He also considered the elliptic case for the same $\mathcal{C}$, but again obtained a comparable result only under the added condition of isotriviality, see [63, Conjecture 9 and Theorem 10]. A related question has been studied in the modular setting by Edixhoven and Richard in [20], see also Richard's work [56] over $\mathbb{Z}$.

We finally come to the modular counterpart of Theorem 1.1 and its generalization to arbitrary number fields.

Theorem 1.3 (Theorem 3.7). *Let K be a number field and let S be a finite set of maximal ideals of $\mathcal{O}_K$. Consider two elliptic curves $E_{1/K}, E_{2/K}$ with potential good reduction outside of S, i.e., such that the j-invariant $j(E_i) \in \mathcal{O}_{K,S}$ for $i = 1, 2$. Suppose that there exists a prime ideal $\mathfrak{p}$ of $\mathcal{O}_{K,S}$ at which both E_1 and E_2 have potential good supersingular reduction. Let p denote the rational prime lying under $\mathfrak{p}$. Then,*

$$\limsup_{D \in \mathbb{D},\, |D| \to \infty} (\deg H_D)^{-1} \log N\big(\gcd\big(H_D(j(E_1)), H_D(j(E_2))\big)\big) \geq \frac{\log p}{p-1} > 0,$$

where $N(\cdot)$ denotes the ideal norm in $\mathcal{O}_{K,S}$.

In particular, Theorem 1.3 shows that the naive analogue of Theorem 1.1 over number fields is false. Namely, the condition in Theorem 1.1 that a and b are multiplicatively independent is equivalent to demanding that the point $(a, b) \in \mathbb{G}^2_{m,\mathbb{C}}(\mathbb{C})$ is not contained in any proper special subvariety of $\mathbb{G}^2_{m,\mathbb{C}}$. In the modular setting, this translates into the condition that a and b are both not singular moduli and that $\Phi_N(a, b) \neq 0$ for all $N \in \mathbb{N}$. However, we will show that there are infinitely many such pairs $(a, b) \in \mathcal{O}^2_{K,S}$ such that a and b are the j-invariants of elliptic curves with a fixed common prime ideal of potential good supersingular reduction. On the other hand, proving that two general elliptic curves have a common supersingular prime is a difficult open problem, already if they are defined over $\mathbb{Q}$. Conjecturally, there are infinitely many common supersingular primes if both E_1 and E_2 do not have complex multiplication, are defined over $\mathbb{Q}$, and are not geometrically isogenous; see [38] and [24], where also an averaged version of this conjecture is proved.

The reader might now wonder about possible elliptic and abelian analogues of Theorem 1.1. Silverman conjectured in [63, Conjecture 1 (a)] an analogue of Theorem 1.1, where the square of the multiplicative group is replaced by the square of an elliptic curve over the rationals. Assuming certain cases of Vojta's conjecture, Silverman proved a generalization of [63, Conjecture 1 (a)] to an arbitrary abelian variety over $\mathbb{Q}$ in [64, Proposition 9] and to a product of an elliptic curve over $\mathbb{Q}$ with $\mathbb{G}_{m,\mathbb{Q}}$ in [64, Theorem 4]. So at least conditionally on Vojta's conjecture, elliptic curves and abelian varieties seem to behave like the multiplicative group and not like the moduli space of elliptic curves. However, unconditionally, nothing non-trivial beyond the results in [9, 15] is known at the time of writing in the setting of abelian and semiabelian varieties over number fields.

There are other examples where the arithmetic behaviour in Shimura varieties and in algebraic groups is different. Let us mention, for example, the S-integrality properties of special points with respect to a divisor in $\mathbb{G}_{m,\bar{\mathbb{Q}}}$ and $Y(1)_{\bar{\mathbb{Q}}}$ respectively, where S is a finite set of rational primes and $\bar{\mathbb{Q}}$ will always denote a fixed algebraic closure of $\mathbb{Q}$: for $\mathbb{G}_{m,\bar{\mathbb{Q}}}$, Baker, Ih, and Rumely proved in [3, Theorem 0.1] that there are at most finitely many special points that are S-integral with respect to some non-special point P, but this fails to hold if P itself is special. For $Y(1)_{\bar{\mathbb{Q}}}$, Habegger proved in [28, Theorem 2] that there are at most finitely many special points that are $\emptyset$-integral with respect to an *arbitrary* finite non-empty set of points, which can also consist of only one special point.

In order to prove Theorem 1.3, we apply [51, Theorem 3] by Michel to find arbitrarily large discriminants $D \in \mathbb{D}$ such that many zeroes of $H_D(T)$ reduce to the reductions of $j(E_1)$ and $j(E_2)$ respectively modulo a fixed prime ideal $\mathfrak{P}$ that lies over $\mathfrak{p}$ in a fixed algebraic closure of K. For our argument to work, it is essential that each such D is coprime to p and that therefore $\mathfrak{p}$ is unramified in the splitting field of $H_D(T)$ over K.

Supersingularity seems to be a fundamental feature of the modular world that the multiplicative one is lacking and that explains some of the differences between the two: it allows several distinct special points in the same Galois orbit to reduce to the same element modulo a maximal ideal lying over some rational prime p while p remains unramified in the corresponding ring class field. Multiplying the discriminant of a singular modulus or the order of a root of unity by powers of p also leads to several distinct elements of the Galois orbit having equal reductions modulo a maximal ideal above p (see Proposition 2.4 for the modular case), but at the same time introduces arbitrarily large ramification over p. It seems likely that the supersingular primes are the only obstacle to proving an analogue of Theorem 1.1 in the modular case. In particular, we can ask for the rate of growth of the norm of the g.c.d. of $H_{D_1}(a)$ and $H_{D_2}(b)$ deprived of all common supersingular prime factors for a, b in some ring of S-integers such that $\Phi_N(a,b) \neq 0$ for all $N \in \mathbb{N}$ and neither a nor b is a singular modulus.

When trying to understand the size of the greatest common divisor of $H_D(a)$ and $H_D(b)$ for a and b in some Dedekind domain R, we were led to consider the extreme case where every prime dividing $H_D(a)$ also divides $H_D(b)$ for all but finitely many $D \in \mathbb{D}$. For which a and b is this possible? This is the modular instance of the so-called *support problem*. If we again replace the polynomials $H_D(T)$ $(D \in \mathbb{D})$ by the polynomials $T^n - 1$ $(n \in \mathbb{N})$, this becomes the *multiplicative support problem*. In the case where R is the ring of S-integers in some number field, Corrales-Rodrigáñez and Schoof have solved this problem in [14, Theorem 1], which, as a special case, yields an answer to a question posed by Erdős at the 1988 number theory conference in Banff. An answer to the question of Erdős also follows from earlier work of Schinzel [57]. Furthermore, Corrales-Rodrigáñez and Schoof solved an analogue of this problem with an elliptic curve in place of the multiplicative group, see [14, Theorem 2]. Later, Larsen solved the problem in the case of an arbitrary abelian variety [39] and Perucca generalized his result to split semiabelian varieties [53]. It is interesting to note that the conclusions of all these results are invariant under localization of the base ring at some finite set of maximal ideals although their hypotheses depend on the base ring. This will also be the case in our own results. One can also investigate the support problem as well as possible analogues of Theorem 1.1 in Shimura varieties other than $Y(1)^2$ or in arithmetic dynamics (for the latter, cf. [31] and [50, Section 5]).

In Section 4, we introduce the support problem for general families of polynomials in T with coefficients in a Dedekind domain which is not a field and revisit the multiplicative support problem as well as its cyclotomic counterpart, where $T^n - 1$ is replaced by the n-th cyclotomic polynomial $\Psi_n(T)$ for $n \in \mathbb{N}$. We show in Theorem 4.5 and Theorem 4.6 how the theorem of Corrales-Rodrigáñez–Schoof [14, Theorem 1] and the theorem of Ihara–Serre–Tate [35, p. 230] can be used to give a comprehensive solution to the multiplicative and cyclotomic support problem in characteristic 0, which is best possible in all cases.

In Section 5, we finally consider the modular support problem. We first solve the function field version of the problem.

Theorem 1.4 (Theorem 5.2). *Let R be the coordinate ring of a smooth affine irreducible curve $\mathcal{C}$ over an algebraically closed field F of characteristic* 0*. Let $A, B \in R \backslash F$ and suppose that there exists $D_0 \in \mathbb{N}$ such that, for all discriminants $D \in \mathbb{D}$ with $|D| > D_0$, every prime ideal of R that divides $H_D(A)$ also divides $H_D(B)$. Then $A = B$.*

In the proof of Theorem 1.4 we rely on Theorem 3.1, but additional arguments are needed to deal with the case where $\Phi_N(A, B) = 0$ for some $N \in \mathbb{N}$, $N > 1$ (see Proposition 5.1, which is inspired by the theory of isogeny volcanoes). We then turn to the modular support problem in the number field case and prove the following theorem.

Theorem 1.5 (Theorem 5.4). *Let K be a number field and let S be a finite set of maximal ideals of $\mathcal{O}_K$. Let $j, j' \in \mathcal{O}_{K,S}$. Suppose that there exists $D_0 \in \mathbb{N}$ such that all the prime ideals of $\mathcal{O}_{K,S}$ dividing $H_D(j)$ also divide $H_D(j')$ for every $D \in \mathbb{D}$ with $|D| > D_0$. Then either $j = j'$ or there exists $\widetilde{D} \in \mathbb{D}$ such that $H_{\widetilde{D}}(j) = H_{\widetilde{D}}(j') = 0$.*

An important ingredient in our proof of Theorem 1.5 is a result of Zarhin [67] that allows us to find many primes of good ordinary reduction for a given elliptic curve without complex multiplication such that the endomorphism ring of its reduction satisfies some suitable local conditions. We also crucially use a result by Khare and

Larsen [34] that implies that two elliptic curves are geometrically isogenous if their reductions modulo $\mathfrak{p}$ are geometrically isogenous for all $\mathfrak{p}$ in a set of prime ideals of density 1 (if the adverb "geometrically" is dropped, then this is a direct consequence of the work of Faltings [23, Korollar 2, p. 361], see also Serre's [60, Proposition, p. IV-15]). Furthermore, the proof relies again on Proposition 5.1.

We do not know whether the conclusion of Theorem 1.5 can be strengthened to saying that $j = j'$ always. However, this strengthened conclusion is certainly false if we assume that $\mathfrak{p} \mid H_D(j) \Rightarrow \mathfrak{p} \mid H_D(j')$ holds just for infinitely many D (and all $\mathfrak{p}$) instead of holding for all but finitely many D (and all $\mathfrak{p}$). The following theorem provides a counterexample.

Theorem 1.6 (Theorem 5.6). *Let*

$$j = \frac{-191025 - 85995\sqrt{5}}{2} \quad \textit{and} \quad j' = \frac{-191025 + 85995\sqrt{5}}{2}$$

be the two singular moduli of discriminant -15 *in* $\overline{\mathbb{Q}}$. *Then for every discriminant* $D \in \mathbb{D}$ *with* $D \equiv 1 \bmod 8$, *the support property holds in both directions, i.e., for every maximal ideal* $\mathfrak{p}$ *of* $\mathbb{Z}[(-1+\sqrt{5})/2]$, *we have that* $\mathfrak{p} \mid H_D(j)$ *if and only if* $\mathfrak{p} \mid H_D(j')$.

2. Preliminaries and notation

Throughout the paper, we adopt the following notation: if K is a number field, we denote its ring of integers by $\mathcal{O}_K$ and for every finite set S of maximal ideals of $\mathcal{O}_K$, we denote by $\mathcal{O}_{K,S}$ the ring of S-integers in $\mathcal{O}_K$. The norm $N(I)$ of a non-zero ideal $I \subseteq \mathcal{O}_{K,S}$ is the index $[\mathcal{O}_{K,S} : I]$. We have $N(IJ) = N(I)N(J)$ for all ideals $I, J \subseteq \mathcal{O}_{K,S}$. Finally, if R is an arbitrary Dedekind domain and $a, b \in R$, we write $\gcd(a, b)$ for their greatest common divisor, i.e., for the ideal $Ra + Rb \subseteq R$.

2.1. Elliptic curves with complex multiplication

If E is an elliptic curve over a field K, we denote its j-invariant by $j(E)$. If L/K is a field extension, we denote the endomorphism ring of the base change E_L of E to L by $\mathrm{End}_L(E)$. We say that E has *complex multiplication* if the canonical inclusion $\mathbb{Z} \hookrightarrow \mathrm{End}_{\overline{K}}(E)$ is strict for some algebraic closure $\overline{K}$ of K. We say that it has *complex multiplication by a ring* $\mathcal{O} \not\simeq \mathbb{Z}$ if $\mathrm{End}_{\overline{K}}(E) \simeq \mathcal{O}$.

Over a field of characteristic 0, an elliptic curve with complex multiplication always has complex multiplication by an imaginary quadratic order $\mathcal{O}$. The j-invariants of the elliptic curves with complex multiplication by the imaginary quadratic order $\mathcal{O}$ of discriminant $D = \mathrm{disc}(\mathcal{O})$ are precisely the zeroes of the corresponding

Hilbert class polynomial $H_D(T)$. Recall that the Hilbert class polynomials $H_D(T)$, where D runs through the set $\mathbb{D} = \{-3, -4, \ldots\}$ of negative discriminants, all belong to $\mathbb{Z}[T]$ and are monic and irreducible in this ring. For all of this in the language of lattices in $\mathbb{C}$, see [17, §13, in particular Proposition 13.2]. The degree of H_D will be denoted by $h(D)$ and equals the class number of the imaginary quadratic order of discriminant D. The discriminant of a singular modulus, i.e., of a zero of some $H_D(T)$, is the discriminant D of the corresponding imaginary quadratic order.

Over fields of positive characteristic, the geometric endomorphism ring of an elliptic curve with complex multiplication is isomorphic either to an order in an imaginary quadratic field or to a maximal order in a quaternion algebra. In the first case or if the elliptic curve does not have complex multiplication, we call the elliptic curve *ordinary*. In the second case, we call it *supersingular*. For an ordinary elliptic curve over a finite field, all the geometric endomorphisms are already defined over the base field as we will now show.

Lemma 2.1. *Let k be a finite field with an algebraic closure $\bar{k}$ and let $E_{/k}$ be an ordinary elliptic curve. Then,* $\mathrm{End}_k(E) = \mathrm{End}_{\bar{k}}(E)$*, where we identify an endomorphism of E with its base change to $\bar{k}$.*

Proof. Since E is ordinary, the identity automorphism id_E and the Frobenius endomorphism π are $\mathbb{Z}$-linearly independent by [32, Chapter 13, Propositions 6.1 and 6.2]. Hence, $\mathrm{End}_k(E)$ has finite index N inside $\mathrm{End}_{\bar{k}}(E)$. There exists a finite Galois extension $k \subseteq k'$ with $k' \subseteq \bar{k}$ such that $\mathrm{End}_{\bar{k}}(E) = \mathrm{End}_{k'}(E)$, where we identify an endomorphism of $E_{k'}$ with its base change to $\bar{k}$. By [27, Theorem 14.84], $\mathrm{End}_k(E)$ is precisely the subset of $\mathrm{End}_{k'}(E)$ fixed by $\mathrm{Gal}(k'/k)$. Since $Nf \in \mathrm{End}_k(E)$ for all $f \in \mathrm{End}_{k'}(E)$ and the latter is an integral domain, it follows that all elements of $\mathrm{End}_{k'}(E)$ are fixed by $\mathrm{Gal}(k'/k)$, and so $\mathrm{End}_{\bar{k}}(E) = \mathrm{End}_{k'}(E) = \mathrm{End}_k(E)$, as desired. ■

2.2. Reduction of elliptic curves

When we say that an elliptic curve E over a number field K has *(potential) good/bad reduction at a maximal ideal* $\mathfrak{p}$ of $\mathcal{O}_{K,S}$, we mean that its base change to the completion $K_{\mathfrak{p}}$ of K at $\mathfrak{p}$ has (potential) good/bad reduction in the sense of [65, VII, Section 5]. The elliptic curve E has *(potential) good ordinary/supersingular reduction at* $\mathfrak{p}$ if its reduction at $\mathfrak{p}$ is (potentially) good and ordinary/supersingular. If E does not have complex multiplication, Serre has proved that for $\mathfrak{p}$ in a set of maximal ideals of natural density 1, the reduction of E modulo $\mathfrak{p}$ is ordinary. This follows from [59, Théorème 20, p. 189 and Remarque 2, p. 190] combined with the facts that the reduction of E at a maximal ideal of prime norm > 3 is supersingular if and only if the trace of the Frobenius endomorphism of the reduced elliptic curve is 0 (see [65, V, Exercise 5.10]) and that the set of maximal ideals of prime norm has natural density 1.

However, understanding the geometric endomorphism ring of the reductions of E modulo $\mathfrak{p}$ for varying $\mathfrak{p}$ is a difficult problem. We will use the following theorem of Zarhin, which allows us to find infinitely many maximal ideals $\mathfrak{p} \subseteq \mathcal{O}_{K,S}$ at which E has good ordinary reduction and such that the endomorphism ring of the reduction of E at each such $\mathfrak{p}$ satisfies some prescribed local conditions.

Theorem 2.2 (Zarhin). *Let L be an imaginary quadratic field and let $\mathcal{O} \subseteq L$ be an order. Let K be a number field with ring of S-integers $\mathcal{O}_{K,S}$ for some fixed set of maximal ideals S and consider an elliptic curve $E_{/K}$ without complex multiplication. Fix a non-empty finite set $\mathcal{P}$ of rational primes and set $\mathcal{O}_\ell := \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ for all $\ell \in \mathcal{P}$. Define $\mathcal{A}$ to be the set of maximal ideals $\mathfrak{p} \subseteq \mathcal{O}_{K,S}$ such that*

(1) *the characteristic of the residue field $k_\mathfrak{p}$ at $\mathfrak{p}$ does not belong to $\mathcal{P}$,*

(2) *the curve E has good ordinary reduction $E_\mathfrak{p}$ at $\mathfrak{p}$, and*

(3) $\mathrm{End}_{k_\mathfrak{p}}(E_\mathfrak{p}) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \simeq \mathcal{O}_\ell$ *for all $\ell \in \mathcal{P}$.*

Then $\mathcal{A}$ has positive density in the set of prime ideals of $\mathcal{O}_{K,S}$.

Proof. If $S = \emptyset$, this is a special case of [67, Theorem 1.3], see [67, Example 1.5]; in [67, Theorem 1.3], the condition that E has ordinary reduction is absent, but this condition can be added since E does not have complex multiplication and therefore the set of ordinary primes for E has density 1 as remarked above. The theorem with $S \neq \emptyset$ follows easily from this case. ■

If E has complex multiplication, then the behaviour of the geometric endomorphism rings of its reductions modulo various maximal ideals $\mathfrak{p}$ of good reduction with residue characteristics p is well understood thanks to the work of Deuring [19]. It is connected to the value of the Kronecker symbol $(\frac{\cdot}{p})$ at the discriminant of the geometric endomorphism algebra of E, see [36, Chapter 13, Theorem 12]. Proposition 2.4, which we will prove now, tells us how the reduction behaviour of a Galois orbit of singular moduli at a fixed maximal ideal $\mathfrak{P}$ in the ring of integers of $\overline{\mathbb{Q}}$ changes if we replace their discriminant by its product with a power of the residue characteristic of $\mathfrak{P}$. This is certainly well known to the expert, but we have not managed to find an appropriate reference in the literature, so we provide a proof here. We begin by establishing the following auxiliary lemma, which is proved in [40, Proposition 2.3 (1)] in the adelic language; for the reader's convenience, we give an alternative proof here. For the definition and basic properties of the ring class field associated to an imaginary quadratic order, we refer the reader to [17, Chapters 8 and 9].

Lemma 2.3. *For every discriminant $\Delta \in \mathbb{D}$, we denote by $L_\Delta \subseteq \overline{\mathbb{Q}}$ the ring class field associated to the imaginary quadratic order of discriminant Δ. Let $p \in \mathbb{N}$ be* *a prime and let $D \in \mathbb{D}$. Then the extension $L_D \subseteq L_{Dp^2}$ is totally ramified at every prime of L_D lying above p.*

Proof. It suffices to show that, for every $k \in \mathbb{N}$ and every discriminant $D \in \mathbb{D}$ such that the conductor of the order of discriminant D is not divisible by p, the extension $L_D \subseteq L_{Dp^{2k}}$ is totally ramified at every prime of L_D lying above p. We write $D = D_0 f_0^2$, where D_0 is a fundamental discriminant and the conductor f_0 is not divisible by p. We set $f = f_0 p^k$ and $L = \mathbb{Q}(\sqrt{D_0}) \subseteq \bar{\mathbb{Q}}$.

Suppose by contradiction that the extension $L_D \subseteq L_{Dp^{2k}}$ is not totally ramified at some prime of L_D lying above p. Since the extension $L \subseteq L_{Dp^{2k}}$ is abelian and the extension $L \subseteq L_D$ is unramified at every prime of L lying above p, it follows that there exists an extension $L \subseteq L'$ such that $L_D \subsetneq L' \subseteq L_{Dp^{2k}}$ and some prime $\mathfrak{p}$ of L lying above p is unramified in $L \subseteq L'$.

We use $I_L(f)$ to denote the group of fractional $\mathcal{O}_L$-ideals that are coprime to $f\mathcal{O}_L$. If J is an ideal of $\mathcal{O}_L$ that divides $f\mathcal{O}_L$, we set

$$P_{L,J,1}(f) := \langle\{\alpha\mathcal{O}_L \in I_L(f); \alpha \in \mathcal{O}_L,\ \alpha \equiv 1 \bmod J\}\rangle \subseteq I_L(f).$$

If $J = j\mathcal{O}_L$ for some $j \in \mathbb{Z}\backslash\{0\}$, we also write $P_{L,j,1}(f)$ instead of $P_{L,J,1}(f)$ and set

$$P_{L,j,\mathbb{Z}}(f) := \langle\{\alpha\mathcal{O}_L \in I_L(f); \alpha \in \mathcal{O}_L,\ \alpha \equiv a \bmod j\mathcal{O}_L \\ \text{for some } a \in \mathbb{Z} \text{ with } \gcd(a, j) = 1\}\rangle.$$

We set $P_{L,1}(f) := P_{L,f,1}(f)$ and $P_{L,\mathbb{Z}}(f) := P_{L,f,\mathbb{Z}}(f)$. Our definition of $I_L(f)$, $P_{L,1}(f)$, and $P_{L,\mathbb{Z}}(f)$ coincides with the definition in [17, Chapter 8]. Furthermore,

$$P_{L,J,1}(f) = I_L(f) \cap P_{L,1}(J) \quad \text{and} \quad P_{L,j,\mathbb{Z}}(f) = I_L(f) \cap P_{L,\mathbb{Z}}(j),$$

where $P_{L,1}(J) := P_{L,J,1}(J)$ and $P_{L,\mathbb{Z}}(j) := P_{L,j,\mathbb{Z}}(j)$ are defined analogously to $P_{L,1}(f)$ and $P_{L,\mathbb{Z}}(f)$.

The Artin map $I_L(f) \to \mathrm{Gal}(L_{Dp^{2k}}/L)$ has kernel equal to $P_{L,\mathbb{Z}}(f)$ and the Artin map $I_L(f) \to \mathrm{Gal}(L_D/L)$ has kernel equal to

$$I_L(f) \cap P_{L,\mathbb{Z}}(f_0) = P_{L,f_0,\mathbb{Z}}(f).$$

We denote by G the kernel of the Artin map $I_L(f) \to \mathrm{Gal}(L'/L)$. Since $L_D \subsetneq L' \subseteq L_{Dp^{2k}}$, we have that $P_{L,f_0,\mathbb{Z}}(f) \supsetneq G \supseteq P_{L,\mathbb{Z}}(f)$ by [17, Theorem 8.6].

The conductor $\mathfrak{f}$ (in the sense of [17, Theorem 8.5]) of the extension $L \subseteq L'$ divides $f\mathcal{O}_L$ and is coprime to $\mathfrak{p}$. We know that $G \supseteq I_L(f) \cap P_{L,1}(\mathfrak{f}) = P_{L,\mathfrak{f},1}(f)$.

We distinguish two cases: first, suppose that $\mathfrak{p}$ is the only prime of L lying above p. Then $\mathfrak{f}$ divides $f_0\mathcal{O}_L$ and it follows that

$$G \supseteq P_{L,\mathbb{Z}}(f) P_{L,f_0,1}(f) = P_{L,f_0,\mathbb{Z}}(f),$$

a contradiction.

Second, suppose that $p\mathcal{O}_L = \mathfrak{p}\overline{\mathfrak{p}}$ for some prime $\overline{\mathfrak{p}} \neq \mathfrak{p}$ of L. Then $\mathfrak{f}$ divides $f_0\overline{\mathfrak{p}}^k$ and it follows that

$$G \supseteq P_{L,\mathbb{Z}}(f)P_{L,f_0\overline{\mathfrak{p}}^k,1}(f).$$

But again, the right-hand side is equal to $P_{L,f_0,\mathbb{Z}}(f)$: suppose that $\alpha\mathcal{O}_L \in I_L(f)$ and $\alpha \in \mathcal{O}_L\backslash\{0\}$ satisfies $\alpha \equiv a \bmod f_0\mathcal{O}_L$ for some $a \in \mathbb{Z}$ with $\gcd(a, f_0) = 1$. Under the natural isomorphisms

$$(\mathcal{O}_L/f_0p^k\mathcal{O}_L)^* \simeq (\mathcal{O}_L/f_0\mathcal{O}_L)^* \times (\mathcal{O}_L/\mathfrak{p}^k)^* \times (\mathcal{O}_L/\overline{\mathfrak{p}}^k)^*$$

and

$$(\mathcal{O}_L/\mathfrak{p}^k)^* \simeq (\mathcal{O}_L/\overline{\mathfrak{p}}^k)^* \simeq (\mathbb{Z}/p^k\mathbb{Z})^*,$$

the element $\alpha \bmod f_0p^k\mathcal{O}_L$ corresponds to a triple (a_0, a_1, a_2) with $a_0 = a + f_0\mathcal{O}_L$ and $a_1, a_2 \in (\mathbb{Z}/p^k\mathbb{Z})^*$. The decomposition

$$(a_0, a_1, a_2) = (a_0, a_2, a_2) \cdot (1, a_1/a_2, 1)$$

then shows that $\alpha\mathcal{O}_L \in P_{L,\mathbb{Z}}(f)P_{L,f_0\overline{\mathfrak{p}}^k,1}(f)$. It follows that $G = P_{L,f_0,\mathbb{Z}}(f)$, which is another contradiction.

Therefore, there is no such L' and we are done. ■

Proposition 2.4. *For every discriminant $D \in \mathbb{D}$, every prime $p \in \mathbb{N}$, and every $n \in \mathbb{N}$, we have*

$$H_{Dp^{2n}}(X) \equiv H_D(X)^k \bmod p,$$

where, if $\mathcal{O}$ denotes the order of discriminant D, we have

$$k = \frac{h(Dp^{2n})}{h(D)} = \frac{2p^{n-1}}{|\mathcal{O}^*|}\left(p - \left(\frac{D}{p}\right)\right).$$

Proof. By [17, Corollary 7.28], we have that

$$\frac{h(Dp^{2n})}{h(D)} = \frac{2p^{n-1}}{|\mathcal{O}^*|}\left(p - \left(\frac{D}{p}\right)\right)$$

for all n, D, and p.

By induction, it now suffices to prove the statement only for $n = 1$ and all D and p since then, for arbitrary $n \geq 1$, we have that

$$H_{Dp^{2n}}(X) \equiv H_{Dp^{2(n-1)}}(X)^{h(Dp^{2n})/h(Dp^{2(n-1)})} \bmod p,$$

which yields the inductive step.

We fix $j \in \overline{\mathbb{Q}}$ such that $H_D(j) = 0$. Let $E_{/\overline{\mathbb{Q}}}$ be an elliptic curve with $j(E) = j$. Since H_D is irreducible over $\mathbb{Q}$, we can fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and an embedding $\mathcal{O} \hookrightarrow \mathbb{C}$ such that $E_{\mathbb{C}}$ is complex-analytically isomorphic to $\mathbb{C}/\mathcal{O}$. Consider a complex elliptic curve E' whose analytification is isomorphic to $\mathbb{C}/(\mathbb{Z} + p\mathcal{O})$. The inclusion $\mathbb{Z} + p\mathcal{O} \subseteq \mathcal{O}$ induces an isogeny of degree p from E' onto $E_{\mathbb{C}}$ and E' has complex multiplication by $\mathbb{Z} + p\mathcal{O}$, which has discriminant Dp^2. It follows that $j(E')$ is an algebraic number and so both E' as well as the isogeny can be defined over $\overline{\mathbb{Q}}$. We will denote the corresponding elliptic curve over $\overline{\mathbb{Q}}$ by E' as well. Letting $j' := j(E') \in \overline{\mathbb{Q}}$, one then has

$$\Phi_p(j', j) = 0 \tag{2.1}$$

by [17, Proposition 14.11], where we recall that Φ_p denotes the p-th modular polynomial.

Let $L_D, L_{Dp^2} \subseteq \overline{\mathbb{Q}}$ be the ring class fields associated to the orders of discriminant D and Dp^2 respectively. By [17, Theorem 11.1 and Proposition 13.2], j and j' are primitive elements for the extensions $\mathbb{Q}(\sqrt{D}) \subseteq L_D$ and $\mathbb{Q}(\sqrt{D}) \subseteq L_{Dp^2}$ of degrees $h(D)$ and $h(Dp^2)$ respectively. Then, the extension $\mathbb{Q} \subseteq L_{Dp^2}$ is Galois, and so the extension $L_D \subseteq L_{Dp^2}$ is Galois as well, of degree $[L_{Dp^2} : L_D] = h(Dp^2)/h(D) =: k$.

We set

$$G := \operatorname{Gal}\bigl(L_{Dp^2}/\mathbb{Q}(\sqrt{D})\bigr) \quad \text{and} \quad G_0 := \operatorname{Gal}\bigl(L_{Dp^2}/L_D\bigr) \subseteq G.$$

We fix representatives $\sigma_1, \dots, \sigma_{h(D)}$ of the right cosets of G_0 in G.

In the following, we fix a prime $\mathfrak{P} \subseteq L_{Dp^2}$ lying above p. By Lemma 2.3, we have that

$$H_{Dp^2}(X) = \prod_{i=1}^{h(D)} \prod_{\sigma \in G_0} \bigl(X - \sigma(\sigma_i(j'))\bigr) \equiv \prod_{i=1}^{h(D)} \bigl(X - \sigma_i(j')\bigr)^k \bmod \mathfrak{P}.$$

Let $\tau \in \operatorname{Gal}(L_{Dp^2}/\mathbb{Q})$ be an element of the decomposition group of $\mathfrak{P}$ that reduces to the Frobenius automorphism $x \mapsto x^p$ in the Galois group of the residue field extension and let N denote the order of this Frobenius automorphism. Since $\tau(\mathfrak{P}) = \mathfrak{P}$, applying τ^t for $t \in \{1, \dots, N\}$ to the above congruence yields N congruences modulo $\mathfrak{P}$. Taking the product of these congruences and using the fact that $H_{Dp^2}(X) \in \mathbb{Z}[X]$, we obtain that

$$H_{Dp^2}(X)^N \equiv \prod_{t=1}^{N} \prod_{i=1}^{h(D)} \bigl(X - \tau^t(\sigma_i(j'))\bigr)^k \bmod \mathfrak{P}.$$

Using (2.1) and Kronecker's congruence relation [17, Theorem 11.18 (v)], we obtain that

$$0 = \Phi_p\bigl(\sigma_i(j'), \sigma_i(j)\bigr) \equiv \bigl(\sigma_i(j') - \sigma_i(j)^p\bigr)\bigl(\sigma_i(j')^p - \sigma_i(j)\bigr) \bmod \mathfrak{P}$$

for all i. Hence, we have that, for each i, either $\sigma_i(j') \equiv \tau(\sigma_i(j)) \bmod \mathfrak{P}$ or $\sigma_i(j) \equiv \tau(\sigma_i(j')) \bmod \mathfrak{P}$, and so

$$\prod_{t=1}^{N}\bigl(X-\tau^t(\sigma_i(j'))\bigr) \equiv \prod_{t=1}^{N}\bigl(X-\tau^t(\sigma_i(j))\bigr) \bmod \mathfrak{P}$$

since $\tau(\mathfrak{P}) = \mathfrak{P}$ and τ^N is the identity modulo $\mathfrak{P}$. Taking the product over $i = 1, \dots, h(D)$, we deduce that

$$H_{Dp^2}(X)^N \equiv \prod_{t=1}^{N}\prod_{i=1}^{h(D)}\bigl(X-\tau^t(\sigma_i(j))\bigr)^k \equiv H_D(X)^{kN} \bmod \mathfrak{P}.$$

Since $H_{Dp^2}(X)$ and $H_D(X)^k$ are both monic, this concludes the proof. ■

2.3. Degrees in function fields

Let F be an algebraically closed field of arbitrary characteristic and let R be the coordinate ring of a smooth affine irreducible curve $\mathscr{C}$ over F. By [27, Example 15.2 (2)], R is a Dedekind domain. It is an example of the kind of Dedekind domains with which we will work in this article. Therefore, the following technical machinery will be useful for us later.

Let K denote the fraction field of R, i.e., the field of rational functions on $\mathscr{C}$. Any $f \in K$ has a degree $\deg f \in \mathbb{N} \cup \{0\}$, defined by

$$\deg f = \begin{cases} [K : F(f)] & \text{if the field extension } F(f) \subseteq K \text{ is finite,} \\ 0 & \text{otherwise.} \end{cases}$$

If $\deg f = 0$, the element f must be algebraic over F since K is a finitely generated field extension of F of transcendence degree 1 and the transcendence degree is additive in towers of field extensions. This implies that f belongs to F since F is algebraically closed.

If $F(f) \subseteq K$ is finite, we can apply [27, Proposition 15.31] with $C_2 = \mathbb{P}^1_F$, $D \in \{[0], [\infty]\}$, C_1 equal to a smooth projective irreducible curve with an open immersion $\mathscr{C} \hookrightarrow C_1$ (cf. [27, Corollary 6.32, Remark 15.15 (3), Theorem 15.21]), and f equal to the finite morphism $C_1 \to C_2$ induced by f (that we also denote by f). It follows that

$$\deg f = -\sum_{x \in C_1(F)} \min\{0, \operatorname{ord}_x(f)\} = \sum_{x \in C_1(F)} \max\{0, \operatorname{ord}_x(f)\}, \qquad (2.2)$$

where $\operatorname{ord}_x(f)$ denotes the order of vanishing of f at x. Note that (2.2) also holds if $f \in F^*$.

Remark 2.5. In particular, we deduce that, for every $f \in K^*$, the degree $\deg f$ coincides with the height $H(f)$ as defined in [42, equation (2), p. 8 and after equation (1), p. 96]; we will use this later when applying Mason's function field version of the *abc* conjecture in positive characteristic.

For future reference, we summarize some basic properties of the degree in the following proposition.

Proposition 2.6. *The degree map has the following properties:*

(1) $\deg(fg) \leq \deg f + \deg g$ *for all* $f, g \in K$*,*

(2) $\deg(f^n) = |n| \deg f$ *for all* $f \in K^*$ *and all* $n \in \mathbb{Z}$*, and*

(3) $\deg f = 0$ *if and only if* $f \in F$*.*

Proof. Property (1) as well as property (2) are clear from (2.2). Property (3) has already been established above. ∎

Since R is a Dedekind domain, we may also define the degree $\deg I$ of a non-zero ideal I of R by stipulating that

(1) $\deg R = 0$,

(2) $\deg I = 1$ if I is a maximal ideal, and

(3) $\deg(IJ) = \deg I + \deg J$ for all non-zero ideals I and J.

Note that $\deg f$ and $\deg(fR)$ are not equal in general, e.g., if $f \in R^* \backslash F^*$.

3. G.C.D.'s and Hilbert class polynomials

We now study the "size" of greatest common divisors of the form $\gcd(H_D(a), H_D(b))$ for varying $D \in \mathbb{D}$ and fixed a, b belonging to several Dedekind domains of interest. As explained in the introduction, this problem is a modular analogue of the more classical question concerning the size of $\gcd(a^n - 1, b^n - 1)$ for $n \in \mathbb{N}$. In this setting, one usually assumes a and b to be multiplicatively independent since otherwise the greatest common divisors involved become trivially large. Equivalently, one assumes that over the fraction field of the Dedekind domain under consideration, the point (a, b) is not contained in any proper special subvariety of $\mathbb{G}_m^2$. Using the dictionary between the multiplicative and the modular world, one sees that this condition translates into taking a and b as the j-invariants of elliptic curves without complex multiplication that are not geometrically isogenous to each other.

We begin with the function field case in characteristic 0, i.e., with the case where a and b are assumed to be elements of the coordinate ring R of a smooth irreducible affine curve defined over an algebraically closed field F of characteristic 0.

Theorem 3.1. *Let F be an algebraically closed field of characteristic* 0*, let R be the coordinate ring of a smooth affine irreducible curve $\mathcal{C}_{/F}$, and let $A, B \in R$. If $\Phi_N(A, B) \neq 0$ for all $N \in \mathbb{N}$, then there exists a non-zero ideal $J \subseteq R$ such that*

$$\gcd(H_{D_1}(A), H_{D_2}(B)) \mid J \quad \textit{or} \quad H_{D_1}(A)H_{D_2}(B) = 0$$

for all $D_1, D_2 \in \mathbb{D}$.

Note that the second alternative in Theorem 3.1 can only occur if either A or B is constant and equal to a singular modulus. Theorem 3.1 is the analogue of the first part of [1, Theorem 1] by Ailon and Rudnick (with $F = \mathbb{C}$ and $R = \mathbb{C}[X]$) that one obtains by substituting $H_{D_1}(T)$, $H_{D_2}(T)$ for $T^k - 1$ and “not j-invariants of geometrically isogenous elliptic curves” for “multiplicatively independent”. Our proof goes along the lines of the proof in [1], but we apply André’s theorem for $Y(1)^2$ instead of Ihara–Serre–Tate’s theorem for $\mathbb{G}_m^2$.

Proof. Suppose first that $A \in F$. Then, for all $D \in \mathbb{D}$, either $H_D(A) = 0$ or $H_D(A) \in R^*$ and so the theorem holds with $J = R$. The same argument works if $B \in F$.

From now on, we assume that $A \notin F$ and $B \notin F$. Set

$$J_{D_1,D_2} = \gcd(H_{D_1}(A), H_{D_2}(B))$$

for $D_1, D_2 \in \mathbb{D}$ and suppose that some maximal ideal $\mathfrak{m}$ of R divides J_{D_1,D_2}. We want to show that $\mathfrak{m}$ has to belong to a finite set that is independent of D_1, D_2.

The tuple (A, B) defines a morphism $\varphi\colon \mathcal{C} \to Y(1)_F^2 \simeq \mathbb{A}_F^2$. Let $\mathcal{C}'$ denote the Zariski closure of the image of φ. Since A is non-constant by assumption, $\mathcal{C}'$ is a curve and φ has finite fibers by [27, Theorems 5.22 (3) and 10.19 and Proposition 15.16 (1)]. Now, the maximal ideal $\mathfrak{m}$ corresponds to a point $Q_{\mathfrak{m}} \in \mathcal{C}(F)$. Since $\mathfrak{m}$ divides J_{D_1,D_2}, we deduce that $P_{\mathfrak{m}} := \varphi(Q_{\mathfrak{m}}) \in \mathcal{C}'(F)$ is a special point. It follows from our assumptions that the number of special points lying on $\mathcal{C}'$ is finite: if $F = \mathbb{C}$, this is a direct consequence of André’s theorem [2]; otherwise, we may reduce to the case where $F = \mathbb{C}$ by embedding into $\mathbb{C}$ some field of finite transcendence degree over $\overline{\mathbb{Q}}$ over which $\mathcal{C}'$ is defined. So $P_{\mathfrak{m}}$ indeed belongs to a finite set that is independent of D_1, D_2. Since φ has finite fibers, the same holds for $Q_{\mathfrak{m}}$. Because the correspondence between $\mathfrak{m}$ and $Q_{\mathfrak{m}}$ is a bijection, the ideal $\mathfrak{m}$ lies in a finite set that does not depend on D_1, D_2.

It remains to show that the order with which a given maximal ideal $\mathfrak{m}$ divides J_{D_1,D_2} is bounded independently of D_1, D_2. Set $e(\mathfrak{m})$ equal to the supremum of the orders with which $\mathfrak{m}$ divides $A - \sigma \neq 0$, where σ runs over the set of all singular moduli. We have $e(\mathfrak{m}) < \infty$ since at most one $A - \sigma$ can be divisible by $\mathfrak{m}$. But $H_{D_1}(A)$ factors as a product of pairwise coprime elements $A - \sigma$, where σ runs over the singular moduli of discriminant D_1. So the order to which $\mathfrak{m}$ divides J_{D_1,D_2} is bounded by the order to which it divides $H_{D_1}(A)$, which is in turn bounded by $e(\mathfrak{m})$. The theorem now follows. ■

Remark 3.2. If we do not assume that $\Phi_N(A, B) \neq 0$ for all $N \in \mathbb{N}$, the theorem becomes false. More precisely, if $\Phi_N(A, B) = 0$ for some positive integer N, then for every $D \in \mathbb{D}$ and for every maximal ideal $\mathfrak{m}$ dividing $H_D(A)$, there exists $D' \in \mathbb{D}$ such that $\mathfrak{m} \mid H_{D'}(B)$. Indeed, with the notation from the proof of Theorem 3.1, if $Q_{\mathfrak{m}}$ is the point of $\mathcal{C}(F)$ corresponding to $\mathfrak{m}$, then $A(Q_{\mathfrak{m}})$ is a singular modulus of discriminant D. Since by specialization $\Phi_N(A(Q_{\mathfrak{m}}), B(Q_{\mathfrak{m}})) = 0$, we deduce that any two elliptic curves over F with j-invariants $A(Q_{\mathfrak{m}})$ and $B(Q_{\mathfrak{m}})$ are isogenous. It follows that also $B(Q_{\mathfrak{m}})$ is a singular modulus of some discriminant $D' \in \mathbb{D}$. This precisely means that $\mathfrak{m} \mid H_{D'}(B)$. Note finally that, if $A \notin F$, the set of maximal ideals dividing some $H_D(A)$ is infinite. Indeed, the image of the morphism $\varphi_A : \mathcal{C} \to \mathbb{A}^1_F$ defined by $A \in R \setminus F$ is then open and dense, hence cofinite in $\mathbb{A}^1_F$ by [27, Proposition 15.4 (1)]. In particular, all but finitely many singular moduli are in the image of φ_A and the result easily follows.

Corollary 3.3. *Let F be an algebraically closed field of characteristic 0, let R be the coordinate ring of a smooth affine irreducible curve $\mathcal{C}_{/F}$, and let $A, B \in R \setminus F$. If $\Phi_N(A, B) \neq 0$ for all $N \in \mathbb{N}$, then for all but finitely many $(D_1, D_2) \in \mathbb{D}^2$ the elements $H_{D_1}(A)$ and $H_{D_2}(B)$ are coprime.*

Proof. Suppose by contradiction that $\gcd(H_{D_1}(A), H_{D_2}(B)) \neq R$ for infinitely many pairs of discriminants $(D_1, D_2) \in \mathbb{D}^2$. Then by Theorem 3.1, there exists some maximal ideal $\mathfrak{m}$ of R dividing $\gcd(H_{D_1}(A), H_{D_2}(B))$ for infinitely many $(D_1, D_2) \in \mathbb{D}^2$.

Let $Q_{\mathfrak{m}} \in \mathcal{C}(F)$ denote the point corresponding to $\mathfrak{m}$. If $\varphi : \mathcal{C} \to Y(1)^2_F$ denotes the morphism induced by (A, B), then the coordinates of $\varphi(Q_{\mathfrak{m}}) \in Y(1)^2(F) \simeq F^2$ are singular moduli of discriminants D_1 and D_2 respectively for infinitely many $(D_1, D_2) \in \mathbb{D}^2$. This is a contradiction and the corollary follows. ■

In the case $F = \mathbb{C}$, $\mathcal{C} = \mathbb{A}^1_F$, and $R = F[X]$, it is easy to find polynomials $A, B \in R$ for which $H_{D_1}(A)$ and $H_{D_2}(B)$ are coprime for every choice of $(D_1, D_2) \in \mathbb{D}^2$. Indeed, it suffices to choose A and B in such a way that the specializations $A(\tau)$ and $B(\tau)$ at complex numbers $\tau \in \mathbb{C}$ are never both singular moduli. As an example, one could take $A = X$ and $B = X + a$, for $a \in \mathbb{C}$ not an algebraic integer. One can even find $A, B \in \mathbb{Z}[X]$ with this property: for instance, the polynomials $A = X$ and $B = X + 1$ satisfy $\gcd(H_{D_1}(A), H_{D_2}(B)) = 1$ for all $(D_1, D_2) \in \mathbb{D}^2$. This follows from the fact that differences of singular moduli are never units in the ring of algebraic integers, see [41, Corollary 1.3].

We now turn to the function field case in positive characteristic. If F is an algebraic closure of a finite field, then the statement of Theorem 3.1 is false as the following theorem shows.

Theorem 3.4. *Let $p \in \mathbb{N}$ be prime and fix an algebraic closure $F = \overline{\mathbb{F}}_p$ of $\mathbb{F}_p$. Let R be the coordinate ring of a smooth affine irreducible curve $\mathcal{C}_{/F}$ and let $A, B \in R \backslash F$. Then*

$$\limsup_{D \in \mathbb{D}, |D| \to \infty} \frac{\deg(\gcd(H_D(A), H_D(B)))}{\deg H_D} > 0.$$

Theorem 3.4 for $R = F[X]$ can be considered a slightly weaker modular analogue of [62, Theorem 4]. See also [16] for an upper bound for the g.c.d. in the multiplicative setting in the function field case in positive characteristic. The hypothesis in Theorem 3.4 that $F = \overline{\mathbb{F}}_p$ rather than an arbitrary field of characteristic p is essential as the following example shows.

Example 3.5. Suppose that F is an algebraic closure of $\mathbb{F}_p(S)$, where S is an independent variable, $\mathcal{C} = \mathbb{A}^1_F$, and $R = F[X]$. Then, $H_{D_1}(X - S)$ and $H_{D_2}(X - S^2)$ are coprime for all $D_1, D_2 \in \mathbb{D}$ since they have no common zeroes in F (for all $D \in \mathbb{D}$, every zero of $H_D(X)$ in F is algebraic over $\mathbb{F}_p$, but S is transcendental over $\mathbb{F}_p$).

In order to prove Theorem 3.4, we will make use of the following preliminary result.

Proposition 3.6. *Let $p \in \mathbb{N}$ be prime and let F, $\mathcal{C}$, R, A, and B be as in Theorem 3.4. Let $\Lambda \subseteq \mathbb{F}_p[T]$ be any set of polynomials such that*

$$\{t \in F; P(t) = 0 \textit{ for some } P \in \Lambda\} = F.$$

Then there exist infinitely many $\alpha \in \mathcal{C}(F)$ for which there is a polynomial $P \in \Lambda$ satisfying $P(A(\alpha)) = P(B(\alpha)) = 0$.

Proof. The idea is to find infinitely many $\alpha \in \mathcal{C}(F)$ such that $B(\alpha)$ is the image of $A(\alpha)$ under some k-th power of the Frobenius automorphism of F, where $k = k(\alpha) \in \mathbb{N} \cup \{0\}$ is allowed to depend on α. Since by assumption there exists $P \in \Lambda$ such that $P(B(\alpha)) = 0$ and the polynomial P has $\mathbb{F}_p$-coefficients, one then has

$$0 = P\big(B(\alpha)\big) = P\big(A(\alpha)^{p^k}\big) = P\big(A(\alpha)\big)^{p^k}$$

for all these α and the result follows.

In order to find infinitely many such points α, we will use the function field version of the abc conjecture in characteristic p, which has been proven by Mason [42, Lemma 10, p. 97]. To this aim, we let $m \in \mathbb{N} \cup \{0\}$ denote the biggest non-negative integer such that there exists $A_0 \in R$ with $A = A_0^{p^m}$. Note that m is well defined thanks to Proposition 2.6 (2)–(3) and the fact that A is non-constant by assumption.

For every $n \in \mathbb{N}$, set $P_n := A_0 - B^{p^n} \in R$. We have $P_n \neq 0$ thanks to the maximality of m, and obviously

$$A_0 - B^{p^n} - P_n = 0.$$

We want to apply [42, Lemma 10, p. 97] to the above equality. First of all, note that $A_0/(-B^{p^n})$ is not a p-th power in the fraction field of R since A_0 is not a p-th power in R and R is integrally closed by [27, Corollary 6.32, Lemma 6.38 (1), Corollary 6.39, Proposition B.70 (1)]. Moreover, by Proposition 2.6 we also have

$$\deg \frac{A_0}{-B^{p^n}} \geq p^n \deg(B) - \deg(A_0) \tag{3.1}$$

and the right-hand side goes to infinity as n increases since $B \notin F$ by hypothesis. Let now $\overline{\mathcal{C}}$ be the smooth projective closure of the curve $\mathcal{C}$ (see [27, Corollary 6.32, Remark 15.15 (3), and Theorem 15.21]) and let $S \subseteq \overline{\mathcal{C}}(F)$ be an arbitrary finite set of points containing $\overline{\mathcal{C}}(F)\backslash\mathcal{C}(F)$ as well as all the zeroes of A_0 and B. Inequality (3.1) shows that if we choose n large enough, then the degree of $A_0/(-B^{p^n})$ will be strictly bigger than $|S| + 2g - 2$, where $g = g(\overline{\mathcal{C}})$ is the genus of $\overline{\mathcal{C}}$. Hence, by [42, Lemma 10, p. 97] and Remark 2.5, there exists $\alpha \in \mathcal{C}(F)\backslash S$ such that the orders of vanishing at α of the functions A_0, B^{p^n}, and P_n are not all equal; note that the set $\overline{\mathcal{C}}(F)$ is in bijection with the set of valuations on the fraction field of R constructed in [42, Chapter VI]. Since our choice of S implies that A_0 and B both do not vanish at α, we deduce that $P_n(\alpha) = 0$. This means precisely that $A(\alpha) = B(\alpha)^{p^{m+n}}$. Now, by repeatedly enlarging the set S, one can find infinitely many points $\alpha \in \mathcal{C}(F)$ with this property. We have reached the desired conclusion. ∎

We remark that, by Deuring's lifting theorem [36, Chapter 13, Theorem 14] (or [13, Theorem 1.7.4.6]) and the fact that every elliptic curve over $\overline{\mathbb{F}}_p$ has endomorphism ring larger than $\mathbb{Z}$, the set $\Lambda = \{H_D(T) \bmod p; D \in \mathbb{D}\}$ satisfies the hypothesis of Proposition 3.6.

Proof of Theorem 3.4. Our goal is to find a sequence $\{D_k\}_{k\in\mathbb{N}}$ of discriminants $D_k \in \mathbb{D}$ such that $|D_k| \to \infty$ as $k \to \infty$ and

$$\liminf_{k\to\infty} \frac{\deg(\gcd(H_{D_k}(A), H_{D_k}(B)))}{\deg H_{D_k}} > 0. \tag{3.2}$$

Proposition 3.6 applied to $\Lambda = \{H_D(T) \bmod p; D \in \mathbb{D}\}$ implies that there exists some discriminant $D_0 \in \mathbb{D}$ and some $\alpha \in \mathcal{C}(F)$ such that

$$H_{D_0}(A(\alpha)) = H_{D_0}(B(\alpha)) = 0.$$

It follows from the definition of the degree of an ideal that

$$\deg\big(\gcd(H_{D_0}(A), H_{D_0}(B))\big) \geq 1.$$

For $k \in \mathbb{N}$, set $D_k = D_0 p^{2k}$. It is clear that $|D_k| \to \infty$ as $k \to \infty$. We can now apply Proposition 2.4 to deduce that

$$\begin{aligned}\deg\bigl(\gcd(H_{D_k}(A), H_{D_k}(B))\bigr) &\geq \frac{\deg H_{D_k}}{\deg H_{D_0}} \deg\bigl(\gcd(H_{D_0}(A), H_{D_0}(B))\bigr)\\ &\geq \frac{\deg H_{D_k}}{\deg H_{D_0}} > 0.\end{aligned}$$

So (3.2) holds and the theorem follows. ■

We finally leave the cozy realm of function fields to enter the more hostile world of number fields. Influenced by the previous discussion, one may be tempted to believe that the modular analogues of the multiplicative results of Bugeaud–Corvaja–Zannier [9] and Corvaja–Zannier [15] should also hold true in this setting. For instance, the aforementioned results inspire the following natural conjecture in the modular framework: for all "well-chosen" $a, b \in \mathbb{Z}$ and for every $\varepsilon > 0$, we have

$$\log\bigl(\gcd(H_D(a), H_D(b))\bigr) < \varepsilon \deg H_D$$

provided that $D \in \mathbb{D}$ is sufficiently large in absolute value. Here "well-chosen" means that neither a nor b is a singular modulus and that furthermore a and b are not j-invariants of geometrically isogenous elliptic curves over $\mathbb{Q}$, conditions that, as we have already remarked above, correspond to multiplicative independence in the multiplicative setting. Perhaps surprisingly, this just stated conjecture turns out to be completely false in general. The reason for this is the possible existence of common supersingular primes for the elliptic curves having a and b as their j-invariants.

Theorem 3.7. *Let K be a number field and let S be a finite set of maximal ideals of $\mathcal{O}_K$. Consider two elliptic curves $E_{1/K}$, $E_{2/K}$ with potential good reduction outside of S, i.e., such that $j(E_i) \in \mathcal{O}_{K,S}$ for $i = 1, 2$. Recall that, for a non-zero ideal I of $\mathcal{O}_{K,S}$, its norm is denoted by $N(I)$. Suppose that there exists a prime ideal $\mathfrak{p}$ of $\mathcal{O}_{K,S}$ at which both E_1 and E_2 have potential good supersingular reduction. Let p denote the rational prime lying under $\mathfrak{p}$. Then*

$$\limsup_{D \in \mathbb{D},\, |D| \to \infty} (\deg H_D)^{-1} \log N\Bigl(\gcd\bigl(H_D(j(E_1)), H_D(j(E_2))\bigr)\Bigr) \geq \frac{\log p}{p-1} > 0.$$

Here, the logarithm of the ideal norm plays the role of the degree of an ideal in the function field case. Both of them count with multiplicity the number of maximal ideals dividing a given non-zero element; deg weights each maximal ideal by 1 while $\log N$ weights each maximal ideal by the logarithm of the cardinality of its residue field.

In order to prove Theorem 3.7, we will crucially rely on an equidistribution result due to Michel [51] concerning supersingular reduction of CM elliptic curves. Theorem 3.8 below, which we will apply to prove Theorem 3.7, is a direct consequence of this result. Let us introduce the setting.

Let $p \in \mathbb{N}$ be a rational prime and fix a prime $\mathfrak{p} \subseteq \overline{\mathbb{Q}}$ lying above it. Let $\overline{\mathbb{F}}_p$ denote the residue field of $\mathfrak{p}$, which is an algebraic closure of $\mathbb{F}_p$. Let L be an imaginary quadratic field and assume that p is inert in L. We denote by $\mathrm{Ell}(\mathcal{O}_L)$ the set of $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves with complex multiplication by $\mathcal{O}_L$ and by $\mathrm{Ell}_{\mathrm{ss}}(\overline{\mathbb{F}}_p)$ the set of isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$. Both sets are finite: indeed, the cardinality of $\mathrm{Ell}(\mathcal{O}_L)$ equals the class number of L while $\mathrm{Ell}_{\mathrm{ss}}(\overline{\mathbb{F}}_p)$ is finite by [65, V, Theorem 3.1]. Moreover, every class in $\mathrm{Ell}(\mathcal{O}_L)$ can be represented by the base change $E_{\overline{\mathbb{Q}}}$ of E to $\overline{\mathbb{Q}}$, where E is an elliptic curve over a number field $L_0 \subseteq \overline{\mathbb{Q}}$ that has good reduction at $\mathfrak{p} \cap L_0$. We define $E_{\overline{\mathbb{Q}}} \bmod \mathfrak{p}$ as the base change to $\overline{\mathbb{F}}_p$ of $E \bmod (\mathfrak{p} \cap L_0)$. We then have a map

$$\Psi_{\mathfrak{p},\mathcal{O}_L} : \mathrm{Ell}(\mathcal{O}_L) \to \mathrm{Ell}_{\mathrm{ss}}(\overline{\mathbb{F}}_p), \quad [E_{\overline{\mathbb{Q}}}] \mapsto [E_{\overline{\mathbb{Q}}} \bmod \mathfrak{p}]$$

that is well defined by [61, II, Proposition 4.4].

Theorem 3.8. *Let D denote the discriminant of L. There exist an absolute constant $\eta > 0$ and a constant $c = c(\mathfrak{p}) \in \mathbb{R}$ such that for each class $[\tilde{E}] \in \mathrm{Ell}_{\mathrm{ss}}(\overline{\mathbb{F}}_p)$, we have*

$$\left|\left\{[E] \in \mathrm{Ell}(\mathcal{O}_L); \Psi_{\mathfrak{p},\mathcal{O}_L}([E]) = [\tilde{E}]\right\}\right| \geq \left((p-1)^{-1} - cD^{-\eta}\right)h(D),$$

where $h(D)$ denotes the class number of L.

Proof. We want to apply [51, Theorem 3] with $G = G_K$. Following [51], we denote the cardinality of $\mathrm{Ell}_{\mathrm{ss}}(\overline{\mathbb{F}}_p)$ by n and its elements by $e_1, \dots, e_n$. We also use the probability measure μ_p on $\mathrm{Ell}_{\mathrm{ss}}(\overline{\mathbb{F}}_p)$ as defined in [51, top of p. 189]. We recall that, for $1 \leq i \leq n$,

$$\mu_p(e_i) := \frac{1/w_i}{\sum_{j=1}^{n} 1/w_j},$$

where w_j is half the cardinality of the automorphism group of any elliptic curve in the class e_j for $j = 1, \dots, n$.

If $p > 5$, it follows from [65, III, Theorem 10.1] and the definition of μ_p that $\mu_p(e_i) \geq (3n)^{-1}$ for all $i = 1, \dots, n$. Furthermore, we have

$$(3n)^{-1} \geq \frac{4}{p+13} \geq (p-1)^{-1}$$

thanks to [32, Chapter 13, Table 1, p. 264] and the fact that $p > 5$.

If $p \in \{2,3,5\}$, then $|\operatorname{Ell}_{\mathrm{ss}}(\overline{\mathbb{F}}_p)| = 1$ thanks to [32, Chapter 13, Theorem 4.1 and the following paragraphs up to and including Table 1], so that $n = 1$ and

$$\mu_p(e_1) = 1 \geq (p-1)^{-1}.$$

Hence, Theorem 3.8 follows from [51, Theorem 3] with $G = G_K$. ■

We can now prove Theorem 3.7.

Proof of Theorem 3.7. Let $\kappa \in (0, 1/(p-1))$ be an arbitrary real number and fix an algebraic closure $\bar{K}$ of K as well as a prime $\mathfrak{P} \subseteq \bar{K}$ lying over $\mathfrak{p}$. By Theorem 3.8, there exist fundamental discriminants $D \in \mathbb{D}$ with $|D|$ arbitrarily large such that p is inert in $\mathbb{Q}(\sqrt{D}) \subseteq \bar{K}$ and

$$\left|\{j \in \bar{K}; H_D(j) = 0, j \equiv j(E_i) \bmod \mathfrak{P}\}\right| \geq (\deg H_D)\kappa \tag{3.3}$$

for $i = 1,2$. For any such D, let $K_D \subseteq \bar{K}$ denote the compositum of K and the Hilbert class field of $\mathbb{Q}(\sqrt{D})$, and set $\mathfrak{P}_D = \mathfrak{P} \cap K_D$. By [61, II, Theorem 4.1], K_D is the splitting field of H_D over $K(\sqrt{D})$. Together with inequality (3.3), this implies that there exist integers $e_{D,i} \geq (\deg H_D)\kappa$ such that

$$H_D\big(j(E_i)\big) = \prod_{j \in K_D,\, H_D(j)=0} \big(j(E_i) - j\big) \in \mathfrak{P}_D^{e_{D,i}}$$

for $i = 1,2$. Since p does not ramify in $\mathbb{Q}(\sqrt{D})$, the extension $K \subseteq K_D$ is unramified over $\mathfrak{p}$ by [61, II, Example 3.3] and [7, Propositions B.2.3 and B.2.4]. We deduce that $H_D(j(E_i)) \in \mathfrak{p}^{e_{D,i}}$ for $i = 1,2$. Together with the lower bound for $e_{D,i}$, this implies that

$$(\deg H_D)^{-1} \log N\big(\gcd\big(H_D(j(E_1)), H_D(j(E_2))\big)\big) \geq \kappa \log N(\mathfrak{p}) \geq \kappa \log p.$$

The theorem follows. ■

Remark 3.9. The careful reader has certainly noticed the similarity between the statements of Theorems 3.4 and 3.7. However, arguing along the lines of the proof of Theorem 3.4 does not suffice to prove Theorem 3.7. First of all, we do not have an analogue of Proposition 3.6 that would allow us to find at least one discriminant whose associated greatest common divisor is non-trivial. Another obstacle is that, by Lemma 2.3, passing from an order of discriminant D to an order of discriminant Dp^2 gives rise to an extension of ring class fields that is totally ramified at each prime above p. Therefore, it is not clear whether the norm of the greatest common divisor increases at all when one passes from discriminant D to discriminant Dp^2.

On the other hand, supersingular primes can be used to prove Theorem 3.4 in some special cases: if there exists some $\alpha \in \mathscr{C}(F)$ such that both $A(\alpha)$ and $B(\alpha)$ are

j-invariants of supersingular elliptic curves, then we can deduce Theorem 3.4 from Theorem 3.8 with a similar proof as the one of Theorem 3.7. In this case, we can even strengthen Theorem 3.4 to say that the limit superior is greater than or equal to $(p-1)^{-1}$. However, since the set of supersingular j-invariants in F is finite, it is clear that, for some choices of $A, B \in R\backslash F$, no such α exists; for instance, take any $A \in R\backslash F$ and $B = A + b$, where $b \in F$ is not a difference of two supersingular j-invariants.

It is easy to construct examples where E_1 and E_2 have no complex multiplication and are not geometrically isogenous to each other, but nevertheless have a common prime of potential good supersingular reduction. Indeed, let us fix any maximal ideal $\mathfrak{p}$ of $\mathcal{O}_{K,S}$; by [17, Theorem 14.18] and since 0 is supersingular in characteristics 2 and 3, we can choose (not necessarily distinct) supersingular j-invariants $j_{1,\mathfrak{p}}, j_{2,\mathfrak{p}} \in \mathcal{O}_{K,S}/\mathfrak{p}$. All but finitely many of the lifts of $j_{1,\mathfrak{p}}$ to $\mathcal{O}_{K,S}$ are not singular moduli since the degree of a singular modulus equals the class number of the corresponding imaginary quadratic order and this goes to ∞ with the absolute value of the discriminant by [37, Chapter XVI, Theorem 4] and [52, Chapter I, Proposition 12.9]. Fix any such lift $j_1 \in \mathcal{O}_{K,S}$. Then, all but finitely many of the lifts of $j_{2,\mathfrak{p}}$ to $\mathcal{O}_{K,S}$ are j-invariants of elliptic curves without complex multiplication as above. Moreover, all but finitely many of these lifts are j-invariants of elliptic curves that are not geometrically isogenous to the elliptic curve with j-invariant j_1 since the existence of such an isogeny implies the existence of an isogeny whose degree is bounded in terms of K and j_1 by the main theorem of [43]. Hence, one can find many examples where the hypothesis of Theorem 3.7 holds although the two elliptic curves have no complex multiplication and are not geometrically isogenous to each other.

We know that there exist infinitely many common supersingular primes for E_1 and E_2 in the following cases:

(1) Both E_1 and E_2 have complex multiplication, see [36, Chapter 13, Theorem 12].

(2) Both E_1 and E_2 do not have complex multiplication, one of them can be defined over a number field with at least one real embedding, and E_1 and E_2 are geometrically isogenous, see [21, 22].

Based on [38, Remark 2, p. 37], Fouvry and Murty conjectured in [24, equation (1.4)] that there are infinitely many common supersingular primes if both E_1 and E_2 do not have complex multiplication, are defined over $\mathbb{Q}$, and are not geometrically isogenous. In the same article, they also prove an averaged version of this conjecture. A similar averaged result is known if both E_1 and E_2 are defined over the rationals, E_1 has complex multiplication, and E_2 does not, see [33, Theorem 10] and [18, pp. 199–200].

We can also consider the following modular version of [1, Conjecture A] by Ailon and Rudnick and [64, Conjecture 10] by Silverman: for which $a, b \in \mathcal{O}_{K,S}$ do there exist infinitely many $D \in \mathbb{D}$ such that $H_D(a)$ and $H_D(b)$ are coprime? Does it suffice to assume that $a \neq b$ or at least that neither a nor b is a singular modulus and $\Phi_N(a,b) \neq 0$ for all $N \in \mathbb{N}$? This problem would be trivial if $H_D(a) \in \mathcal{O}_{K,S}^*$ or $H_D(b) \in \mathcal{O}_{K,S}^*$ for infinitely many $D \in \mathbb{D}$. If a and b are not both singular moduli and $S \neq \emptyset$, then it is an open problem whether this can happen or not. We can at least show that $H_D(a)$ cannot belong to $\mathcal{O}_{K,S}^*$ for all but finitely many $D \in \mathbb{D}$.

Theorem 3.10. *Let K be a number field and let S be a finite set of maximal ideals of $\mathcal{O}_K$. Let $j \in \mathcal{O}_{K,S}$ and let $E_{/K}$ be an elliptic curve with $j(E) = j$. Then*

$$\limsup_{D\in\mathbb{D},\,|D|\to\infty} P_{\mathrm{o}}\big(H_D(j)\big) = \infty,$$

where $P_{\mathrm{o}}(a)$ is defined as follows: $P_{\mathrm{o}}(0) = \infty$ and for $a \in \mathcal{O}_{K,S}\backslash\{0\}$, $P_{\mathrm{o}}(a)$ denotes the largest norm of a prime factor of a which is of good ordinary reduction for E and $P_{\mathrm{o}}(a) = 1$ if no such prime factor exists.

If $P(a)$ denotes the largest norm of a prime factor of $a \in \mathcal{O}_{K,S}\backslash(\mathcal{O}_{K,S}^* \cup \{0\})$ and $P(a) = \infty$ or 1 for $a = 0$ and $a \in \mathcal{O}_{K,S}^*$ respectively, then

$$\lim_{D\in\mathbb{D},\,|D|\to\infty} P\big(H_D(j)\big) = \infty$$

is equivalent to the fact that, for every finite set $\widetilde{S}$ of maximal ideals of $\mathcal{O}_K$, there are at most finitely many $D \in \mathbb{D}$ such that $H_D(j)$ is an $\widetilde{S}$-unit. As mentioned above, it is still an open problem whether this is true or not. It is known if either $\widetilde{S} = \emptyset$ [28] or if j is a singular modulus [29]. See [6, 10–12, 58] for work on making these results effective.

These results actually provide another example besides Theorem 3.7 where the analogy between Shimura varieties and algebraic groups fails to hold perfectly. Namely, there is a discrepancy between Habegger's [28, Theorem 2] in the modular case and [3, Theorem 0.1] by Baker, Ih, and Rumely in the multiplicative case: for instance, in the modular case, for *every* algebraic integer j, the algebraic number $H_D(j)$ is an algebraic unit for at most finitely many $D \in \mathbb{D}$ whereas in the multiplicative case, for a non-zero algebraic integer a, $\Psi_n(a)$ is an algebraic unit for at most finitely many $n \in \mathbb{N}$ if and only if a is not a root of unity. The elliptic case behaves analogously to the multiplicative case, see [3, Theorem 0.2].

We can ask whether removing the supersingular prime factors eliminates all these discrepancies: certainly, if $j \in \mathcal{O}_{K,S}$ is a singular modulus, then $N(H_D(j))$ is divisible only by supersingular primes for j for infinitely many $D \in \mathbb{D}$. Does the converse hold as well?

Proof of Theorem 3.10. Fix an algebraic closure $\bar{K}$ of K. In the proof, we will repeatedly use the fact that there exist infinitely many primes of good ordinary reduction for E, see Section 2.2. The goal of our proof is to construct a strictly decreasing sequence of discriminants D for which $P_{\mathrm{o}}(H_D(j))$ goes to ∞. We do this recursively as follows. Let $\mathfrak{p}_1 \subseteq \mathcal{O}_{K,S}$ be a maximal ideal of good ordinary reduction for E and choose a prime $\mathfrak{P}_1 \subseteq \bar{K}$ lying above it. By Deuring's Lifting theorem [36, Chapter 13, Theorem 14] (or [13, Theorem 1.7.4.6]), the fact that every elliptic curve over a finite field has complex multiplication, and Proposition 2.4, there exist a discriminant $D_{\mathfrak{p}_1} \in \mathbb{Z}_{<0}$ and an elliptic curve $E_{\mathfrak{p}_1/\bar{K}}$ with complex multiplication by the imaginary quadratic order of discriminant $D_{\mathfrak{p}_1}$ such that

$$E_{\mathfrak{p}_1} \bmod \mathfrak{P}_1 \simeq E_{\bar{K}} \bmod \mathfrak{P}_1 \quad \text{and} \quad H_{D_{\mathfrak{p}_1}}(j) \neq 0.$$

Note that this implies in particular that $\mathfrak{p}_1$ divides $H_{D_{\mathfrak{p}_1}}(j)$, so that

$$N(\mathfrak{p}_1) \leq P_{\mathrm{o}}\big(H_{D_{\mathfrak{p}_1}}(j)\big) < \infty.$$

Suppose now that we have constructed a sequence of primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_{n-1}$ such that $N(\mathfrak{p}_1) < \cdots < N(\mathfrak{p}_{n-1})$ and a sequence of discriminants $D_{\mathfrak{p}_1} > \cdots > D_{\mathfrak{p}_{n-1}}$ such that $N(\mathfrak{p}_m) \leq P_{\mathrm{o}}(H_{D_{\mathfrak{p}_m}}(j)) < \infty$ for all $m \in \{1, \ldots, n-1\}$. We take some maximal ideal $\mathfrak{p}_n$ of good ordinary reduction for E such that

$$N(\mathfrak{p}_n) > \max_{m=1,\ldots,n-1} \big\{P_{\mathrm{o}}\big(H_{D_{\mathfrak{p}_m}}(j)\big)\big\}.$$

For the same reasons as above, there exist a prime $\mathfrak{P}_n \subseteq \bar{K}$ lying above $\mathfrak{p}_n$, a discriminant $D_{\mathfrak{p}_n}$, and an elliptic curve $E_{\mathfrak{p}_n/\bar{K}}$ with complex multiplication by the imaginary quadratic order of discriminant $D_{\mathfrak{p}_n}$ satisfying

$$E_{\mathfrak{p}_n} \bmod \mathfrak{P}_n \simeq E \bmod \mathfrak{P}_n, \quad H_{D_{\mathfrak{p}_n}}(j) \neq 0, \quad |D_{\mathfrak{p}_n}| > |D_{\mathfrak{p}_{n-1}}|.$$

This implies that $N(\mathfrak{p}_n) \leq P_{\mathrm{o}}\big(H_{D_{\mathfrak{p}_n}}(j)\big) < \infty$.

Iterating this construction, we find a sequence of discriminants $(D_{\mathfrak{p}_n})_{n\in\mathbb{N}}$ with the desired properties. This concludes the proof. ■

Remark 3.11. For $a \in \mathcal{O}_{K,S} \backslash \{0\}$, let us denote by $P_{\mathrm{ss}}(a)$ the largest norm of a prime factor of a which is of good supersingular reduction for E and set $P_{\mathrm{ss}}(a) = 1$ if there is no such prime factor and $P_{\mathrm{ss}}(0) = \infty$. If there are infinitely many primes of good supersingular reduction for E, which is known in certain cases thanks to [21,22], then we can follow the proof of Theorem 3.10 to show that

$$\limsup_{D\in\mathbb{D},\, |D|\to\infty} P_{\mathrm{ss}}\big(H_D(j)\big) = \infty.$$

4. The support problem

In the previous section, we studied $\gcd(H_D(a), H_D(b))$ for varying $D \in \mathbb{D}$ and fixed a, b in some Dedekind domain. This greatest common divisor is as big as possible if $H_D(a)$ divides $H_D(b)$ (or vice versa). We now want to investigate in which cases this can happen for all but finitely many discriminants D. In fact, we want to understand more generally in which cases the set of prime ideals dividing $H_D(a)$ (its *support*) is contained in the set of prime ideals dividing $H_D(b)$ for all but finitely many D. If we pass from the modular to the multiplicative world and replace the polynomials $H_D(T)$ $(D \in \mathbb{D})$ by the polynomials $T^n - 1$ $(n \in \mathbb{N})$, then this question has been answered by Corrales-Rodrigáñez and Schoof [14].

We are therefore led to introduce a general setting which encompasses both versions of this problem: let R be a Dedekind domain which is not a field and let $\mathcal{N}$ be an arbitrary countably infinite set. We are given a polynomial $f_n(T) \in R[T]$ for each $n \in \mathcal{N}$ and two elements $a, b \in R$. If for all but finitely many $n \in \mathcal{N}$, every prime ideal factor of $f_n(a)$ also divides $f_n(b)$, i.e., if the *support property* holds for all but finitely many $n \in \mathcal{N}$, what can we say about a and b? Following [14], we will refer to this question as the *support problem for the polynomials* $f_n(T) \in R[T]$ $(n \in \mathcal{N})$. Clearly, the answer cannot be of universal nature and it depends very much on R and on the polynomials $f_n(T)$ for $n \in \mathcal{N}$.

In many of the instances of the support problem that we will consider later, there are some trivial subcases that are easily dealt with. We present them in the following examples:

Example 4.1 (Isotriviality). Let F be an algebraically closed field and let R be the coordinate ring of a smooth affine irreducible curve $\mathcal{C}_{/F}$. Recall that R is a Dedekind domain by [27, Example 15.2 (2)]. In this example, we study the case where $f_n(T) \in F[T] \subseteq R[T]$ for all $n \in \mathcal{N}$ and either $a \in F$ or $b \in F$. We will see that the support problem is often trivial in this case.

(1) Set

$$Z := \{\tau \in F;\, f_n(\tau) = 0 \text{ for infinitely many } n \in \mathcal{N} \text{ such that } f_n \neq 0\}.$$

For instance, if the polynomials $f_n(T)$ $(n \in \mathcal{N})$ are pairwise coprime, then $Z = \emptyset$. For every $a \in F \backslash Z$ and for all but finitely many $n \in \mathcal{N}$ such that $f_n \neq 0$, the values $f_n(a)$ are non-zero and hence units in R. In particular, for every $b \in R$, we have that $f_n(a)$ divides $f_n(b)$ for all but finitely many $n \in \mathcal{N}$.

On the other hand, if $a \in Z$ and for all but finitely many $n \in \mathcal{N}$, every prime ideal dividing $f_n(a)$ also divides $f_n(b)$, then we deduce that $f_{n_0}(b) = 0$ for some $n_0 \in \mathcal{N}$ such that $f_{n_0} \neq 0$. It follows that $b \in F$ since F is algebraically closed.

(2) Let now $f_n(T) \in F[T]$ $(n \in \mathcal{N})$ and $b \in F$ be such that

$$Z_b := \bigcup_{n \in \mathcal{N},\, f_n(b) \neq 0} \{\tau \in F;\, f_n(\tau) = 0\}$$

is infinite. For instance, if the polynomials $f_n(T)$ $(n \in \mathcal{N})$ are all non-constant and pairwise coprime, then this holds for every choice of $b \in F$. It in particular implies that the set of polynomials $f_n(T)$ that do not have b as a zero is infinite. Since $f_n(T) \in F[T]$ and $b \in F$, the value $f_n(b)$ is a unit in R as soon as $f_n(b) \neq 0$. If for all but finitely many $n \in \mathcal{N}$, every prime ideal factor of $f_n(a)$ also divides $f_n(b)$, it follows that $f_n(a)$ is a unit for all but finitely many $n \in \mathcal{N}$ such that $f_n(b) \neq 0$, which implies that $a - \tau \in R^*$ for all but finitely many $\tau \in Z_b$. Since Z_b is infinite, the morphism $\mathcal{C} \to \mathbb{A}^1_F$ induced by a must then be constant by [27, Proposition 15.4 (1)] and it follows that $a \in F$.

On the other hand, if Z_b is finite and no element of Z_b belongs to the image of the morphism $\mathcal{C} \to \mathbb{A}^1_F$ induced by a, then, for all $n \in \mathcal{N}$, every prime ideal dividing $f_n(a)$ also divides $f_n(b)$ since either $f_n(b) = 0$ or $f_n(a)$ is equal, up to scaling by a constant in F^*, to a product of factors $a - \tau \in R^*$ for $\tau \in Z_b$.

Example 4.2 (Frobenius). Suppose that $\mathbb{F}_q \subseteq R$ for some prime power q and that $f_n(T) \in \mathbb{F}_q[T] \subseteq R[T]$ for all $n \in \mathcal{N}$. Then, for every $c \in R$ and for all $k, \ell \in \mathbb{Z}$, $k, \ell \geq 0$, we have that every prime ideal that divides $f_n(c^{q^k}) = f_n(c)^{q^k}$ also divides $f_n(c^{q^\ell}) = f_n(c)^{q^\ell}$ for all $n \in \mathcal{N}$. Thus, if $a = c^{q^k}$ and $b = c^{q^\ell}$, then, for all $n \in \mathcal{N}$, every prime ideal dividing $f_n(a)$ also divides $f_n(b)$.

In the case of the *multiplicative support problem*, i.e., if $\mathcal{N} = \mathbb{N}$ and $f_n(T) := T^n - 1$ for $n \in \mathcal{N}$, we have that $f_n(a) \mid f_n(a^k)$ for every $a \in R$, every $k \in \mathbb{N} \cup \{0\}$, and every $n \in \mathcal{N}$. If $a \in R^*$, this also holds for negative exponents k since $f_n(a^{-1}) = -f_n(a)a^{-n}$. Answering a question of Erdős at the 1988 number theory conference in Banff, Corrales-Rodrigáñez and Schoof solved the multiplicative support problem in the number field case by proving that these are the only possibilities if $ab \neq 0$:

Theorem 4.3 (Corrales-Rodrigáñez–Schoof [14, Theorem 1]). *Let K be a number field and let S be a finite set of maximal ideals of $\mathcal{O}_K$. If $a, b \in \mathcal{O}_{K,S} \backslash \{0\}$ satisfy that for all but finitely many $n \in \mathbb{N}$, every prime ideal of $\mathcal{O}_{K,S}$ dividing $a^n - 1$ also divides $b^n - 1$, then $b = a^k$ for some $k \in \mathbb{Z}$.*

The case where the hypothesis holds for all $n \in \mathbb{N}$ is exactly the result of Corrales-Rodrigáñez–Schoof; the general case then directly follows by a short argument that we provide below.

In the proof of Theorem 4.3 as well as in many of the proofs that follow, we will sometimes enlarge S to a bigger set S'. When doing this, we will always identify the primes of $\mathcal{O}_{K,S'}$ as well as the primes of $\mathcal{O}_{K,S}$ with subsets of the primes of $\mathcal{O}_K$

by identifying $\mathfrak{p}$ with $\mathfrak{p} \cap \mathcal{O}_K$. We will also implicitly use that divisibility by primes of $\mathcal{O}_{K,S}$ outside of S' is preserved when we replace S by S'.

Proof. Let us assume that the hypothesis holds for $n > N_0$ for some $N_0 \in \mathbb{N}$ and let us see how the theorem follows from the case where the hypothesis holds for all $n \in \mathbb{N}$, which is [14, Theorem 1]: if a is not a root of unity, then one just has to replace S by a set $S' \supseteq S$ that contains all prime factors of $\prod_{i=1}^{N_0}(a^i - 1)$. If, on the other hand, a is a root of unity, then $a^n - 1 = 0$ for infinitely many $n \in \mathbb{N}$ and one deduces that b is a root of unity and even, by taking n equal to two consecutive sufficiently large multiples of the order of a, that the order of b divides the order of a. Thus, b is a power of a, as desired. ■

The zeroes of $T^n - 1$ in $\mathbb{C}$ are the roots of unity of order dividing n. It might seem more natural to look at the polynomials whose zeroes are the roots of unity of order precisely n since these are the minimal polynomials over $\mathbb{Q}$ of the special points of $\mathbb{G}_{m,\mathbb{C}}$ just as the Hilbert class polynomials are the minimal polynomials over $\mathbb{Q}$ of the special points of $Y(1)_{\mathbb{C}}$. Thus, we replace the polynomials $T^n - 1$ by the cyclotomic polynomials $\Psi_n(T)$ ($n \in \mathbb{N} =: \mathcal{N}$) to create the *cyclotomic support problem*. To prove the analogue of Theorem 4.3, we need the following lemma.

Lemma 4.4. *Let K be a number field, let S be a finite set of maximal ideals of $\mathcal{O}_K$, and fix a maximal ideal $\mathfrak{p} \subseteq \mathcal{O}_{K,S}$ of residue characteristic p. The following are equivalent for $a \in \mathcal{O}_{K,S} \backslash \mathfrak{p}$ and $k \in \mathbb{N}$ coprime to p:*

(1) *a has order k modulo $\mathfrak{p}$,*

(2) *$\Psi_{kp^\ell}(a) \in \mathfrak{p}$ for some $\ell \in \mathbb{Z}_{\geq 0}$, and*

(3) *$\Psi_{kp^\ell}(a) \in \mathfrak{p}$ for all $\ell \in \mathbb{Z}_{\geq 0}$.*

Proof. It is clear that (1) implies (2) and that (3) implies (1), just take $\ell = 0$ and, for the second implication, use that the polynomial $T^k - 1$ modulo $\mathfrak{p}$ is separable. Finally, for every $\ell \in \mathbb{Z}_{\geq 1}$, we have the identity

$$\Psi_{kp^\ell}(T) \equiv \left(\Psi_k(T)\right)^{(p-1)p^{\ell-1}} \bmod p,$$

which one can deduce from the identity

$$T^{kp^\ell} - 1 \equiv (T^k - 1)^{p^\ell} \bmod p$$

using double induction on (k, ℓ), and so (2) implies (3). ■

We are now ready to solve the cyclotomic support problem as a direct consequence of Theorem 4.3.

Theorem 4.5. *Let K be a number field, let S be a finite set of maximal ideals of $\mathcal{O}_K$, and fix $N_0 \in \mathbb{N}$. If $a, b \in \mathcal{O}_{K,S} \backslash \{0\}$ satisfy that for all $n \in \mathbb{N}$ with $n > N_0$, every prime ideal of $\mathcal{O}_{K,S}$ dividing $\Psi_n(a)$ also divides $\Psi_n(b)$, then either a and b are roots of unity of the same order or $b = a^{\pm 1}$.*

The conclusion of Theorem 4.5 is best possible: if a and b are roots of unity of the same order k and $\mathfrak{p}$ is a maximal ideal of $\mathcal{O}_{K,S}$ of residue characteristic p, then Lemma 4.4 implies that a and b both have order k_0 modulo $\mathfrak{p}$ where p does not divide k_0 and $k = k_0 p^{\ell_0}$ for some $\ell_0 \in \mathbb{Z}_{\geq 0}$. Hence, Lemma 4.4 implies that for $n \in \mathbb{N}$, $\Psi_n(a) \in \mathfrak{p}$ if and only if $n = k_0 p^{\ell}$ for some $\ell \in \mathbb{Z}_{\geq 0}$ if and only if $\Psi_n(b) \in \mathfrak{p}$. So the hypothesis of the support problem holds. The same is true if $b = a^{-1} \in \mathcal{O}_{K,S}^*$ since a and a^{-1} have the same order modulo every maximal ideal of $\mathcal{O}_{K,S}$.

Proof. If a is a root of unity, k is its order, and $\mathfrak{p}$ is a maximal ideal of $\mathcal{O}_{K,S}$ of residue characteristic p, then $\Psi_{kp^{\ell}}(a) \in \mathfrak{p}$ for all $\ell \in \mathbb{Z}_{\geq 0}$ by Lemma 4.4. Choosing ℓ large enough and applying our hypothesis on a and b, we deduce that $\Psi_{kp^{\ell}}(b) \in \mathfrak{p}$ for some $\ell \in \mathbb{Z}_{\geq 0}$ and so, again by Lemma 4.4, $\Psi_k(b) \in \mathfrak{p}$. Varying $\mathfrak{p}$, we deduce that $\Psi_k(b) = 0$ and we are done.

If a is not a root of unity, then, after enlarging S if necessary, we can assume without loss of generality that $a \in \mathcal{O}_{K,S}^*$ and that $\prod_{i=1}^{N_0} \Psi_i(a) \in \mathcal{O}_{K,S}^*$ so that the support property holds for all $n \in \mathbb{N}$. Observe now that this property also holds in the other direction: if $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_{K,S}$ dividing $\Psi_n(b)$ for some $n \in \mathbb{N}$, then $\mathfrak{p}$ also divides $\Psi_n(a)$. Indeed, let p be the residue characteristic of $\mathfrak{p}$ and let m be the order of a modulo $\mathfrak{p}$, which is well defined since $a \notin \mathfrak{p}$. It follows that $\mathfrak{p} \mid \Psi_m(a)$ and the support property implies that $\mathfrak{p} \mid \Psi_m(b)$. By Lemma 4.4, b has order m modulo $\mathfrak{p}$. On the other hand, since we assumed that $\mathfrak{p} \mid \Psi_n(b)$, writing $n = n_0 p^{\ell}$ with $p \nmid n_0$, we must have $m = n_0$ by Lemma 4.4. Using once more Lemma 4.4, we deduce that $\mathfrak{p} \mid \Psi_{n_0 p^{\ell}}(a) = \Psi_n(a)$, as wanted.

We conclude that for all $n \in \mathbb{N}$, a prime ideal of $\mathcal{O}_{K,S}$ divides $a^n - 1 = \prod_{i \mid n} \Psi_i(a)$ if and only if it divides $\prod_{i \mid n} \Psi_i(b) = b^n - 1$. Thus, Theorem 4.3 implies that $b = a^k$ and $a = b^r$ for some $k, r \in \mathbb{Z}$. Hence, we have $a^{|kr-1|} = 1$ and, since by assumption a is not a root of unity, this yields $kr = 1$, so $k \in \{\pm 1\}$. The proof is concluded. ∎

The next theorem resolves the function field case of the multiplicative and the cyclotomic support problem in characteristic 0.

Theorem 4.6. *Let R be the coordinate ring of a smooth affine irreducible curve $\mathcal{C}$ over an algebraically closed field F of characteristic 0. Let $A, B \in R \backslash F$ and let $N_0 \in \mathbb{N}$. The following hold:*

(1) *Suppose that for all $n \in \mathbb{N}$ with $n > N_0$, every prime ideal of R that divides $A^n - 1$ also divides $B^n - 1$. Then $B = A^k$ for some $k \in \mathbb{Z}\backslash\{0\}$.*

(2) *Suppose that for all $n \in \mathbb{N}$ with $n > N_0$, every prime ideal of R that divides $\Psi_n(A)$ also divides $\Psi_n(B)$. Then $B = A^{\pm 1}$.*

The case where $A \in F$ or $B \in F$ is uninteresting, see Example 4.1. Note that the set Z_B in Example 4.1 (2) is in both cases infinite for all $B \in F\backslash\{1\}$ (and in case (2) even for all $B \in F$). In both cases of Theorem 4.6, we begin by proving that A and B are multiplicatively dependent; our proof of this fact runs along the same lines as the proof of [1, Theorem 1] by Ailon and Rudnick in the case $\mathcal{C} = \mathbb{A}^1_{\mathbb{C}}$.

Proof. Throughout the proof, we treat both cases simultaneously until the very end, where case (2) receives some extra attention. The tuple (A, B) defines a rational map $\varphi\colon \mathcal{C} \dashrightarrow \mathbb{G}^2_{m,F}$. Let $\mathcal{C}'$ denote the Zariski closure of the image of φ. Since A is non-constant, $\mathcal{C}'$ is a curve and φ has finite fibers. Thanks to [27, Proposition 15.4 (1)], applied to the morphism $\mathcal{C} \to \mathbb{A}^1_F$ induced by A, we can assume, after increasing N_0 if necessary, that for every root of unity ϑ of order $n > N_0$ there exists some maximal ideal $\mathfrak{m}_\vartheta$ of R dividing $A - \vartheta$. It then follows by hypothesis that $\mathfrak{m}_\vartheta$ also divides $B - \vartheta'$ for some root of unity ϑ', and so

$$(\vartheta, \vartheta') \in \mathcal{C}'(F) \subseteq \mathbb{G}^2_{m,F}(F) \simeq (F^*)^2.$$

Varying n shows that $\mathcal{C}'$ contains a Zariski dense set of special points. By the theorem of Ihara–Serre–Tate [35], $\mathcal{C}'$ is a special subvariety of $\mathbb{G}^2_{m,F}$ and so A, B are multiplicatively dependent. Since $A, B \notin F$, it follows that there exist coprime non-zero integers $k, \ell \in \mathbb{Z}$ and a root of unity η of order r such that $A^k B^\ell = \eta$ holds in the fraction field of R.

Let p denote a prime such that $p > \max\{N_0, |k|, |\ell|, r\}$ and let ζ be a root of unity such that $\xi := \eta\zeta^{-k}$ has order $|\ell|rp$. It follows that the order m of ζ is divisible by p and divides $|k\ell|rp$. By our assumptions on N_0 and p, there exists some maximal ideal $\mathfrak{m}_\zeta$ of R dividing $A - \zeta$.

Choose $\epsilon \in \{1, -1\}$ such that $|k| = \epsilon k$. We know that $A - \zeta$ divides

$$\begin{aligned}\eta^{-\epsilon}\big(A^{|k|} - \zeta^{|k|}\big) &= \eta^{-\epsilon}\big(A^{|k|} - (\eta\xi^{-1})^\epsilon\big)\\ &= \eta^{-\epsilon}\big(\eta^\epsilon B^{-\epsilon\ell} - (\eta\xi^{-1})^\epsilon\big) = B^{-\epsilon\ell} - \xi^{-\epsilon}\end{aligned}$$

in R. In particular, if $-\epsilon\ell = -|\ell|$, then $B \in R^*$ and $A - \zeta$ divides

$$-B^{|\ell|}\xi^\epsilon\big(B^{-|\ell|} - \xi^{-\epsilon}\big) = B^{|\ell|} - \xi^\epsilon$$

in R. It follows in any case that $A - \zeta$ divides $(B^{|\ell|} - \xi)(B^{|\ell|} - \xi^{-1})$.

Since $\mathfrak{m}_\zeta$ divides $A - \zeta$, we deduce that $\mathfrak{m}_\zeta$ also divides $(B^{|\ell|} - \xi)(B^{|\ell|} - \xi^{-1})$ and so divides $B - \xi'$ for some root of unity ξ' of order $\ell^2 rp$. At the same time, $\mathfrak{m}_\zeta$ also divides $B^m - 1$ by hypothesis. Since m divides $|k\ell|rp$, $\mathfrak{m}_\zeta$ divides $B^{|k\ell|rp} - 1$ and so divides $B - \zeta'$ for some root of unity ζ' of order dividing $|k\ell|rp$. It follows that $\zeta' = \xi'$, so ℓ divides k and $\ell \in \{\pm 1\}$ since k and ℓ are coprime.

After taking the reciprocals of both sides of the equation $A^k B^\ell = \eta$ and replacing (k, η) by $(-k, \eta^{-1})$ if necessary, we can assume without loss of generality that $\ell = -1$, i.e., that $B = \eta^{-1} A^k$ in the fraction field of R. Let again p denote a prime such that $p > \max\{N_0, |k|, r\}$ and let ζ be a root of unity of order p. By our assumption on N_0, there exists some maximal ideal $\mathfrak{m}_\zeta$ of R dividing $A - \zeta$. It follows that $\mathfrak{m}_\zeta$ divides $B - \eta^{-1}\zeta^k$, while also dividing $B^p - 1$ by hypothesis. The order of $\eta^{-1}\zeta^k$ is rp and so $r = 1$. Hence, we have $\eta = 1$ and we deduce that $B = A^k$.

In case (1), we are now done. In case (2), let again p denote a prime such that $p > \max\{N_0, |k|\}$ and let ζ be a root of unity of order $p|k|$. By our assumption on N_0, there exists some maximal ideal $\mathfrak{m}_\zeta$ of R dividing $A - \zeta$. It follows that $\mathfrak{m}_\zeta$ divides $B - \zeta^k$ while also dividing $B - \zeta'$ for some root of unity ζ' of order $p|k|$ by hypothesis. We deduce that $\zeta' = \zeta^k$, so $p|k| = p$ and $k \in \{\pm 1\}$. ■

5. The modular support problem

Let R be a Dedekind domain. Recall that $\mathbb{D} = \{D \in \mathbb{Z}_{<0};\, D \equiv 0, 1 \bmod 4\}$ and that, for $D \in \mathbb{D}$, $H_D(T)$ denotes the image under the canonical ring homomorphism $\mathbb{Z}[T] \to R[T]$ of the Hilbert class polynomial associated to an imaginary quadratic order of discriminant D. The *modular support problem* for R is the support problem for the family of polynomials $H_D(T) \in R[T]$ $(D \in \mathbb{D})$. We will consider the cases where R is either the coordinate ring of a smooth affine irreducible curve over an algebraically closed field of characteristic 0 or a ring of S-integers in some number field.

We start by proving an auxiliary proposition that will be used in both cases. It is inspired by the theory of isogeny volcanoes.

Proposition 5.1. *Let F be an algebraically closed field. Let $E_{/F}$ and $E'_{/F}$ denote two elliptic curves with complex multiplication by the same imaginary quadratic order $\mathcal{O}$ and let $\varphi\colon E \to E'$ be an isogeny with cyclic kernel such that* $\deg\varphi$ *and* $\operatorname{disc}(\mathcal{O})\max\{1, \operatorname{char}(F)\}$ *are coprime. Then, there is no prime ℓ that divides* $\deg\varphi$ *and is inert in the fraction field of $\mathcal{O}$.*

Proof. Since $\gcd(\deg\varphi, \max\{1, \operatorname{char}(F)\}) = 1$, the isogeny φ is separable. Let $P \in E(F)$ be a generator of $\ker\varphi$. Fix an abstract isomorphism $\iota\colon \operatorname{End}_F(E) \to \operatorname{End}_F(E')$

and set $\mathfrak{a} = \{\alpha \in \mathrm{End}_F(E); \alpha(P) = 0\}$. Then, $\mathfrak{a}$ is an ideal of $\mathrm{End}_F(E)$. We begin by showing that $[\mathrm{End}_F(E) : \mathfrak{a}] = \deg \varphi$.

We have $[\mathrm{End}_F(E) : \mathfrak{a}] = |\{\beta(P); \beta \in \mathrm{End}_F(E)\}|$. We want to show that $\beta(P) \in \ker \varphi$ for every $\beta \in \mathrm{End}_F(E)$. Let $\sigma : \mathrm{End}_F(E) \to \mathrm{End}_F(E)$ denote the unique nontrivial ring automorphism of $\mathrm{End}_F(E)$. One can check that for every endomorphism $\beta \in \mathrm{End}_F(E)$, there exists $\beta' \in \{\iota(\beta), \iota(\sigma(\beta))\}$ such that $\varphi \circ \beta = \beta' \circ \varphi$. Indeed, since φ is separable, it follows from [65, III, Corollary 4.11] that there exists $\beta'' \in \mathrm{End}_F(E')$ such that $(\deg \varphi)(\varphi \circ \beta) = \beta'' \circ \varphi$. Hence,

$$Q(\beta'') \circ \varphi = \varphi \circ Q\big((\deg \varphi)\beta\big) = 0,$$

where Q denotes the minimal polynomial of $(\deg \varphi)\beta$ in $\mathbb{Z}[T]$. We deduce that $Q(\beta'') = 0$ and so

$$\beta'' \in \big\{(\deg \varphi)\iota(\beta), (\deg \varphi)\iota\big(\sigma(\beta)\big)\big\}.$$

It follows that $\varphi \circ \beta = \beta' \circ \varphi$ for some $\beta' \in \{\iota(\beta), \iota(\sigma(\beta))\}$, as desired. This implies that $\varphi(\beta(P)) = \beta'(\varphi(P)) = 0$, so $\beta(P) \in \ker \varphi$. Since $\ker \varphi = \mathbb{Z} \cdot P$, we deduce that

$$|\{\beta(P); \beta \in \mathrm{End}_F(E)\}| = \deg \varphi,$$

so $[\mathrm{End}_F(E) : \mathfrak{a}] = \deg \varphi$.

Since $\gcd(\deg \varphi, \mathrm{disc}(\mathcal{O})) = 1$, this implies that $\mathfrak{a}$ is invertible (see [17, Proposition 7.4 and Lemma 7.18]).

Aiming for a contradiction, we now assume that there exists a prime ℓ that divides $\deg \varphi$ and is inert in the fraction field of $\mathcal{O}$. Since $\gcd(\deg \varphi, \mathrm{disc}(\mathcal{O})) = 1$, it follows from [17, Proposition 7.20] that there exists an ideal $\mathfrak{b}$ of $\mathrm{End}_F(E)$ such that $\mathfrak{a} = \ell\mathfrak{b}$ and

$$\deg \varphi = [\mathrm{End}_F(E) : \mathfrak{a}] = \ell^2 [\mathrm{End}_F(E) : \mathfrak{b}].$$

Hence, $\mathfrak{b} = \{\alpha \in \mathrm{End}_F(E); \ell\alpha \in \mathfrak{a}\} = \{\alpha \in \mathrm{End}_F(E); \alpha(\ell P) = 0\}$. By [65, III, Proposition 4.12], there exist an elliptic curve $E''_{/F}$ and a separable isogeny $\psi : E \to E''$ whose kernel is generated by ℓP. We have

$$\deg \psi = |\mathbb{Z} \cdot \ell P| \le |\{\beta(\ell P); \beta \in \mathrm{End}_F(E)\}| = [\mathrm{End}_F(E) : \mathfrak{b}] = \ell^{-2} \deg \varphi$$

or, equivalently, $(\deg \varphi)/(\deg \psi) \ge \ell^2$.

Since $\ker \psi \subseteq \ker \varphi$ and ψ is separable, [65, III, Corollary 4.11] implies that there exists an isogeny $\xi : E'' \to E'$ such that $\varphi = \xi \circ \psi$. Since φ is separable, also ξ is separable. By [65, III, Theorem 4.10 (c)] together with the above, we have

$$|\ker \xi| = \deg \xi = \frac{\deg \varphi}{\deg \psi} \ge \ell^2.$$

But $\ker \xi = \psi(\ker \varphi) \simeq (\ker \varphi)/(\ker \psi) \simeq \mathbb{Z}/\ell\mathbb{Z}$, and we get the desired contradiction. ∎

5.1. The modular support problem over function fields of characteristic 0

In this section, we consider the case where R is the coordinate ring of a smooth affine irreducible curve over an algebraically closed field F of characteristic 0. Since the Hilbert class polynomials are irreducible over $\mathbb{Q}$, monic, and pairwise distinct, it suffices, thanks to Example 4.1, to consider the problem for $A, B \in R\backslash F$. The following theorem gives a complete solution to the modular support problem in this setting.

Theorem 5.2. *Let R be the coordinate ring of a smooth affine irreducible curve $\mathscr{C}$ over an algebraically closed field F of characteristic* 0. *Let $A, B \in R\backslash F$ and suppose that there exists $D_0 \in \mathbb{N}$ such that for all discriminants $D \in \mathbb{D}$ with $|D| > D_0$ every prime ideal of R that divides $H_D(A)$ also divides $H_D(B)$. Then $A = B$.*

Proof. We first show that $\Phi_N(A, B) = 0$ for some $N \in \mathbb{N}$, where we recall that Φ_N denotes the N-th modular polynomial. Suppose by contradiction that this is not the case. Then Theorem 3.1 yields a non-zero ideal J of R such that

$$\gcd\big(H_D(A), H_D(B)\big) \mid J$$

for all $D \in \mathbb{D}$. By our assumption, every prime ideal of R that divides some $H_D(A)$ ($D \in \mathbb{D}$ with $|D| > D_0$) also divides the ideal J. On the other hand, since $H_D(A)$ and $H_{D'}(A)$ are coprime for $D, D' \in \mathbb{D}$ with $D \neq D'$, we deduce from [27, Proposition 15.4 (1)] applied to the morphism $\mathscr{C} \to \mathbb{A}^1_F = Y(1)_F$ induced by A that for infinitely many $D \in \mathbb{D}$, there exists a maximal ideal $\mathfrak{m}_D$ that divides $H_D(A)$. So J must be divisible by infinitely many pairwise distinct maximal ideals, which contradicts the fact that $J \neq (0)$. Hence there exists $N \in \mathbb{N}$ such that $\Phi_N(A, B) = 0$.

Our goal is now to show that $N = 1$. This would yield the desired result, since

$$\Phi_1(A, B) = A - B.$$

Assume then, again by contradiction, that $N > 1$ and let $p \in \mathbb{N}$ be a prime factor of N.

The morphisms $\psi_A, \psi_B : \mathscr{C} \to Y(1)_F$ induced by A, B are non-constant, so in particular, by [27, Proposition 15.4 (1)], the set $Y(1)_F \backslash \psi_A(\mathscr{C})$ is finite. By enlarging D_0 if necessary, we can assume without loss of generality that $\sigma \in \psi_A(\mathscr{C})$ for every singular modulus σ whose discriminant D satisfies $|D| > D_0$. By Dirichlet's theorem on primes in arithmetic progressions, there exists a fundamental discriminant $D \in \mathbb{D}$ with $|D| > D_0$ such that $\gcd(D, N) = 1$ and p is inert in $K := \mathbb{Q}(\sqrt{D}) \subseteq \bar{\mathbb{Q}}$.

By our assumption on D_0, there exist an elliptic curve $E_{/F}$ and a point $P \in \mathscr{C}(F)$ such that

$$\mathrm{End}_F(E) \simeq \mathcal{O}_K$$

and $\psi_A(P) = j(E) \in Y(1)(F) \simeq F$ is the j-invariant of E. Let $\mathfrak{m}_P$ denote the maximal ideal of R corresponding to P. Clearly, $\mathfrak{m}_P \mid H_D(A)$.

By assumption, $\mathfrak{m}_P$ divides $H_D(B)$ and so $\psi_B(P)$ is the j-invariant of an elliptic curve $E'_{/F}$ with complex multiplication by $\mathcal{O}_K$. We know that

$$\Phi_N\big(\psi_A(P), \psi_B(P)\big) = 0,$$

so by [17, Proposition 14.11], there exists an isogeny $\varphi\colon E \to E'$ of degree N with cyclic kernel. This contradicts Proposition 5.1 with $\ell = p$. We conclude that $N = 1$ and the theorem follows. ∎

5.2. The modular support problem over number fields

In this section, we analyze the modular support problem over a ring of S-integers in a number field. In all but finitely many exceptional cases, we will be able to show that the conclusion of Theorem 5.2 stays true. However, the proof is much more involved. We first prove an auxiliary lemma that is a modular analogue of Lemma 4.4.

Lemma 5.3. *Let K be a number field, let S be a finite set of maximal ideals of $\mathcal{O}_K$, and let $\mathfrak{p}$ denote a maximal ideal of $\mathcal{O}_{K,S}$ of residue characteristic p. The following are equivalent for $a \in \mathcal{O}_{K,S}$ and a discriminant $D \in \mathbb{D}$:*

(1) *there exist a finite field extension $K \subseteq L$, a singular modulus $j \in L$ of discriminant D, and a prime $\mathfrak{P}$ of L lying above $\mathfrak{p}$ such that $a \equiv j \bmod \mathfrak{P}$,*

(2) *$H_{Dp^{2\ell}}(a) \in \mathfrak{p}$ for some $\ell \in \mathbb{Z}_{\geq 0}$, and*

(3) *$H_{Dp^{2\ell}}(a) \in \mathfrak{p}$ for all $\ell \in \mathbb{Z}_{\geq 0}$.*

Proof. Choosing $\ell = 0$, we see immediately that (1) implies (2) and that (3) implies (1) with L equal to a splitting field of H_D over K.

Since $p \in \mathfrak{p}$, it follows from Proposition 2.4 that for every $\ell \in \mathbb{Z}_{\geq 0}$, there exists $k \in \mathbb{N}$ such that

$$H_{Dp^{2\ell}}(a) \equiv H_D(a)^k \bmod \mathfrak{p}.$$

Hence, (2) and (3) are equivalent and we are done. ∎

We are now ready to prove Theorem 1.5 that we restate here for the reader's convenience.

Theorem 5.4. *Let K be a number field and let S be a finite set of maximal ideals of $\mathcal{O}_K$. Let $j, j' \in \mathcal{O}_{K,S}$. Suppose that there exists $D_0 \in \mathbb{N}$ such that all the prime ideals of $\mathcal{O}_{K,S}$ dividing $H_D(j)$ also divide $H_D(j')$ for every $D \in \mathbb{D}$ with $|D| > D_0$. Then, either $j = j'$ or there exists $\tilde{D} \in \mathbb{D}$ such that $H_{\tilde{D}}(j) = H_{\tilde{D}}(j') = 0$.*

Proof. Denote by E_j, $E_{j'}$ any two fixed elliptic curves over K with j-invariants j, j' respectively. We begin by showing that, under the hypothesis of the theorem, the two curves are geometrically isogenous.

Fix an algebraic closure $\bar{K}$ of K. Let $\mathfrak{p} \subseteq \mathcal{O}_{K,S}$ be a prime ideal of good reduction for E_j and $E_{j'}$ and let $\mathfrak{P}$ be a prime of $\bar{K}$ lying above it. By Deuring's lifting theorem [36, Chapter 13, Theorem 14] (or [13, Theorem 1.7.4.6]), there exist a discriminant $D \in \mathbb{D}$ and an elliptic curve $(E_D)_{/\bar{K}}$ with complex multiplication by the order of discriminant D such that

$$E_D \bmod \mathfrak{P} \simeq E_j \bmod \mathfrak{P}.$$

In particular, $\mathfrak{p} \mid H_D(j)$ so that, by Lemma 5.3, $\mathfrak{p} \mid H_{Dp^{2n}}(j)$ for every $n \in \mathbb{N}$, where p denotes the residue characteristic of $\mathfrak{p}$. Choosing n large enough, we deduce from the hypothesis of the theorem that $\mathfrak{p} \mid H_{Dp^{2n}}(j')$ and then, again by Lemma 5.3, that $\mathfrak{p} \mid H_D(j')$. Hence, there exists an elliptic curve $(E'_D)_{/\bar{K}}$ with complex multiplication by the order of discriminant D such that

$$E'_D \bmod \mathfrak{P} \simeq E_{j'} \bmod \mathfrak{P}.$$

After fixing an embedding of $\bar{K}$ into $\mathbb{C}$, one can show that $E_D(\mathbb{C}) \simeq \mathbb{C}/\mathfrak{a}$ for some non-zero ideal $\mathfrak{a}$ of the imaginary quadratic order of discriminant D in $\mathbb{C}$ and similarly for $E'_D(\mathbb{C})$. Hence, E_D and E'_D are isogenous over $\mathbb{C}$ and therefore over $\bar{K}$.

It follows that also $E_j \bmod \mathfrak{P}$ and $E_{j'} \bmod \mathfrak{P}$ are isogenous. Hence, for all but finitely many maximal ideals $\mathfrak{p}$ of $\mathcal{O}_{K,S}$, the reduced elliptic curves E_j and $E_{j'}$ modulo $\mathfrak{p}$ are geometrically isogenous. By [34, Theorem 1] we conclude that $(E_j)_{\bar{K}}$ and $(E_{j'})_{\bar{K}}$ are isogenous. In particular, the geometric endomorphism rings of E_j and $E_{j'}$ must have the same $\mathbb{Z}$-rank.

It now suffices to consider two cases.

Case 1. Both E_j and $E_{j'}$ do not have complex multiplication.

Let $\varphi\colon (E_j)_{\bar{K}} \to (E_{j'})_{\bar{K}}$ be an isogeny and set $d = \deg \varphi$. We can assume without loss of generality that φ has cyclic kernel. If $d = 1$, then φ is an isomorphism and $j = j'$. Suppose then by contradiction that $d > 1$ and hence $j \neq j'$ since E_j does not have complex multiplication. We want to apply Theorem 2.2 with the following inputs:

(i) We take $\mathcal{P}$ to be the set of rational primes dividing $dN(\mathfrak{K})$, where $\mathfrak{K} \subseteq \mathcal{O}_{K,S}$ denotes the ideal generated by $\prod_{D \in \mathbb{D}, |D| \le D_0} H_D(j)$. Note that $\mathcal{P}$ is finite since j is not a singular modulus, and $\mathcal{P} \neq \emptyset$ because $d > 1$ by assumption.

(ii) We take L to be an imaginary quadratic field where all primes $\ell \in \mathcal{P}$ are inert. For instance, we can take L of discriminant $-\Delta$ where Δ is a prime that is congruent to 3 modulo 4 and satisfies suitable congruence conditions modulo $4\prod_{\ell \in \mathcal{P}} \ell$ (such a Δ exists by Dirichlet's theorem on primes in arithmetic progressions). We also take $\mathcal{O} = \mathcal{O}_L$ to be the ring of integers in L.

Since E_j does not have complex multiplication and E_j and $E_{j'}$ are geometrically isogenous, by Theorem 2.2 there exist infinitely many maximal ideals $\mathfrak{p} \subseteq \mathcal{O}_{K,S}$ such that $\mathfrak{p} \nmid d\mathfrak{K}$, E_j and $E_{j'}$ have good ordinary reduction modulo $\mathfrak{p}$, and

$$\mathrm{End}_{k_\mathfrak{p}}(E_j \bmod \mathfrak{p}) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \simeq \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_\ell =: \mathcal{O}_\ell \tag{5.1}$$

for all $\ell \in \mathcal{P}$. In particular, denoting by $\mathcal{A}$ this infinite set of primes obtained from Theorem 2.2 and setting $R_\mathfrak{p} := \mathrm{End}_{k_\mathfrak{p}}(E_j \bmod \mathfrak{p})$ for all primes $\mathfrak{p} \in \mathcal{A}$, we deduce from our choice of L and from (5.1) that all primes $\ell \in \mathcal{P}$ are inert in the fraction field $L_\mathfrak{p}$ of $R_\mathfrak{p}$ for every $\mathfrak{p} \in \mathcal{A}$. Moreover, (5.1) also implies that the conductor of $R_\mathfrak{p}$ is not divisible by any $\ell \in \mathcal{P}$ since, by [25, equation (1.8), p. 109], $\mathcal{O}_\ell$ is the ring of integers of the local field $L \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$, which is isomorphic to a quadratic extension of $\mathbb{Q}_\ell$. Finally, we remark that $R_\mathfrak{p}$ can be identified with $\mathrm{End}_{\overline{k}_\mathfrak{p}}(E_j \bmod \mathfrak{p})$ by Lemma 2.1, where $\overline{k}_\mathfrak{p}$ denotes a fixed algebraic closure of $k_\mathfrak{p}$.

Fix now $\mathfrak{p} \in \mathcal{A}$ and set $\widetilde{E}_j := E_j \bmod \mathfrak{p}$. By Deuring's lifting theorem [36, Chapter 13, Theorem 14] (or [13, Theorem 1.7.4.6]), there exist an elliptic curve $E_{/\overline{K}}$ with complex multiplication by an imaginary quadratic order of some discriminant D and a prime $\mathfrak{P} \subseteq \overline{K}$ lying above $\mathfrak{p}$ such that $E \bmod \mathfrak{P} \simeq (\widetilde{E}_j)_{\overline{k}_\mathfrak{p}}$, where we identify the residue field of $\mathfrak{P}$ and $\overline{k}_\mathfrak{p}$ via a fixed isomorphism. In particular, $\mathfrak{p} \mid H_D(j)$. Since by construction $\mathfrak{p} \nmid \mathfrak{K}$, we must have $|D| > D_0$ so that $\mathfrak{p} \mid H_D(j')$ by hypothesis. This implies that $\widetilde{E}_{j'} := E_{j'} \bmod \mathfrak{p}$ and $\widetilde{E}_j$ have complex multiplication by the same imaginary quadratic order $R_\mathfrak{p}$ by [36, Chapter 13, Theorem 12]. Moreover, by [61, II, Proposition 4.4] the reduction of φ modulo $\mathfrak{P}$ gives an isogeny $\widetilde{\varphi}\colon (\widetilde{E}_j)_{\overline{k}_\mathfrak{p}} \to (\widetilde{E}_{j'})_{\overline{k}_\mathfrak{p}}$ of degree d. Since the residue characteristic p of $\mathfrak{p}$ does not divide d, the kernel of $\widetilde{\varphi}$ must be equal to the reduction of $\ker\varphi$ modulo $\mathfrak{P}$ by [65, III, Theorem 4.10 (c) and VII, Proposition 3.1 (b)]. Hence, $\widetilde{\varphi}$ has cyclic kernel. Since every prime dividing d does not divide $\mathrm{disc}(R_\mathfrak{p})p$ and is inert in $L_\mathfrak{p}$ by construction, but $d > 1$, we can apply Proposition 5.1 to deduce a contradiction. Hence, $j = j'$, and this concludes the proof in this case.

Case 2. Both E_j and $E_{j'}$ have complex multiplication.

Let $D_j \in \mathbb{D}$ be the discriminant of $\mathrm{End}_{\overline{K}}(E_j)$. Take $p \in \mathbb{N}$ to be a prime such that $(D_j/p) = 1$ and let $E_{/\overline{K}}$ be an elliptic curve with complex multiplication by the imaginary quadratic order of discriminant $p^{2n}D_j$ for some fixed $n \in \mathbb{N}$. By [36, Chapter 13, Theorem 12], for every prime $\mathfrak{P} \subseteq \overline{K}$ lying above p, the reduction of E modulo $\mathfrak{P}$ is an elliptic curve with complex multiplication by the imaginary quadratic order of discriminant D_j, and by Proposition 2.4 we can choose E in such a way that $\mathfrak{P} \mid (j - j(E))$, and hence $\mathfrak{p} \mid H_{p^{2n}D_j}(j)$.

If we now choose n sufficiently large, the hypothesis of the theorem implies that we also have that $\mathfrak{p} \mid H_{p^{2n}D_j}(j')$. Again, it follows from [36, Chapter 13, Theorem 12] that $E_{j'}$ has complex multiplication by an order of discriminant $D_{j'} = p^{2k} D_j$ for some $k \in \mathbb{Z}_{\geq 0}$. Arguing in the same way with a prime $\ell \neq p$ such that $(D_j/\ell) = 1$, we conclude that there exists $r \in \mathbb{Z}_{\geq 0}$ such that

$$D_{j'} = p^{2k} D_j = \ell^{2r} D_j$$

and, since $\gcd(D_j, p\ell) = 1$, we deduce that $D_{j'} = D_j$. In particular, we have

$$H_{D_j}(j) = H_{D_j}(j') = H_{D_{j'}}(j') = 0,$$

as desired. ■

Remark 5.5. In the proof of Theorem 5.2, we knew, for algebro-geometric reasons, that all but finitely many imaginary quadratic orders could be obtained as the geometric endomorphism rings of specializations of the elliptic curve with j-invariant A. For the proof of Theorem 5.4, we only have Theorem 2.2 by Zarhin, which yields a weaker analogue of this statement. However, this analogous statement is still strong enough to allow us to create a situation where Proposition 5.1 applies.

In the case where $H_{\widetilde{D}}(j) = H_{\widetilde{D}}(j') = 0$ for some $\widetilde{D} \in \mathbb{D}$, it is unclear whether the support property can be satisfied for all but finitely many $D \in \mathbb{D}$. Numerical experiments seem to suggest that this should be true only if $j = j'$. On the other hand, we will now present an example of two distinct Galois conjugate singular moduli for which the support property holds for 25% of all $D \in \mathbb{D}$. In particular, if the support property holds for infinitely many $D \in \mathbb{D}$, this does not imply that $j = j'$. We do not know if there are any other examples of this nature.

Theorem 5.6. *Let*

$$j_1 = \frac{-191025 - 85995\sqrt{5}}{2} \quad \textit{and} \quad j_2 = \frac{-191025 + 85995\sqrt{5}}{2}$$

be the two singular moduli of discriminant -15 *in* $\bar{\mathbb{Q}}$. *Then for every discriminant* $D \in \mathbb{D}$ *with* $D \equiv 1 \bmod 8$, *the support property holds in both directions, i.e., for every maximal ideal* $\mathfrak{p}$ *of* $\mathbb{Z}[(-1+\sqrt{5})/2]$, *we have*

$$\mathfrak{p} \mid H_D(j_1) \quad \Leftrightarrow \quad \mathfrak{p} \mid H_D(j_2).$$

Proof. In this proof, we will use the notion of two isogenies being equivalent, which we now recall. Let F be an arbitrary algebraically closed field. If E_1, E_2, and E_3 are three elliptic curves over F and if $\varphi\colon E_1 \to E_2$ and $\psi\colon E_1 \to E_3$ are two isogenies, we say that φ and ψ are *equivalent* if there exists an isomorphism $\xi\colon E_2 \to E_3$ such that

$\xi \circ \varphi = \psi$. If $\deg \varphi$ and $\deg \psi$ are not divisible by $\mathrm{char}(F)$ and so φ and ψ are separable, then this is the same as requiring that $\ker \varphi = \ker \psi$ by [65, III, Corollary 4.11]. Of course, if φ and ψ are equivalent, then $j(E_2) = j(E_3)$.

We fix an embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. Let $E_{/\mathbb{C}}$ be an elliptic curve with complex multiplication by an imaginary quadratic order $\mathcal{O} \subseteq \overline{\mathbb{Q}}$ of discriminant $D \equiv 1 \bmod 8$ and fix an isomorphism $[\cdot]_E \colon \mathcal{O} \to \mathrm{End}_{\mathbb{C}}(E)$. The hypothesis that $D \equiv 1 \bmod 8$ implies that $2\mathcal{O} = \mathfrak{p}_2\mathfrak{p}_2'$, where $\mathfrak{p}_2, \mathfrak{p}_2' \subseteq \mathcal{O}$ are distinct Galois conjugate invertible ideals of norm 2 (see [17, Proposition 7.20]).

We have that $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$ for some invertible ideal Λ of $\mathcal{O}$ (see [17, Theorem 10.14]). Under this isomorphism, the $\mathfrak{p}_2$-torsion subgroup

$$E[\mathfrak{p}_2] := \{P \in E(\mathbb{C}); [\alpha]_E(P) = 0 \text{ for all } \alpha \in \mathfrak{p}_2\}$$

corresponds to $(\mathfrak{p}_2^{-1}\Lambda)/\Lambda$. Hence, for the quotient $(E_{\mathfrak{p}_2})_{/\mathbb{C}}$ of E by $E[\mathfrak{p}_2]$, we have that $E_{\mathfrak{p}_2}(\mathbb{C}) \simeq \mathbb{C}/\mathfrak{p}_2^{-1}\Lambda$.

We now apply [61, II, Proposition 1.2 (a) (ii)] with $\mathfrak{a} = \mathfrak{p}_2^{-1}$ to deduce that the endomorphism ring of $(E_{\mathfrak{p}_2})_{/\mathbb{C}}$ is isomorphic to $\mathcal{O}$. For this, note that [61, II, Proposition 1.2 (a) (ii)], although formulated only for maximal orders, also holds for an arbitrary order (with the same proof) as long as the fractional ideal $\mathfrak{a}$ (for the given order) is invertible. Let $\varphi \colon E \to E_{\mathfrak{p}_2}$ denote an isogeny with kernel $E[\mathfrak{p}_2]$. The degree of φ is equal to the norm of $\mathfrak{p}_2$, which is 2. Similarly, there exists an isogeny $\varphi' \colon E \to E_{\mathfrak{p}_2'}$ of degree 2 with kernel $E[\mathfrak{p}_2']$ such that $(E_{\mathfrak{p}_2'})_{/\mathbb{C}}$ is an elliptic curve with complex multiplication by $\mathcal{O}$ where $E[\mathfrak{p}_2']$ is defined analogously to $E[\mathfrak{p}_2]$. The isogenies φ, φ' are not equivalent since $\mathfrak{p}_2 + \mathfrak{p}_2' = \mathcal{O}$ and therefore $E[\mathfrak{p}_2] \neq E[\mathfrak{p}_2']$. This shows in particular that every elliptic curve with complex multiplication by an imaginary quadratic order of discriminant $D \equiv 1 \bmod 8$ admits two non-equivalent isogenies of degree 2 towards elliptic curves with complex multiplication by the same order.

In the case $D = -15$, these isogenies can be described explicitly in complex analytic terms. For $k \in \{1, 2\}$, denote by $(E_k)_{/\overline{\mathbb{Q}}}$ a fixed elliptic curve such that $j(E_k) = j_k$. Since $2\mathcal{O} = \mathfrak{p}_2\mathfrak{p}_2'$, where $\mathfrak{p}_2 = (2, (1 + \sqrt{-15})/2)$ is non-principal, it follows from [61, II, Proposition 1.2] that there exist complex analytic isomorphisms

$$\xi_1 \colon E_i(\mathbb{C}) \to \mathbb{C}/\mathcal{O}, \quad \xi_2 \colon E_k(\mathbb{C}) \to \mathbb{C}/\mathfrak{p}_2, \quad \{i, k\} = \{1, 2\}.$$

We then see that the map $z \mapsto 2z$ induces an isogeny $\mathbb{C}/\mathcal{O} \to \mathbb{C}/\mathfrak{p}_2$ with kernel $\mathfrak{p}_2'^{-1}/\mathcal{O}$ and an isogeny $\mathbb{C}/\mathcal{O} \to \mathbb{C}/\mathfrak{p}_2'$ with kernel $\mathfrak{p}_2^{-1}/\mathcal{O}$. Since $\mathfrak{p}_2$ and $\mathfrak{p}_2'$ are in the same ideal class in $\mathrm{Pic}(\mathcal{O})$, we have $\mathbb{C}/\mathfrak{p}_2 \simeq \mathbb{C}/\mathfrak{p}_2'$, and we thus obtain two inequivalent isogenies $\varphi_1, \varphi_2 \colon (E_i)_{\mathbb{C}} \to (E_k)_{\mathbb{C}}$. Since E_1 and E_2 are defined over $\overline{\mathbb{Q}}$, both these isogenies are base changes of isogenies $E_i \to E_k$ that we will denote by φ_1 and φ_2 as well. We can assume without loss of generality, after maybe applying an automorphism of $\overline{\mathbb{Q}}$ which maps $\sqrt{5}$ to $-\sqrt{5}$, that $i = 1$ and $k = 2$.

We are now ready to conclude the proof of the theorem. Since j_1 and j_2 are Galois conjugate, it suffices to prove that $\mathfrak{p} \mid H_D(j_1)$ implies that $\mathfrak{p} \mid H_D(j_2)$ for every maximal ideal $\mathfrak{p}$ of $\mathbb{Z}[(-1+\sqrt{5})/2]$. Fix a negative discriminant $D \equiv 1 \bmod 8$, a maximal ideal $\mathfrak{p}$ of $\mathbb{Z}[(-1+\sqrt{5})/2]$ such that $\mathfrak{p} \mid H_D(j_1)$, and a prime $\mathfrak{P} \subseteq \overline{\mathbb{Q}}$ lying above $\mathfrak{p}$. Since E_1 and E_2 have complex multiplication, they both have good reduction at $\mathfrak{P}$. As a first step, assume that $\mathfrak{p}$ lies above 2. Since 2 is inert in $\mathbb{Q}(\sqrt{5})$ and j_1, j_2 are Galois conjugate, we deduce that $\mathfrak{p} = (2)$ and

$$\mathfrak{p} \mid H_D(j_1) \quad \Leftrightarrow \quad \mathfrak{p} \mid H_D(j_2).$$

Assume from now on that $\mathfrak{p}$ does not lie above 2 and that $\mathfrak{p}$ divides $H_D(j_1)$. To ease notation, we will use a tilde $\widetilde{\cdot}$ to denote the reduction of some object (curve, morphism, etc.) modulo $\mathfrak{P}$. It follows from our assumption that there exists $j \in \overline{\mathbb{Q}}$ such that $H_D(j) = 0$ and $j_1 \equiv j \mod \mathfrak{P}$. Fix an elliptic curve $(E_j)_{/\overline{\mathbb{Q}}}$ with $j(E_j) = j$. The above discussion shows that E_j admits at least two non-equivalent degree-2 isogenies $\psi_k \colon E_j \to E_{D,k}$ for $k \in \{1,2\}$, where

$$\operatorname{End}_{\overline{\mathbb{Q}}}(E_{D,k}) \simeq \mathbb{Z}\left[\frac{D+\sqrt{D}}{2}\right].$$

We set $j_{D,k} := j(E_{D,k})$ so that $H_D(j_{D,k}) = 0$ for $k \in \{1,2\}$ (it is possible that $j_{D,1} = j_{D,2}$, e.g., if $D = -15$). Since the aforementioned elliptic curves all have complex multiplication, they all have good reduction at $\mathfrak{P}$. Let $E_j[2]$ denote the 2-torsion subgroup of E_j, then the reduction map $E_j[2] \to \widetilde{E_j}[2]$ is injective by [65, VII, Proposition 3.1 (b)]. It follows that, for $k \in \{1,2\}$, the kernel of $\widetilde{\psi}_k$ is precisely the reduction modulo $\mathfrak{P}$ of $\ker \psi_k \subseteq E_j[2]$ since $\deg \widetilde{\psi}_k = \deg \psi_k = 2$ by [61, II, Proposition 4.4]. Hence, $\ker \widetilde{\psi}_1 \neq \ker \widetilde{\psi}_2$ and so the reduced isogenies $\widetilde{\psi}_1, \widetilde{\psi}_2$ are non-equivalent. Similarly, it follows that also the reduced isogenies $\widetilde{\varphi}_1$ and $\widetilde{\varphi}_2$ are non-equivalent. On the other hand, the elliptic curve $\widetilde{E}_1 \simeq \widetilde{E}_j$ cannot have more than three non-equivalent isogenies of degree 2 since there are only three distinct subgroups of order 2 of the 2-torsion subgroup of $\widetilde{E}_1$. Hence, there exist $i, k \in \{1,2\}$ such that the isogeny $\widetilde{\varphi}_i$ is equivalent to the isogeny $\widetilde{\psi}_k$. This in particular implies that $\widetilde{j}_2 = \widetilde{j}_{D,k}$, and we conclude that $\mathfrak{p}$ divides $H_D(j_2)$, as desired. ∎

Acknowledgements. We thank Jorge Mello, Pieter Moree, and Jonathan Pila for useful discussions and suggestions. We also thank the referee for their many comments and suggestions, which led to an improvement of the exposition. The first-named author is grateful to the Max-Planck-Institut für Mathematik in Bonn for its hospitality and financial support. The second-named author thanks the Mathematical Institute of the University of Oxford and his host there, Jonathan Pila, for hosting him as a visitor for the duration of his Early Postdoc Mobility grant. He also thanks the first-named author for his hospitality.

Funding. Francesco Campagna is supported by ANR-20-CE40-0003 Jinvariant and is a member of the INDAM group GNSAGA. Gabriel Dill was supported by the Swiss National Science Foundation through the Early Postdoc Mobility grant no. P2BSP2_195703. The authors have received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement no. 945714).

References

[1] N. Ailon and Z. Rudnick, Torsion points on curves and common divisors of $a^k - 1$ and $b^k - 1$. *Acta Arith.* **113** (2004), no. 1, 31–38 Zbl 1057.11018 MR 2046966

[2] Y. André, Finitude des couples d'invariants modulaires singuliers sur une courbe algébrique plane non modulaire. *J. Reine Angew. Math.* **505** (1998), 203–208 Zbl 0918.14010 MR 1662256

[3] M. Baker, S.-i. Ih, and R. Rumely, A finiteness property of torsion points. *Algebra Number Theory* **2** (2008), no. 2, 217–248 Zbl 1182.11030 MR 2377370

[4] F. Barroero, L. Capuano, and A. Turchet, Greatest common divisor results on semiabelian varieties and a conjecture of Silverman. *Res. Number Theory* **10** (2024), no. 1, article no. 17 Zbl 7801558 MR 4693335

[5] D. Bertrand, D. Masser, A. Pillay, and U. Zannier, Relative Manin–Mumford for semi-Abelian surfaces. *Proc. Edinb. Math. Soc. (2)* **59** (2016), no. 4, 837–875 Zbl 1408.14139 MR 3570118

[6] Yu. Bilu, P. Habegger, and L. Kühne, No singular modulus is a unit. *Int. Math. Res. Not. IMRN* (2020), no. 24, 10005–10041 Zbl 1467.11059 MR 4190395

[7] E. Bombieri and W. Gubler, *Heights in Diophantine geometry*. New Math. Monogr. 4, Cambridge University Press, Cambridge, 2006 Zbl 1115.11034 MR 2216774

[8] E. Bombieri, D. Masser, and U. Zannier, Intersecting a curve with algebraic subgroups of multiplicative groups. *Int. Math. Res. Not. IMRN* (1999), no. 20, 1119–1140 Zbl 0938.11031 MR 1728021

[9] Y. Bugeaud, P. Corvaja, and U. Zannier, An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$. *Math. Z.* **243** (2003), no. 1, 79–84 Zbl 1021.11001 MR 1953049

[10] Y. Cai, Bounding the difference of two singular moduli. *Mosc. J. Comb. Number Theory* **10** (2021), no. 2, 95–110 Zbl 1470.11064 MR 4276350

[11] F. Campagna, On singular moduli that are S-units. *Manuscripta Math.* **166** (2021), no. 1-2, 73–90 Zbl 1480.11079 MR 4296371

[12] F. Campagna, Effective bounds on differences of singular moduli that are S-units. *Math. Proc. Cambridge Philos. Soc.* **174** (2023), no. 2, 415–450 Zbl 1534.11084 MR 4545213

[13] C.-L. Chai, B. Conrad, and F. Oort, *Complex multiplication and lifting problems*. Math. Surveys Monogr. 195, American Mathematical Society, Providence, RI, 2014 Zbl 1298.14001 MR 3137398

[14] C. Corrales-Rodrigáñez and R. Schoof, The support problem and its elliptic analogue. *J. Number Theory* **64** (1997), no. 2, 276–290 Zbl 0922.11086 MR 1453213

[15] P. Corvaja and U. Zannier, A lower bound for the height of a rational function at S-unit points. *Monatsh. Math.* **144** (2005), no. 3, 203–224 Zbl 1086.11035 MR 2130274

[16] P. Corvaja and U. Zannier, Greatest common divisors of $u-1,\ v-1$ in positive characteristic and rational points on curves over finite fields. *J. Eur. Math. Soc. (JEMS)* **15** (2013), no. 5, 1927–1942 Zbl 1325.11060 MR 3082249

[17] D. A. Cox, *Primes of the form x^2+ny^2*. Second edn., Pure Appl. Math. (Hoboken), John Wiley, Hoboken, NJ, 2013 Zbl 1275.11002 MR 3236783

[18] C. David and F. Pappalardi, Average Frobenius distribution for inerts in $\mathbb{Q}(i)$. *J. Ramanujan Math. Soc.* **19** (2004), no. 3, 181–201 Zbl 1193.11054 MR 2139503

[19] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hansischen Univ.* **14** (1941), 197–272 Zbl 0025.02003 MR 0005125

[20] B. Edixhoven and R. Richard, A mod p variant of the André-Oort conjecture. *Rend. Circ. Mat. Palermo (2)* **69** (2020), no. 1, 151–157 Zbl 1460.11084 MR 4148780

[21] N. D. Elkies, The existence of infinitely many supersingular primes for every elliptic curve over **Q**. *Invent. Math.* **89** (1987), no. 3, 561–567 Zbl 0631.14024 MR 0903384

[22] N. D. Elkies, Supersingular primes for elliptic curves over real number fields. *Compos. Math.* **72** (1989), no. 2, 165–172 Zbl 0708.14020 MR 1030140

[23] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.* **73** (1983), no. 3, 349–366 Zbl 0588.14026 MR 0718935

[24] É. Fouvry and M. R. Murty, Supersingular primes common to two elliptic curves. In *Number theory (Paris, 1992–1993)*, pp. 91–102, London Math. Soc. Lecture Note Ser. 215, Cambridge University Press, Cambridge, 1995 Zbl 0852.11029 MR 1345175

[25] A. Fröhlich and M. J. Taylor, *Algebraic number theory*. Cambridge Stud. Adv. Math. 27, Cambridge University Press, Cambridge, 1991 Zbl 0744.11001 MR 1215934

[26] D. Ghioca, L.-C. Hsia, and T. Tucker, A variant of a theorem by Ailon–Rudnick for elliptic curves. *Pacific J. Math.* **295** (2018), no. 1, 1–15 Zbl 1450.11061 MR 3778323

[27] U. Görtz and T. Wedhorn, *Algebraic geometry I*. Adv. Lect. Math., Vieweg and Teubner, Wiesbaden, 2010 Zbl 1213.14001 MR 2675155

[28] P. Habegger, Singular moduli that are algebraic units. *Algebra Number Theory* **9** (2015), no. 7, 1515–1524 Zbl 1334.11046 MR 3404647

[29] S. Herrero, R. Menares, and J. Rivera-Letelier, There are at most finitely many singular moduli that are S-units. *Compos. Math.* **160** (2024), no. 4, 732–770 Zbl 7825739 MR 4713026

[30] M. Hindry, Autour d'une conjecture de Serge Lang. *Invent. Math.* **94** (1988), no. 3, 575–603 Zbl 0638.14026 MR 0969244

[31] K. Huang, Generalized greatest common divisors for orbits under rational functions. *Monatsh. Math.* **191** (2020), no. 1, 103–123 Zbl 1448.11118 MR 4050112

[32] D. Husemöller, *Elliptic curves*. Second edn., Grad. Texts in Math. 111, Springer, New York, 2004 Zbl 1040.11043 MR 2024529

[33] K. James and E. Smith, Average Frobenius distribution for the degree two primes of a number field. *Math. Proc. Cambridge Philos. Soc.* **154** (2013), no. 3, 499–525 Zbl 1328.11061 MR 3044212

[34] C. B. Khare and M. Larsen, Abelian varieties with isogenous reductions. *C. R. Math. Acad. Sci. Paris* **358** (2020), no. 9-10, 1085–1089 Zbl 1482.11085 MR 4196779

[35] S. Lang, Division points on curves. *Ann. Mat. Pura Appl. (4)* **70** (1965), 229–234 Zbl 0151.27401 MR 0190146

[36] S. Lang, *Elliptic functions*. Second edn., Grad. Texts in Math. 112, Springer, New York, 1987 Zbl 0615.14018 MR 0890960

[37] S. Lang, *Algebraic number theory*. Second edn., Grad. Texts in Math. 110, Springer, New York, 1994 Zbl 0811.11001 MR 1282723

[38] S. Lang and H. Trotter, *Frobenius distributions in* GL_2*-extensions*. Lect. Notes Math. 504, Springer, Berlin-New York, 1976 Zbl 0329.12015 MR 0568299

[39] M. Larsen, The support problem for abelian varieties. *J. Number Theory* **101** (2003), no. 2, 398–403 Zbl 1039.11040 MR 1989894

[40] J. Li, S. Li, and Y. Ouyang, Factorization of Hilbert class polynomials over prime fields. 2021, arXiv:2108.00168v2

[41] Y. Li, Singular units and isogenies between CM elliptic curves. *Compos. Math.* **157** (2021), no. 5, 1022–1035 Zbl 1480.11080 MR 4251608

[42] R. C. Mason, *Diophantine equations over function fields*. London Math. Soc. Lecture Note Ser. 96, Cambridge University Press, Cambridge, 1984 Zbl 0533.10012 MR 0754559

[43] D. Masser and G. Wüstholz, Estimating isogenies on elliptic curves. *Invent. Math.* **100** (1990), no. 1, 1–24 Zbl 0722.14027 MR 1037140

[44] D. Masser and U. Zannier, Torsion anomalous points and families of elliptic curves. *C. R. Math. Acad. Sci. Paris* **346** (2008), no. 9-10, 491–494 Zbl 1197.11066 MR 2412783

[45] D. Masser and U. Zannier, Torsion anomalous points and families of elliptic curves. *Amer. J. Math.* **132** (2010), no. 6, 1677–1691 Zbl 1225.11078 MR 2766181

[46] D. Masser and U. Zannier, Torsion points on families of squares of elliptic curves. *Math. Ann.* **352** (2012), no. 2, 453–484 Zbl 1306.11047 MR 2874963

[47] D. Masser and U. Zannier, Torsion points on families of products of elliptic curves. *Adv. Math.* **259** (2014), 116–133 Zbl 1318.11075 MR 3197654

[48] D. Masser and U. Zannier, Torsion points on families of simple abelian surfaces and Pell's equation over polynomial rings. *J. Eur. Math. Soc. (JEMS)* **17** (2015), no. 9, 2379–2416 Zbl 1328.11068 MR 3420511

[49] D. Masser and U. Zannier, Torsion points, Pell's equation, and integration in elementary terms. *Acta Math.* **225** (2020), no. 2, 227–313 Zbl 1470.11163 MR 4205408

[50] Y. Matsuzawa, Vojta's conjecture, heights associated with subschemes, and primitive prime divisors in arithmetic dynamics. 2020, arXiv:2012.04693v1

[51] P. Michel, The subconvexity problem for Rankin–Selberg L-functions and equidistribution of Heegner points. *Ann. of Math. (2)* **160** (2004), no. 1, 185–236 Zbl 1068.11033 MR 2119720

[52] J. Neukirch, *Algebraic number theory*. Grundlehren Math. Wiss. 322, Springer, Berlin, 1999 Zbl 0956.11021 MR 1697859

[53] A. Perucca, Two variants of the support problem for products of abelian varieties and tori. *J. Number Theory* **129** (2009), no. 8, 1883–1892 Zbl 1230.11077 MR 2522711

[54] R. Pink, A common generalization of the conjectures of André–Oort, Manin–Mumford, and Mordell–Lang, 2005, https://people.math.ethz.ch/~pink/ftp/AOMMML.pdf, visited on 14 April 2025

[55] M. Raynaud, Courbes sur une variété abélienne et points de torsion. *Invent. Math.* **71** (1983), no. 1, 207–233 Zbl 0564.14020 MR 0688265

[56] R. Richard, A two-dimensional arithmetic André–Oort problem. *Bull. Lond. Math. Soc.* **55** (2023), no. 3, 1459–1488 Zbl 1546.11090 MR 4618237

[57] A. Schinzel, On the congruence $a^x \equiv b \pmod{p}$. *Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys.* **8** (1960), 307–309. Reprinted in *Selecta. Vol. II: Elementary, Analytic and Geometric Number Theory*, pp. 909–911, Herit. Eur. Math., European Mathematical Society, Zürich, 2007 Zbl 0094.25504 MR 0125070; Zbl 1115.11002 MR 2383195

[58] S. Schmid, Integrality properties in the moduli space of elliptic curves: CM case. *Int. J. Number Theory* **17** (2021), no. 7, 1671–1696 Zbl 1482.11093 MR 4295378

[59] J.-P. Serre, Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.* **54** (1981), 123–201 Zbl 0496.12011 MR 0644559

[60] J.-P. Serre,*Abelian l-adic representations and elliptic curves*. Second edn., Advanced Book Classics, Addison-Wesley, Redwood City, CA, 1989 Zbl 0709.14002 MR 1043865

[61] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*. Grad. Texts in Math. 151, Springer, New York, 1994 Zbl 0911.14015 MR 1312368

[62] J. H. Silverman, Common divisors of $a^n - 1$ and $b^n - 1$ over function fields. *New York J. Math.* **10** (2004), 37–43 Zbl 1120.11045 MR 2052363

[63] J. H. Silverman, Common divisors of elliptic divisibility sequences over function fields. *Manuscripta Math.* **114** (2004), no. 4, 431–446 Zbl 1128.11015 MR 2081943

[64] J. H. Silverman, Generalized greatest common divisors, divisibility sequences, and Vojta's conjecture for blowups. *Monatsh. Math.* **145** (2005), no. 4, 333–350 Zbl 1197.11070 MR 2162351

[65] J. H. Silverman, *The arithmetic of elliptic curves*. Second edn., Grad. Texts in Math. 106, Springer, Dordrecht, 2009 Zbl 1194.11005 MR 2514094

[66] U. Zannier, *Some problems of unlikely intersections in arithmetic and geometry*. Ann. of Math. Stud. 181, Princeton University Press, Princeton, NJ, 2012 Zbl 1246.14003 MR 2918151

[67] Yu. G. Zarhin, Endomorphism rings of reductions of elliptic curves and Abelian varieties (in Russian). *Algebra i Analiz* **29** (2017), no. 1, 110–144. English translation: *St. Petersburg Math. J.* **29** (2018), no. 1, 81–106 Zbl 1411.11051 MR 3660686

[68] B. Zilber, Exponential sums equations and the Schanuel conjecture. *J. London Math. Soc. (2)* **65** (2002), no. 1, 27–44 Zbl 1030.11073 MR 1875133

Received 6 October 2022.

Francesco Campagna

LMBP UMR 6620 - CNRS, Université Clermont Auvergne, Campus des Cézeaux 3, place Vasarely, 63178 Aubière, France; francesco.campagna@uca.fr

Gabriel A. Dill

Institut de Mathématiques, Université de Neuchâtel, Rue Emile-Argand 11, 2000 Neuchâtel, Switzerland; gabriel.dill@unine.ch