SHIMURA CURVES AND THE ABC CONJECTURE

HECTOR PASTEN

Abstract. We develop a general framework to study Szpiro's conjecture and the *abc* conjecture by means of Shimura curves and their maps to elliptic curves, introducing new techniques that allow us to obtain several unconditional results for these conjectures. We first prove various general results about modular and Shimura curves, including bounds for the Manin constant in the case of additive reduction, a detailed study of maps from Shimura curves to elliptic curves and comparisons between their degrees, and lower bounds for the Petersson norm of integral modular forms on Shimura curves. Our main applications for Szpiro's conjecture and the *abc* conjecture include improved effective bounds for the Faltings height of elliptic curves over $\mathbb{Q}$ in terms of the conductor, bounds for products of p-adic valuations of the discriminant of elliptic curves over $\mathbb{Q}$ which are polynomial on the conductor, and results that yield a modular approach to Szpiro's conjecture over totally real number fields with the expected dependence on the discriminant of the field. These applications lie beyond the scope of previous techniques in the subject. A main difficulty in the theory is the lack of q-expansions, which we overcome by making essential use of suitable integral models and CM points. Our proofs require a number of tools from Arakelov geometry, analytic number theory, Galois representations, complex-analytic estimates on Shimura curves, automorphic forms, known cases of the Colmez conjecture, and results on generalized Fermat equations.

Contents

Date: July 5, 2018.

2010 *Mathematics Subject Classification.* Primary 11G18; Secondary 11G05, 14G40.

Key words and phrases. Shimura curves, elliptic curves, *abc* conjecture.

This research was partially supported by a Benjamin Peirce Fellowship (at Harvard) and by a Schmidt Fellowship and NSF Grant DMS-1128155 (at IAS).

1. Introduction

This work concerns Szpiro's conjecture, the *abc* conjecture and related questions. Our main innovation is the introduction of several techniques related to Shimura curve parametrizations of elliptic curves in order to study these problems. As we will see, this new framework leads to unconditional results that lie out of the reach of the existing approaches in the literature. For our methods to work, we need to establish a number of general results of independent interest in the theory classical modular curves and Shimura curves. These include boundedness of the Manin constant, almost-surjectivity of the map on component groups for Shimura curve parametrizations in the case of Cerednik-Drinfeld reduction, refinements of the Ribet-Takahashi formula, and lower bounds for the Petersson norm of integral quaternionic modular forms.

In the context of Szpiro's conjecture and the *abc* conjecture, the main applications of the theory developed in this work concern three aspects:

(1) *Effective and explicit unconditional estimates for the Faltings height of elliptic curves over $\mathbb{Q}$ in terms of the conductor.* Our estimates are stronger than the existing results in the literature. Effectivity with explicit constants is a relevant aspect, since in the past even weaker bounds have been useful for explicitly solving Diophantine equations in practice. We introduce a method to prove such estimates by only considering congruences of Hecke eigenforms (as opposed to congruences of general modular forms), which not only leads to better unconditional estimates, but it also allows us to obtain further refinements under GRH. Shimura curves help us to reduce the number of such congruences that must be considered, leading to further improvements.

(2) *Bounds for products of valuations.* For coprime positive integers a, b, c with $a + b = c$, the theory of linear forms in p-adic logarithms allows one to bound all the p-adic valuations of the product abc, by a power of the radical $\mathrm{rad}(abc)$. Our methods, instead, provide such a polynomial bound for the *product* of all these p-adic valuations. We also obtain analogous statements for elliptic curves, by showing that the product of the exponents of the minimal discriminant is bounded polynomially on the conductor. This gives us access to prove results outside the realm of known exponential versions of the *abc* conjecture and Szpiro's conjecture that are currently available in the literature. For instance, we prove that the product of all p-adic Tamagawa factors of an elliptic curve over $\mathbb{Q}$ (the so-called "fudge factor" appearing in the Birch and Swinnerton-Dyer conjecture) is bounded by a power of the conductor. We also give an upper bound in terms of the level for the number of primes to which level-lowereing congruences (in the sense of Ribet) can occur, showing in a precise way that they are not too numerous. Unlike classical modular approaches to the *abc* conjecture where one tries to bound the degree of a modular parametrization $X_0(N) \to E$ for an elliptic curve E, our strategy focuses on comparing the degree of maps $X \to E$ for a fixed elliptic curve E and several Shimura curves X. Also, our method is global, in the sense that we work with the product of several local contributions simultaneously, unlike linear forms in p-adic logarithms.

(3) *A modular approach over totally real fields.* We prove that the Faltings height of modular elliptic curves over totally real fields can be bounded in terms of the degree of modular parametrizations coming from Shimura curves, with a contribution from the discriminant of the number field agreeing with well-known conjectures. Bounds of this sort over $\mathbb{Q}$ (without the discriminant term) are classical, but the usual argument does not extend beyond $\mathbb{Q}$ since the relevant Shimura curves do not have cusps. We overcome this difficulty by means of Arakelov geometry and the theory of Heegner points. Our results have two main consequences: On the one hand, they provide evidence

for Vojta's conjecture on algebraic points of bounded degree in the aspect of the dependence on the logarithmic discriminant. On the other hand, we can use effective multiplicity one results for automorphic representations on GL_2 over number fields along with existing modularity results in order to bound the degree of such a parametrization, obtaining unconditional estimates in this context comparable to what is known over $\mathbb{Q}$.

After briefly formulating the main motivating problems, the rest of this introduction is devoted to present our main results and to give an outline of the paper. First we discuss our general results on arithmetic of modular curves and Shimura curves, and then we will present in more detail the applications in the context of Szpiro's conjecture and the *abc* conjecture mentioned in (1), (2), and (3) above.

1.1. **The problems.** Let us briefly state the motivating problems; we take this opportunity to introduce some basic notation. Precise details will be recalled in Section 3.

For an elliptic curve E over $\mathbb{Q}$ we write Δ_E for the absolute value of its minimal discriminant and N_E for its conductor. In the early eighties, Szpiro formulated the following conjecture:

Conjecture 1.1 (Szpiro's conjecture; cf. [91])**.** *There is a constant $\kappa > 0$ such that for all elliptic curves E over $\mathbb{Q}$ we have $\Delta_E < N_E^{\kappa}$.*

The radical $\mathrm{rad}(n)$ of a positive integer n is defined as the product of the primes dividing n without repetition. Let's recall here a simple version of the *abc* conjecture of Masser and Oesterlé.

Conjecture 1.2 (*abc* conjecture)**.** *There is a constant $\kappa > 0$ such that for all coprime positive integers a, b, c with $a + b = c$ we have $abc < \mathrm{rad}(abc)^{\kappa}$.*

Both conjectures are open. There are stronger versions in the literature (cf. [76]), but we keep these simpler formulations for the sake of exposition.

A classical construction of Frey [36] shows that Szpiro's conjecture implies the *abc* conjecture: To a triple of coprime positive integers a, b, c with $a + b = c$ one associates the Frey-Hellegouarch elliptic curve $E_{a,b,c}$ given by the affine equation $y^2 = x(x - a)(x + b)$. Then Δ_E and N_E are equal to $(abc)^2$ and $\mathrm{rad}(abc)$ respectively, up to a bounded power of 2 (cf. Section 3 for details and references). Thus, Szpiro's conjecture in the case of Frey-Hellegouarch elliptic curves implies the *abc* conjecture as stated above.

In the rest of this introduction we will freely use Landau's notation O, as well as Vinogradov's notation $\ll$ (we include a reminder of these definitions in Section 2). In particular, $X \ll Y$ means the same as $X = O(Y)$. If the implicit constants are not absolute and depend on some parameters, this will be indicated by subscripts.

If there is any risk of confusion, we will use the subscript "(?)" in an equality or inequality to indicate that the claimed expression is conjectural.

1.2. **Results on modular curves and Shimura curves.** The notation in this paragraph is standard, and it will be recalled in detail in Section 3 and Section 4.

For a positive integer N we have the modular curve $X_0(N)$ over $\mathbb{Q}$ with Jacobian $J_0(N)$ and a standard embedding $X_0(N) \to J_0(N)$ defined over $\mathbb{Q}$ induced by the cusp $i\infty$. Write $\mathfrak{h}$ for the complex upper half plane. The space of weight 2 cuspforms for $\Gamma_0(N)$ is denoted by $S_2(N)$. The complex uniformization $\mathfrak{h} \to \Gamma_0(N)\backslash\mathfrak{h} \cup \{cusps\} = X_0(N)_{\mathbb{C}}$ induces an identification $S_2(N) \simeq H^0(X_0(N)_{\mathbb{C}}, \Omega^1_{X_0(N)_{\mathbb{C}}/\mathbb{C}})$. Given a newform $f \in S_2(N)$ with rational Hecke eigenvalues and normalized by requiring that the first Fourier coefficient be 1, we consider the associated optimal quotient $q : J_0(N) \to A$ over $\mathbb{Q}$, where A is an elliptic curve of conductor N. So we get the modular parametrization $\phi : X_0(N) \to A$. The pull-back of a global Néron differential ω_A of A to $\mathfrak{h}$ has the form $2\pi i c_f f(z)dz$ for a certain rational number c_f called the *Manin constant* of f, which we assume to be positive by adjusting the sign of ω_A. It is known that c_f is an integer [30] and it is conjectured that $c_f = 1$. The latter is proved in the case when A has semi-stable reduction (i.e. N squarefree) by work of Mazur [70], Abbes-Ullmo-Raynaud [1], and Cesnavicius [16]. See [2] for further results and references.

In the additive reduction case (i.e. N is allowed to have repeated prime factors) not much is known. We can mention that some special cases of additive reduction at primes $p > 7$ have been considered by Edixhoven [30], but in general it is not clear how to control the Manin constant beyond the semi-stable case. We prove a general result in the case of additive reduction: If additive reduction is restricted to a fixed finite set of primes, then c_f is uniformly bounded.

Theorem 1.3 (Bounding the Manin constant; cf. Corollary 10.2)**.** *Let S be a finite set of primes. There is a positive integer $\mathscr{M}_S$ that only depends on S such that the following holds:*

Let N be a positive integer which is squarefree away from S (i.e. if $p^2|N$ for a prime p, then $p \in S$). Let $f \in S_2(N)$ be a Fourier normalized Hecke newform with rational Hecke eigenvalues. Then the associated Manin constant satisfies $c_f \leq \mathscr{M}_S$.

Besides the applications in the theory discussed in this work, the previous result also fills a gap in the literature concerning the equivalence of the *height conjecture* and the *modular degree conjecture* for elliptic curves over $\mathbb{Q}$, see Remark 3.3.

Take N a positive integer and $f \in S_2(N)$ a Fourier normalized Hecke newform with rational eigenvalues as above. A factorization $N = DM$ is *admissible* if D the product of an even number of different primes and $(D, M) = 1$. For such a factorization we have a Shimura curve $X_0^D(M)$ over $\mathbb{Q}$ attached to the quaternion algebra of discriminant D, with level $\Gamma_0^D(M)$. The Jacquet-Langlands correspondence applied to f gives an optimal quotient $q_{D,M} : J_0^D(M) \to A_{D,M}$ over $\mathbb{Q}$, where $J_0^D(M)$ is the Jacobian of $X_0^D(M)$ and $A_{D,M}$ is an elliptic curve isogenous to A over $\mathbb{Q}$. For an abelian variety B over $\mathbb{Q}$ and a prime p we write $\Phi_p(B)$ for the group of geometric components of the special fibre at p of the Néron model of B. At a prime $p|D$ the reduction of $J_0^D(M)$ is purely toric and the map $\Phi_p(J_0^D(M)) \to \Phi_p(A_{D,M})$ induced by $q_{D,M}$ has been considered by a number of authors [6, 85, 97, 77]. The question of whether this map is surjective has been considered in [77] in the case when N is squarefree but it remains open, despite the fact that it has been implicitly assumed as known elsewhere in the literature. In fact, in [77] some closely related constructions are given (outside the realm of modular and Shimura curves) where the analogous map is not surjective, which makes the problem rather delicate. We prove that this map is in fact almost-surjective, in the sense that the size of its cokernel can be uniformly bounded independently of N.

Theorem 1.4 (Bounds for the cokernel on component groups; cf. Theorem 6.17)**.** *There is a constant κ such that if N is a squarefree positive integer, $N = DM$ is an admissible factorization where M is not a prime number, and $q_{D,M} : J_0^D(M) \to A_{D,M}$ is an optimal elliptic curve quotient associated to a Fourier normalized Hecke newform $f \in S_2(N)$ with rational eigenvalues, then for each prime $p|D$ we have that*

$$\#\text{cokernel}(\Phi_p(J_0^D(M)) \to \Phi_p(A_{D,M})) \leq \kappa.$$

Beyond the semi-stable case, we also prove such a uniform bound for the cokernel in the case of Frey-Hellegouarch elliptic curves, see Theorem 6.17. The proof of our cokernel bounds has a somewhat unusual arithmetic input: We need various results on generalized Fermat equations, including those of Darmon and Granville [23] on the equation $Ax^p + By^q = Cz^r$.

Our interest in surjectivity of the induced map on components in the case of $p|D$, comes from the Ribet-Takahashi formula [85] which we now recall.

The endomorphism $q_{D,M} \circ q_{D,M}^\vee \in \mathrm{End}(A_{D,M})$ is multiplication by a positive integer that we denote by $\delta_{D,M}$. When $D = 1$ one has $\delta_{1,N} = \deg(\phi : X_0(N) \to A)$ and in general one can relate $\delta_{D,M}$ to the degree of a suitably chosen morphism $X_0^D(M) \to A_{D,M}$, although it is not exactly equal. The precise comparison of $\delta_{D,M}$ with the degree of a suitably constructed modular parametrization $X_0^D(M) \to A_{D,M}$ over $\mathbb{Q}$ is achieved in Corollary 5.3.

Ribet and Takahashi [85] compared $\delta_{1,N}$ to its quaternionic counterpart $\delta_{D,M}$ for general D provided that M is squarefree and it is not a prime. The formula is

$$\frac{\delta_{1,N}}{\delta_{D,M}} = \gamma \cdot \prod_{p|D} v_p(\Delta_A)$$

where γ is a certain rational number possibly depending on all the data, and supported only at primes ℓ where the Galois module $A[\ell]$ is reducible. For our applications it is crucial to control the error factor γ at all primes, even in cases where some Galois modules $A[\ell]$ are reducible. More precisely, we need to show that γ is a rational number of "small" height, since one of the main goals of this work is to give global estimates. Among other technical tools, Theorem 1.4 (and more generally, Theorem 6.17) allows us to do so.

Theorem 1.5 (Global comparison of $\delta_{1,N}$ and $\delta_{D,M}$; cf. Corollary 6.2)**.** *With the previous notation, suppose that either*

(i) *N is squarefree and M is not a prime number; or*
(ii) *A is isogenous to a Frey-Hellegouarch elliptic curve and M is divisible by at least two odd prime numbers.*

Then we have

$$\log\left(\prod_{p|D} v_p(\Delta_A)\right) = \log\delta_{1,N} - \log\delta_{D,M} + O\left(\frac{\log D}{\log\log D}\right)$$

where the implicit constant is absolute (in particular, independent of N or A).

We refer to Theorem 6.1 for a more general result allowing additive reduction at a given finite set of primes.

Let us now mention a result which is intrinsic about the arithmetic of quaternionic modular forms, independet of the discussion on modular parametrizations of elliptic curves. Consider a positive integer N and an admissible factorization $N = DM$ with $D > 1$ so that we are not in the case of the classical modular curve $X_0(N)$. Then $X_0^D(M)$ does not have cuspidal points and therefore, its modular forms do not have a Fourier expansion. Let us focus on $S_2^D(M)$, the space of weight 2 modular forms on $\mathfrak{h}$ associated to $X_0^D(M)$. As in the case of $X_0(N)$, we have an identification $S_2^D(M) \simeq H^0(X_0^D(M)_{\mathbb{C}}, \Omega^1_{X_0^D(M)_{\mathbb{C}}/\mathbb{C}})$. By lack of Fourier expansion, a natural definition of "integral" modular form can be given as follows.

The curve $X_0^D(M)$ has a standard integral model $\mathscr{X}_0^D(M)$ which is flat and projective over $\mathbb{Z}$, coming from certain moduli problem of "fake elliptic curves". We define a modular form in $S_2^D(M)$ to be *integral* if, under the previous identification, it belongs to $H^0(\mathscr{X}_0^D(M)^0, \Omega^1_{\mathscr{X}_0^D(M)/\mathbb{Z}})$ where $\mathscr{X}_0^D(M)^0$ is the smooth locus of $\mathscr{X}_0^D(M) \to \operatorname{Spec}\mathbb{Z}$ (the locus where the relative differentials give an invertible sheaf). We denote by $\mathscr{S}_2^D(M)$ the $\mathbb{Z}$-module of integral modular forms in $S_2^D(M)$.

The space $S_2^D(M)$ has a standard norm given by the (non-normalized) Petersson inner product, and a natural question of arithmetic relevance is: *How small is the shortest non-zero vector in $\mathscr{S}_2^D(M)$?* The analogous question for $D = 1$ can be approached by the q-expansion principle: Integrality on a formal neighborhood of the cusp $i\infty$ agrees with integrality of the Fourier expansion at this cusp, and the latter has direct implications for the problem of giving lower bounds for the Petersson norm. In absence of Fourier expansions the problem is much more difficult. We prove that the shortest non-zero vector of $\mathscr{S}_2^D(M)$ cannot be too small in terms of the level; more precisely, we prove a lower bound which is reciprocal of a power of $N = DM$, with no semi-stability restriction.

Theorem 1.6 (Integral forms are not too small; cf. Theorem 14.1)**.** *Given $\epsilon > 0$ there is a constant $C_\epsilon > 0$ depending only on ϵ such that the following holds:*

Let N be a positive integer and consider an admissible factorization $N = DM$ with $D > 1$. Every non-zero $h \in \mathscr{S}_2^D(M)$ has Peterson norm bounded from below by

$$\frac{C_\epsilon}{N^{\frac{5}{6}+\epsilon} \cdot M^{1/2}}.$$

Our method extends to higher weight forms. We only consider the case of weight 2 to simplify the exposition and because this is the case relevant for our intended applications.

The proof falls into the context of Arakelov geometry. First we compare the Petersson norm (which is an L^2-norm) to an L^∞-norm, which requires lower bounds for the injectivity radius of the complex curve $X_0^D(M)_\mathbb{C}$ (cf. Section 8). Then we reduce the problem to finding small values of integral modular forms, which in turn reduces to the problem of finding algebraic points which are conveniently located in the arithmetic surface $\mathscr{X}_0^D(M)$, and at the same time have small Arakelov height with respect to certain arithmetic Hodge bundle endowed with a hyperbolic metric. We construct the required points as Heegner points, for which height formulas are available when $M = 1$ (by results of Kudla-Rapoport-Yang [60, 61] and Yuan-Zhang [114] in the context of Colmez's conjecture). This can be suitably extended to our case (general M) by a local analysis of integral models (cf. Section 9). However, the precise choice of Heegner points is not straightforward and it involves analytic number theory (cf. Section 11) in order to ensure that the relevant points are in fact conveniently located (sieve theory) and that the height is small (averaging and zero-density estimates for L-functions due to Heath-Brown).

Most of the previous analysis regarding norms and Heegner points will also be carried out in more generality for Shimura curves over totally real fields, as this is necessary for our study of Szpiro's conjecture over such fields in Section 18. The appendix (by R. Lemke Oliver and J. Thorner) provides a suitable zero-density estimate in this context.

1.3. **Effective height bounds and congruences.** The modularity theorem for elliptic curves (cf. [109, 99, 10]) opens the possibility of studying Szpiro's conjecture over $\mathbb{Q}$ by means of modular forms. Such an approach was already considered in the eighties by Frey [36]; let us briefly recall this classical approach (cf. Section 3 for details).

Let E be an elliptic curve of conductor $N = N_E$. By the modularity theorem, there is an optimal modular parametrization $\phi : X_0(N) \to A$ for a certain elliptic curve A isogenous to E over $\mathbb{Q}$. A computation shows that $\log \Delta_E \leq 12h(E) + 16$ where $h(E)$ is the Faltings height of E, and that

$$h(E) \leq \frac{1}{2} \log \deg \phi + 9. \tag{1}$$

Hence, Szpiro's conjecture would follow if one can show that the modular degree $\delta_{1,N} = \deg \phi$ is bounded polynomially on the conductor N.

This approach was used by Murty and Pasten [74] to give explicit and effective bounds of the form

$$h(E) \ll N \log N \tag{2}$$

with good implicit constants, by first bounding the modular degree $\delta_{1,N}$. This leads to effective estimates for solutions of the S-unit equation, Mordell's equation, and other diophantine problems. See also [57]. These estimates are not only of theoretical interest; recently, they have been given a practical implementation by von Känel and Matschke [58].

Similarly, given an elliptic curve E over $\mathbb{Q}$ and an admissible factorization $N = DM$ of its conductor, we have the optimal quotients $q_{D,M} : J_0^D(M) \to A_{D,M}$ with $A_{D,M}$ isogenous to E over $\mathbb{Q}$, and the associated quantities $\delta_{D,M} = \delta_{D,M}(E)$. A natural question is whether bounds for the numbers $\delta_{D,M}(E)$ are useful in the study of Szpiro's conjecture, beyond the classical case $D = 1$.

We show that this is indeed the case, despite the fact that for classical modular parametrizations the argument heavily uses q-expansions at cuspidal points of $X_0(N)$, while cuspidal points and q-expansions are not available when $D > 1$.

Theorem 1.7 (cf. Theorem 7.6)**.** *Let $\epsilon > 0$. For all elliptic curves E of conductor $N \gg_\epsilon 1$ (with an effective implicit constant), and for any admissible factorization $N = DM$ we have*

$$\log|\Delta_E| < (6+\epsilon)\log\delta_{D,M}(E) \quad \textit{and} \quad h(E) < \left(\frac{1}{2}+\epsilon\right)\log\delta_{D,M}(E).$$

This result is obtained from Theorem 6.1, which is a stronger and more precise version of Theorem 1.5. The motivation for using $\delta_{D,M}$ instead of simply using $\delta_{1,N}$ is practical: For an admissible factorization $N = DM$, the curve $X_0^D(M)$ usually has genus smaller than that of $X_0(N)$, which can be expected to lead to bounds for $\delta_{D,M}$ of better quality than for $\delta_{1,N}$. In order to make this expectation precise we need to discuss congruences of modular forms.

Classically, to bound the modular degree $\delta_{1,N}$ one relies on a theorem of Ribet [112, 18, 3]. Let $f \in S_2(N)$ be the Hecke newform attached to an elliptic curve $E/\mathbb{Q}$ of conductor N, and let m_f be the largest positive integer such that for some $g \in S_2(N)$ orthogonal to f (with respect to the Petersson inner product) with Fourier coefficients in $\mathbb{Z}$, we have that $f \equiv g \mod m_f$ in terms of Fourier expansion. The number m_f is called the congruence modulus of f and Ribet's theorem says that $\delta_{1,N}|m_f$. Thus, an approach to bound $\delta_{1,N}$ consists of controlling possible congruences of f with other modular forms in $S_2(N)$ with Fourier coefficients in $\mathbb{Z}$ —this is precisely how the estimate (2) is proved in [74].

It is natural to expect that a similar approach should allow one to bound $\delta_{D,M}$ in terms of congruences, which in principle should lead to better bounds since the Jacquet-Langlands transfer gives an isomorphism of $S_2^D(M)$ with the D-new part of $S_2(N)$ (as opposed to the whole space). Unfortunately this is not clear: The lack of Fourier expansions when $D > 1$ leaves us with no obvious analogue of Ribet's theorem.

We provide an alternative method based on congruences of systems of Hecke eigenvalues (thus only involving eigenforms) instead of Fourier expansions of all modular forms orthogonal to a given $f \in S_2(N)$. For an admissible factorization $N = DM$ we let $\mathbb{T}_{D,M}$ be the Hecke algebra acting on $S_2^D(M)$, and for a system of Hecke eigenvalues $\chi : \mathbb{T}_{D,M} \to \bar{\mathbb{Q}}$ we let $[\chi]$ be the class of its Galois conjugates. Given a $\mathbb{Z}$-valued system of Hecke eigenvalues $\chi_0 : \mathbb{T}_{D,M} \to \mathbb{Z}$ and a different system of Hecke eigenvalues $\chi : \mathbb{T}_{D,M} \to \bar{\mathbb{Q}}$, we define the congruence modulus $\eta_{[\chi_0]}([\chi]) := [\mathbb{Z} : \chi_0(\ker(\chi))]$; this is a well-defined positive integer that measures congruences between χ_0 and χ in a precise way (cf. Proposition 5.4, which also gives a way to estimate these numbers).

Theorem 1.8 (Hecke eigenvalue congruences; cf. Theorem 5.5)**.** *Let $\chi_0 : \mathbb{T}_{D,M} \to \mathbb{Z}$ be the system of Hecke eigenvalues attached to an elliptic curve $E/\mathbb{Q}$ of conductor N, where $N = DM$ is an admissible factorization. The number $\delta_{D,M}$ divides*

$$\prod_{[\chi]\neq[\chi_0]} \eta_{[\chi_0]}([\chi]).$$

The product runs over all classes $[\chi]$ of systems of Hecke eigenvalues on $\mathbb{T}_{D,M}$ different from $[\chi_0]$.

This result is related to the notion of "primes of fusion" of Mazur, but for our purposes it is not enough to only have information of the primes that support these congruences.

The previous theorem gives a way to estimate $\delta_{D,M}$ and thus to apply Theorem 1.7. Let us state here the case of restricted additive reduction (this is of practical interest —for instance, applications to S-unit equations only need to allow additive reduction at 2). See Section 7 for more precise and general results. Here, φ is Euler's function.

Theorem 1.9. *(cf. Corollary 7.8) Let S be a finite set of primes and let P be the product of the elements of S. For $\epsilon > 0$ and $N \gg_{\epsilon,S} 1$ (with an effective implicit constant), if E is an elliptic curve over $\mathbb{Q}$ semi-stable away from S, then we have*

$$h(E) < \begin{cases} \frac{P}{\varphi(P)}\,(\epsilon + 1/48)\,\varphi(N)\log N & \textit{unconditional} \\ \frac{P}{\varphi(P)}\,(\epsilon + 1/24)\,\varphi(N)\log\log N & \textit{under GRH.} \end{cases}$$

If $S = \emptyset$ then the factor $P/\varphi(P)$ is 1, and for P large enough one has $P/\varphi(P) < 2\log\log P$.

We observe that these estimates are better than (2), and that we were able to get an improvement under GRH. This last feature is due to the fact that Theorem 1.8 concerns congruences of Hecke eigenforms (whose L-functions and Rankin-Selberg L-functions are expected to satisfy GRH) while the method of using Ribet's congruence modulus m_f is not well-suited for an application of GRH as it concerns modular forms that are not necessarily eigenforms.

Although the classical case $D = 1$ is not the main intended application of Theorem 1.8, let us mention what happens here. When $D = 1$, our result gives better numerical estimates than by using Ribet's theorem on the congruence modulus m_f (the method used in [74]). Since our estimates in the case $D = 1$ are superior to the bounds recently used in [58] for solving a number of Diophantine equations, we spell out the precise bounds in Theorem 7.5. For the moment, we mention that we obtain bounds of the form

$$h(E) < \left(\frac{1}{48} + \epsilon\right) N \log N$$

while the estimates in [74] with the improvements of [58] take the form

$$h(E) < \left(\frac{1}{16} + \epsilon\right) N \log N.$$

1.4. **Product of valuations.** For a prime number p, we let $v_p : \mathbb{Q}^\times \to \mathbb{Z}$ be the p-adic valuation.

One of the main consequences of the new techniques introduced in this work is the fact that we provide a natural framework for proving global estimates on the products of p-adic valuations. For instance, in the context of the *abc* conjecture we obtain the following unconditional result.

Theorem 1.10 (Product of valuations for *abc* triples; cf. Theorem 16.7)**.** *Let $\epsilon > 0$. There is a number $K_\epsilon > 0$ depending only on ϵ such that for all coprime positive integers a, b, c with $a + b = c$ we have*

$$\prod_{p|abc} v_p(abc) < K_\epsilon \cdot \mathrm{rad}(abc)^{\frac{8}{3}+\epsilon}.$$

For comparison purposes, let us recall that the strongest unconditional results on the *abc* conjecture available in the literature have been obtained from the theory of linear forms in (p-adic) logarithms and take the form

$$\max_{p|abc} v_p(abc) < K_\epsilon \cdot \mathrm{rad}(abc)^{\alpha+\epsilon} \tag{3}$$

for a fixed positive exponent α, where the value $\alpha = 15$ was obtained by Stewart-Tijdeman in 1986 [93], $\alpha = 2/3$ was obtained by Stewart-Yu in 1991 [94], and $\alpha = 1/3$ was obtained by Stewart-Yu in 2001 [95]. Theorem 1.10 on the other hand gives a bound for the *product* (instead of the maximum) of the p-adic valuations in terms of a power of the radical. This is an intrinsic feature of our method as it naturally leads to global estimates with simultaneous contribution of several primes, as opposed to linear forms in p-adic logarithms where the contribution of each prime needs to be studied independently. Our result seems beyond the scope of what transcendental methods (linear forms in logarithms) can prove; see Paragraph 15.2 for details on this comparison, as well as the comments after Theorem 1.15.

An equivalent (and more elementary) formulation of Theorem 1.10 is the following.

Theorem 1.11 ("$d(abc)$-Theorem"; cf. Theorem 16.7)**.** *Let $\epsilon > 0$. There is a number $K_\epsilon > 0$ depending only on ϵ such that for all coprime positive integers a, b, c with $a + b = c$ we have*

$$d(abc) < K_\epsilon \cdot \operatorname{rad}(abc)^{\frac{8}{3}+\epsilon}.$$

Here, $d(n)$ is the number of divisors of a positive integer n.

The bound (3) provided by transcendental methods is equivalent to $\log c \ll_\epsilon \operatorname{rad}(abc)^{\alpha+\epsilon}$ (with the same exponent α) due to the ϵ in the exponent, and it is often stated in this way. Thus, it might also be instructive to compare the quantities $\log c$ and $d(abc)$ not just on theoretical grounds, but on actual examples instead. The next table records this comparison for the top five highest quality (in the standard terminology) known abc triples [90]:

a	b	c	$\log c$	$d(abc)$
2	$3^{10}109$	23^5	15.677...	264
11^2	$3^2 5^6 7^3$	$2^{21}23$	17.691...	11 088
$19 \cdot 1307$	$7 \cdot 29^2 31^8$	$2^8 3^{22} 5^4$	36.152...	223 560
283	$5^{11}13^2$	$2^8 3^8 17^3$	22.833...	23 328
1	$2 \cdot 3^7$	$5^4 7$	8.383...	160.

Our methods also allow us to prove analogous results for elliptic curves, see Section 16. For instance, we obtain

Theorem 1.12 (Product of valuations for elliptic curves; cf. Theorem 16.5)**.** *Let $\epsilon > 0$. There is a number $K_\epsilon > 0$ depending only on ϵ such that for every semi-stable elliptic curve E over $\mathbb{Q}$ we have*

$$\prod_{p|N_E} v_p(\Delta_E) < K_\epsilon \cdot N_E^{\frac{11}{2}+\epsilon}.$$

We refer the reader to Section 16 for this and other more general estimates. In fact, we also obtain similar results when additive reduction is allowed on a fixed finite set of primes, which is necessary in the proof of Theorem 1.10.

Before outlining an idea of how these results are proved, let us discus some applications.

First, let us consider Ribet's level-lowering theory [82]. For an elliptic curve E over $\mathbb{Q}$ and its associated newform $f \in S_2(N_E)$, this theory applies to primes ℓ dividing some exponent in the prime factorization of Δ_E (under some additional assumptions such as irreducibility of the Galois module $E[\ell]$) and it is interesting to know how many of these primes can an elliptic curve have. It turns out that not too many:

Theorem 1.13 (Counting level-lowering primes; cf. Corollary 16.6)**.** *For an elliptic curve E over $\mathbb{Q}$, let*

$$L(E) := \{\ell \text{ prime } : \exists p \text{ prime such that } p|N_E \text{ and } \ell | v_p(\Delta_E)\}.$$

There is a constant c such that for all semi-stable elliptic curves E over $\mathbb{Q}$ we have

$$\#L(E) < \frac{6 \log N_E}{\log \log N_E} + c.$$

A second application concerns a folklore (and widely believed) conjecture. For a prime number p and an elliptic curve E over $\mathbb{Q}$, the local Tamagawa factor is $\operatorname{Tam}_p(E) = [E(\mathbb{Q}_p) : E^0(\mathbb{Q}_p)]$ where $E^0(\mathbb{Q}_p)$ is the subgroup of points of $E(\mathbb{Q}_p)$ that extend to $\mathbb{Z}_p$-sections on the connected component of the Néron model of E over $\mathbb{Z}_p$. The global Tamagawa factor is then defined as $\operatorname{Tam}(E) = \prod_p \operatorname{Tam}_p(E)$ (usually called "fudge factor" in the context of the Birch and Swinnerton-Dyer conjecture).

Conjecture 1.14 (Fudge factors are small; folklore)**.** *Let $\epsilon > 0$. There is a constant K_ϵ depending only on ϵ such that for all elliptic curves E over $\mathbb{Q}$ we have* $\mathrm{Tam}(E) < K_\epsilon \cdot N_E^\epsilon$.

This conjecture often plays a role in the analysis of the special value formula in the Birch and Swinnerton-Dyer conjecture, and it is known that it follows from Szpiro's conjecture. More precisely, de Weger [107] and Hindry [49] have observed the following: A local analysis of the numbers $\mathrm{Tam}_p(E)$ shows that $\mathrm{Tam}(E) \le d(\Delta_E)^2$. Then the elementary divisor bound $d(n) < \exp(\kappa(\log n)/\log\log n)$ (for a suitable constant $\kappa > 0$; this is sharp up to the choice of κ) gives

$$\mathrm{Tam}(E) < \exp\left(\frac{2\kappa\log\Delta_E}{\log\log\Delta_E}\right).$$

Hence, Conjecture 1.14 would follow from a (conjectural) estimate of the form

$$\log\Delta_E =_{(?)} o\left((\log N_E)\log\log N_E\right).$$

In particular, it would follow from Szpiro's conjecture.

In unconditional grounds, our results on products of valuations allow us to prove:

Theorem 1.15 (Polynomial-in-conductor bound for the fudge factor; cf. Corollary 16.3 and Theorem 16.5)**.** *Let S be a finite set of primes and let $\epsilon > 0$. There is a number $K_{S,\epsilon} > 0$ depending only on ϵ and S such that for every elliptic curve E over $\mathbb{Q}$ satisfying*

(i) *is semi-stable away from S, and*

(ii) *E has at least two primes of multiplicative reduction,*

we have

$$\mathrm{Tam}(E) < K_{S,\epsilon} \cdot N_E^{\frac{11}{2}+\epsilon}.$$

Furthermore, when $S = \emptyset$ (i.e. for semi-stable elliptic curves) assumption (ii) can be dropped.

We observe that if instead of using our results on products of valuations one wants to prove Theorem 1.15 by means of the de Weger-Hindry approach, then one would need partial results for Szpiro's conjecture of the form

$$\log\Delta_E \le_{(?)} \left(\frac{11}{2}+\epsilon\right)(\log N_E)\log\log N_E + O_\epsilon(1).$$

At present, this is far beyond reach; such an estimate would be *exponentially* stronger than anything available today! In fact, the best available unconditional bounds for $\log\Delta_E$ in terms of N_E are of the form $\log\Delta_E \ll_\epsilon N_E^{\alpha+\epsilon}$ for some fixed $\alpha > 0$ (currently, the record is $\alpha = 1$ for all elliptic curves over $\mathbb{Q}$ [74], or $\alpha = 1/3$ for Frey-Hellegouarch elliptic curves [95]). It should be noted that Conjecture 1.14 is not a mild conjecture; it implies a sub-exponential version of Szpiro's conjecture of the form $\log\Delta_E \ll_\epsilon N_E^\epsilon$, which is currently an open problem.

Let us now give an idea of the technique used to prove our estimates on products of valuations. We recall that the classical modular approach to Szpiro's conjecture only focuses on modular parametrizations of the form $X_0(N) \to E$, while our results in Paragraph 1.3 consider, more generally, maps of the form $X_0^D(M) \to E$. However, here we consider a very different strategy. Namely, instead of trying to bound the degree of a map $X \to E$ in terms of the conductor of E, we consider several maps of this form for a fixed elliptic curve E while we let X vary over Shimura curves. Then our aim is to bound the *variation* of the degrees of such maps, not the degrees themselves.

Although at present it seems that bounding each $\delta_{D,M}$ polynomially on the conductor N is out of reach (in fact, such a bound would imply Szpiro's conjecture! cf. Theorem 1.7), it turns out that the comparison ratios $\delta_{1,N}/\delta_{D,M}$ are more accessible and we can unconditionally bound them polynomially on N. Furthermore, these bounds give valuable arithmetic information thanks to our extension of the Ribet-Takahashi formula (cf. Theorem 1.5 and more generally Theorem 6.1). This is how we approach the problem of bounding products of valuations.

The previous idea, however, only gives a starting point. The precise way in which we bound the ratios $\delta_{1,N}/\delta_{D,M}$ is rather delicate: First we express this ratio as a ratio of Petersson norms, which inevitably comes with a contribution of the Manin constant (including cases of additive reduction such as for Frey-Hellegouarch elliptic curves). The latter is controlled by our Theorem 1.3. Crucially, we need to show that the Petersson norm of certain quaternionic modular form is not too small, and this is done by Theorem 1.6, which, as explained before, requires a number of tools and techniques including Arakelov geometry, height formulas for Heegner points, and analytic number theory.

1.5. **Totally real case.** A limitation of the classical modular approach to Szpiro's conjecture by means of bounding the degree of modular parametrizations of elliptic curves, is that so far it is only available over $\mathbb{Q}$, while Szpiro's conjecture can also be formulated over number fields.

Namely, given a number field F and an elliptic curve E over F we let $\mathfrak{N}_E$ be the conductor ideal of E and we let N_E be its norm. Also, we let Δ_E be the norm of the discriminant ideal of E (this is compatible with our earlier notation in the case $F = \mathbb{Q}$).

Conjecture 1.16 (Szpiro [91])**.** *Let F be a number field. There is are constants $c, \kappa > 0$ depending only on F such that for all semi-stable elliptic curves E over F we have $\Delta_E < c \cdot N_E^{\kappa}$.*

Following Szpiro's formulation in [91], we only state this conjecture for semi-stable elliptic curves, but of course one can make a similar conjecture without that assumption.

One can also ask about the dependence of c and κ on F, and Szpiro [91] also suggests that any fixed $\kappa > 6$ should work, in which case c depends on the choice of κ and on the number field F in some unspecified manner. For a number field F we let d_F be the absolute value of its discriminant. General conjectures of Vojta [103, 104] suggest that one should be able to take $c = c(F)$ as a power of d_F provided that $[F : \mathbb{Q}]$ remains bounded. Parshin [78] proved that such a dependence on F would follow from a conjectural Bogomolov-Miyaoka-Yau inequality in arithmetic. See also [49] where Hindry notes that this expectation would also follow from a generalization of Szpiro's conjecture to higher dimensional abelian varieties and restriction of scalars.

Our methods allow us to provide a modular approach to Szpiro's conjecture over totally real number fields analogous to the estimate (1) and to Theorem 1.7.

Theorem 1.17 (Modular approach to Szpiro's conjecture over totally real number fields; cf. Theorem 18.10)**.** *Let n be a positive integer. There is a constant $c_n > 0$ only depending on n such that the following holds:*

Let F be a totally real number field with $[F : \mathbb{Q}] = n$. Let E be a semi-stable elliptic curve over F which is modular over F and assume that the number of primes of bad reduction of E has opposite parity to n. Let X be the Shimura curve over F attached to an indefinite F-quaternion algebra of discriminant $\mathfrak{N}_E$ (which exists by the parity assumption) and let $\phi : X \to E$ be a non-constant morphism over F (which exists by the modularity assumption). Let $h(E)$ be the Faltings height of E. Then we have

$$h(E) < \frac{1}{2}\log(\deg\phi) + c_n \cdot (\log N_E + \log d_F)$$

and

$$\frac{1}{n}\log(\Delta_E) < 6\log(\deg\phi) + c_n \cdot (\log N_E + \log d_F)\,.$$

This reduces to Szpiro's conjecture over F to an appropriate upper bound for the minimal degree of maps of the form $X \to E$, thus providing an approach to Szpiro's conjecture over number fields other than $\mathbb{Q}$ by means of modularity techniques. The precise bound that we expect for the modular degree in this setting is formulated as Conjecture 18.11.

Furthermore, the dependence on F that we obtain in Theorem 1.17 is precisely through d_F in the expected way, which can be regarded as evidence towards this aspect of Szpiro's conjecture over a varying field F of bounded degree and Vojta's conjecture for algebraic points of bounded degree.

Let us make two technical remarks about the assumptions in Theorem 1.17.

- The parity assumption might be removed with additional technical work by considering Shimura curves associated to non-maximal compact open subgroups —for the sake of simplicity we only consider the maximal case here, but the necessary technical work is similar to our computations for the case $F = \mathbb{Q}$, done in Section 9. Alternatively, one can base change to a suitable auxiliary quadratic extension.
- The modularity assumption is, by now, a rather reasonable working hypothesis, thanks to the spectacular available progress on this matter. For instance, now it is known that all elliptic curves over real quadratic fields are modular [34].

We implement the previous two remarks in a concrete case, obtaining:

Theorem 1.18 (cf. Theorem 18.12)**.** *If the bound for the modular degree formulated in Conjecture 18.11 holds for modular elliptic curves over real quadratic fields and their totally real quadratic extensions, then there is an absolute constant $c > 0$ such that the following holds:*

For every real quadratic field F and every semi-stable elliptic curve E over F which does not have everywhere good reduction, we have

$$h(E) \leq c \cdot \log(d_F N_E) \quad \text{and} \quad \Delta_E \leq (d_F N_E)^c.$$

Note that the conclusion of the previous result does not require E to be modular; as we will see, modularity in the necessary cases holds by [34] and [29].

A modular parametrization ϕ as in Theorem 1.17 does not need to be minimal (its degree appears as an upper bound). The existence of these modular parametrizations under the assumption of modularity (for suitable conductors) is well-known in the context of the Birch and Swinnerton-Dyer conjecture, see for instance [113]. For our purposes, however, it is desirable to make the degree of modular parametrizations as small as possible. We give such an economic construction in Theorem 18.4 and Theorem 18.5.

Theorems 18.4 and 18.5 moreover compare $\deg \phi$ to a certain number δ_E which is analogous to the numbers $\delta_{D,M}$ from our discussion over $\mathbb{Q}$. This is relevant because our Theorem 1.8 admits a straightforward generalization to the setting of modular parametrizations over totally real fields, which allows us to bound δ_E in terms of congruences of systems of Hecke eigenvalues. From here, together with results on effective multiplicity one for GL_2, we can obtain *unconditional* bounds such as the following:

Theorem 1.19 (cf. Theorem 18.14)**.** *Let F be a totally real number field and let $\epsilon > 0$. For all semi-stable elliptic curves E over F satisfying that the number of places of bad reduction of E has opposite parity to $[F : \mathbb{Q}]$, we have $\log \delta_E \ll_{F,\epsilon} N_E^{1+\epsilon}$, hence*

$$h(E) \ll_{F,\epsilon} N_E^{1+\epsilon} \quad \text{and} \quad \log \Delta_E \ll_{F,\epsilon} N_E^{1+\epsilon}.$$

Note that here we do not need to assume modularity. This is thanks to results in [34], cf. Theorem 18.14 below. Also, the parity assumption is not essential (it can be relaxed by an argument along the lines of Section 9, as mentioned above) and we include it only to simplify the proofs.

The dependence of number $K_{F,\epsilon}$ on F comes from two sources: An application of Faltings theorem for rational points on curves used in the modularity theorems of [34], and the existing literature on effective multiplicity one for GL_2 over number fields. As proved in [34], for real quadratic F one can avoid the use of Faltings theorem and obtain a completely explicit modularity theorem. Thus, in order to get an explicit dependence on F (at least for real quadratic fields) in Theorem 1.19 one would need effective multiplicity one for GL_2 over *varying* number fields, which seems to be an interesting open problem in analytic number theory. See [11, 66, 106] for the case of a fixed number field, which is what we use for Theorem 1.19.

Let us briefly outline the ideas in the proof of Theorem 1.17. Unlike Theorem 1.7, when $F \neq \mathbb{Q}$ we are left with no choice of Shimura curve with cuspidal points, which forces us to intrinsically work on the compact quotient case. We show that for a suitably metrized line sheaf $\hat{\omega}$ (which is *not* the Arakelov canonical sheaf) on an integral model of the elliptic curve E and for well-chosen algebraic points $P \in E(\bar{F})$, one has $h(E) = h_{\hat{\omega}}(P)$ where $h(E)$ is the Faltings height of E and $h_{\hat{\omega}}(P)$ is the Arakelov height of P. Suitable choice of quadratic CM extensions K/F and their associated Heegner points $P_K \in X(\bar{F})$ provide an acceptable choice of $P = \phi(P_K)$ and, up to carefully comparing the metrics, the problem now reduces to showing that such a Heegner point in X of small height (with respect to a metrized arithmetic Hodge bundle) does indeed exist.

The comparison of metrics yields a correction factor which accounts for the term $\log \deg \phi$ in the upper bound of Theorem 1.17, and it uses our $L^2 - L^\infty$ comparison of norms (cf. Section 8) already used in the proof of Theorem 1.6.

On the other hand, the construction of the Heegner points of small height is done in a way similar to that in the proof of our Theorem 1.6. Here, the technical difficulties are again coming from integral models and analytic number theory. The theory of Yuan and Zhang [114] provides the necessary material on integral models, the arithmetic Hodge bundle, and height formulas for Heegner points in Shimura curves in the totally real case. The necessary facts from analytic number theory are obtained from two sources: The construction of auxiliary CM extensions of F is reduced to a sieve theory problem over $\mathbb{Q}$ which is more approachable, while the zero-density estimates that we use (which are analogous to those of Heath-Brown that we use over $\mathbb{Q}$) were kindly provided to us by Lemke Oliver and Thorner in the Appendix —see also [63] by the same authors of the Appendix, which gives a zero-density estimate strong enough to prove, for instance, Theorem 1.17 in the case when F is obtained as a tower of cyclic extensions, such as needed for Theorem 1.18.

1.6. **Other references.** We conclude this introduction by briefly recalling some literature around the *abc* conjecture, although only tenuously related to our work. We are not attempting to make a survey on the *abc* conjecture and the list is by no means complete, but we feel that it is close in taste to the topics in this article.

First, we mention that in [33] the set of elliptic curves failing Szpiro's conjecture (over $\mathbb{Q}$, for a given exponent) is shown to be small in a precise asymptotic sense.

In [101], Ullmo gave estimates for the Faltings height of $J_0(N)$ when N is squarefree coprime to 6. He conjectured that the Faltings height of $J_0(N)$ is somewhat evenly distributed among the simple factors of $J_0(N)$ according to their dimension, which would imply a form of Szpiro's conjecture thanks to his height estimates.

In [79], Prasanna established integrality results in the context of the Jacquet-Langlands correspondence for Shimura curves, which allowed him to compute local contributions of the Faltings height of jacobians of Shimura curves over $\mathbb{Q}$ away from an explicit set of primes.

In [35], Freixas i Montplet used the Jacquet-Langlands correspondence to compute Arakelov-theoretic invariants of certain Shimura curves over $\mathbb{Q}$, but only after discarding the contribution of finitely many primes.

Despite all this progress, the computation (or asymptotic evaluation) in terms of the level of the Faltings height of the jacobian of quaternionic Shimura curves remains open. This is not used in our work.

From a completely different angle, S.-W. Zhang [116] showed that appropriate bounds on the height of the Gross-Schoen cycle in triple products of curves, would imply the *abc* conjecture.

Ullmo [102] obtained higher dimensional analogues of part of the results of Ribet and Takahashi [85], and used them to prove the existence of level-lowering congruences of modular forms in some cases by showing *lower* bounds for the Hida constant —a higher dimensional analogue of the modular degree. However, no connections with the *abc* conjecture are established (the latter seems to be closer to the problem of giving upper bounds for the Hida constant).

Regarding the *abc* conjecture for number fields other than $\mathbb{Q}$, the method of linear forms in logarithms is available and it has been worked out by Surroca [96] obtaining effective unconditional exponential bounds. Sharper exponential bounds have been proved by Győry [45]. However, as in the case of $\mathbb{Q}$, this approach has well understood technical limitations; see Baker's article [7] for a discussion on conjectural strengthenings to the theory of linear forms in logarithms that would be needed in order to approach the *abc* conjecture.

2. General notation

For later reference, let us record here the basic notation used throughout the paper. Further notation and preliminary material will be introduced as needed.

If X and Y are function on some set with X complex valued and Y positive real valued, Landau's notation $X = O(Y)$ means that there is a constant $c > 0$ such that $|X| \le c \cdot Y$ pointwise. This means exactly the same as Vinogradov's notation $X \ll Y$. For instance, $X = O(1)$ (or equivalently, $X \ll 1$) means that X is a bounded function. The number c in the previous definition is referred to as "implicit constant". If the implicit constant depends on any choice of other parameters, this will always be indicated as a subscript in the notation O or $\ll$. It is also customary to write $X \asymp Y$ when both $X \ll Y$ and $Y \ll X$ hold.

We will be using the following arithmetic functions: $\varphi(n)$ is the Euler totient function, $d(n)$ is the number of divisors of n, $\sigma_1(n)$ is the sum of the divisors of n, $\omega(n)$ is the number of distinct prime divisors of n, and $\mu(n)$ is the Möbius function.

Recall from the introduction that for a number field F the absolute value of its discriminant is d_F. Also, if E is an elliptic curve over F, we write $\mathfrak{N}_E$ for its conductor ideal, whose norm is denoted by N_E. We write Δ_E for the norm of the minimal discriminant ideal of E.

Note that when $F = \mathbb{Q}$, the absolute value of the minimal discriminant of E is precisely Δ_E, and the conductor of E equals N_E. We will often write simply N instead of N_E if there is no risk of confusion. We will be willing to discard finitely many (isomorphism classes of) elliptic curves in several of our arguments, which is the same as letting N be large enough, by Shafarevich's theorem. Such a reduction is of course effective.

Let N be a positive integer. We will say that a factorization $N = DM$ is *admissible* if D, M are coprime positive integers with D being the product of an even number of distinct prime factors, possibly $D = 1$.

Given a positive integer N with an admissible factorization $N = DM$, we denote by $X_0^D(M)$ the canonical model over $\mathbb{Q}$ (determined by special points) of the compact Shimura curve associated to an Eichler order of index M for the quaternion $\mathbb{Q}$-algebra of discriminant D. The particular case $D = 1, M = N$ is simply denoted by $X_0(N)$. The Jacobian of $X_0^D(M)$ (resp. $X_0(N)$) is denoted by $J_0^D(M)$ (resp. $J_0(N)$). Later, in Section 4, we will review in closer detail some relevant facts about Shimura curves that will be needed in the arguments.

Write $S_2(N)$ for the complex vector space of weight 2 holomorphic cuspidal modular forms for the congruence subgroup $\Gamma_0(N)$. Given an elliptic curve E over $\mathbb{Q}$, the modularity theorem [109, 99, 10] associates to E a unique Fourier-normalized Hecke eigenform $f \in S_2(N)$ with rational Hecke eigenvalues. Here, $N = N_E$ and f is a newform of level N. Associated to f, the Eichler-Shimura construction gives an optimal quotient $q_{1,N} : J_0(N) \to A_{1,N}$ defined over $\mathbb{Q}$, with $A_{1,N}$ isogenous to E. More generally, for each admissible factorization $N = DM$, the Jacquet-Langlands correspondence gives an optimal quotient $q_{D,M} : J_0^D(M) \to A_{D,M}$ defined over $\mathbb{Q}$, with $A_{D,M}$ isogenous to E. (As usual, the word "optimal" means "with connected kernel".)

In this setting, the (D,M)-*modular degree* of E (or simply *modular degree* if the pair (D,M) is understood), denoted by $\delta_{D,M}$ is defined as follows: The dual map $q_{D,M}^\vee : A_{D,M} \to J_0^D(M)$ satisfies that $q_{D,M} q_{D,M}^\vee \in \mathrm{End}(E)$ is multiplication by a positive integer, and $\delta_{D,M}$ is defined to be this integer. For $D = 1$, we simply call $\delta_{1,N}$ the modular degree of E. Although the notation $\delta_{D,M}$ does not indicate the elliptic curve E, these numbers do depend on E, and sometimes it will be convenient to make this dependence explicit by writing $\delta_{D,M}(E)$ instead.

The integers $\delta_{D,M}$ are a central object in this paper. We will see in Corollary 5.3 that they are "almost" equal to the degree of suitably chosen maps $\phi_{D,M} : X_0^D(M) \to E_{D,M}$, but a priori they cannot be interpreted in this way. In fact, for $D \neq 1$ the curve $X_0^D(M)$ does not have $\mathbb{Q}$-rational points (not even cuspidal points) so it is not a priori clear how to map $X_0^D(M)$ to $J_0^D(M)$.

In the particular case $D = 1$, however, the cusp $i\infty$ is $\mathbb{Q}$-rational and we can use it to define an embedding $j_N : X_0(N) \to J_0(N)$. The composition $\phi = q_{1,N} j_N : X_0(N) \to A_{1,N}$ is well-known to have degree $\delta_{1,N}$.

We will consider the pull-back of relative differentials in several contexts, so let us introduce the notation once and for all. Given morphisms of B-schemes $f : X \to Y$ for a base scheme B, the sheaf $f^*\Omega^1_{Y/B}$ is not in general a sub-sheaf of $\Omega^1_{X/B}$, and for sections $s \in H^0(V, \Omega^1_{Y/B})$ (V open in Y) the section f^*s belongs to $H^0(f^{-1}V, f^*\Omega^1_{X/B})$. Nevertheless, there is a canonical map $f_{X/Y/B} : f^*\Omega^1_{Y/B} \to \Omega^1_{X/B}$ sitting in the fundamental exact sequence $f^*\Omega^1_{Y/B} \to \Omega^1_{X/B} \to \Omega^1_{X/Y} \to 0$, and we define $f^\bullet s \in H^0(f^{-1}V, \Omega^1_{X/B})$ to be the image of f^*s under $f_{X/Y/B}$. A similar construction applies in the analytic setting.

3. Review of the classical modular approach

In this section we recall the classical modular approach to the *abc* conjecture and Szpiro's conjecture. Except for Remark 3.3 below (which fills a gap in the literature), everything in this section is well-known and we include it for later reference, and to clarify the similarities and differences with our approach in other parts of the paper. In fact, none of our results stated in the introduction is obtained directly from the classical approach reviewed in this section, although some of the ideas will be useful.

Given a triple a, b, c of coprime positive integers with $a + b = c$, the Frey-Hellegouarch elliptic curve $E_{a,b,c}$ is defined by the affine equation

$$y^2 = x(x-a)(x+b).$$

One directly checks that $E_{a,b,c}$ is semi-stable away from 2. Furthermore (cf. p.256-257 in [89]), $\Delta_{E_{a,b,c}} = 2^s(abc)^2$ and $N_{E_{a,b,c}} = 2^t \mathrm{rad}(abc)$ for integers s, t with $-8 \le s \le 4$ and $-1 \le t \le 7$. See [28] for a detailed analysis of the local invariants at $p = 2$ (possibly after twisting $E_{a,b,c}$ by -1). From here, it is clear that Conjecture 1.1 implies Conjecture 1.2 and that any partial result for Conjecture 1.1 which applies to Frey-Hellegouarch elliptic curves yields a partial result for the *abc* conjecture.

For an elliptic curve E over $\mathbb{Q}$, let $h(E)$ be the Faltings height of E over $\mathbb{Q}$ (this is not the semi-stable Faltings height). For ω_E a global Néron differential of E we have

$$h(E) = -\frac{1}{2} \log \left(\frac{i}{2} \int_{E(\mathbb{C})} \omega_E \wedge \overline{\omega_E} \right).$$

Furthermore, by a formula of Silverman [88] we get

$$\log \Delta_E \le 12h(E) + 16. \tag{4}$$

At this point it is appropriate to recall:

Conjecture 3.1 (Height conjecture, cf. [36]). *There is a constant κ such that for all elliptic curves E over $\mathbb{Q}$ we have $h(E) < \kappa \cdot \log N_E$.*

By the previous discussion, the height conjecture implies Szpiro's conjecture.

We have the standard modular parameterization $\phi = q_{1,N} j_N : X_0(N) \to A_{1,N}$ whose degree is $\delta_{1,N} = \delta_{1,N}(E)$. The degree of a minimal isogeny between $A_{1,N}$ and E is uniformly bounded by 163 thanks to Mazur [70] and Kenku [59], so Lemma 5 in [32] gives

$$|h(A_{1,N}) - h(E)| \le \frac{1}{2}\log 163 < 3.$$

Let $f \in S_2(N)$ be the associated normalized Hecke eigenform and let c_f denote the (positive) Manin constant of the optimal quotient $A_{1,N}$, which is defined as the absolute value of the scalar c satisfying that the pull-back of the Néron differential $\omega_{A_{1,N}}$ to $\mathfrak{h}$ via the composition $\mathfrak{h} \to X_0(N) \to A_{1,N}$ is $2\pi i c f(z)dz$. The Manin constant is a positive integer (cf. [30]); further details on the Manin constant will be discussed in Section 10.

Let us fix the notation

$$\mu_{\mathfrak{h}}(z) = \frac{dx \wedge dy}{y^2} \qquad (z = x + yi \in \mathfrak{h})$$

for the usual hyperbolic measure on $\mathfrak{h}$.

Frey [36] observed that by pulling-back the $(1,1)$-form $\omega_{A_{1,N}} \wedge \overline{\omega}_{A_{1,N}}$ from $A_{1,N}$ to $X_0(N)$, one obtains

$$\log \delta_{1,N}(E) = 2\log(2\pi c_f) + 2\log(\|f\|_{2,\Gamma_0(N)}) + 2h(A_{1,N}) \tag{5}$$

where the Petersson norm of f is given by

$$\|f\|^2_{2,\Gamma_0(N)} := \int_{\Gamma_0(N)\backslash\mathfrak{h}} |f(z)|^2 y^2 d\mu_{\mathfrak{h}}(z).$$

Since the Manin constant c_f is a positive integer and since f has Fourier coefficients in $\mathbb{Z}$, one finds by integrating $f \cdot \bar{f}$ on $\{z \in \mathfrak{h} : |x| < 1/2 \text{ and } y > 1\}$ that

$$\log(2\pi c_f) + \log(\|f\|_{2,\Gamma_0(N)}) > -6.$$

(Actually, as pointed out in [73], one has $2\log \|f\|_{2,\Gamma_0(N)} \sim \log N$ with an effective error term by [50], but the previous lower bound is trivial and sufficient for our current purposes.) Therefore by (5) we obtain

$$h(E) \le h(A_{1,N}) + 3 \le \frac{1}{2}\log \delta_{1,N} + 9. \tag{6}$$

Thus, the height conjecture (and hence, Szpiro's conjecture) would follow from the following:

Conjecture 3.2 (Modular degree conjecture; cf. [36]). *As E varies over elliptic curves over $\mathbb{Q}$, we have*

$$\log \delta_{1,N}(E) \ll \log N_E.$$

Remark 3.3. Actually, Frey formulated in [36] the modular degree conjecture as the (seemingly weaker) bound $\log(\delta_{1,N}/c_f^2) \ll \log N_E$, which has exactly the same consequences for Szpiro's conjecture. It is this version involving the Manin constant which is known to be equivalent to the height conjecture, see [68]. Other expositions (such as [92] or [73]) formulate the degree conjecture as we did above in Conjecture 3.2, but at present it is not clear that this version is equivalent to the height conjecture. Our bounds for the Manin constant (cf. Corollary 10.2) show that this is indeed the case if additive reduction is restricted to a fixed finite set of primes, such as for Frey-Hellegouarch elliptic curves. The latter fills a gap in Theorem 1 of [73] (repeated elsewhere in the literature) concerning the equivalence of the *abc* conjecture and the modular degree conjecture for Frey-Hellegouarch elliptic curves.

4. Preliminaries on Shimura curves

In this section we recall some facts about the theory of Shimura curves. We work over $\mathbb{Q}$ for simplicity, as this is the case that will be used most of the time in this work. Just in Section 18 we will need algebraic and arithmetic results about Shimura curves over totally real number fields, and the necessary facts will be recalled there.

The results in this section are by now standard. They can be found in [43], [87], and [115], among other references. We include them to fix the notation and to simplify the exposition.

4.1. **Shimura curves.** Let D be a squarefree positive integer with an even number of prime divisors, possibly $D = 1$. Let B the unique (up to isomorphism) quaternion $\mathbb{Q}$-algebra ramified exactly at the primes dividing D. For each prime $p \nmid D$ fix an isomorphism $B_p = M_2(\mathbb{Q}_p)$, and under this identification we take the maximal order $O_p = M_2(\mathbb{Z}_p)$. For $v|D$ we also let O_p denote a maximal order in the completion B_p. These choices determine a maximal order $O_B \subseteq B$ with $O_B \otimes \mathbb{Z}_p = O_p$ in B_p, for each prime p. We also fix an identification at the infinite place $B_\infty = M_2(\mathbb{R})$, which determines an action of $B^\times$ on $\mathfrak{h}^\pm = \mathbb{C} \smallsetminus \mathbb{R}$ by fractional linear transformations.

Let $\mathbb{A}^\infty = \mathbb{Q} \otimes \hat{\mathbb{Z}}$ be the ring of finite adeles of $\mathbb{Q}$. Let $\mathbb{B} := B \otimes \mathbb{A}^\infty$ and write $O_\mathbb{B} = O_B \otimes_\mathbb{Z} \hat{\mathbb{Z}}$, the maximal order in $\mathbb{B}$ induced by O_B. For each compact open subgroup $U \subseteq \mathbb{B}^\times$ let X_U be the compactified Shimura curve over $\mathbb{Q}$ associated to U. More precisely, the set of complex points of X_U is the complex curve

$$X_U^{an} = B^\times \backslash \mathfrak{h}^\pm \times \mathbb{B}^\times / U \cup \{cusps\}$$

and the model over $\mathbb{Q}$ is the canonical one defined in terms of special points. The cuspidal points are necessary only when $D = 1$. The curve X_U is irreducible over $\mathbb{Q}$.

4.2. **Projective system.** For $U \subseteq V$ compact open subgroups of $\mathbb{B}^\times$, the natural map $X_U \to X_V$ is defined over $\mathbb{Q}$, and they define a projective system $\{X_U\}_U$. The limit is a $\mathbb{Q}$-scheme X whose complex points are given by

$$X^{an} = B^\times \backslash \mathfrak{h}^\pm \times \mathbb{B}^\times \cup \{cusps\}.$$

The scheme X comes with a right $\mathbb{B}^\times$ action by $\mathbb{Q}$-automorphisms, under which $X/U \simeq X_U$. This right $\mathbb{B}^\times$ action is compatible with the right action on the projective system $\{X_U\}_U$ given by the F-maps $\cdot g : X_U \to X_{g^{-1}Ug}$ for $g \in \mathbb{B}^\times$.

4.3. **Components.** Let $\mathbb{Q}_+^\times$ be the set of strictly positive rational numbers. Let $B_+^\times$ be the subgroup of $B^\times$ consisting of elements with reduced norm in $\mathbb{Q}_+^\times$. Then $B_+^\times$ acts on the upper half plane $\mathfrak{h}$, and the natural map

$$B_+^\times \backslash \mathfrak{h} \times \mathbb{B}^\times / U \to B^\times \backslash \mathfrak{h}^\pm \times \mathbb{B}^\times / U$$

is an isomorphism. So, we can identify X_U^{an} with the compactification of the former. Let $\mathrm{rn} : \mathbb{B} \to \mathbb{A}^\infty$ be the reduced norm, then the connected components of X_U^{an} are indexed by the class group $C(U) := \mathbb{Q}_+^\times \backslash \mathbb{A}^{\infty,\times} / \mathrm{rn}(U)$ via the natural map induced by rn. The number of connected components of X_U^{an} is $h_U := \#C(U)$. The component associated to $a \in C(U)$ is denoted by $X_{U,a}^{an}$.

Given $g \in \mathbb{B}^\times$ define

$$\Gamma_{U,g} := gUg^{-1} \cap B_+^\times.$$

We see that $\Gamma_{U,g} \subseteq GL_2(\mathbb{R})^+$, and its image $\tilde{\Gamma}_{U,g}$ in $PSL_2(\mathbb{R})$ is a discrete subgroup acting on $\mathfrak{h}$ on the left. This gives rise to the (compactified) complex curve

$$X_{U,g}^{an} := \tilde{\Gamma}_{U,g} \backslash \mathfrak{h} \cup \{cusps\}$$

where the cusps are only needed if $D = 1$. It comes with the obvious complex uniformization

$$\xi_{U,g} : \mathfrak{h} \to X_{U,g}^{an}.$$

For each $a \in C(U)$ choose $g_a \in \mathbb{B}^\times$ with $[\mathrm{rn}(g_a)] = a$ in $C(U)$. One has the bi-holomorphic bijection

$$(7) \qquad \coprod_{a\in C(U)} \tilde{\Gamma}_{U,g_a}\backslash\mathfrak{h} \cup \{cusps\} \to X_U^{an}, \quad \tilde{\Gamma}_{U,g_a}\cdot z \mapsto [z, g_a]$$

respecting the projections onto $C(U)$. We can identify the component $X_{U,a}^{an}$ with X_{U,g_a}^{an}. Thus, after the choice of g_a for each $a \in C(U)$ is made, there is no harm in simplifying the notation as follows: $\Gamma_{U,a} = \Gamma_{U,g_a}$, $\tilde{\Gamma}_{U,a} = \tilde{\Gamma}_{U,g_a}$, and $X_{U,a}^{an} = X_{U,g_a}^{an}$.

Let H_U be the field extension of $\mathbb{Q}$ associated to $C(U)$ by class field theory. Each component $X_{U,a}^{an}$ has a model $X_{U,a}$ over H_U, so that $X_U \otimes H_U = \coprod_{a\in C(U)} X_{U,a}$.

4.4. **Heegner points.** We say that an imaginary quadratic field K satisfies the *Heegner hypothesis for D* if every prime $p|D$ is inert in K. In particular, $K/\mathbb{Q}$ is unramified at primes dividing D.

Let K satisfy the Heegner hypothesis for D. Then there is a $\mathbb{Q}$-algebra embedding $\psi : K \to B$ which is *optimal* in the sense that $\psi^{-1}O_B = O_K$; we fix such an optimal embedding. We have that $\psi(K^\times) \subseteq B_+^\times$ and there is a unique $\tau_K \in \mathfrak{h}$ which is fixed by all elements of $\psi(K^\times)$ (a more accurate notation would be $\tau_{K,\psi}$, but any other choice of optimal embedding leads to an equivalent theory). These choices determine the point

$$P_K = [\tau_K, 1] \in B_+^\times\backslash\mathfrak{h} \times \mathbb{B}^\times \subseteq X^{an}$$

which maps to a point $P_{K,U} \in X_U^{an}$ for each compact open subgroup U. The point P_K (hence, all the $P_{K,U}$) is algebraic and defined over K^{ab}, the maximal abelian extension of K. Since ψ was chosen as an optimal embedding, it follows from Shimura reciprocity that the point $P_{K,O_{\mathbb{B}}^\times}$ of $X_{O_{\mathbb{B}}^\times}$ has residue field H_K, the Hilbert class field of K.

We will refer to these points as *D-Heegner points*.

4.5. **Jacobians.** We adopt the convention that the Jacobian of an irreducible curve *is* the Albanese variety, so that its dual is the identity component of the Picard variety —this clarification is relevant in terms of functoriality. The Jacobian of X_U is denoted by J_U, and the torus of its complex points is J_U^{an}. Similarly, for $X_{U,a}$ its Jacobian is $J_{U,a}$, having $J_{U,a}^{an}$ as set of complex points. Note that J_U is defined over $\mathbb{Q}$ and $J_{U,a}$ is defined over H_U. Furthermore $J_{U,a}^{an}$ is the Jacobian of the irreducible complex curve $X_{U,a}^{an}$, while the points of J_U^{an} correspond to divisor classes on X_U^{an} having degree 0 on each component $X_{U,a}^{an}$, hence $J_U^{an} = \prod_{a\in C(U)} J_{U,a}^{an}$. This decomposition is defined over H_U, namely $J_U \otimes H_U = \prod_{a\in C(U)} J_{U,a}$.

4.6. **Modular forms and differentials.** The space of cuspidal holomorphic weight 2 modular forms for the discrete subgroup $\tilde{\Gamma}_{U,a}$ acting on $\mathfrak{h}$ is denoted by $S_{U,a}$ (the cuspidal condition is only needed when $D = 1$). All the curves $X_{U,a}^{an}$ have the same genus g_U, and the uniformization $\xi_{U,a} : \mathfrak{h} \to \tilde{\Gamma}_{U,a}\backslash\mathfrak{h}$ induces by pull-back an isomorphism $\Psi_{U,g_a} = \Psi_{U,a} : H^0(X_{U,a}^{an}, \Omega^1) \to S_{U,a}$ given by the condition that the image of a differential α is the modular form $\Psi_{U,a}(\alpha) \in S_{U,a}$ satisfying that

$$\xi_{U,a}^\bullet\alpha = \Psi_{U,a}(\alpha)dz$$

with z the complex variable on $\mathfrak{h}$. In particular $\dim S_{U,a} = g_U$. Thus we get isomorphisms

$$H^0(X_U, \Omega^1) \otimes \mathbb{C} \simeq H^0(X_U^{an}, \Omega^1) = \bigoplus_{a\in C(U)} H^0(X_{U,a}^{an}, \Omega^1) \simeq \bigoplus_{a\in C(U)} S_{U,a}.$$

The inner product $(-,-)_U$ on $H^0(X_U^{an},\Omega^1)$ is defined so that the direct summands $H^0(X_{U,a}^{an},\Omega^1)$ are orthogonal, and for $\omega_1,\omega_2\in H^0(X_{U,a}^{an},\Omega^1)$

$$(\omega_1,\omega_2)_U := \frac{i}{2}\int_{X_{U,a}^{an}} \omega_1\wedge\overline{\omega_2}.$$

The (non-normalized) Petersson inner product $\langle -,-\rangle_{U,a}$ on $S_{U,a}$ is defined by

$$\langle h_1,h_2\rangle_{U,a} := \int_{\tilde{\Gamma}_{U,a}\backslash\mathfrak{h}} h_1(z)\overline{h_2(z)}\Im(z)^2 d\mu_{\mathfrak{h}}(z)$$

for $h_1,h_2\in S_{U,a}$. We note that for $\omega_1,\omega_2\in H^0(X_{U,a}^{an},\Omega^1)$ we get

$$(\omega_1,\omega_2)_U = \langle \Psi_{U,a}(\omega_1),\Psi_{U,a}(\omega_2)\rangle_{U,a}.$$

Thus, $(-,-)_U$ will also be called the Petersson inner product.

4.7. **Classical subgroups.** Using the maximal order $O_{\mathbb{B}}$ of $\mathbb{B}$ we recall some standard choices for U. For a positive integer n, define $U^D(n)=(1+nO_{\mathbb{B}})^\times$. These open compact subgroups $U^D(n)$ determine a cofinal system in the projective system $\{X_U\}_U$. We say that a compact open U has level n if $U^D(n)\subseteq U$ and for every other positive integer n' with $U^D(n')\subseteq U$ we have $n|n'$.

For M coprime to D we define $U_0^D(M)$ prime by prime as follows. For $p\nmid M$ finite, we let $U_0^D(M)_p=O_p$, i.e. maximal at p. For $p|M$ the identification $B_p=M_2(\mathbb{Q}_p)$ allows us to define

$$U_0^D(M)_p=\left\{g\in GL_2(\mathbb{Z}_p): g\equiv\begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \mod M\right\}.$$

The subgroup $U_1^D(M)$ is defined similarly, except that the last condition is replaced by

$$U_1^D(M)_p=\left\{g\in GL_2(\mathbb{Z}_p): g\equiv\begin{bmatrix} * & * \\ 0 & 1 \end{bmatrix} \mod M\right\}.$$

Both $U_0^D(M)$ and $U_1^D(M)$ have level M.

For the groups $U^D(n)$, $U_0^D(M)$, and $U_1^D(M)$, the notation X_U is replaced by $X^D(n)$, $X_0^D(M)$, and $X_1^D(M)$ respectively (the upper script D keeps track of the quaternion algebra, up to isomorphism —all other relevant choices are implicit). Similarly for their Jacobians, sets of complex points, components, spaces of modular forms (always cuspidal of weight 2), etc. To simplify notation, we may omit the upper script D in the case $D=1$.

The reduced norm maps $U=U_0^D(M_1)\cap U_1^D(M_2)$ surjectively onto the maximal open compact subgroup $\hat{\mathbb{Z}}^\times\subseteq\mathbb{A}^{\infty,\times}$, so $C(U)$ is trivial in this case, as the narrow class number of $\mathbb{Q}$ is 1. Thus, the Shimura curve associated to a compact open subgroup of the form $U_0^D(M_1)\cap U_1^D(M_2)$ is geometrically connected.

4.8. **Hecke action.** (cf. [115] Sec. 1.4, 3.2) Let U be a compact open subgroup of $\mathbb{B}^\times$ of level m. Recall that for each positive integer n coprime to Dm one has a Hecke correspondence $T_{U,n}^c$ on X_U. It is defined over $\mathbb{Q}$ and has degree $\sigma_1(n)$, the sum of divisors of n, in the sense that the induced push-forward map $Div(X_U)\to Div(X_U)$ multiplies degrees by $\sigma_1(n)$.

Hecke correspondences generate a commutative ring $\mathbb{T}_U^c$. This ring acts (contravariantly) by endomorphisms on $H^0(X_U,\Omega^1)$ via pull-back and trace. Let $\mathbb{T}_U$ be the image of $\mathbb{T}_U^c$ in $\mathrm{End}_{\mathbb{Q}}H^0(X_U,\Omega^1)$, and denote by $T_{U,n}$ the image of $T_{U,n}^c$. The ring $\mathbb{T}_U^c$ also acts (covariantly) by endomorphisms on J_U, and the image of $\mathbb{T}_U^c$ in $\mathrm{End}_{\mathbb{Q}}J_U$ is isomorphic to $\mathbb{T}_U$. In fact, the action of $\mathbb{T}_U$ on J_U is compatible with that on $H^0(X_U,\Omega^1)$ in the following sense: The action of $\mathbb{T}_U$ on J_U induces by pull-back an action on $H^0(J_U,\Omega^1)$, and the canonical isomorphism $H^0(J_U,\Omega^1)\simeq H^0(X_U,\Omega^1)$ is $\mathbb{T}_U$-equivariant for this action.

4.9. **Systems of Hecke eigenvalues.** For M coprime to D and for $U = U_0^D(M)$ we write $\mathbb{T}_{D,M}$ instead of $\mathbb{T}_U$, similarly for the Hecke operators $\mathbb{T}_{D,M,n}$. The action of $\mathbb{T}_{D,M}$ on $V_{D,M} := H^0(X_0^D(M), \Omega^1) \otimes \mathbb{C}$ is simultaneously diagonalizable, which gives rise to systems of Hecke eigenvalues $\chi : \mathbb{T}_{D,M} \to \mathbb{C}$. Such a χ takes values in the ring of integers of a totally real number field. The associated isotypical subspaces $V_{D,M}^{\chi}$ are orthogonal to each other for the Petersson product.

If $m|M$ the map $X_0^D(M) \to X_0^D(m)$ induces by pull-back an inclusion $V_{D,m} \subseteq V_{D,M}$, which satisfies that for n coprime to DM one has $T_{D,M,n}|_{V_{D,m}} = T_{D,m,n}$. Hence we can lift systems of Hecke eigenvalues from $\mathbb{T}_{D,m}$ to $\mathbb{T}_{D,M}$. Those $\chi : \mathbb{T}_{D,M} \to \mathbb{C}$ arising in this way for $m|M$ with $m \neq M$ are called old, and the remaining χ are called new. The minimal $m|M$ from which χ arises is called the level of χ. Multiplicity one holds for the new eigenspaces, that is, if χ is new then $\dim V_{D,M}^{\chi} = 1$ (cf. [115]).

In the previous discussion, one can of course replace $V_{D,M}$ by $S_2^D(M) := S_{U_0^D(M)}$.

4.10. **Jacquet-Langlands.** Write $N = DM$ with M coprime to D and observe that our notation gives $S_2^1(N) = S_2(N)$ when $D = 1$, where as usual $S_2(N)$ denotes the space of weight 2 holomorphic cuspidal modular forms for the congruence subgroup $\Gamma_0(N)$.

For d a divisor of N, write $S_2(N)^d = \oplus_{d|\chi} S_2(N)^{\chi}$ where the notation " $d|\chi$ " means that χ varies over the systems of Hecke eigenvalues of $\mathbb{T}_{1,N}$ whose level is divisible by d. The Jacquet-Langlands correspondence gives an isomorphism

$$JL : S_2^D(M) \to S_2(N)^D$$

such that for every n coprime to N we have

$$JL \circ T_{D,M,n} = T_{1,N,n}|_{S_2(N)^D} \circ JL.$$

Hence, JL induces a quotient map $\mathbb{T}_{1,N} \to \mathbb{T}_{D,M}$ which realizes the systems of Hecke eigenvalues of $\mathbb{T}_{D,M}$ precisely as the systems of Hecke eigenvalues of $\mathbb{T}_{1,N}$ with level divisible by D.

4.11. **The Shimura construction.** We say that two systems of Hecke eigenvalues $\chi_1, \chi_2 : \mathbb{T}_{D,M} \to \bar{\mathbb{Q}}$ are equivalent if $\chi_1 = \sigma\chi_2$ for some automorphism $\sigma \in G_{\mathbb{Q}}$. The equivalence class of χ is denoted by $[\chi]$. Note that the degree of the field generated by the values of χ is $\#[\chi]$, and the property that $[\chi]$ be new is well-defined. All the elements of $[\chi]$ have the same kernel, which we denote by $\mathbb{I}_{[\chi]}$.

Given a class $[\chi]$ of systems of Hecke eigenvalues, define the (connected) abelian subvariety

$$K_{[\chi]} := \mathbb{I}_{[\chi]} \cdot J_0^D(M) \leq J_0^D(M).$$

Then $K_{[\chi]}$ is defined over $\mathbb{Q}$ and one obtains the quotient $q_{[\chi]} : J_0^D(M) \to A_{[\chi]}$ with kernel $K_{[\chi]}$, also defined over $\mathbb{Q}$. If $[\chi]$ is new, then the abelian variety $A_{[\chi]}$ is simple over $\mathbb{Q}$ and has dimension $\#[\chi]$. Since $K_{[\chi]}$ is $\mathbb{T}_{D,M}$-stable, $\mathbb{T}_{D,M}$ also acts on $A_{[\chi]}$ making $q_{[\chi]}$ Hecke equivariant.

Furthermore, $\mathrm{End}(A_{[\chi]})$ contains a ring $O_{[\chi]}$ isomorphic to $\chi(\mathbb{T}_{D,M})$ (for any χ in $[\chi]$) which is an order in a totally real field of degree $\#[\chi]$. Fixing any choice of χ and isomorphism $O_{[\chi]} \simeq \chi(\mathbb{T}_{D,M})$, we have that $\mathbb{T}_{D,M}$ acts on $A_{[\chi]}$ via χ. Thus, the kernel of $\mathbb{T}_{D,M} \to \mathrm{End}(A_{[\chi]})$ is precisely $\mathbb{I}_{[\chi]}$.

The maps $q_{[\chi]}$ induce an isogeny $J_0^D(M) \to \prod_{[\chi]} A_{[\chi]}$. Given any $[\chi]$ define $B_{[\chi]}$ as the identity component of the kernel of $J_0^D(M) \to \prod_{[\chi'] \neq [\chi]} A_{[\chi']}$. That is, $B_{[\chi]}$ is the identity component of $\bigcap_{[\chi'] \neq [\chi]} K_{[\chi']}$. The abelian variety $B_{[\chi]}$ is defined over $\mathbb{Q}$, it is stable under the action of $\mathbb{T}_{D,M}$, and it is the largest abelian subvariety of $J_0^D(M)$ on which $\mathbb{I}_{[\chi]}$ acts as 0. The composition $B_{[\chi]} \to J_0^D(M) \to A_{[\chi]}$ is an isogeny defined over $\mathbb{Q}$, thus, $J_0^D(M) = \sum_{[\chi]} B_{[\chi]}$.

5. The degree of Shimura curve parameterizations

5.1. **The modular degree.** In this section we fix an elliptic curve A over $\mathbb{Q}$ of conductor N which is an optimal quotient $q : J_0^D(M) \to A$ for an admissible factorization $N = DM$. The associated modular degree $\delta_{D,M}$ will be simply denoted by δ. The kernel of q is denoted by K, the image of $q^\vee : A \to J_0^D(M)$ is denoted by B, and the system of Hecke eigenvalues attached to A is denoted by χ_0. Note that χ_0 is $\mathbb{Z}$-valued. Also, since $q^\vee$ is an injective, we get an isomorphism $A[\delta] \to B[\delta] = K \cap B$ which respects both the Galois action and the Hecke action.

The goal of this section is to develop some tools to handle the quantity δ.

5.2. **Maps to the Jacobian.** Since $X_0^D(M)$ does not have a canonical embedding into $J_0^D(M)$ when $D > 1$, we cannot a priori interpret δ as the degree of a map $X_0^D(M) \to A$, unlike the case of classical modular parameterizations.

Let us momentarily address the general case. Let $U \subseteq \mathbb{B}^\times$ be a compact open subgroup of level m. Let $t : X_U \rightsquigarrow X_U$ be an algebraic correspondence defined over $\mathbb{Q}$ of degree 0 (meaning that it multiplies degrees of divisors by 0) with the following additional property (*): t maps complex points $x \in X_U^{an}$ to degree zero divisors $t(x)$ supported on the same complex component containing x. Then for each $a \in C(U)$ one gets a morphism $j_{t,a} : X_{U,a}^{an} \to J_{U,a}^{an}$, and via the canonical isomorphism $J_U^{an} = \prod_a J_{U,a}^{an}$ they descend to a morphism $j_t : X_U \to J_U$ defined over $\mathbb{Q}$. By construction, for each $a \in C_U^{an}$ the following diagram commutes:

$$\begin{tikzcd}
X_{U,a}^{an} \arrow[r] \arrow[d] & X_U^{an} \arrow[d] \\
Jac_{\mathbb{C}}(X_{U,a}^{an}) \arrow[r] & J_U^{an}.
\end{tikzcd}$$

We obtain a morphism $j_t^\bullet : H^0(J_U, \Omega^1) \to H^0(X_U, \Omega^1)$ which has no reason to be an isomorphism (e.g. take $t = 0$). Since the ring $\mathbb{T}_U^c$ of Hecke correspondences is commutative, we get that if in addition $t \in \mathbb{T}_U^c$, then for every n coprime to Dm we have $j_t^\bullet \circ T_{U,n} = T_{U,n} \circ j_t^\bullet$. In particular, the map $j_t^\bullet$ is $\mathbb{T}_U$-equivariant.

A particularly convenient choice of $t \in \mathbb{T}_U^c$ of degree 0 is given by the *Eisenstein correspondences*

$$E_{U,n}^c := T_{U,n}^c - \sigma_1(n) \cdot \Delta_U$$

where Δ_U is the diagonal correspondence of X_U, and n is coprime to Dm.

In the particular case $U = U_0^D(M)$, taking n coprime to $N = DM$ and recalling that $C(U_0^D(M))$ is trivial (thus, condition (*) trivially holds), we can define $j_{D,M,n} : X_0^D(M) \to J_0^D(M)$ as the map j_t with $t = E_{D,M,n}^c := E_{U_0^D(M),n}^c$. This need not be an embedding.

5.3. **Shimura curve parameterizations.** Returning to our setting $U = U_0^D(M)$ and the elliptic curve A arising as an optimal quotient $q : J_0^D(M) \to A$, for each n coprime to N we obtain a map

$$\phi_{D,M,n} = q j_{D,M,n} : X_0^D(M) \to A$$

defined over $\mathbb{Q}$.

Proposition 5.1. *The morphism $\phi_{D,M,n}$ is non-constant of degree $(a_n(A) - \sigma_1(n))^2 \cdot \delta$, where $a_n(A)$ is the n-th coefficient of the L-function of the elliptic curve A.*

Proof. Choose any complex point $p_0 \in X_0^D(M)^{an}$ and consider the embedding $j_{p_0} : X_0^D(M)^{an} \to J_0^D(M)^{an}$ over $\mathbb{C}$, given by $x \mapsto [x - p_0]$. One easily checks that the $\mathbb{C}$-map $\phi_{p_0} = q j_{p_0} : X_0^D(M)^{an} \to A_{\mathbb{C}}$ has degree equal to the modular degree δ.

Let $E_{D,M,n}$ be the image of $E^c_{D,M,n}$ under $\mathbb{T}^c_{D,M} \to \mathbb{T}_{D,M} \subseteq \mathrm{End}(J_0^D(M))$. A direct computation shows that for each complex point $x \in X_0^D(M)^{an}$

$$j_{D,M,n}(x) = (E_{D,M,n} \circ j_{p_0})(x) + j_{D,M,n}(p_0).$$

By the Eichler-Shimura congruence relation we have that $E_{D,M,n}$ acts on A as multiplication by $a_n(A) - \sigma_1(n)$. Composing with q we get that for every complex point $x \in X_0^D(M)^{an}$

$$\phi_{D,M,n}(x) = (a_n(A) - \sigma_1(n)) \cdot \phi_{p_0}(x) + \phi_{D,M,n}(p_0).$$

Note that $a_n(A) - \sigma_1(n) \neq 0$ by Hasse's bound. The result follows. □

Lemma 5.2. *For every positive integer N there is a prime $\ell \leq 2 + 2\log N$ with $\ell \nmid N$.*

Proof. This is an elementary fact, cf. [40]. □

Corollary 5.3. *With the previous notation, there is a non-constant morphism $\phi : X_0^D(M) \to A$ defined over $\mathbb{Q}$ such that δ divides $\deg \phi$ and moreover $\delta \leq \deg \phi \leq (9 \log N)^2 \cdot \delta$.*

Proof. In Proposition 5.1 we can choose $n = \ell$ a prime not dividing $N = DM$ of size $\ell \leq 2 + 2\log N < 3 \log N$ (as $N \geq 11$). Finally, by Hasse's bound we get

$$|a_\ell(A) - (\ell + 1)|^2 \leq (\ell + 2\ell^{1/2} + 1)^2 < 9\ell^2 < 81(\log N)^2.$$

□

5.4. **Spectral decomposition of the modular degree.** Given $[\chi]$ an equivalence class of systems of eigenvalues on $\mathbb{T}_{D,M}$ different to $[\chi_0]$, let us define the *congruence modulus*

$$\eta_{[\chi_0]}([\chi]) := [\mathbb{Z} \cdot f : \mathbb{I}_{[\chi]} \cdot f]$$

where f is any non-zero element of $V_{D,M}^{\chi_0}$ (unique up to scalar). It is easy to see that the primes dividing $\eta_{[\chi_0]}([\chi])$ correspond to congruence primes in a suitable sense, but more is true. This positive integer measures the congruences between the systems of Hecke eigenvalues χ and χ_0 in the following precise sense.

Proposition 5.4. *The number $\eta_{[\chi_0]}([\chi])$ is the largest positive integer m with the following property: Given any polynomial $P \in \mathbb{Z}[x_1, \ldots, x_\ell]$ and positive integers $n_1, \ldots, n_\ell$ coprime to N, if*

$$P(\chi(T_{D,M,n_1}), \ldots, \chi(T_{D,M,n_\ell})) = 0,$$

then m divides the integer $P(\chi_0(T_{D,M,n_1}), \ldots, \chi_0(T_{D,M,n_1}))$, which equals $P(a_{n_1}(A), \ldots, a_{n_\ell}(A))$.

Proof. Clear from the definitions and the relation between the values of χ_0 and the L-function of A given by the Eichler-Shimura congruence. □

The previous proposition not only justifies the name of the congruence modulus, but also, it will be useful for estimating the size of $\eta_{[\chi_0]}([\chi])$. In the classical setting of the modular curve $X_0(N)$, the numbers $\eta_{[\chi_0]}([\chi])$ measure congruences between *eigenforms* and can be computed using Fourier expansions (of course, in the more general setting the Fourier expansions are not available).

The relation with the (D, M)-modular degree is given by

Theorem 5.5. *The (D, M)-modular degree δ divides*

$$\prod_{[\chi] \neq [\chi_0]} \eta_{[\chi_0]}([\chi]).$$

The product runs over all classes $[\chi]$ of systems of Hecke eigenvalues on $\mathbb{T}_{D,M}$ different to $[\chi_0]$.

We give two different proofs of this fact, as they can be of independent interest.

5.5. **First proof: torsion of abelian varieties.** Enumerate the classes of systems of Hecke eigenvalues on $\mathbb{T}_{D,M}$ as $c_0, c_1, \dots, c_s$ with $c_0 = [\chi_0]$. Write A_j and B_j instead of A_{c_j} and B_{c_j}, in particular $A_0 = A$ and $B_0 = B$. Define the following abelian sub-varieties of $J_0^D(M)$:

$$C_i := \sum_{j=i+1}^{s} B_j, \quad i = -1, 0, 1, \dots, s.$$

For each $0 \le j \le s$ define $G_j = B_j \cap C_j$. Note that B_j/G_j is an abelian variety defined over $\mathbb{Q}$ with a natural $\mathbb{T}_{D,M}$-action, such that the quotient $B_j \to B_j/G_j$ is a $\mathbb{T}_{D,M}$-equivariant isogeny.

Consider the addition maps $\sigma_j : B_j \times C_j \to C_{j-1}$. Geometrically, their kernels are

$$\ker(\sigma_j) = \{(P, -P) : P \in G_j(\bar{F})\}.$$

If we compose the induced isomorphism $C_{j-1} \simeq (B_j \times C_j)/\ker(\sigma_j)$ with the projection onto B_j/G_j and restrict to $B_0 \cap C_{j-1}$, then for each $1 \le j \le s$ we obtain a map

$$u_j : B_0 \cap C_{j-1} \to B_j/G_j$$

defined over $\mathbb{Q}$. Note that u_j is $\mathbb{T}_{\mathfrak{D},\mathfrak{M}}$-equivariant with respect to the $\mathbb{T}_{D,M}$-actions on $B_0 \cap C_{j-1}$ and on B_j/G_j.

First proof of Theorem 5.5. Let p be a prime number and let $\alpha = v_p(\delta)$. We will show that p^α divides $\prod_{j=1}^{s} \eta_{c_0}(c_j)$.

We inductively define algebraic points $Q_j \in J_0^D(M)$ and integers $\gamma_j \ge 0$ for $0 \le j \le s$. Let $Q_0 \in B_0 \cap C_0 = B_0[\delta]$ be any algebraic point of order exactly p^α and set $\gamma_j = 0$. For $0 \le j < s$, let

$$\gamma_{j+1} := \min\{\gamma \ge 0 : p^\gamma Q_j \in C_{j+1}\} \quad \text{and} \quad Q_{j+1} := p^{\gamma_{j+1}} Q_j.$$

Note that γ_{j+1} exists and it is at most α, and that for each j we have that $Q_j \in C_j$. Also, Q_0 has order p^α and $Q_s = 0$ because $C_s = (0)$. All the points Q_j are multiples of Q_0 so that they have order a power of p, and more precisely for $1 \le j \le s$ we have that

$$\operatorname{ord}(Q_j) = \operatorname{ord}(Q_{j-1})/p^{\gamma_j}.$$

Hence, for each $0 \le j \le s$ we have $\operatorname{ord}(Q_j) = p^{\alpha - \sum_{i \le j} \gamma_i}$ and taking $j = s$ we get $\alpha = \sum_{i=0}^{s} \gamma_i$. Thus, it suffices to show that p^{γ_j} divides $\eta_{c_0}(c_j) = [\mathbb{Z}f : \mathbb{I}_{c_j} f]$ for each $1 \le j \le s$.

Let us fix an index $1 \le j \le s$. We have $Q_{j-1} \in B_0$ as it is a multiple of Q_0. Hence $Q_{j-1} \in B_0 \cap C_{j-1}$, thus we can evaluate u_j at Q_{j-1} to get the point $u_j(Q_{j-1}) \in B_j/G_j$.

We claim that p^{γ_j} divides $\operatorname{ord}(u_j(Q_{j-1}))$. If $\gamma_j = 0$ then there is nothing to prove, so let us consider the case $\gamma_j > 0$. Observe that $\operatorname{ord}(u_j(Q_{j-1}))$ is a power of p, so it suffices to show that given any integer $0 \le \gamma < \gamma_j$ one has $p^\gamma u_j(Q_{j-1}) \ne 0$. For the sake of contradiction, suppose that $p^\gamma u_j(Q_{j-1}) = 0$ for some $0 \le \gamma < \gamma_j$. Recall that $Q_{j-1} \in C_{j-1}$, and choose some $(Q'_{j-1}, Q''_{j-1}) \in \sigma_j^{-1}(Q_{j-1})$. Then $p^\gamma Q'_{j-1} \in G_j$ because $p^\gamma u_j(Q_{j-1}) = 0$. This means that $(-p^\gamma Q'_{j-1}, p^\gamma Q'_{j-1}) \in \ker(\sigma_j)$, and since $(Q'_{j-1}, Q''_{j-1}) \in \sigma_j^{-1}(Q_{j-1})$, we deduce that the following point is in $\sigma_j^{-1}(p^\gamma Q_{j-1}) \subseteq B_j \times C_j$:

$$(-p^\gamma Q'_{j-1}, p^\gamma Q'_{j-1}) + p^\gamma (Q'_{j-1}, Q''_{j-1}) = (0, p^\gamma Q_{j-1}).$$

In particular, $p^\gamma Q_{j-1} \in C_j$ which contradicts the minimality of γ_j. Thus, p^{γ_j} divides $\operatorname{ord}(u_j(Q_{j-1}))$.

Finally, take any $t \in \mathbb{I}_{c_j}$ and $0 \ne f \in V_{D,M}^{\chi_0}$. Then $tf = \chi_0(t)f$. Since t annihilates B_j, it also annihilates B_j/G_j, thus $t \cdot u_j(Q_{j-1}) = 0$. As $Q_{j-1} \in B_0$, we get $tQ_{j-1} = \chi_0(t)Q_{j-1}$ so that

$$0 = t \cdot u_j(Q_{j-1}) = u_j(tQ_{j-1}) = u_j(\chi_0(t)Q_{j-1}) = \chi_0(t)u_j(Q_{j-1}).$$

Thus $\operatorname{ord}(u_j(Q_{j-1}))$ divides $\chi_0(t)$, which gives $p^{\gamma_j} | \mu_t$. Therefore p^{γ_j} divides $[\mathbb{Z}f : \mathbb{I}_{c_j} f]$. □

5.6. **Second proof: projectors and the Hecke algebra.** Write $\mathbb{E} = \mathrm{End}(J_0^D(M))$. Then $\mathbb{E}$ has a right action via pull-back on $H^0(J_0^D(M)^{an}, \Omega^1)$ which is canonically isomorphic to $V_{D,M}$. This right action on $V_{D,M}$ extends the action of the commutative subring $\mathbb{T}_{D,M} \subseteq \mathbb{E}$. Since $\mathbb{E}$ acts faithfully on $V_{D,M}$ we can identify $\mathbb{E}^{op}$ with its image in $\mathrm{End}_{\mathbb{C}}(V_{D,M})$.

Let $\pi_0 \in \mathrm{End}_{\mathbb{C}}(V_{D,M})$ be the orthogonal projection (with respect to the Petersson inner product) onto the subspace $V_{D,M}^{\chi_0}$. Equivalently, π_0 is the projection onto the factor $V_{D,M}^{\chi_0}$ in the direct sum decomposition $V_{D,M} = \oplus_\chi V_{D,M}^{\chi}$.

Lemma 5.6. *$\pi_0 \in \mathbb{E}^{op} \otimes \mathbb{Q}$. Furthermore, the denominator of π_0 with respect to $\mathbb{E}^{op}$ is the modular degree δ. That is, δ is the least positive integer m with the property that $m\pi_0 \in \mathbb{E}^{op}$.*

Proof. In the case of the classical modular curve $X_0(N)$ this is proved in [18], see also [3]. The general case is not harder, and we include a proof for the convenience of the reader.

Consider the map $\varpi = q^\vee \circ q : J_0^D(M) \to J_0^D(M)$ where we recall that $q : J_0^D(M) \to A$. Note that $\varpi \in \mathbb{E}$ and $\varpi|_B : B \to B$ is multiplication by δ, by definition of the modular degree. Taking pull-back of holomorphic differentials and recalling the isogeny decomposition $J_0^D(M) \to \prod_{[\chi]} A_{[\chi]}$ we see that $\varpi = \delta\pi_0$ in $\mathrm{End}_{\mathbb{C}}(V_{D,M})$.

It only remains to prove that given any positive integer m such that $\varpi_m := m\pi_0$ is in $\mathbb{E}$, on has that δ divides m. In fact, take such an m. From the isogeny decomposition of $J_0^D(M)$ one deduces that $\varpi_m \cdot J_0^D(M) = B \subseteq J_0^D(M)$. Hence, we obtain a map $J_0^D(M) \to B \simeq A$ defined over $\mathbb{Q}$ whose restriction to B is multiplication by m. Recalling the definition of δ in terms of the optimal quotient map q, we see that δ divides m. □

Second proof of Theorem 5.5. For each system of Hecke eigenvalues $\chi : \mathbb{T}_{D,M} \to \bar{\mathbb{Q}}$, let L_χ be the totally real number field generated by $\chi(\mathbb{T}_{D,M})$. The rule $t \mapsto (\chi(t))_\chi$ defines a ring morphism

$$\psi : \mathbb{T}_{D,M} \to \prod_\chi L_\chi$$

which is injective because $\mathbb{T}_{D,M}$ acts faithfully on $V_{D,M} = \oplus_\chi V_{D,M}^{\chi}$.

For each class c of systems of Hecke eigenvalues on $\mathbb{T}_{D,M}$, define the ring $R_c := \prod_{\chi \in c} L_\chi$ so that we can re-write the previous ring morphism as

$$\psi : \mathbb{T}_{D,M} \to \prod_c R_c. \tag{8}$$

Fix a choice of non-zero $f \in V_{D,M}^{\chi_0}$. For each class $c' \neq [\chi_0]$, choose an element $t_{c'} \in \mathbb{I}_{c'}$ such that $t_{c'} \cdot f = \eta_{[\chi_0]}(c') \cdot f$. Then we have that the $[\chi_0]$-component of $\psi(t_{c'})$ in (8) is $\eta_{[\chi_0]}(c')$, while the c'-component of $\psi(t_{c'})$ is 0.

Finally, let $\varpi = \prod_{c \neq [\chi_0]} t_c \in \mathbb{T}_{D,M} \subseteq \mathbb{E}$ and observe that $\psi(\varpi) \in \prod_c R_c$ has the integer $\prod_{c \neq [\chi_0]} \eta_{[\chi_0]}(c)$ in the $[\chi_0]$-component, and 0 in all other components. It follows that

$$\varpi = \left(\prod_{c \neq [\chi_0]} \eta_{[\chi_0]}(c) \right) \pi_0,$$

and by Lemma 5.6 we get that δ divides $\prod_{c \neq [\chi_0]} \eta_{[\chi_0]}(c)$. □

6. A refinement of the Ribet-Takahashi formula

6.1. **Notation.** Consider an elliptic curve E defined over $\mathbb{Q}$ with conductor $N = N_E$. Recall that for each admissible factorization $N = DM$ we have the optimal quotients $q_{D,M} : J_0^D(M) \to A_{D,M}$ with modular degree $\delta_{D,M}$ respectively. The elliptic curves $A_{D,M}$ are isogenous over $\mathbb{Q}$ to E, although they need not be isomorphic.

In this section we consider E (and N) as varying. So, the implicit constants in error terms will always be independent of E. In fact, as always in this paper, any dependence of the implicit constants on other parameters will be indicated explicitly as a subscript.

6.2. **The formula.** Ribet and Takahashi (cf. [85] and [97]) proved a formula for the fraction $\delta_{1,N}/\delta_{D,M}$, which in the case when E has no non-trivial rational cyclic isogeny and M is squarefree but not prime, reads

$$\frac{\delta_{1,N}}{\delta_{D,M}} = \prod_{p|D} v_p(\Delta_E).$$

The requirement that M be squarefree can be relaxed to some extent. However, the above equality is known to be false in cases when E has non-trivial isogenies, and the formula of Ribet and Takahashi in the general case includes a correction factor which takes into account reducible residual Galois representations.

The correction factor is a rational number supported on primes ℓ for which the Galois representation $E[\ell]$ is reducible, although the exponents of those primes are not controlled in the literature.

For our purposes, we will need a version of the Ribet-Takahashi formula with finer control on this correction factor, not just the primes of its support. In our result, additional efforts are made in order to have refined estimates for semi-stable elliptic curves and for Frey-Hellegouarch elliptic curves, which are our main cases of interest —nevertheless, we also provide good estimates in the general case.

For an elliptic curve E over $\mathbb{Q}$ of conductor N with an admissible factorization $N = DM$, we define the positive rational number $\gamma_{D,M,E}$ by the formula

$$\frac{\delta_{1,N}}{\delta_{D,M}} = \gamma_{D,M,E} \cdot \prod_{p|D} v_p(\Delta_E). \tag{9}$$

This is the correction factor that we need to control.

For a positive rational number $x \in \mathbb{Q}_{>0}$ the numerator and denominator of x are the unique coprime positive integers a, b (respectively) with $x = a/b$. With this notation, we prove:

Theorem 6.1. *Let E be an elliptic curve over $\mathbb{Q}$ of conductor N and let $N = DM$ be an admissible factorization. The numerator of $\gamma_{D,M,E}$ is supported on primes ≤ 163 and it is bounded from above by $163^{\omega(D)}$. In particular, we have*

$$\log \delta_{1,N} \leq \log \delta_{D,M} + \log \left(\prod_{p|D} v_p(\Delta_E) \right) + 5.1 \cdot \omega(D). \tag{10}$$

Furthermore, the following upper bounds for the denominator of $\gamma_{D,M,E}$ hold:

(a) *Let S be a finite set of primes. There is a positive integer κ_S depending only on S and supported on primes ≤ 163 such that if E is semi-stable away from S, then the denominator of $\gamma_{D,M,E}$ is less than or equal to $\kappa_S^{\omega(D)} D$. In particular,*

$$\log \left(\prod_{p|D} v_p(\Delta_E) \right) \leq \log \delta_{1,N} - \log \delta_{D,M} + \log D + O_S(\omega(D))$$

where the implicit constant only depends on S.

(b) *There is an absolute integer constant $\kappa \geq 1$ supported on primes ≤ 163 which satisfies the following: Suppose that either*

(b.1) *E is semi-stable and M is not a prime number; or*

(b.2) *E is a Frey-Hellegouarch elliptic curve and M is divisible by at least two odd primes.*

Then the denominator of $\gamma_{D,M,E}$ divides $\kappa^{\omega(D)}$. In particular,

$$\log\left(\prod_{p|D} v_p(\Delta_E)\right) \le \log\delta_{1,N} - \log\delta_{D,M} + O(\omega(D))$$

where the implicit constant is absolute.

An immediate consequence is the following:

Corollary 6.2. *Let E be an elliptic curve of conductor N and consider an admissible factorization $N = DM$. Suppose that either*

(i) *E is semi-stable and M is not a prime number; or*

(ii) *E is a Frey-Hellegouarch elliptic curve and M is divisible by at least two odd prime numbers.*

Then we have that the logarithmic height of the rational number $\gamma_{D,M,E}$ is

$$h(\gamma_{D,M,E}) \ll \omega(D) \ll \frac{\log D}{\log\log D}$$

and in particular

$$\log\left(\prod_{p|D} v_p(\Delta_E)\right) = \log\delta_{1,N} - \log\delta_{D,M} + O\left(\frac{\log D}{\log\log D}\right)$$

where the implicit constants are absolute.

At this point, let us make a heuristic (and admittedly naive) remark. The estimates for $\gamma_{D,M,E}$ in the previous results say $\delta_{1,N}/\delta_{D,M}$ is approximately equal to $\prod_{p|D} v_p(\Delta_E)$ (after taking logarithms). This can be seen as an *arithmetic analogue of partial derivatives* in the following sense:

Given a monomial $x_1^{e_1}\cdots x_n^{e_n}$ and a subset $J \subseteq \{1,\dots,n\}$ we can recover the product of the exponents e_j for $j \in J$ as a "rate of change in the direction of the selected variables x_j for $j \in J$"

$$\prod_{j\in J} e_j = \frac{\partial^{|J|}}{\prod_{j\in J}\partial x_j} x_1^{e_1}\cdots x_n^{e_n}|_{\mathbf{x}=(1,\dots,1)}.$$

If we write the factorization $\Delta_E = \prod_{p|N} p^{v_p(\Delta_E)}$ and consider the expression on the right as a monomial, then "formal partial derivatives with respect to the primes $p|D$ " would produce the factor $\prod_{p|D} v_p(\Delta_E)$. On the other hand, the fraction $\delta_{1,N}/\delta_{D,M}$ can be seen as a "rate of change in the direction of the selected primes $p|D$", since it measures the variation of the degree of a modular parametrization of the elliptic curve E under consideration when we change the modular curve $X_0(N)$ by the Shimura curve $X_0^D(M)$.

While this heuristic might be relevant in the context of the usual analogies between function fields and number fields, we remark that the arguments in this paper do not depend on it.

6.3. **Lemmas on congruences.** If A is an elliptic curve over $\mathbb{Q}$ and m is a positive integer, the Galois representation on $A[m]$ is denoted by

$$\rho_{A[m]} : G_{\mathbb{Q}} \to GL_2(\mathbb{Z}/m\mathbb{Z}).$$

This depends on a choice of isomorphism $A[m] \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, and the image of $\rho_{A[m]}$ is well-defined up to conjugation.

Lemma 6.3. *Let $\ell > 163$ be a prime. For every elliptic curve A over $\mathbb{Q}$ of conductor N there are infinitely many primes $r \nmid \ell N$ satisfying*

$$a_r(A) \not\equiv r + 1 \mod \ell.$$

Proof. As $\ell > 163$, from [70] we have that $A[\ell]$ is an irreducible Galois module, and the claim follows from the proof of Theorem 5.2(c) in [82]. □

Lemma 6.4. *Let $\ell \leq 163$ be a prime and let A be an elliptic curve of conductor N. There is a positive integer $e = e(\ell, A)$ satisfying:*

- $\ell^e < 2050 \log(N)$
- *There are infinitely many primes $r \nmid \ell N$ such that*

$$a_r(A) \not\equiv r + 1 \mod \ell^e.$$

Proof. By Lemma 5.2 there is a prime $r_0 \nmid \ell N$ with

$$r_0 \leq 2 + 2\log(\ell N) \leq 2 + 2\log(163N).$$

Take e so that $\ell^e \geq 4\log(163N)$, then $\ell^e > |r_0 + 1 - a_{r_0}(A)| \neq 0$ (by Hasse's bound) obtaining $\ell^e \nmid r_0 + 1 - a_{r_0}(A)$. As $\ell \leq 163$ and $N \geq 11$, we see that this can be achieved with $\ell^e < 2050\log(N)$.

The existence of this particular r_0 implies the existence of infinitely many primes r as wanted, by Chebotarev's theorem applied to the character

$$\mathrm{Tr}\, \rho_{A[\ell^e]} - \mathrm{Tr}\,(1 \oplus \chi_{cyc})$$

where $\chi_{cyc} : G_{\mathbb{Q}} \to (\mathbb{Z}/\ell^c\mathbb{Z})^\times$ is the cyclotomic character. □

Lemma 6.5. *Let ℓ be a prime. There is a positive integer $c(\ell)$ depending only on ℓ such that for any given $n \geq c(\ell)$ there is a finite set $\mathscr{F}(\ell, n) \subseteq \mathbb{Q}$ with the following property:*

Let A be an elliptic curve defined over $\mathbb{Q}$ with j-invariant j_A. If $j_A \notin \mathscr{F}(\ell, n)$, then

$$im(\rho_{A[\ell^n]}) \supseteq \{\gamma \in SL_2(\mathbb{Z}/\ell^n\mathbb{Z}) : \gamma \equiv I \mod \ell^{c(\ell)}\}. \tag{11}$$

Proof. For each positive integer m and each subgroup $H \leq GL_2(\mathbb{Z}/m\mathbb{Z})$ such that $\det(H) = (\mathbb{Z}/m\mathbb{Z})^\times$, there is a congruence subgroup $\Gamma_H \leq SL_2(\mathbb{Z})$ and a geometrically connected, open congruence modular curve Y_H defined over $\mathbb{Q}$ with a map $\pi_H : Y_H \to Y(1) = \mathbb{A}^1$ over $\mathbb{Q}$. The set of complex points of Y_H is $\Gamma_H \backslash \mathfrak{h}$. Distinct m and H can give the same Γ_H. It is a classical result that for congruence subgroups the genus grows with the level (cf. [22]).

If A is an elliptic curve over $\mathbb{Q}$ with $\rho_{A[m]}(G_{\mathbb{Q}})$ conjugate to a subgroup of such an H, then it gives rise to a $\mathbb{Q}$-rational point $P_H(A, m) \in Y_H(\mathbb{Q})$ satisfying $\pi_H(P_H(A, m)) = j_A$.

Given a positive integer m and an elliptic curve $A/\mathbb{Q}$ we define the subgroup

$$H_{A,m} = \rho_{A[m]}(G_{\mathbb{Q}}) \leq GL_2(\mathbb{Z}/m\mathbb{Z}).$$

Observe that $\det(H_{A,m}) = (\mathbb{Z}/m\mathbb{Z})^\times$ because $\det \rho_{A[m]}(Frob_p) = p \mod m$ for all but finitely many primes p, and note also that $P_{H_{A,m}}(A, m) \in Y_{H_{A,m}}(\mathbb{Q})$.

Given a positive integer c and taking $m = \ell^n$ for some $n \geq c$, the failure of (11) can be expressed by saying that H_{A,ℓ^n} does not contain the group

$$S_{c,\ell^n} := \{\gamma \in SL_2(\mathbb{Z}/\ell^n\mathbb{Z}) : \gamma \equiv I \mod \ell^c\}.$$

We note that the level of $\Gamma_{H_{A,\ell^n}}$ is certain power of ℓ. If (11) fails, then the level of $\Gamma_{H_{A,\ell^n}}$ is larger than ℓ^c, for otherwise H_{A,ℓ^n} would contain S_{c,ℓ^n}. Thus, suitable choice of c will ensure that whenever (11) fails for A and $n \geq c$, one has that $Y_{H_{A,\ell^n}}$ has geometric genus at least 2. For ℓ and $n \geq c$ fixed, there are only finitely many groups $H_{A,\ell^n} \leq GL_2(\mathbb{Z}/\ell^n\mathbb{Z})$ as we vary A, all of them giving modular curves of geometric genus at least 2. Let $H_1, ...H_t$ be these finitely many subgroups, then we can take $\mathscr{F}(\ell, n) = \cup_{i=1}^t \pi_{H_i}(Y_{H_i}(\mathbb{Q}))$, which is finite by Faltings's theorem. We take $c(\ell) = c$. □

Lemma 6.6. *Let ℓ be a prime. There is a positive integer $b = b_\ell$ and a finite set $\mathscr{G}_\ell \subseteq \mathbb{Q}$, both depending only on ℓ, such that the following holds:*

Let A be an elliptic curve over $\mathbb{Q}$ with $j_A \notin \mathscr{G}_\ell$. There are infinitely many primes $r \nmid N\ell$ with $a_r(A) \not\equiv r+1 \mod \ell^b$.

Proof. Let $c = c(\ell)$ be as in Lemma 6.5. We claim that $b = 4c$ and $\mathscr{G}_\ell = \mathscr{F}(\ell, b)$ have the desired property. For the sake of contradiction, let A be an elliptic curve over $\mathbb{Q}$ with $j_A \notin \mathscr{G}_\ell$ and suppose that all sufficiently large primes r satisfy

$$X^2 - a_r(A)X + r \equiv (X-1)(X-r) \mod \ell^b.$$

The Cayley-Hamilton theorem applied to the action on $A[\ell^b]$ of the Frobenius element $F_r = \rho_{A[\ell^b]}(Frob_r)$, gives that $(F_r - 1) \circ (F_r - r)$ is the zero endomorphism on $A[\ell^b]$ for all but finitely many primes r. Note that by Lemma 6.5

$$\gamma := \begin{bmatrix} 1+\ell^{2c} & \ell^c \\ \ell^c & 1 \end{bmatrix} \in im(\rho_{A[\ell^b]})$$

so the Chebotarev density theorem gives infinitely many primes r for which $F_r = \gamma$. We have

$$\ker(\gamma - 1) = \ker \begin{bmatrix} \ell^{2c} & \ell^c \\ \ell^c & 0 \end{bmatrix} = \ell^{b-c} A[\ell^b]$$

so that $\# \ker(\gamma - 1) = \ell^{2c}$. On the other hand, we have that

$$\gamma - r = \begin{bmatrix} 1 - r + \ell^{2c} & \ell^c \\ \ell^c & 1-r \end{bmatrix}$$

has image of size at least ℓ^{b-c} (by looking at the top-right entry, say), so that $\# \ker(\gamma - r) \leq \ell^{b+c}$. It follows that for each of the infinitely many primes r with $F_r = \gamma$ we have

$$\ell^{2b} = \# \ker((F_r - 1) \circ (F_r - r)) \leq \# \ker(\gamma - 1) \cdot \# \ker(\gamma - r) \leq \ell^{b+3c}$$

which is not possible, because $b = 4c$. □

Lemma 6.7. *Let S be a finite set of primes. For all primes ℓ there is an integer $\beta_S(\ell)$ with the following properties:*

(i) *If $\ell > 163$, then we have $\beta_S(\ell) = 1$.*

(ii) *For every elliptic curve $A/\mathbb{Q}$ semi-stable away from S, there are infinitely many primes r such that $a_r(A) \not\equiv r+1 \mod \ell^{\beta_S(\ell)}$.*

Proof. Given a finite set of primes S and a finite set of rational numbers J, there are only finitely many elliptic curves over $\mathbb{Q}$ with j-invariant in J and semi-stable reduction outside S. Then, up to finitely many elliptic curves over $\mathbb{Q}$ (depending on S and ℓ), the result now follows from Lemmas 6.3 and 6.6. For those possible finitely many exceptional elliptic curves, we conclude by Lemmas 6.3 and 6.4. □

6.4. **Component groups.** Let A be an abelian variety over $\mathbb{Q}$ and let $\mathscr{A}$ be its Néron model. For a prime p, we denote by $\Phi_p(A)$ the group of geometric connected components of $\mathscr{A}_p$, the special fibre at p. Then $\Phi_p(A)$ is a finite abelian group with a $G_{\mathbb{F}_p}$-action, and the rule $A \mapsto \Phi_p(A)$ is functorial. Given $\theta : A \to B$ a morphism of abelian varieties over $\mathbb{Q}$, we write $\theta_{p,*} : \Phi_p(A) \to \Phi_p(B)$ for the induced map. In the particular case of multiplication by an integer n, that is $[n] : A \to A$, we have that $[n]_{p,*}$ is multiplication by n on $\Phi_p(A)$.

Let $X_p(A)$ be the character group $Hom_{\overline{\mathbb{F}}_p}(\tau_p(A), \mathbb{G}_m)$ where $\tau_p(A)$ is the toric part of $\mathscr{A}_p$. One has the monodromy pairing $u_{A,p} : X_p(A) \times X_p(A^\vee) \to \mathbb{Z}$ which, in the case when A comes with an isomorphism $A \simeq A^\vee$ (e.g. when A is the Jacobian of a curve, in particular when A is an elliptic curve) becomes a $\mathbb{Z}$-valued bilinear pairing on $X_p(A)$.

Suppose now that A is an elliptic curve over $\mathbb{Q}$ with multiplicative reduction at p. Then $\Phi_p(A)$ is a cyclic group of order $c_p(A) := v_p(\Delta_A)$.

Lemma 6.8. *Let A and B be elliptic curves which are isogenous over $\mathbb{Q}$ and suppose that p is a prime of multiplicative reduction for one (hence both) of them. Then $c_p(A)/c_p(B)$ is a rational number whose multiplicative height is at most 163. In particular, it is supported on primes ≤ 163.*

Proof. Let $\alpha : A \to B$ be an isogeny of minimal degree; be results of Mazur [70] and Kenku [59] we know that $n := \deg(\alpha) \leq 163$. Let $\beta : B \to A$ be the dual isogeny, so that $\beta\alpha = [n]$ on A. Since A and B have multiplicative reduction at p, we have isomorphisms of abstract groups $\Phi_p(A) = \mathbb{Z}/c_p(A)\mathbb{Z}$ and $\Phi_p(B) = \mathbb{Z}/c_p(B)\mathbb{Z}$, under which we obtain a commutative diagram

$$\begin{tikzcd}
\mathbb{Z}/c_p(A)\mathbb{Z} \arrow[r, "\alpha_{p,*}"] \arrow[dr, "n\cdot"'] & \mathbb{Z}/c_p(B)\mathbb{Z} \arrow[d, "\beta_{p,*}"] \\
& \mathbb{Z}/c_p(A)\mathbb{Z}.
\end{tikzcd}$$

From this we get that $c_p(A)/(n, c_p(A)) = \#im(n\cdot)$ divides $\#im(\beta_{p,*})$, which divides $c_p(B)$. Thus, the numerator of $c_p(A)/c_p(B)$ divides n, and similarly for the denominator using $\alpha\beta$ instead. □

6.5. **Some Diophantine equations.** Our proof of Theorem 6.1 requires control on integer solutions of certain Diophantine problems which are variations of Fermat's last theorem.

Lemma 6.9. *Let S be a finite set of primes. Let A, B, C be non-zero integers. Let p, q, r be positive integers satisfying*

$$\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1.$$

The equation

$$Ax^p + By^q = Cz^r$$

has only finitely many integer solutions $(x, y, z) \in \mathbb{Z}^3$ under the restriction that x, y, z do not have common prime factors outside S.

Proof. The proof is the same as for Theorem 2 in [23]. One has to repeat the argument given in p.526-527 of *loc. cit.* replacing the set of places V_{ABC} by $V_{ABC} \cup S$. □

Lemma 6.10. *Let $L \geq 7$ be an integer and let S be a finite set of primes. There is a number $N_0 = N_0(L, S)$ depending only on L and S such that there is no elliptic curve E over $\mathbb{Q}$ with conductor $N_E \geq N_0$, semi-stable reduction away from S, and with minimal discriminant of the form $\Delta_E = n \cdot k^L$ with n and k integers such that all the prime factors of n are in S.*

Proof. For E semi-stable away from S, the quantities c_4 and c_6 associated to a minimal Weierstrass equation of E can only share prime factors from $S' = S \cup \{2, 3\}$, cf. Exercise 8.21 in [89]. Recall that $\pm 1728\Delta_E = c_4^3 - c_6^2$ (cf. p.259 *loc. cit.*), then elliptic curves E with $\Delta_E = n \cdot k^L$ for some integers n, k with n an S-unit give integer solutions for equations of the form

$$A \cdot x^L = y^3 - z^2$$

where the integer $A \neq 0$ is only divisible by primes in S', and $\gcd(y, z)$ is only divisible by primes in S'. Furthermore, for S and L fixed, one only needs to consider finitely many equations of this sort, as it is only necessary to consider coefficients A whose prime factorization has exponents $< L$ (this reduction might modify the coordinate x of a solution, but it does not modify the coordinates y, z). Since $1/2 + 1/3 + 1/L > 1$, Lemma 6.9 gives that each one of these finitely many equations has only finitely many solutions, and we obtain only a finite list of possible quantities c_4 and c_6 (coming from the coordinates y, z of these finitely many solutions).

Thus, for fixed S and L, there are only finitely many elliptic curves E over $\mathbb{Q}$ with $\Delta_E = n \cdot k^L$ for some integers n, k with n an S-unit. □

Lemma 6.11. *Let $\ell \geq 11$ be a prime number. Let E be a semi-stable elliptic curve over $\mathbb{Q}$. Then Δ_E is not a perfect ℓ-th power.*

Proof. Since E is semi-stable, the residual Galois representation $\rho_{E[\ell]}$ is surjective onto $GL_2(\mathbb{F}_\ell)$ by Theorem 4 in [70]. Hence it is absolutely irreducible and we can apply Ribet's level-lowering results [82] as in the proof of Fermat's last theorem. Thus Δ_E is not a perfect ℓ-th power. (See also Lemma 2 in [85].) □

Lemma 6.12. *Let a, b, c be coprime positive integers with $a + b = c$ and $(a, b, c) \neq (1, 1, 2)$. Let E be the associated Frey-Hellegouarch elliptic curve and write $2^{v_2(\Delta_E)}\Delta'_D = \Delta_E$ (that is, Δ'_E is the odd part of Δ_E). Let $\ell \geq 3$ be a prime number. Then Δ'_E is not a perfect ℓ-th power.*

Proof. Suppose that Δ'_E is a perfect ℓ-th power. Recall that $\Delta_E = 2^s(abc)^2$ for some integer s with $-8 \leq s \leq 4$ (cf. Section 3). Since a, b, c are pairwise coprime we see that the odd parts of them are perfect ℓ-th powers. Exactly one of a, b, c is even, so the equation $a + b = c$ yields a solution of

$$x^\ell + 2^m y^\ell + z^\ell = 0$$

in pairwise coprime integers x, y, z with x and z odd, $xyz \neq 0$, and $0 \leq m < \ell$.

By Wiles's theorem we see that $m \neq 0$.

By Ribet's Theorem 3 in [84] we see that $1 < m < \ell$ is not possible either.

So $m = 1$. Then by Darmon and Merel [24] we obtain that the solution must be trivial in the sense that $xyz = \pm 1$. This has the consequence that $abc = 2$, hence, $(a, b, c) = (1, 1, 2)$, which was excluded. □

6.6. **Set-up for the proof of Theorem 6.1.** For given elliptic curve E of conductor N we will vary over admissible factorizations $N = DM$. This has the effect that in the discussion below, our notation will not explicitly refer to E but instead we only keep track of the admissible factorization under consideration.

Given an admissible factorization $N = DM$ and a prime p, the map $q_{D,M} : J_0^D(M) \to A_{D,M}$ induces the map

$$q_{D,M,p,*} : \Phi_p(J_0^D(M)) \to \Phi_p(A_{D,M})$$

on the groups of geometric components, and we will need to analyze the size of the image and cokernel of these maps for various primes p:

$$\begin{aligned} i_p(D, M) &= \#\text{image}(q_{D,M,p,*}) \\ j_p(D, M) &= \#\text{cokernel}(q_{D,M,p,*}). \end{aligned}$$

A first result towards Theorem 6.1 is the following one, already included in [85].

Proposition 6.13. *Let $N = DM$ be an admissible factorization of the conductor of E, and suppose that p, r are two distinct primes dividing D. Let us write $D = dpr$. Then*

$$\begin{aligned} \frac{\delta_{d,prM}}{\delta_{dpr,M}} &= \frac{c_p(A_{d,prM}) \cdot c_r(A_{dpr,M})}{i_p(d, prM)^2 \cdot j_r(dpr, M)^2} \\ &= \frac{c_r(A_{d,prM}) \cdot c_p(A_{dpr,M})}{i_r(d, prM)^2 \cdot j_p(dpr, M)^2}. \end{aligned}$$

Proof. Except for the notation, this is Theorem 2 in [85] —symmetry on p and r follows from the fact that $\delta_{d,prM}/\delta_{dpr,M}$ is symmetric on p and r.

At this point one must note that the proof in *loc. cit.* does not need M to be squarefree, specially, Proposition 1 does not use this assumption and one just needs multiplicative reduction at the two primes p, q according to the notation of *loc. cit.* (In fact, *loc. cit.* only uses the assumption that M is squarefree in p.11113 for the proof of the second part of Theorem 1.) □

The main technical difficulty in the proof of Theorem 6.1 is to show that the terms $i_p(d, prM)$ and $j_r(dpr, M)$ from the previous result are "small", even when the relevant elliptic curves have some reducible residual Galois representation. At this point we can already take care of the image term.

Lemma 6.14. *Let S be a finite set of primes. If $N = DM$ is squarefree away from S and p exactly divides M, then for every prime ℓ we have*

$$v_\ell(i_p(D, M)) \leq \beta_S(\ell) - 1$$

with $\beta_S(\ell)$ as in Lemma 6.7. In particular, if $N = DM$ is squarefree away from S, and p exactly divides M, then $i_p(J_0^D(M), \chi_{D,M})$ divides an integer κ_S which only depends on the set S and, moreover, κ_S is supported on the primes ≤ 163.

Before proving this, we remark that [85] and [97] omit the analysis of the primes ℓ for which the Galois representation $E[\ell]$ is reducible. In our case this is a very serious issue; for instance, $E[2]$ is always reducible for Frey-Hellegouarch curves. Since our ultimate goal is to establish global bounds, we cannot omit the contribution of any prime.

Proof of Lemma 6.14. We follow the idea of the proof of Proposition 3 in [85]. The group $\Phi_p(J_0^D(M))$ is Eisenstein in the sense that for $r \nmid N$, the Hecke operator T_r acts on it as multiplication by $r + 1$ (cf. [83]). On the other hand, since $A_{D,M}$ is the optimal quotient associated to $\chi_{D,M}$, the action of T_r on $J_0^D(M)$ induces multiplication by $\chi_{D,M}(T_r) = a_r(A_{D,M})$ on $A_{D,M}$. Hence, $r + 1 - a_r(A_{D,M})$ acts as 0 on $im(\xi_{p,*})$, which is a cyclic group of order $i_p(J_0^D(M), \chi_{D,M})$ because it is a subgroup of the cyclic group $\Phi_p(A_{D,M})$.

It follows that $i_p(J_0^D(M), \chi_{D,M})$ divides $r + 1 - a_r(A_{D,M})$ for every prime $r \nmid N$. Let ℓ be a prime, then, under the assumption that N is squarefree away from S, Lemma 6.7 affords infinitely many primes r for which $v_\ell(r + 1 - a_r(A_{D,M})) < \beta_S(\ell)$. Taking any of these primes r gives the result. □

The cokernel term, however, is much more delicate and we analyze it the next paragraph.

We remark that in Theorem 2.4 of [97] it is asserted that $q_{D,M,p,*} : \Phi_p(J_0^D(M)) \to \Phi_p(A_{D,M})$ is surjective when $p|D$. This would imply that $j_r(D, M) = 1$. Unfortunately the proof in [97] has a serious gap as explained in detail in [77], see the last paragraph of Section 1 in [77]. This gap affects the main result of [97] —we leave it to the reader to see what other references in the literature are affected by this issue. For our purposes this is not a serious problem, and we can control the cokernel by other means.

6.7. **Switching primes.** For simplicity, we write $\mathscr{P} = \{2, 3, 5, ...\}$ for the set of prime numbers.

Lemma 6.15. *Let S be a finite set of primes. There is a function $\alpha_{S,1} : \mathscr{P} \to \mathbb{Z}_{\geq 0}$ supported on primes ≤ 163 (i.e. taking the value 0 at each prime larger than 163) and depending only on the choice of S, such that the following holds:*

Let E be an elliptic curve over $\mathbb{Q}$, semi-stable away from S, and of conductor N. Let $N = DM$ be an admissible factorization. If p, r are two (possibly equal) primes dividing D, then for every prime ℓ we have

$$v_\ell(j_p(D, M)) \leq v_\ell(c_r(E)) + \alpha_{S,1}(\ell).$$

Proof. If $p = r$, then by definition $j_p(D, M)$ divides $c_p(A_{D,M}) = \#\Phi_p(A_{D,M})$, so the result follows from Lemma 6.8.

Suppose now that $p \neq r$. By Proposition 6.13, Lemma 6.8, and Lemma 6.14, we obtain

$$|v_\ell(j_p(D, M)) - v_\ell(j_r(D, M))| \leq \alpha_S(\ell)$$

for some function $\alpha_S : \mathscr{P} \to \mathbb{Z}_{\geq 0}$ supported on primes ≤ 163. The desired estimate now follows from the previous case. □

Lemma 6.16. *Let S be a finite set of primes. There is a function $\alpha_{S,2} : \mathscr{P} \to \mathbb{Z}_{\geq 0}$ supported on primes ≤ 163 and depending only on the choice of S, such that the following holds:*

Let E be an elliptic curve over $\mathbb{Q}$, semi-stable away from S, and of conductor N. Let $N = DM$ be an admissible factorization and suppose that M is divisible by at least two primes of multiplicative reduction for E. If p, r are two primes of multiplicative reduction for E with $p|D$ and $r|M$, then for every prime ℓ we have

$$v_\ell(j_p(D, M)) \leq v_\ell(c_r(E)) + \alpha_{S,2}(\ell).$$

Proof. Since D has an even number of prime factors and by our hypothesis on M, there are primes q, t of multiplicative reduction for E with $q \neq p$ and $t \neq r$, such that $q|D$ and $t|M$. Let us write $D = pqd$ and $M = rtm$.

From the equations

$$\frac{\delta_{d,pqrtm}}{\delta_{pqd,rtm}} \cdot \frac{\delta_{pqd,rtm}}{\delta_{pqrtd,m}} = \frac{\delta_{d,pqrtm}}{\delta_{pqrtd,m}} = \frac{\delta_{d,pqrtm}}{\delta_{prd,qtm}} \cdot \frac{\delta_{prd,qtm}}{\delta_{pqrtd,m}}$$

and Proposition 6.13, we deduce that the expression

$$\frac{c_q(A_{d,pqrtm}) \cdot c_p(A_{pqd,rtm})}{i_q(d, pqrtm)^2 \cdot j_p(pqd, rtm)^2} \cdot \frac{c_r(A_{pqd,rtm}) \cdot c_t(A_{pqrtd,m})}{i_r(pqd, rtm)^2 \cdot j_t(pqrtd, m)^2} \tag{12}$$

is equal to the expression

$$\frac{c_p(A_{d,pqrtm}) \cdot c_r(A_{prd,qtm})}{i_p(d, pqrtm)^2 \cdot j_r(prd, qtm)^2} \cdot \frac{c_q(A_{prd,qtm}) \cdot c_t(A_{pqrtd,m})}{i_q(prd, qtm)^2 \cdot j_t(pqrtd, m)^2}, \tag{13}$$

and we observe that $j_t(pqrtd, m)$ appears in both.

By Lemma 6.8, Lemma 6.14, and the equality of (12) and (13), we see that there is a function $\alpha'_S : \mathscr{P} \to \mathbb{Z}_{\geq 0}$ depending only on the choice of S and supported on primes ≤ 163 such that for every prime ℓ we have

$$|v_\ell(j_p(pqd, rtm)) - v_\ell(j_r(prd, qtm))| \leq \alpha'_S(\ell).$$

From this and Lemma 6.15 (on the prime $r|prd$) we deduce

$$v_\ell(j_p(pqd, rtm)) \leq v_\ell(j_r(prd, qtm)) + \alpha'_S(\ell) \leq v_\ell(c_r(E)) + \alpha'_S(\ell) + \alpha_{S,1}(\ell).$$

□

6.8. **Bounding the cokernel.** The following result shows that $j_p(D, M)$ is uniformly bounded for $p|D$ in the cases on which we are mainly interested, and without assuming irreducibility of residual Galois representations.

Theorem 6.17. *There is a function $\alpha : \mathscr{P} \to \mathbb{Z}_{\geq 0}$ supported on primes ≤ 163, such that the following holds:*

Let E be an elliptic curve over $\mathbb{Q}$ of conductor N. Let $N = DM$ be an admissible factorization and suppose that either

(i) *E is semi-stable and M is not a prime number, or*
(ii) *E is a Frey-Hellegouarch elliptic curve and M is divisible by at least two odd primes (which are necessarily of multiplicative reduction).*

Let p be a prime with $p|D$. Then for every prime ℓ we have

$$v_\ell(j_p(D, M)) \leq \alpha(\ell).$$

Hence, there is an absolute integer constant $\kappa \geq 1$ supported on primes ≤ 163 such that $j_p(D, M)$ divides κ under these assumptions.

In particular, $j_p(D, M)$ is uniformly bounded under these assumptions.

Proof. Let us first consider the case (i). If $\ell \geq 11$ then Lemma 6.11 gives that there is some prime $r|N$ such that $\ell \nmid c_r(E)$. On the other hand, we see from Lemma 6.10 (with $S = \emptyset$ and $L = \ell^3$) that if $\ell \leq 7$ then there is some prime $r|N$ such that $\ell^3 \nmid c_r(E)$, except, perhaps, for finitely many elliptic curves which can be discarded without affecting the result. In either case, we choose such an $r|N$. If $r|D$ we invoke Lemma 6.15, and if $r|M$ we appeal to Lemma 6.16, so that in either case we conclude that

$$v_\ell(j_p(D,M)) \leq v_\ell(c_r(E)) + \alpha_1(\ell) \leq \alpha_2(\ell)$$

for certain functions $\alpha_1, \alpha_2 : \mathscr{P} \to \mathbb{Z}_{\geq 0}$ supported on primes ≤ 163 and independent of the choice of any elliptic curve. This proves the result in case (i).

The proof in case (ii) is similar, but we apply Lemma 6.12 instead of Lemma 6.11, and then we apply Lemma 6.10 using the finite set of primes $S = \{2\}$ instead of $S = \emptyset$. □

One also has the following weaker estimate which nonetheless works in complete generality.

Lemma 6.18. *Let E be an elliptic curve over $\mathbb{Q}$ of conductor N and consider an admissible factorization $N = DM$. Let p be a prime with $p|D$. Then $j_p(D,M)$ divides $p-1$ if p is odd, and it divides 2 if $p = 2$. In particular, $j_p(D,M) \leq p$.*

Proof. We base-change the map $\phi_{D,M} : J_0^D(M) \to A_{D,M}$ to $\mathbb{Q}_p$ and consider the special fibre at p of the corresponding Néron models. After an unramified quadratic twist (which does not affect the computation of $j_p(D,M)$ as this quantity concerns the geometric components of special fibres) we reduce to the split toric reduction case, and then the result follows from Corollary 3.5 in [77]. □

6.9. **Bounding the correction factor.**

Proof of Theorem 6.1. Consider any factorization of N of the form $N = dprm$ where d is squarefree with an even number of prime factors, p and r are distinct primes not dividing d, and m is coprime to dpr. By Proposition 6.13 and Lemma 6.8 we have

$$\frac{\delta_{d,prm}}{\delta_{dpr,m}} = \frac{u_{d,p,r,m}}{i_p(d,prm)^2 j_r(dpr,m)^2} \cdot c_p(E)c_r(E) \tag{14}$$

where $u_{d,p,r,m}$ is certain rational number supported on primes ≤ 163 with multiplicative height at most 163. Repeated applications of this observation (to sequentially remove prime factors from D) give the result regarding the numerator of $\gamma_{D,M,E}$. More precisely, choosing a prime factorization $D = p_1 r_1 \cdots p_n r_n$ we apply the previous analysis to the expression

$$\frac{\delta_{1,N}}{\delta_{D,M}} = \frac{\delta_{1,N}}{\delta_{p_1r_1,N/(p_1r_1)}} \cdot \frac{\delta_{p_1r_1,N/(p_1r_1)}}{\delta_{p_1r_1p_2r_2,N/(p_1r_1p_2r_2)}} \cdots \frac{\delta_{D/(p_nr_n),p_nr_nM}}{\delta_{D,M}}.$$

The estimate (10) follows since an upper bound for the numerator of $\gamma_{D,M,E}$ is also an upper bound for this rational number.

The result of item (a) regarding the denominator of $\gamma_{D,M,E}$ follows in a similar fashion. Here one also uses Lemma 6.14 on the factors $i_p(d,prm)^2$ occurring in the various applications of (14), and Lemma 6.18 on the factors $j_r(dpr,m)^2$. For this we choose a prime factorization $D = p_1r_1 \cdots p_nr_n$ in some order satisfying $r_i < p_i$ for each i. Then we sequentially apply (14) and the previous estimates to the pairs of factors (p_i, r_i). By Lemma 6.18, the total contribution of the cokernel factors to the denominator of $\gamma_{D,M,E}$ is bounded by $r_1^2 \cdots r_n^2 < p_1r_1 \cdots p_nr_n = D$ since we chose $r_i < p_i$.

Finally, the result of item (b) is also obtained by a similar argument. Here, the cokernel factors $j_r(dpr,m)^2$ are controlled by Theorem 6.17 instead of Lemma 6.18, giving the claimed stronger estimates in this case. □

7. Bounding the modular degree

Our goal in this section is to give bounds for the modular degrees $\delta_{D,M}$ associated to an elliptic curve E of conductor N, with $N = DM$ an admissible factorization (both unconditionally and under the Generalized Riemann Hypothesis) and to use them in the context of Szpiro's conjecture. This last point needs some attention; the classical modular approach to Szpiro's conjecture translates bound for $\delta_{1,N}$ into bounds for the Faltings height of an elliptic curve, but the analogous transition is not available in the literature for the more general case of $\delta_{D,M}$ due to the lack of a Fourier expansion for the modular forms in $S_2^D(M)$ when $D > 1$.

7.1. **Counting systems of Hecke eigenvalues.**

Let $s(n) = \dim S_2(n)^{new}$ and let $r_{D,M}$ be the number of systems of Hecke eigenvalues on $\mathbb{T}_{D,M}$. Here, N is a positive integer and $N = DM$ is an admissible factorization. By multiplicity one in $S_2(n)^{new}$ and by the Jacquet-Langlands correspondence we have

$$r_{D,M} = \sum_{m|M} s(Dm).$$

On the other hand, from Theorem 1 in [69] (see also Appendix B in [46]) together with Lemma 17 in [69], we have the following bound for $s(n)$:

$$s(n) \leq \frac{\varphi(n)}{12} + \frac{7}{12} \cdot 2^{\omega(n)} + \mu(n).$$

The functions $\varphi, 2^\omega, \mu$ are mutiplicative, $(D, M) = 1$ and D is squarefree, so we find

$$\begin{aligned} r_{D,M} &\leq \frac{\varphi(D)}{12} \sum_{m|M} \varphi(m) + \frac{7 \cdot 2^{\omega(D)}}{12} \sum_{m|M} 2^{\omega(m)} + \mu(D) \sum_{m|M} \mu(m) \\ &\leq \frac{1}{12} \cdot \varphi(D)M + \frac{7}{12} \cdot d(DM^2) + 1. \end{aligned}$$

Writing $N = DM$, we deduce:

Proposition 7.1. *We have*

$$r_{D,M} \leq \frac{1}{12} \cdot \varphi(D)M + \frac{7}{12} \cdot d(DM^2) + 1.$$

Thus, given $\epsilon > 0$, for $N \gg_\epsilon 1$ with an effective implicit constant, we have

$$r_{D,M} < \left(\frac{1}{12} + \epsilon\right) \cdot \varphi(D)M.$$

(The asymptotic bound follows by recalling that $\varphi(n) \gg n/\log\log n$.) We remark that similar methods give $r_{D,M} \gg \varphi(D)M$.

7.2. **Unconditional bound.**

Theorem 7.2. *Given any elliptic curve E over $\mathbb{Q}$ with conductor N and an admissible factorization $N = DM$, we have*

$$\log \delta_{D,M}(E) \leq \left(\frac{1}{12} \cdot \varphi(D)M + \frac{7}{12} \cdot d(DM^2)\right) \left(\log N + \frac{4 \log N}{\log\log N}\right).$$

Furthermore, given any $\epsilon > 0$, for $N \gg_\epsilon 1$ with an effective implicit constant, we have

$$\log \delta_{D,M} < \left(\frac{1}{24} + \epsilon\right) \varphi(D)M \log N.$$

Proof. First we bound $\eta_{[\chi_{D,M}]}(c)$ for $c \neq [\chi_{D,M}]$ a class of systems of Hecke eigenvalues on $\mathbb{T}_{D,M}$. Let $f \in S_2(N)$ be the normalized newform corresponding to $\chi_{D,M}$ by Jacquet-Langlands. Take any $\chi \in c$, let $d|M$ be its level and let $g \in S_2(Dd)^{new} \subseteq S_2(N)$ be the only normalized newform which corresponds to χ by Jacquet-Langlands.

We have $f \neq g$. Furthermore, the modular forms F, G obtained by deleting the Fourier coefficients of f, g (respectively) of index not coprime to N, have level dividing N^2 (cf. the proof of Theorem 1 in [5]). Hence, the Fourier expansions of F and G differ at some index bounded by $2(\dim S_2(N^2) - 1)$. It follows that there is some integer n_c coprime to $N = DM$ satisfying $a_{n_c}(f) \neq a_{n_c}(g)$ and

$$n_c \leq \frac{N^2}{6}\prod_{p|N}\left(1+\frac{1}{p}\right) \leq \frac{1}{6}\cdot N^2(1+\log N) < N^3. \tag{15}$$

Let $P(x) \in \mathbb{Z}[x]$ be the (monic) minimal polynomial of $a_{n_c}(g) = \chi(T_{D,M,n_c})$. Then $\deg(P) \leq \#c$ and

$$0 \neq |P(a_{n_c}(f))| \leq (2d(n_c)\cdot n_c^{1/2})^{\#c}$$

where we have used the Hasse-Weil bound on the Fourier coefficients of a normalized eigenform of weight 2. From [75] we have the following explicit bound for the divisor function $d(n)$, valid for $n > 2$:

$$d(n) < \exp\left(1.5379\cdot(\log 2)\frac{\log n}{\log\log n}\right) < 3^{\log n/\log\log n}. \tag{16}$$

By Proposition 5.4, the previous divisor bound, and the inequalities in (15) we obtain

$$\begin{aligned}\eta_{[\chi_{D,M}]}(c) &\leq (2d(n_c)\cdot n_c^{1/2})^{\#c}\\ &< 3^{\#c\cdot(\log N^3)/(\log\log N^3)}\cdot N^{\#c}\cdot(1+\log N)^{\#c/2}\\ &< 3.7^{\#c\cdot(\log N^3)/(\log\log N^3)}\cdot N^{\#c}\\ &< 3.7^{\#c\cdot(\log N^3)/(\log\log N)}\cdot N^{\#c}.\end{aligned}$$

So we get

$$\log\eta_{[\chi_{D,M}]}(c) < \#c\cdot\left(\log N + \frac{4\log N}{\log\log N}\right).$$

Varying $c \neq [\chi_{D,M}]$ over the classes of systems of Hecke eigenvalues on $\mathbb{T}_{D,M}$, Theorem 5.5 gives

$$\begin{aligned}\log\delta_{D,M} &\leq \sum_{c\neq[\chi_{D,M}]}\log\eta_{[\chi_{D,M}]}(c)\\ &< (r_{D,M}-1)\cdot\left(\log N + \frac{4\log N}{\log\log N}\right).\end{aligned}$$

Here we used the fact that $r_{D,M} = \sum_c \#c$, summing over all classes c of systems of Hecke eigenvalues on $\mathbb{T}_{D,M}$. By Proposition 7.1, we obtain the claimed explicit bound.

The proof of the asymptotic bound is similar, but using instead the (effective) estimate

$$n_c \ll_\epsilon N^{1+\epsilon}$$

from Lemma 11 in [73]. □

7.3. **Under GRH.** The following result follows from Proposition 5.22 in [53] specialized to classical modular forms —the necessary properties for Rankin-Selberg L-functions in this setting have been established in [64]. See also [41].

Theorem 7.3. *There is an effective constant C such that the following holds:*

Let f, g be normalized Hecke newforms of weight 2 and level dividing N. Assume that the Generalized Riemann Hypothesis holds for the Rankin-Selberg L-functions $L(s, f \otimes f)$ and $L(s, f \otimes g)$. Then there is a prime number $p_{f,g} < C \cdot (\log N)^2$ not dividing N, satisfying $a_{p_{f,g}}(f) \neq a_{p_{f,g}}(g)$.

Using this, we get

Theorem 7.4. *Suppose that the Generalized Riemann Hypothesis for Rankin-Selberg L-functions of modular forms holds. Let $\epsilon > 0$. Then for $N \gg_\epsilon 1$ with an effective implicit constant, we have*

$$\log \delta_{D,M} \leq \left(\frac{1}{12} + \epsilon\right) \varphi(D) M \log\log N.$$

Proof. The proof is similar to that of Theorem 7.2, except that we replace the integer n_c by the prime $p_{f,g}$, with c, f and g as in the cited proof, and $p_{f,g}$ as in Theorem 7.3. □

7.4. **Application to Szpiro's conjecture: Classical modular parameterizations.** The classical modular approach to Szpiro's conjecture (cf. Section 3, especially the estimates (4) and (6)) together with our bounds for $\delta_{D,M}$ specialized to $D = 1, M = N$, give:

Theorem 7.5. *For all elliptic curves E over $\mathbb{Q}$ of conductor N we have*

$$h(E) \leq \frac{1}{24}\left(N + 7d(N^2)\right)\left(\log N + \frac{4 \log N}{\log\log N}\right) + 9$$

and

$$\log |\Delta_E| \leq \frac{1}{2}\left(N + 7d(N^2)\right)\left(\log N + \frac{4 \log N}{\log\log N}\right) + 124.$$

Furthermore, given $\epsilon > 0$, for $N \gg_\epsilon 1$ with an effective implicit constant we have

$$h(E) < \left(\frac{1}{48} + \epsilon\right) N \log N \quad \textit{and} \quad \log |\Delta_E| < \left(\frac{1}{4} + \epsilon\right) N \log N.$$

Finally, if we assume GRH, for $N \gg_\epsilon 1$ with an effective implicit constant we have

$$h(E) < \left(\frac{1}{24} + \epsilon\right) N \log\log N \quad \textit{and} \quad \log |\Delta_E| < \left(\frac{1}{2} + \epsilon\right) N \log\log N.$$

7.5. **Application to Szpiro's conjecture: Shimura curve parameterizations.** Here is an extension of the modular approach to Szpiro's conjecture, using Shimura curve parameterizations coming from $X_0^D(M)$ instead of the classical modular parameterization from $X_0(N)$.

Theorem 7.6 (The Shimura curve approach to *abc*)**.** *Let $\epsilon > 0$. For all elliptic curves E of conductor $N \gg_\epsilon 1$ (with an effective implicit constant), and for any admissible factorization $N = DM$ we have*

$$\log |\Delta_E| < (6 + \epsilon) \log \delta_{D,M}(E) \quad \textit{and} \quad h(E) < \left(\frac{1}{2} + \epsilon\right) \log \delta_{D,M}(E).$$

Proof. The case $D = 1$ is known, so we can assume $D > 1$. The classical modular approach gives upper bounds for $h(E)$ and $\log |\Delta_E|$ in terms of $\log \delta_{1,N}$ (cf. (4) and (6)). The result now follows from the first (effective) inequality in Theorem 6.1, together with the estimates

$$\begin{aligned}\log \prod_{p\mid D} v_p(\Delta_E) &\leq \log d(\Delta_E) \\ &< \frac{1.07\log|\Delta_E|}{\log\log|\Delta_E|} \qquad \text{(by the divisor bound (16))} \\ &\leq \frac{1.07\log|\Delta_E|}{\log\log N} \qquad \text{(for the first bound)} \\ &\leq \frac{1.07\,(12h(E)+16)}{\log\log N} \qquad \text{(by (4); for the second bound).}\end{aligned}$$

□

Of course, instead of the current asymptotic formulation, Theorem 7.6 can be given an exact formulation more amenable for computations with a completely explicit error term if desired.

Theorem 7.6 together with our bounds for the modular degree (cf. Theorems 7.2 and 7.4) give:

Theorem 7.7. *For $\epsilon > 0$ and $N \gg_\epsilon 1$ (with an effective implicit constant), for each admissible factorization $N = DM$ we have the following bounds valid for all elliptic curves E over $\mathbb{Q}$ with conductor N:*

$$h(E) < \begin{cases} (\epsilon + 1/24)\,\varphi(D)M\log N & \textit{with an accessible error term} \\ (\epsilon + 1/48)\,\varphi(D)M\log N & \textit{unconditional} \\ (\epsilon + 1/24)\,\varphi(D)M\log\log N & \textit{under GRH} \end{cases}$$

and similarly

$$\log|\Delta_E| < \begin{cases} (\epsilon + 1/2)\,\varphi(D)M\log N & \textit{with an accessible error term} \\ (\epsilon + 1/4)\,\varphi(D)M\log N & \textit{unconditional} \\ (\epsilon + 1/2)\,\varphi(D)M\log\log N & \textit{under GRH.} \end{cases}$$

The comment “with an accessible error term” refers to the fact that the bound can be obtained with completely explicit lower order terms if desired, thanks to the first estimate in Theorem 7.2.

Let us remark that in the almost semi-stable case one can replace $\varphi(D)M$ by $\varphi(N)$ by suitable choice of admissible factorization $N = DM$. Let us record the result here.

Corollary 7.8. *Let S be a finite set of primes and let P be the product of the elements of S. For $\epsilon > 0$ and $N \gg_{\epsilon,S} 1$ (with an effective implicit constant), if E is an elliptic curve over $\mathbb{Q}$ semi-stable away from S, then we have*

$$h(E) < \begin{cases} \frac{P}{\varphi(P)}\,(\epsilon + 1/48)\,\varphi(N)\log N & \textit{unconditional} \\ \frac{P}{\varphi(P)}\,(\epsilon + 1/24)\,\varphi(N)\log\log N & \textit{under GRH} \end{cases}$$

and similarly

$$\log|\Delta_E| < \begin{cases} \frac{P}{\varphi(P)}\,(\epsilon + 1/4)\,\varphi(N)\log N & \textit{unconditional} \\ \frac{P}{\varphi(P)}\,(\epsilon + 1/2)\,\varphi(N)\log\log N & \textit{under GRH.} \end{cases}$$

Note that if $S = \emptyset$ (i.e., for semi-stable elliptic curves) the factor $P/\varphi(P)$ is 1, and that for $P \gg_\epsilon 1$ one has $P/\varphi(P) < (e^\gamma + \epsilon)\log\log P < 2\log\log P$.

Proof. Let p_N be the largest prime factor of N away from S. Then for all but finitely many E we have that p_N exists. Furthermore, $p_N \to \infty$ as $N \to \infty$ by Shafarevich's theorem.

Let N be sufficiently large, so that p_N exists. If N has an even number of prime factors away from S, take D to be the product of them. Otherwise, take D as the product of them except p_N. Let $M = N/D$, then

$$\varphi(D)M = \varphi(N)\prod_{p|M}\left(1-\frac{1}{p}\right)^{-1} \leq \varphi(N)\prod_{p|p_N P}\left(1-\frac{1}{p}\right)^{-1} = \varphi(N)\cdot\frac{p_N}{p_N-1}\cdot\frac{P}{\varphi(P)}.$$

The result now follows from Theorem 7.7. Note that this argument is effective. □

8. Norm comparisons

8.1. **The result.**

This section is purely analytic and there is no additional difficulty in momentarily considering a more general case.

Let F be a totally real number field of degree n with real embeddings τ_j $(1 \leq j \leq n)$. Let B be a quaternion *division* F-algebra with exactly one split place at infinity, say τ_1. Let $\mathbb{B} = B \otimes \hat{\mathbb{Z}}$ and let $B_+^\times$ be the elements of $B^\times$ with totally positive reduced norm. For each compact open subgroup $U \subseteq \mathbb{B}^\times$ and for each $g \in \mathbb{B}^\times$ consider the group $\Gamma_{U,g} = gUg^{-1} \cap B_+^\times$ and its image $\tilde{\Gamma}_{U,g}$ in $PSL_2(\mathbb{R})$ via τ_1. The quotient $X_{U,g}^{an} = \tilde{\Gamma}_{U,g}\backslash\mathfrak{h}$ is a compact, connected, complex curve, because $\mathbb{B}$ is a division algebra.

Let $S_{U,g}$ be the space of weight 2 holomorphic modular forms for the action of $\tilde{\Gamma}_{U,g}$ on $\mathfrak{h}$. Since we are assuming that B is a division algebra, the cuspidality condition would be vacuous.

On $S_{U,g}$ we have the L^2-norm induced by the Petersson inner product

$$\|h\|_{U,g,2} := \left(\int_{\tilde{\Gamma}_{U,g}\backslash\mathfrak{h}} |h(z)|^2 \Im(z)^2 d\mu_{\mathfrak{h}}(z)\right)^{1/2}.$$

We also have the supremum norm on $S_{U,g}$

$$\|h\|_{U,g,\infty} := \sup_{z\in\mathfrak{h}} |h(z)|\Im(z).$$

(Observe that the L^2-norm is not normalized, so it is not invariant by shrinking U.) Our goal in this section is to compare these two norms.

Theorem 8.1. *Keep the previous notation. There is a number $\nu_n > 0$ depending only on the degree $n = [F : \mathbb{Q}]$, such that if $\tilde{\Gamma}_{U,g}$ acts freely on $\mathfrak{h}$, then for all $h \in S_{U,g}$ we have*

$$\|h\|_{U,g,\infty} \leq \nu_n \cdot \|h\|_{U,g,2}.$$

Note that $\tilde{\Gamma}_{U,g}$ acts freely on $\mathfrak{h}$ if and only if the quotient map $\mathfrak{h} \to X_{U,g}^{an}$ is unramified. This can always be achieved by suitably shrinking U; however, for our purposes later, we will need to be precise about this point.

These two norms have been compared in the case of classical modular curves (non-compact case, see for instance [8]) or in the compact case assuming that the weight is large (cf. [25]). As in the non-compact case, one might expect that for every $\epsilon > 0$, the quantity ν_n should be replaced by a factor $\ll_{n,\epsilon} Vol(X_{U,g})^{-1/2+\epsilon}$, where the volume is taken with respect to $d\mu_{\mathfrak{h}}$. Improvements in this direction are available in the non-compact case (see for instance [8]), but the techniques do not work in the absence of Fourier expansions. In any case, Theorem 8.1 suffices for our purposes.

8.2. **Injectivity radius.**

Let U be an open compact subgroup of $\mathbb{B}^\times$, let $g \in \mathbb{B}^\times$, and write $\Gamma := \Gamma_{U,g} = gUg^{-1} \cap B_+^\times$.

For $\gamma \in B_+^\times$ we write γ^* and $\tilde{\gamma}$ for its image in $SL_2(\mathbb{R})$ and in $PSL_2(\mathbb{R})$ respectively (via τ_1).

The systole of Γ is defined as

$$\sigma_\Gamma := \min\{d_{\mathfrak{h}}(x, \tilde{\gamma}\cdot x) : x \in \mathfrak{h}, \gamma \in \Gamma, x \neq \tilde{\gamma}\cdot x\}$$

where $d_{\mathfrak{h}}$ is the hyperbolic distance in $\mathfrak{h}$. Note that σ_Γ is twice the injectivity radius ρ_Γ of $X^{an}_{U,g}$.

Recall that if $u \in SL_2(\mathbb{R})$ is hyperbolic (i.e. $|tr(u)| > 2$), then for every $x \in \mathfrak{h}$ we have

$$d_{\mathfrak{h}}(x, \gamma x) = 2 \log |\lambda_u|$$

where λ_u is the eigenvalue of u with largest absolute value. We say that $\gamma \in B^\times_+$ is hyperbolic if γ^* is, and we write $\lambda_\gamma = \lambda_{\gamma^*}$.

Lemma 8.2. *Let $\gamma \in \Gamma$ be hyperbolic. Define $\beta := \mathrm{rn}(\gamma)^{-1}\gamma^2$, where, as before,* rn *denotes the reduced norm. Then we have the following:*

(i) *$\beta \in B^\times_+$, $\mathrm{rn}(\beta) = 1$ and it is in some maximal order of B.*

(ii) *β is hyperbolic and $d_{\mathfrak{h}}(x, \tilde{\beta}x) = 2d_{\mathfrak{h}}(x, \tilde{\gamma}x)$ for every $x \in \mathfrak{h}$*

(iii) *Let $K = F(\lambda_\beta)$. Then $[K : F] = 2$.*

(iv) *$\lambda_\beta \in O^\times_K$.*

(v) *$1/\lambda_\beta$ is a conjugate of λ_γ over F.*

(vi) *all other conjugates of λ_β over $\mathbb{Q}$ (if any) have modulus* 1*.*

Proof. Since $\gamma \in \Gamma \subseteq B^\times_+$, we have the first two assertions in (i). Also, since $\gamma \in gUg^{-1} \cap B^\times$ we see that $\mathrm{rn}(\gamma) \in O^\times_F$, so $\mathrm{rn}(\gamma)^{-1}\gamma^2$ is in some maximal order of B, proving (i). Item (ii) follows because $\tilde{\beta} = \tilde{\gamma}^2$.

In view of (i), the properties (iii)-(vi) for β are known, see for instance Section 12.3 of [67]. □

In particular, λ_β as in the previous lemma is a *Salem number* of degree $2n$, where $n = [F : \mathbb{Q}]$. Using the available partial progress on Lehmer's conjecture for the Mahler measure, one gets

Lemma 8.3. *If $\tilde{\Gamma}_{U,g}$ acts freely on $\mathfrak{h}$, then*

$$\rho_\Gamma \geq \frac{1}{2(\log(6n))^3}.$$

Proof. Since B is a division algebra, $\tilde{\Gamma}_{U,g}$ contains no non-trivial parabolic elements, and since it acts freely on $\mathfrak{h}$, it contains no elliptic elements either. Thus, every non-hyperbolic $\gamma \in \Gamma$ satisfies $\tilde{\gamma} = I$. It follows that there is $\gamma \in \Gamma$ hyperbolic with

$$2\rho_\Gamma = d_{\mathfrak{h}}(i, \tilde{\gamma} \cdot i) = \frac{1}{2} d_{\mathfrak{h}}(i, \tilde{\beta} \cdot i) = \log |\lambda_\beta| \qquad (i = \sqrt{-1} \in \mathfrak{h})$$

with β as in the previous lemma. The bound now follows from Corollary 2 in [105]. (We remark that even weaker bounds would suffice for our purposes, but we choose to use Voutier's result for the sake of concreteness.) □

8.3. **Proof of the norm comparison.** Recall that on $\mathfrak{h}$ (with complex variable $z = x + iy$) we consider the volume form

$$d\mu_{\mathfrak{h}}(z) = \frac{dx \wedge dy}{y^2}.$$

On the open unit disc $\mathbb{D}$ (with complex variable $w = u + vi$), let us consider

$$d\mu_{\mathbb{D}}(w) = \frac{4du \wedge dv}{(1 - (u^2 + v^2))^2}.$$

These volume forms come from the usual hyperbolic metrics $d_{\mathfrak{h}}$ and $d_{\mathbb{D}}$ on $\mathfrak{h}$ and $\mathbb{D}$ respectively, with constant curvature -1. For $z \in \mathfrak{h}$, $w \in \mathbb{D}$ and $r > 0$, we let $B_{\mathfrak{h}}(z, r)$ and $B_{\mathbb{D}}(w, r)$ be the corresponding balls of hyperbolic radius r centered at z and w respectively.

For any $\tau \in \mathfrak{h}$, the biholomorphic map

$$c_\tau : \mathbb{D} \to \mathfrak{h}, \quad c_\tau(w) = \Re(\tau) - \Im(\tau) i \cdot \frac{w + i}{w - i}$$

is an isometry for $d_{\mathbb{D}}$ and $d_{\mathfrak{h}}$. Furthermore, it satisfies $c_\tau(0)=\tau$ and $c_\tau^* d\mu_{\mathfrak{h}} = d\mu_{\mathbb{D}}$.

Lemma 8.4. *Let $t>0$ and let $B(0,t)$ be the Euclidean ball in $\mathbb{C}$ centered at 0 with radius t. Let h be holomorphic on a neighborhood of $B(0,t)$. Then*

$$\pi t^2 |h(0)|^2 \le \int_{B(0,t)} |h(z)|^2 dx\wedge dy.$$

Proof. This is immediate from expanding h as a power series and integrating $h\cdot \bar{h}$. □

Lemma 8.5. *Let $f:\mathfrak{h}\to\mathbb{C}$ be holomorphic, let $\tau\in\mathfrak{h}$ and let $r>0$. Then*

$$|f(\tau)|^2\Im(\tau)^2 \le \frac{e^{2r}}{4\pi(\tanh(r/2))^2}\int_{B_{\mathfrak{h}}(\tau,r)} |f(z)|^2 y^2 d\mu_{\mathfrak{h}}(z).$$

Proof. Let $f_\tau = c_\tau^* f$. It is a holomorphic function on $\mathbb{D}$ and we have

$$\begin{aligned}\int_{B_{\mathfrak{h}}(\tau,r)} |f(z)|^2 y^2 d\mu_{\mathfrak{h}}(z) &= \int_{B_{\mathbb{D}}(0,r)} |f_\tau(w)|^2 \Im(c_\tau(w))^2 d\mu_{\mathbb{D}}(w)\\ &= \int_{B_{\mathbb{D}}(0,r)} |f_\tau(w)|^2 \Im(c_\tau(w))^2 \frac{4du\wedge dv}{(1-(u^2+v^2))^2}\\ &\ge 4\int_{B_{\mathbb{D}}(0,r)} |f_\tau(w)|^2 \Im(c_\tau(w))^2 du\wedge dv.\end{aligned}$$

Note that

$$\inf\{\Im(c_\tau(w)) : w\in B_{\mathbb{D}}(0,r)\} = \inf\{\Im(z) : z\in B_{\mathfrak{h}}(\tau,r)\} = e^{-r}\Im(\tau)$$

and that if $B(0,t)$ denotes the Euclidean ball of radius t centered at 0, then we have $B(0,t) = B_{\mathbb{D}}(0,r)$ for $t=\tanh(r/2)$. So, from the previous lemma we get

$$\begin{aligned}\int_{B_{\mathfrak{h}}(\tau,r)} |f(z)|^2 y^2 d\mu_{\mathfrak{h}}(z) &\ge 4e^{-2r}\Im(\tau)^2 \int_{B(0,\tanh(r/2))} |f_\tau(w)|^2 du\wedge dv\\ &\ge 4\pi e^{-2r}(\tanh(r/2))^2\Im(\tau)^2|f(\tau)|^2.\end{aligned}$$

□

Proof of Theorem 8.1. Choose $\tau_0\in\mathfrak{h}$ such that $|h(\tau_0)|\Im(\tau_0) = \|h\|_{U,g,\infty}$ and apply Lemma 8.5 with $\tau=\tau_0$ and $2r = 1/(\log(6n))^3$. This choice of r together with Lemma 8.3 ensure

$$\int_{B_{\mathfrak{h}}(\tau,r)} |h(z)|^2 y^2 d\mu_{\mathfrak{h}} \le \|h\|^2_{U,g,2}.$$

□

9. Differentials on integral models

9.1. **Relative differentials on Shimura curves.** We now return to the case $F=\mathbb{Q}$.

Given a compact open subgroup $U\subseteq \mathbb{B}^\times$ contained in $O_{\mathbb{B}}^\times$, we write m_U for its level and $X_0^D(M,U)$ for the Shimura curve over $\mathbb{Q}$ associated to the compact open subgroup $U\cap U_0^D(M)$. Here, $N=DM$ is an admissible factorization, D is the discriminant of B, and we always assume m_U coprime to D.

Let $\mathscr{X}_0^D(M,U)$ be the standard integral model for $X_0^D(M,U)$ over $\mathbb{Z}[m_U^{-1}]$, constructed as coarse moduli scheme for the moduli problem of abelian surfaces with quaternionic multiplication (i.e. fake elliptic curves) and $U_0^D(M)\cap U$-structure. (This direct moduli approach to integral models is available as we are working over $\mathbb{Q}$.)

Let $p\nmid m_U$ be a prime. For $p|D$ the reduction of $\mathscr{X}_0^D(M,U)$ is of Cerednik-Drinfeld type, for $p|M$ it is of Deligne-Rapoport type, and for $p\nmid Nm_U$ the integral model has good reduction.

Let $\mathscr{X}_0^D(M,U)^0$ be the smooth locus of $\mathscr{X}_0^D(M,U) \to \operatorname{Spec}\mathbb{Z}[m_U^{-1}]$. It is obtained from $\mathscr{X}_0^D(M,U)$ by removing the supersingular points in the special fibres of characteristic dividing D, and removing supersingular points and non-reduced components of the special fibres of characteristic dividing M (non-reduced components in characteristic p only occur when $p^2|M$).

There is a natural forgetful $\mathbb{Z}[m_U^{-1}]$-map

$$\pi_{M,U}^D : \mathscr{X}_0^D(M,U) \to \mathscr{X}_0^D(1,U).$$

Given $N = DM$, we say that U is *good enough* for (D,M) if the following conditions are satisfied:

(i) m_U is coprime to N;

(ii) $\operatorname{rn}(U) = \hat{\mathbb{Z}}$;

(iii) $U \subseteq U_1^D(\ell)$ for some prime $\ell \geq 5$ with $\ell \nmid D$.

See [12] for details on these conditions. Thus, when U is good enough for (D,M), we have that both $\mathscr{X}_0^D(1,U)/\mathbb{Z}[m_U^{-1}]$ and $\mathscr{X}_0^D(M,U)/\mathbb{Z}[m_U^{-1}]$ are fine moduli spaces for the associated moduli problems (by (i) and (iii)), and they have geometrically connected generic fibre (by (i) and (ii)). In this section we prove:

Theorem 9.1. *Suppose that U is good enough for (D,M). The integer M anihilates the sheaf of relative differentials $\Omega^1_{\pi^D_{M,U}}$ on $\mathscr{X}_0^D(M,U)^0$.*

Assuming this result for the moment, we obtain:

Corollary 9.2. *Suppose that U is good enough for (D,M). On $\mathscr{X}_0^D(M,U)^0$, the canonical morphism of sheaves*

$$(\pi_{M,U}^D)^*\Omega^1_{\mathscr{X}_0^D(1,U)^\circ/\mathbb{Z}[m_U^{-1}]} \to \Omega^1_{\mathscr{X}_0^D(M,U)^\circ/\mathbb{Z}[m_U^{-1}]}$$

is injective and its cokernel is annihilated by M.

Proof. The map is injective because it is non-zero, and on the smooth locus the two sheaves are invertible.

The assertion about the cokernel follows from the fundamental exact sequence of relative differentials and the previous theorem. □

9.2. **Fibres at primes dividing M.** Suppose that $U \subseteq O_{\mathbb{B}}^\times$ is good enough for (D,M).

Let p be a prime dividing M, and let n, m be positive integers defined by $p \nmid m$ and $M = p^n m$. The fibre of $\mathscr{X}_0^D(M,U)$ at p is described as follows (cf. Chapter 13 in [56], suitably adapted to moduli of fake elliptic curves; see [12, 48] for this adaptation):

Put $k = \mathbb{F}_p$. The fibre $\mathscr{X}_0^D(M,U) \otimes k$ is formed by $n+1$ copies of $\mathscr{X}_0^D(m,U) \otimes k$ with suitable multiplicities, crossing at supersingular points. More precisely, for any pair of integers $a, b \geq 0$ with $a + b = n$, there is a geometrically integral closed sub-scheme $F_{a,b}$ of $\mathscr{X}_0^D(M,U) \otimes k$, isomorphic to the curve $\mathscr{X}_0^D(m,U) \otimes k$ and occurring with multiplicity $\varphi(p^{\min\{a,b\}})$ in $\mathscr{X}_0^D(M,U) \otimes k$, where φ is Euler's function. Then the irreducible components of $\mathscr{X}_0^D(M,U) \otimes k$ are precisely the curves $F_{a,b}$, with multiplicity $\varphi(p^{\min\{a,b\}})$, crossing at the super-singular points of $\mathscr{X}_0^D(M,U) \otimes k$. Note that $F_{n,0}$ and $F_{0,n}$ occur with multiplicity 1.

The map $\mathscr{X}_0^D(M,U) \to \mathscr{X}_0^D(m,U)$ induces maps $f_{a,b} : F_{a,b} \to \mathscr{X}_0^D(m,U) \otimes k$. The morphism $f_{n,0}$ is an isomorphism, and $f_{0,n}$ has degree p^n.

For the sake of exposition, let us recall that in the simplest case $U = O_{\mathbb{B}}^\times$, $D = 1$, $m = 1$, the above mentioned facts correspond to Kronecker's congruence for the modular polynomials Φ_{p^n}, namely

$$\Phi_{p^n}(X,Y) \equiv \prod_{\substack{a,b\geq 0\\ a+b=n\\ c=\min\{a,b\}}} (X^{p^{a-c}} - Y^{p^{b-c}})^{\phi(p^c)} \mod p.$$

9.3. **Annihilation of relative differentials.**

Lemma 9.3. *If U is good enough for (D, M), then the sheaf $\Omega^1_{\pi^D_{M,U}}$ is supported on the special fibres at primes dividing M, i.e.,*

$$\Omega^1_{\pi^D_{M,U}}|_{\mathscr{X}_0^D(M,U)[M^{-1}]} = 0.$$

Proof. Note that $\mathscr{X}_0^D(M,U)\otimes\mathbb{Z}[M^{-1}] = \mathscr{X}_0^D(1,U')$ with $U' = U_0(M)\cap U$. Since U is good enough for (D, M), we get that U' is good enough for $(D, 1)$. Since U and U' are contained in $U_1^D(\ell)$ with $\ell \geq 5$, the morphism $\mathscr{X}_0^D(1,U') \to \mathscr{X}_0^D(1,U)[M^{-1}]$ induced by the inclusion $U' \subseteq U$ is étale, hence the result. □

Proof of Theorem 9.1. First we perform a preliminary reduction.

Write $M = p^n m$ with p a prime, $p \nmid m$ and $n \geq 1$. Consider the forgetful map $\pi : \mathscr{X}_0^D(M,U) \to \mathscr{X}_0^D(m,U)$ and the factorization $\pi^D_{M,U} = \pi^D_{m,U}\pi$. We have the exact sequence

$$\pi^*\Omega^1_{\pi^D_{m,U}} \to \Omega^1_{\pi^D_{M,U}} \to \Omega^1_\pi \to 0.$$

Note that upon inverting p, the map π becomes the forgetful $\mathbb{Z}[(pm_U)^{-1}]$-morphism

$$\mathscr{X}_0^D(m,U') \to \mathscr{X}_0^D(m,U) \otimes \mathbb{Z}[p^{-1}]$$

with $U' = U \cap U_0^D(p^n)$, which is étale because U is good enough. So, $\Omega^1_\pi[p^{-1}] = 0$. Furthermore, it also follows that away from characteristic p we have $\pi^{-1}\mathscr{X}_0^D(m,U)^0[1/p] = \mathscr{X}_0^D(M,U)^0[1/p]$. Thus, if one knows that m annihilates $\Omega^1_{\pi^D_{m,U}}|_{\mathscr{X}_0^D(m,U)^0}$, then the previous exact sequence would show that m also annihilates $\Omega^1_{\pi^D_{M,U}}|_{\mathscr{X}_0^D(M,U)^0}$ away from characteristc p. To complete the argument, it would suffice that p^n annihilates $\Omega^1_{\pi^D_{M,U}}|_{\mathscr{X}_0^D(M,U)^0}$ after inverting m. This would follow if we show that p^n annihilates $\Omega^1_{\pi^D_{p^n,U''}}|_{\mathscr{X}_0^D(p^n,U'')^0}$ where $U'' = U \cap U_0^D(m)$, because $\mathscr{X}_0^D(1,U'') \to \mathscr{X}_0^D(1,U) \otimes \mathbb{Z}[1/m]$ is étale.

From the previous analysis, we see —by induction on the number of distinct prime factors of M— that it suffices to prove the result in the particular case $M = p^n$ for p a prime and $n \geq 1$. So let's assume that this is the case.

By Lemma 9.3 we only need to show that p^n annihilates $\Omega^1_{\pi^D_{p^n,U}}|_{\mathscr{X}_0^D(p^n,U)^0}$ étale-locally on the fibre at p of $\mathscr{X}_0^D(p^n,U)^0$, that is, for points on the ordinary locus of the components $F_{n,0}$ and $F_{0,n}$ of the special fibre at p.

Write $k = \mathbb{F}_p$, let K be an algebraic closure of k and let W be the ring of Witt vectors of K. Let $y_0 \in \mathscr{X}_0^D(p^n,U)^0$ be a closed point with residue characteristic p and let $x_0 \in \mathscr{X}_0^D(1,U)^0$ be its image under $\pi^D_{p^n,U}$. Let y be a K-valued point in $\mathscr{X}_0^D(p^n,U)^0 \otimes W$ lying above y_0 and let x be its image in $\mathscr{X}_0^D(1,U)^0 \otimes W$. Let $\mathscr{A} = W[[T]]$ so that we have an isomorphisms of complete local rings involving the completed strict henselization of $\mathscr{O}_{\mathscr{X}_0^D(1,U)^0,x_0}$ (cf. p.133-134 in [56]):

$$(\mathscr{O}^{s.h.}_{\mathscr{X}_0^D(1,U)^0,x_0})^\wedge \simeq \widehat{\mathscr{O}}_{\mathscr{X}_0^D(1,U)^0\otimes W,x} \simeq \mathscr{A}. \tag{17}$$

Since x is in the ordinary locus, Serre-Tate theory (cf. section 8.9 in [56], see also [12] for an adaptation to deformations of fake elliptic curves) gives $\mathscr{A}$ the structure of a $\mathbb{Z}[q, q^{-1}]$-algebra by letting q be the Serre-Tate parameter of the pull-back of the universal family over $\mathscr{X}_0^D(1,U)$ (recall that U is good enough). Denote the image of q in $\mathscr{A}$ again by q, so that $q \in \mathscr{A}^\times$.

By the isomorphism (17), we have that $(\mathscr{O}^{s.h.}_{\mathscr{X}_0^D(p^n,U)^0,y_0})^\wedge$ is a finite $\mathscr{A}$-algebra under the pull-back map. By Theorem 13.6.6 in [56], this $\mathscr{A}$-algebra structure can be described as follows:

$$(\mathscr{O}^{s.h.}_{\mathscr{X}_0^D(p^n,U)^0,y_0})^\wedge \simeq \mathscr{B} := \begin{cases} \mathscr{A} & \text{if } y_0 \in F_{n,0} \cap \mathscr{X}_0^D(p^n,U)^0 \\ \mathscr{A}[Z]/(Z^{p^n}-q) & \text{if } y_0 \in F_{0,n} \cap \mathscr{X}_0^D(p^n,U)^0. \end{cases}$$

Finally, let us check that p^n annihilates the étale stalk $\Omega^{1,et}_{\pi^D_{p^n,U},y}$. It suffices to check this after completion. We have

$$(\Omega^{1,et}_{\pi^D_{p^n,U},y})^\wedge \simeq \Omega^1_{\pi^D_{p^n,U},y_0} \otimes (\mathscr{O}^{et}_{\mathscr{X}_0^D(p^n,U)^0,y})^\wedge \simeq \Omega^1_{\pi^D_{p^n,U},y_0} \otimes (\mathscr{O}^{s.h.}_{\mathscr{X}_0^D(p^n,U)^0,y_0})^\wedge \simeq \Omega^1_{\mathscr{B}/\mathscr{A}}.$$

If the ordinary point y_0 belongs to $F_{n,0}$, then the previous module is $\Omega^1_{\mathscr{A}/\mathscr{A}} = (0)$. On the other hand, if $y_0 \in F_{0,n}$ then using the fact that $\frac{d}{dZ}(Z^{p^n}-q) = p^n Z^{p^n-1}$ we find

$$\Omega^1_{\mathscr{B}/\mathscr{A}} \simeq \frac{\mathscr{A}[Z]}{(Z^{p^n}-q, p^n Z^{p^n-1})}.$$

Since $p^n q = Z\cdot p^n Z^{p^n-1} - p^n\cdot(Z^{p^n}-q)$ and $q \in \mathscr{A}^\times$, we see that the previous module is a quotient of $\mathscr{A}[Z]/p^n\mathscr{A}[Z]$, hence, it is annihilated by p^n. □

10. Bounds for the Manin constant

10.1. **The Manin constant.** Given an elliptic curve A over $\mathbb{Q}$ with conductor N, which is an optimal quotient $q : J_0(N) \to A$ with associated normalized newform $f \in S_2(N)$, we write c_f for its Manin constant (cf. Section 3). Thus, letting ω_A be a global Néron differential for A, the pull-back of ω_A under $\mathfrak{h} \to X_0(N) \to A$ is $2\pi i c_f f(z)dz$. Here, the map $X_0(N) \to A$ is $\phi = qj_N$. Multiplying ω_A by -1 if necessary, we assume that c_f is positive.

Edixhoven [30] proved that c_f is a non-zero integer. After the work of Mazur [70] and Abbes, Ullmo, and Raynaud [1] we know that if $v_p(N) \le 1$ then $v_p(c_f) = 0$, except, perhaps, for $p = 2$ in which case the assumption $v_2(N) \le 1$ only gives $v_2(c_f) \le 1$. (See [2] and the references therein for more results on the Manin constant.) This last caveat at $p = 2$ has been removed by recent work of Cesnavicius [16], so that now one knows that for every prime p the following implication holds:

$$v_p(N) \le 1 \Rightarrow p \nmid c_f.$$

Since the conductor of the elliptic curve A is N, we know that in the relevant cases

$$v_p(N) \le \begin{cases} 8 & \text{if } p = 2 \\ 5 & \text{if } p = 3 \\ 2 & \text{if } p \ge 5. \end{cases} \tag{18}$$

It is desirable to have control on $v_p(c_f)$ at all primes, not just when $v_p(N) \le 1$. However, not much is known about $v_p(c_f)$ in the general case. See [30] for some additional results when $p > 7$ is a prime of additive reduction[1].

We will prove:

Theorem 10.1. *Let S be a finite set of primes and let p be a prime number. There is a constant $\mu_{S,p}$ depending only on S and p, such that for every optimal elliptic curve A over $\mathbb{Q}$ with semi-stable reduction outside S and with associated newform $f \in S_2(N)$, we have*

$$v_p(c_f) \le \mu_{S,p}.$$

[1] In recent personal communication, Bas Edixhoven outlined a strategy that seems promising for obtaining further progress on these matters. Our methods, however, are completely different.

The following is an immediate consequence of the previous theorem and the known results about the Manin constant at primes with $v_p(N) \leq 1$.

Corollary 10.2. *Let S be a finite set of primes. There is a constant $\mathscr{M}_S$ depending only on S such that for every optimal elliptic curve A defined over $\mathbb{Q}$ with semi-stable reduction away from S and with associated newform $f \in S_2(N)$, we have $c_f \leq \mathscr{M}_S$.*

The proof of these results is motivated by the existing literature, especially [2, 15, 30]. Our main new contribution is the idea of working with towers of suitable modular curves with additional level structure to get good integral models, and our method to deal with the case when the additional level structure makes the relevant eigenform an old form.

10.2. **Setup for the proof of Theorem 10.1.** Let us fix a set of primes S, a prime number p, a positive integer $n \geq 2$, and an auxiliary prime number $\ell \geq 5$ different from p. We will prove:

Theorem 10.3. *There is a bound $\mathscr{B} = \mathscr{B}(S, p, n, \ell)$ such that for any given optimal elliptic curve A with conductor $N = p^n m$ and with associated newform $f \in S_2(N)$, satisfying that $p \nmid m$ and that m squarefree away from S, one has $v_p(c_f) \leq \mathscr{B}$.*

Note that the existence of such an A and our assumption $n \geq 2$ force $p \in S$.

For notational convenience, we will fix an optimal elliptic curve A as in Theorem 10.3 for the rest of this section. So we need to state explicitly the parameters on which each bound depends, and we will do so by adding appropriate subscripts to the asymptotic notation $\ll$, $O(-)$, $\asymp$.

Theorem 10.1 will follow by fixing the choice $\ell = 5$ unless $p = 5$ in which case we take $\ell = 7$, and from the fact that $n \leq 8$ by (18). The cases of semi-stable reduction at p (that is, $n = 0$ or 1) follow from the existing literature.

Since ℓ has to be chosen uniformly bounded, we are forced to consider the cases $\ell \mid N$ and $\ell \nmid N$ (equivalently, $\ell \mid m$ and $\ell \nmid m$) separately, the second being the more laborious.

Let $R = \mathbb{Z}_{(p)}$. Given an R-module M, we define

$$v(M) = \begin{cases} \infty & \text{if no power of } p \text{ annihilates } M_{tor}; \\ \min\{k \geq 0 : p^k \cdot M_{tor} = (0)\} & \text{otherwise.} \end{cases}$$

Since R is DVR, whenever M is finitely generated we have that $v(M)$ is finite and there is an element $x \in M$ such that $v(M) = v(\langle x \rangle)$.

When N is a free R-module, we say that $x \in N$ is primitive if $x \neq 0$ and $v(N/\langle x \rangle) = 0$.

More generally, for a $\mathbb{Z}$-module G, we write $v(G) := v(G[p^\infty])$. We observe that when G is a finitely generated $\mathbb{Z}$-module, $v(G)$ is the p-adic valuation of the exponent of the finite group G_{tor}.

10.3. **A projective system of curves.** In this section, m will always denote a positive integer coprime to p (possibly divisible by ℓ), and we will consider the curves $X_m := X_{U_0(p^n m) \cap U_1(\ell)}$. The notation X_m (and related notation to be introduced below) will be used with this meaning only in the present Section 10.

The curves X_m are defined over $\mathbb{Q}$ and are geometrically irreducible. The cusp $i\infty$ defines a $\mathbb{Q}$-rational point in X_m (possibly after conjugation of the open compact group $U_1(\ell)$, depending on conventions; cf. Variant 8.2.2 in [27]). The integral model over $\mathbb{Z}[1/\ell]$ provided by the theory of Deligne-Rapoport [26], Katz-Mazur [56] and Cesnavicius [14] can be base-changed to R, obtaining an integral model that we denote by $\mathscr{X}_m/R$. Then $\mathscr{X}_m$ is regular (since $\ell \geq 5$) and $\mathscr{X}_m \to \operatorname{Spec}(R)$ is flat and proper. Hence, $\mathscr{X}_m \to \operatorname{Spec}(R)$ is Gorenstein, and Grothendieck's duality theory (cf. [26]) applies. The relative dualizing sheaf is denoted by ω_m and it is invertible. Furthermore, for $m|m'$ both coprime to p, the forgetful map $\mathscr{X}_{m'} \to \mathscr{X}_m$ is etale and the pull back of ω_m is $\omega_{m'}$.

Let J_m be the Jacobian of X_m over $\mathbb{Q}$, and let $\mathscr{J}_m$ be the Néron model over R.

Since $\mathscr{X}_m/R$ has sections (e.g. the one induced by the cusp $i\infty$) and has some fibre components with multiplicity 1 (from the standard description of the special fibre at p) we see from Theorem 1, Sec. 9.7 [9] that $\mathrm{Pic}^0_{\mathscr{X}_m/R}$ is a scheme, the canonical map $\mathrm{Pic}^0_{\mathscr{X}_m/R} \to \mathscr{J}_m^0$ to the identity component of $\mathscr{J}_m$ is an isomorphism, and there are canonical identifications $H^1(\mathscr{X}_m, \mathscr{O}_{\mathscr{X}_m}) = \mathrm{Lie}(\mathrm{Pic}^0_{\mathscr{X}_m/R}) \simeq \mathrm{Lie}(\mathscr{J}_m)$.

Dualizing we obtain the R-isomorphisms

$$H^0(\mathscr{J}_m, \Omega^1) \simeq \mathrm{Lie}(\mathscr{J}_m)^\vee \simeq H^1(\mathscr{X}_m, \mathscr{O}_{\mathscr{X}_m})^\vee \simeq H^0(\mathscr{X}_m, \omega_m). \tag{19}$$

The cusp $i\infty$ defines a $\mathbb{Q}$-rational point of $X_0(p^n m, \ell)$, hence, an R-section $[i\infty]$ on $\mathscr{X}_m$. Let $\mathscr{X}_m^\infty$ be the open set of $\mathscr{X}_m$ obtained by deleting from $\mathscr{X}_m$ the fibre components that do not meet $[i\infty]$. In this way, $[i\infty]$ induces an R-morphism $j_m : \mathscr{X}_m^\infty \to \mathrm{Pic}^0(\mathscr{X}_m/R) = \mathscr{J}_m^0 \subseteq \mathscr{J}_m$. On $\mathscr{X}_m^\infty$ we have a canonical isomorphism between $\Omega^1_{\mathscr{X}_m/R}$ and ω_m, hence we obtain by pull-back

$$j_m^\bullet : H^0(\mathscr{J}_m, \Omega^1) \to H^0(\mathscr{X}_m^\infty, \omega_m).$$

One can check (say, by base change to $\mathbb{C}$) that this map factors through (19). In particular

$$v(\mathrm{coker}(j_m^\bullet)) = v\left(\frac{H^0(\mathscr{X}_m^\infty, \omega_m)}{H^0(\mathscr{X}_m, \omega_m)}\right).$$

On the étale projective system $\{\mathscr{X}_m\}_{p\nmid m}$ the invertible sheaves ω_m are compatible by pull-back as explained above. One can check that the theory of Conrad (cf. [21], specially Theorem B.3.2.1) for comparing integral structures applies in this slightly modified setting, which gives:

Theorem 10.4. *As m varies over integers coprime to p, we have*

$$v(\mathrm{coker}(j_m^\bullet)) = v\left(\frac{H^0(\mathscr{X}_m^\infty, \omega_m)}{H^0(\mathscr{X}_m, \omega_m)}\right) \ll_{p,n,\ell} 1. \tag{20}$$

In our application, note that we will be taking $n \le 8$ and $\ell = 5$ or 7, so the implicit constant will be bounded just in terms of p.

10.4. **Some reductions.** Let us write $X_{0,m} = X_0(p^n m)$, $J_{0,m} = J_0(p^n m)$, and consider the standard integral model $\mathscr{X}_{0,m} = \mathscr{X}_0(p^n m) \otimes R$ as well as the Néron model over R of $J_{0,m}$, which we denote by $\mathscr{J}_{0,m}$.

Let A be an elliptic curve of conductor $p^n m$ and assume that we have an optimal quotient $q : J_{0,m} \to A$. Let $\mathscr{A}$ be the Neron model of A over R, and let $\omega \in H^0(\mathscr{A}, \Omega^1)$ be a Neron differential.

Consider the embedding $j : X_{0,m} \to J_{0,m}$ induced by the cusp $i\infty$, and the modular parameterization $\phi = qj$. These extend to maps

$$\mathscr{X}_{0,m}^\infty \to \mathscr{J}_{0,m} \to \mathscr{A}$$

(that we still call j, q, ϕ) by the Néron mapping property, where $\mathscr{X}_{0,m}^\infty$ is obtained from $\mathscr{X}_{0,m}$ by deleting the fibre components that do not meet the section $[i\infty]$. The special fibre of $\mathscr{X}_{0,m}^\infty$ is irreducible and the p-adic valuation of the Manin constant c_f is the vanishing order $\phi^\bullet\omega$ along it, as a section of the line bundle $\Omega^1_{\mathscr{X}_{0,m}^\infty/R}$. Then one has

$$v_p(c_f) = v\left(\frac{H^0(\mathscr{X}_{0,m}^\infty, \Omega^1)}{R \cdot \phi^\bullet\omega}\right).$$

That the expression on the right agrees with the vanishing order of $\phi^\bullet\omega$ on the special fibre of $\mathscr{X}_{0,m}^\infty$ as a section of $\Omega^1_{\mathscr{X}_{0,m}^\infty/R}$, is seen by considerations on q-expansions along the section $[i\infty]$.

Unfortunately, the geometry of $\mathscr{X}_{0,m}$ is not convenient (in particular, duality theory is an issue). So we relate the previous expression to $\mathscr{X}_m$ instead, using the forgetful degeneracy map $\alpha : \mathscr{X}_m \to \mathscr{X}_{0,m}$. We have

$$v_p(c_f) = v\left(\frac{H^0(\mathscr{X}_{0,m}^\infty, \Omega^1)}{R \cdot \phi^\bullet \omega}\right) \leq v\left(\frac{H^0(\mathscr{X}_m^\infty, \Omega^1)}{R \cdot (\phi\alpha)^\bullet \omega}\right) \tag{21}$$

because α maps the cusp at infinity to the cusp at infinity, so, it restricts to $\mathscr{X}_m^\infty \to \mathscr{X}_{0,m}^\infty$.

However, there is the inconvenience (for later in our argument) that when $\ell \nmid m$, the modular form attached to A is no longer new for the group $U_0(p^n m) \cap U_1(\ell)$, and in that case we are led to also consider the standard second degeneracy map $\beta : \mathscr{X}_m \to \mathscr{X}_{0,m}$ induced on complex points by the map $z \mapsto \ell z$ on $\mathfrak{h}$.

The map β sends the cusp $i\infty$ to itself, so it restricts to $\mathscr{X}_m^\infty \to \mathscr{X}_{0,m}^\infty$, giving

$$v_p(c_f) = v\left(\frac{H^0(\mathscr{X}_{0,m}^\infty, \Omega^1)}{R \cdot \phi^\bullet \omega}\right) \leq v\left(\frac{H^0(\mathscr{X}_m^\infty, \Omega^1)}{R \cdot (\phi\beta)^\bullet \omega}\right). \tag{22}$$

When $\ell \nmid m$, it is important to note (say, by looking at q-expansions) that $(\phi\alpha)^\bullet\omega$ and $(\phi\beta)^\bullet\omega$ are R-linearly independent.

10.5. **The case $\ell \mid m$.** Suppose that $\ell | m$. Then the newform $f \in S_2(p^n m)$ attached to A for the group $U_0(p^n m)$ continues to be new for the group $U_0(p^n m) \cap U_1(\ell)$. Then we have an optimal quotient $\theta : J_m \to C$ with C an elliptic curve over $\mathbb{Q}$ isogenous to A. By optimality of θ, there is an isogeny $\pi : C \to A$ over $\mathbb{Q}$ such that the following diagram of morphisms over $\mathbb{Q}$ commutes

$$\begin{tikzcd} J_m \arrow[r, "\theta"] \arrow[d, "\alpha_*"] & C \arrow[d, "\pi"] \\ J_{0,m} \arrow[r, "q"] & A. \end{tikzcd} \tag{23}$$

Here, α_* is induced by the degeneracy map $\alpha : X_m \to X_{0,m}$ under Albanese functoriality.

Let $\mathscr{C}$ be the Néron model of C over R. We have the commutative diagram of R-morphisms

$$\begin{tikzcd} \mathscr{X}_m^\infty \arrow[r, "j_m"] \arrow[d, "\alpha"'] & \mathscr{J}_m \arrow[r, "\theta"] \arrow[d, "\alpha_*"] & \mathscr{C} \arrow[d, "\pi"] \\ \mathscr{X}_{0,m}^\infty \arrow[r, "j"] & \mathscr{J}_{0,m} \arrow[r, "q"] & \mathscr{A}. \end{tikzcd}$$

Dualizing (23), we find that $\alpha_*^\vee = \alpha^*$ (induced by Picard functoriality) extends $\pi^\vee$ after composition with the inclusions $q^\vee$ and $\theta^\vee$. Thus, $\deg \pi$ divides $\deg \alpha$, and the latter is

$$[U_0(p^n m) : U_0(p^n m) \cap U_1(\ell)] \leq [U(1) : U_1(\ell)].$$

Hence

$$v_p(\deg \pi) \ll_\ell 1.$$

Let $a \geq 0$ be an integer such that $\tilde{\omega} := p^{-a}\pi^\bullet\omega$ is a Néron differential on $\mathscr{C}$, and note that $a \leq v_p(\deg \pi) \ll_\ell 1$. Then we have

$$v_p(c_f) \leq v\left(\frac{H^0(\mathscr{X}_m^\infty, \Omega^1)}{R \cdot (\phi\alpha)^\bullet \omega}\right) = v\left(\frac{H^0(\mathscr{X}_m^\infty, \Omega^1)}{R \cdot \phi_m^\bullet \tilde{\omega}}\right) + a$$

where $\phi_m = \theta j_m$. Note that

$$v\left(\frac{H^0(\mathscr{X}_m^\infty, \Omega^1)}{R \cdot \phi_m^\bullet \tilde{\omega}}\right) \leq v(\mathrm{coker}(j_m^\bullet)) + v\left(\frac{H^0(\mathscr{J}_m, \Omega^1)}{R \cdot \theta^\bullet \tilde{\omega}}\right)$$

because $j_m^\bullet : H^0(\mathscr{J}_m, \Omega^1) \to H^0(\mathscr{X}_m^\infty, \Omega^1)$ is injective. So by (20) we deduce

$$v_p(c_f) \leq v\left(\frac{H^0(\mathscr{J}_m, \Omega^1)}{R \cdot \theta^\bullet \tilde{\omega}}\right) + O_{p,n,\ell}(1). \tag{24}$$

Let $\chi : \mathbb{T}_{U_0(p^n m)\cap U_1(\ell)} \to \mathbb{Z}$ be the system of Hecke eigenvalues attached to the optimal quotient θ. Let $P_\chi : H^0(\mathscr{J}_m, \Omega^1)_\mathbb{Q} \to H^0(\mathscr{J}_m, \Omega^1)_\mathbb{Q}$ be the orthogonal projection onto the χ-component with respect to the Petersson inner product. Observe that $\theta^\bullet \tilde{\omega} \in H^0(\mathscr{J}_m, \Omega^1)^\chi$, and from the equation $\theta\theta^\vee = [\deg \phi_m] \in \mathrm{End}(C)$ we deduce that the following diagram commutes:

$$\begin{tikzcd}
R \cdot \tilde{\omega} \arrow[r, "(\deg \phi_m)\cdot"] \arrow[d, "\theta^\bullet"'] & R \cdot \tilde{\omega} \\
H^0(\mathscr{J}_m, \Omega^1) \arrow[r] & \frac{H^0(\mathscr{J}_m,\Omega^1)}{(H^0(\mathscr{J}_m,\Omega^1)^\chi)^\perp} \arrow[u]
\end{tikzcd}$$

The rightmost arrow is induced by $(\theta^\vee)^\bullet$ and the fact that $\ker((\theta^\vee)^\bullet) = (H^0(\mathscr{J}_m, \Omega^1)^\chi)^\perp$. The bottom-right term in the diagram can be replaced by $P_\chi(H^0(\mathscr{J}_m, \Omega^1))$, which is an R-module of rank 1, and the bottom arrow can be replaced by P_χ. Chasing the image of $\tilde{\omega}$ we deduce

$$v_p(\deg \phi_m) \geq v\left(\frac{H^0(\mathscr{J}_m, \Omega^1)}{R \cdot \theta^\bullet \tilde{\omega}}\right) + v\left(\frac{P_\chi(H^0(\mathscr{J}_m, \Omega^1))}{H^0(\mathscr{J}_m, \Omega^1)^\chi}\right). \tag{25}$$

In [3] Theorem 3.6 (a), it is shown that the modular exponent (which equals the modular degree in the elliptic curve case) divides the *congruence exponent* (defined in terms of Fourier expansions at $i\infty$) for groups of the form $U_0(N)$ and $U_1(N)$. The same proof works for intermediate subgroups such as $U_0(p^n m) \cap U_1(\ell)$. So, the integer $\deg \phi_m$ divides the congruence exponent, which by definition is the exponent of

$$\frac{S_m(\mathbb{Z})}{(S_m(\mathbb{Z})^\chi)^\perp + S_m(\mathbb{Z})^\chi}$$

where $S_m(\mathbb{Z})$ is the subgroup of $S_2(U_0(p^n m) \cap U_1(\ell))$ consisting of modular forms with Fourier coefficients at $i\infty$ in $\mathbb{Z}$. By the q-expansion principle, we have a canonical isomorphism $S_m(\mathbb{Z}) \otimes R = H^0(\mathscr{X}_m^\infty, \Omega^1) = H^0(\mathscr{X}_m^\infty, \omega_m)$, which together with (19) gives

$$\begin{aligned}
v_p(\deg \phi_m) &\leq v\left(\frac{H^0(\mathscr{X}_m^\infty, \omega_m)}{(H^0(\mathscr{X}_m^\infty, \omega_m)^\chi)^\perp + H^0(\mathscr{X}_m^\infty, \omega_m)^\chi}\right) \\
&\leq v\left(\frac{H^0(\mathscr{X}_m^\infty, \omega_m)}{(H^0(\mathscr{X}_m, \omega_m)^\chi)^\perp + H^0(\mathscr{X}_m, \omega_m)^\chi}\right) \\
&\leq v\left(\frac{H^0(\mathscr{X}_m, \omega_m)}{(H^0(\mathscr{X}_m, \omega_m)^\chi)^\perp + H^0(\mathscr{X}_m, \omega_m)^\chi}\right) + v\left(\frac{H^0(\mathscr{X}_m^\infty, \omega_m)}{H^0(\mathscr{X}_m, \omega_m)}\right) \\
&= v\left(\frac{P_\chi(H^0(\mathscr{J}_m, \Omega^1))}{H^0(\mathscr{J}_m, \Omega^1)^\chi}\right) + v(\mathrm{coker}(j_m^\bullet)).
\end{aligned}$$

It follows from (20) and (25) that

$$v\left(\frac{H^0(\mathscr{J}_m, \Omega^1)}{R \cdot \theta^\bullet \tilde{\omega}}\right) \ll_{p,n,\ell} 1$$

which by (24) proves

$$v_p(c_f) \ll_{p,n,\ell} 1.$$

This concludes the proof of Theorem 10.3 in the case $\ell | m$. Note that the bound is independent of S, and we actually obtain

$$v_p(c_f) \leq 2v(\mathrm{coker}(j_m^\bullet)) + v_p(\deg \pi).$$

10.6. **The case $\ell \nmid m$.** Now we assume that $\ell \nmid m$ (and, as always, $\ell \neq p$). Then the newform $f \in S_2(p^n m)$ attached to A for the group $U_0(p^n m)$ is no longer new for the group $U_0(p^n m) \cap U_1(\ell)$. In fact, let $\chi : \mathbb{T}_{U_0(p^n m)\cap U_1(\ell)} \to \mathbb{Z}$ be the system of Hecke eigenvalues attached to this old form, then $\dim_{\mathbb{Q}} H^0(J_m, \Omega^1)^\chi = 2$, which is explained by the two degeneracy maps $\alpha, \beta : X_m \to X_{0,m}$.

Nevertheless, attached to χ we have an optimal quotient $\theta : J_m \to \Sigma$ over $\mathbb{Q}$, where Σ is an abelian surface isogenous to $A \times A$. By optimality of θ and considering the relevant cotangent spaces, we see that there is an isogeny $\pi : \Sigma \to A \times A$ over $\mathbb{Q}$ making the following diagram commutative:

$$\begin{tikzcd} J_m \arrow[r, "\theta"] \arrow[d, "\alpha_* \times \beta_*"] & \Sigma \arrow[d, "\pi"] \\ J_{0,m}^2 \arrow[r, "q \times q"] & A \times A. \end{tikzcd} \tag{26}$$

Lemma 10.5. *There is an integer $u \ll_{S,p,\ell} 1$ such that p^u annihilates the p-primary part of the kernel of π.*

Proof. Let $\sigma : X_m \to X_0(p^n m\ell)$ be the forgetful map, and write $\alpha_0, \beta_0 : X_0(p^n m\ell) \to X_{0,m}$ for the two degeneracy maps. We have $\alpha = \alpha_0\sigma$ and $\beta = \beta_0\sigma$, hence, the following diagram commutes:

$$\begin{tikzcd} J_0(p^n m\ell) \arrow[r, "\sigma^*"] & J_m & \Sigma^\vee \arrow[l, "\theta^\vee"'] \\ J_{0,m}^2 \arrow[u, "\alpha_0^* + \beta_0^*"] & J_{0,m}^2 \arrow[l, "="'] \arrow[u, "\alpha^* + \beta^*"'] & A \times A \arrow[l, "q^\vee \times q^\vee"'] \arrow[u, "\pi^\vee"'] \end{tikzcd} \tag{27}$$

The kernel of $\pi^\vee$ is Cartier-dual to that of π, so, it suffices to prove the claim for $\ker(\pi^\vee)$ instead.

The maps $q^\vee \times q^\vee$ and $\theta^\vee$ are injective as they are duals of optimal quotients, so, it suffices to bound a power of p that annihilates the p-primary part of $\ker(\alpha^* + \beta^*) \cap q^\vee(A) \times q^\vee(A)$.

Note that $\sigma_*\sigma^* = [\deg \sigma] \in \mathrm{End}(J_0(p^n m))$, so $v(\ker(\sigma^*)) \ll_\ell 1$. Hence

$$v\left(\ker((\alpha^* + \beta^*) \circ (q^\vee \times q^\vee))\right) = v\left(\ker((\alpha_0^* + \beta_0^*) \circ (q^\vee \times q^\vee))\right) + O_\ell(1)$$

and moreover $\ker((\alpha_0^* + \beta_0^*) \circ (q^\vee \times q^\vee))$ is isomorphic to

$$Z = \ker(\alpha_0^* + \beta_0^*) \cap (q^\vee(A) \times q^\vee(A)).$$

By Ihara's lemma in Ribet's formulation [81, 83], we have that $\ker(\alpha_0^* + \beta_0^*)$ is Eisenstein (in Mazur's terminology), so that for every prime $r \nmid pm\ell$ one has that T_r acts as $r + 1$ on it. On the other hand, when $r \nmid pm\ell$ we have that T_r acts as $\chi(T_r) = a_r(A)$ on $A \times A \subseteq J_{0,m}^2$. Thus, if Z has a (geometric) point of exact order p^e, we see that for all primes $r \nmid pm\ell$ we have $a_r(A) \equiv r + 1 \bmod p^e$. By Lemma 6.7 we obtain $e \ll_{S,p} 1$, which concludes the proof. □

The modular exponent $\tilde{n}_\Sigma$ of the optimal quotient $\theta : J_m \to \Sigma$ is defined as in [3], namely, as the exponent of the group $\ker(\theta\theta^\vee)$. The theory of [3] applies to the abelian surface Σ as in the first example of Section 3 in *loc. cit.*, with only some minor modifications due to the fact that we are working with the group $U_0(p^n m) \cap U_1(\ell)$ rather than a group of the form $U_0(N)$ or $U_1(N)$.

Consider the map

$$\tau = \pi\theta : J_m \to A \times A.$$

Then $\tau\tau^\vee = \pi\theta\theta^\vee\pi^\vee$, so that $v(\ker(\tau\tau^\vee)) = v_p(\tilde{n}_\Sigma) + O_{S,p,\ell}(1)$ by the previous lemma.

On the other hand, from the description $\tau = (q \times q) \circ (\alpha_* \times \beta_*) = (q\alpha_*) \times (q\beta_*)$ we see that

$$\tau\tau^\vee = [\deg(\phi)\deg(\alpha)]_A \times [\deg(\phi)\deg(\beta)]_A = [\deg(\phi)\deg(\alpha)]_{A\times A}. \tag{28}$$

It follows that

$$v_p(\deg(\phi)\deg(\alpha)) = v_p(\tilde{n}_\Sigma) + O_{S,p,\ell}(1). \tag{29}$$

Take any $\tilde{\omega} \in H^0(\mathscr{A}^2, \Omega^1)$ primitive. We make two observations about $\tilde{\omega}$.

First, we have

$$v\left(\frac{H^0(\mathscr{X}_m^\infty, \Omega^1)}{R \cdot (\tau j_m)^\bullet \tilde{\omega}}\right) \leq v(\operatorname{coker}(j_m^\bullet)) + v\left(\frac{H^0(\mathscr{J}_m, \Omega^1)}{R \cdot \tau^\bullet \tilde{\omega}}\right). \tag{30}$$

Secondly, we have

$$v_p(\deg(\phi)\deg(\alpha)) \geq v\left(\frac{H^0(\mathscr{J}_m, \Omega^1)}{R \cdot \tau^\bullet \tilde{\omega}}\right) + v\left(\frac{P_\chi(H^0(\mathscr{J}_m, \Omega^1))}{H^0(\mathscr{J}_m, \Omega^1)^\chi \cap \mathbb{Q} \cdot \tau^\bullet \tilde{\omega}}\right). \tag{31}$$

This last bound is proved by recalling (28), chasing $\tilde{\omega}$ in the diagram

$$\begin{tikzcd}
H^0(\mathscr{A}^2, \Omega^1) \arrow[r, "(\tau\tau^\vee)^\bullet"] \arrow[d, "\tau^\bullet"'] & H^0(\mathscr{A}^2, \Omega^1) \\
H^0(\mathscr{J}_m, \Omega^1) \arrow[r] & \frac{H^0(\mathscr{J}_m, \Omega^1)}{(H^0(\mathscr{J}_m, \Omega^1)^\chi)^\perp} \arrow[u]
\end{tikzcd},$$

noticing that the rightmost arrow is injective, replacing the bottom right term in the diagram by $P_\chi(H^0(\mathscr{J}_m, \Omega^1))$, and noticing that $H^0(\mathscr{J}_m, \Omega^1) \cap \mathbb{Q} \cdot \tau^\bullet \tilde{\omega} = H^0(\mathscr{J}_m, \Omega^1)^\chi \cap \mathbb{Q} \cdot \tau^\bullet \tilde{\omega}$. Here, P_χ is the orthogonal projection onto the χ-isotypical component.

Furthermore, since $\tau^\bullet$ maps $H^0(\mathscr{A}^2, \Omega^1)$ into $H^0(\mathscr{J}_m, \Omega^1)^\chi$ with torsion cokernel, we see that there is some $\tilde{\omega}_0 \in H^0(\mathscr{A}^2, \Omega^1)$ primitive such that

$$v\left(\frac{P_\chi(H^0(\mathscr{J}_m, \Omega^1))}{H^0(\mathscr{J}_m, \Omega^1)^\chi \cap \mathbb{Q} \cdot \tau^\bullet \tilde{\omega}_0}\right) = v\left(\frac{P_\chi(H^0(\mathscr{J}_m, \Omega^1))}{H^0(\mathscr{J}_m, \Omega^1)^\chi}\right)$$

We fix a choice of such an $\tilde{\omega}_0$, and for it we obtain from (29), (30), (31) and (20) that

$$v\left(\frac{P_\chi(H^0(\mathscr{J}_m, \Omega^1))}{H^0(\mathscr{J}_m, \Omega^1)^\chi}\right) + v\left(\frac{H^0(\mathscr{X}_m^\infty, \Omega^1)}{R \cdot (\tau j_m)^\bullet \tilde{\omega}_0}\right) \leq v_p(\tilde{n}_\Sigma) + O_{S,p,n,\ell}(1). \tag{32}$$

By [3] as in the case $\ell | m$ above, the modular exponent $\tilde{n}_\Sigma$ divides the congruence exponent associated to Σ, and one deduces

$$v_p(\tilde{n}_\Sigma) \leq v\left(\frac{P_\chi(H^0(\mathscr{J}_m, \Omega^1))}{H^0(\mathscr{J}_m, \Omega^1)^\chi}\right) + v(\operatorname{coker}(j_m^\bullet))$$

which together with (32) gives

$$v\left(\frac{H^0(\mathscr{X}_m^\infty, \Omega^1)}{R \cdot (\tau j_m)^\bullet \tilde{\omega}_0}\right) \ll_{S,p,n,\ell} 1. \tag{33}$$

Recall that we had a Neron differential $\omega \in H^0(\mathscr{A}, \Omega^1)$. Let π_1, π_2 be the two projections $\mathscr{A}^2 \to \mathscr{A}$ and let $\omega_i = \pi_i^\bullet \omega$. Then ω_1, ω_2 generate $H^0(\mathscr{A}^2, \Omega^1)$ as an R-module and we can write $\tilde{\omega}_0 = r_1\omega_1 + r_2\omega_2$ with $r_1, r_2 \in R$, at least one of them a unit. We observe that

$$\begin{aligned}
(\tau j_m)^\bullet \tilde{\omega}_0 &= r_1(\tau j_m)^\bullet(\omega_1) + r_2(\tau j_m)^\bullet(\omega_2) \\
&= r_1(\tau j_m)^\bullet \pi_1^\bullet(\omega) + r_2(\tau j_m)^\bullet \pi_2^\bullet(\omega) \\
&= r_1(\pi_1 \tau j_m)^\bullet(\omega) + r_2(\pi_2 \tau j_m)^\bullet(\omega) \\
&= r_1(q\alpha_* j_m)^\bullet(\omega) + r_2(q\beta_* j_m)^\bullet(\omega) \\
&= r_1(qj\alpha)^\bullet(\omega) + r_2(qj\beta)^\bullet(\omega) \\
&= r_1(\phi\alpha)^\bullet(\omega) + r_2(\phi\beta)^\bullet(\omega).
\end{aligned}$$

We claim that

$$\min\left\{v\left(\frac{H^0(\mathscr{X}_m^\infty,\Omega^1)}{R\cdot(\phi\alpha)^\bullet(\omega)}\right), v\left(\frac{H^0(\mathscr{X}_m^\infty,\Omega^1)}{R\cdot(\phi\beta)^\bullet(\omega)}\right)\right\} \leq v\left(\frac{H^0(\mathscr{X}_m^\infty,\Omega^1)}{R\cdot(\tau j_m)^\bullet\tilde{\omega}_0}\right). \tag{34}$$

In fact, this follows by interpreting the three terms appearing in the expression as the vanishing orders of the corresponding differential forms along the (irreducible) special fibre of $\mathscr{X}_m^\infty$.

Finally, from (21) and (22) we obtain

$$v_p(c_f) \leq \min\left\{v\left(\frac{H^0(\mathscr{X}_m^\infty,\Omega^1)}{R\cdot(\phi\alpha)^\bullet(\omega)}\right), v\left(\frac{H^0(\mathscr{X}_m^\infty,\Omega^1)}{R\cdot(\phi\beta)^\bullet(\omega)}\right)\right\}.$$

By (33) and (34) we get

$$v_p(c_f) \ll_{S,p,n,\ell} 1$$

which concludes the proof of Theorem 10.3 in the case $\ell \nmid m$. This completes the proof of Theorem 10.3, hence, of Theorem 10.1.

11. Counting imaginary quadratic extensions of $\mathbb{Q}$

11.1. **The counting result.** We will be interested in having a suitable Heegner point in $X_0^D(M)$. This will be achieved by showing the existence of sufficiently many imaginary quadratic extensions $K/\mathbb{Q}$ satisfying certain technical conditions.

For a Dirichlet character χ, we let $L(s,\chi)$ be its L-function. If D is a fundamental discriminant, we write K_D for the quadratic number field of discriminant D, and χ_D for the non-trivial quadratic Dirichlet character associated to K_D. The counting result is the following.

Theorem 11.1. *There is a uniform constant κ such that the following holds:*

Let $\theta > 0$. For $x > 1$ and coprime positive integers D and M, let $S_\theta(D,M,x)$ be the set of positive integers d satisfying the following conditions:

(i) $x < d \leq 2x$
(ii) $d \equiv -1 \mod 4$ *and d is squarefree (hence, $-d$ is a fundamental discriminant);*
(iii) *p splits in K_{-d} for each prime $p|M$*
(iv) *p is inert in K_{-d} for each prime $p|D$*
(v) $\#Cl(K_{-d}) > d^{0.5-\theta}$
(vi) $\left|\frac{L'}{L}(1,\chi_{-d})\right| < \kappa \log\log d.$

Then, writing $N = DM$, we have that for $x \gg_\theta 1$

$$\#S_\theta(D,M,x) = \frac{x}{2^{\omega(N)+1}\zeta(2)\prod_{p|2N}(1+\frac{1}{p})} + O(x^{1/2}N^{1/4}(\log N)^{1/2})$$

where the implicit constant is absolute.

Corollary 11.2. *Let $\theta > 0$ and $\delta > 0$. With the notation of Theorem 11.1, for $N \gg_{\theta,\delta} 1$ and $x > N^{0.5+\delta}$, we have*

$$\#S_\theta(D,M,x) > x^{1-\delta}.$$

11.2. **Preliminaries on L-functions.** We need two analytic results about $L(s,\chi_D)$ where D is a fundamental discriminant.

The next result is Corollary 2.5 in [62].

Proposition 11.3. *Let $\epsilon > 0$. There is a number $c_\epsilon > 0$ depending only on ϵ such that the bound*

$$\left|\frac{L'}{L}(1,\chi_D)\right| < c_\epsilon \log\log|D|$$

holds for all but $O_\epsilon(x^\epsilon)$ fundamental discriminants D with $|D| < x$.

We also need Siegel's classical bound for the class number. The following explicit version is due to Tatuzawa [98].

Proposition 11.4. *Let $0 < \epsilon < 1/12$. For $-d$ a negative fundamental discriminant with $d > e^{1/\epsilon}$, the bound*
$$\#Cl(\mathbb{Q}(\sqrt{-d})) > 0.2 \cdot d^{0.5-\epsilon}$$
holds with at most one exception.

11.3. **Lemmas on squarefrees.**

Lemma 11.5. *Let $m > 1$ be a positive integer and let χ be a non-principal Dirichlet character to the modulus m (not necessarily primitive). For $x \geq 1$ we have*
$$\left| \sum_{d \leq x} \mu^2(d)\chi(d) \right| \leq 5x^{1/2}m^{1/4}(\log m)^{1/2}.$$

Proof. When $x \leq m^{1/2} \log m$ we see that the required sum is bounded by
$$x \leq x^{1/2}m^{1/4}(\log m)^{1/2}$$
so we may assume that $x > m^{1/2} \log m$.

Let $y \leq x^{1/2}$ be a positive integer. We have
$$\sum_{d \leq x} \mu^2(d)\chi(d) = \sum_{d \leq x} \chi(d) \sum_{k^2 | d} \mu(k) = \sum_{k \leq x^{1/2}} \mu(k)\chi(k^2) \sum_{r \leq x/k^2} \chi(r) = S_1 + S_2$$
where S_1 corresponds to terms with $k \leq y$, and S_2 corresponds to those with $y < k \leq x^{1/2}$. By Polya-Vinogradov
$$|S_1| \leq 2ym^{1/2} \log m,$$
while for S_2 we have the trivial bound
$$|S_2| \leq x \sum_{k > y} \frac{1}{k^2} < \frac{x}{y}.$$
Take $y = \lceil x^{1/2}m^{-1/4}(\log m)^{-1/2} \rceil$ and note that
$$\frac{x^{1/2}}{m^{1/4}(\log m)^{1/2}} \leq y \leq \frac{2x^{1/2}}{m^{1/4}(\log m)^{1/2}}$$
because $x > m^{1/2} \log m$. The result follows. □

Lemma 11.6. *Let a be and odd residue class modulo 4, let m be a positive integer and let $x > 1$. Then*
$$\sum_{\substack{d \leq x \\ (d,m)=1 \\ d \equiv a\,(4)}} \mu^2(d) = \frac{x}{2\zeta(2) \prod_{p|2m} \left(1 + \frac{1}{p}\right)} + O(x^{1/2}m^{1/4}(\log m)^{1/2}).$$

Proof. Let ψ_0 and ψ be the principal and the non-principal characters modulo 4 respectively. By the previous lemma we have
$$2 \sum_{\substack{d \leq x \\ (d,m)=1 \\ d \equiv a\,(4)}} \mu^2(d) = \sum_{\substack{d \leq x \\ (d,m)=1}} \mu^2(d)\psi_0(d) + \psi(a) \sum_{\substack{d \leq x \\ (d,m)=1}} \mu^2(d)\psi(d)$$
$$= \sum_{\substack{d \leq x \\ (d,2m)=1}} \mu^2(d) + O(x^{1/2}m^{1/4}(\log m)^{1/2}).$$

The number of positive integers coprime to A up to a bound y is

$$\sum_{n\le y}\sum_{b|(A,n)}\mu(b)=\sum_{b|A}\mu(b)\Big(\frac{y}{b}+O(1)\Big)=\frac{\phi(A)y}{A}+O(2^{\omega(A)}).$$

Taking $A=2m$ and writing $\mu^2(d)=\sum_{b^2|d}\mu(b)$ we find

$$\begin{aligned}\sum_{\substack{d\le x\\(d,2m)=1}}\mu^2(d)&=\sum_{\substack{b\le x^{1/2}\\(b,2m)=1}}\mu(b)\sum_{\substack{c\le x/b^2\\(c,2m)=1}}1\\&=\frac{\phi(2m)x}{2m}\sum_{\substack{b\le x^{1/2}\\(b,2m)=1}}\frac{\mu(b)}{b^2}+O(2^{\omega(m)}x^{1/2})\\&=\frac{\phi(2m)x}{2m}\sum_{\substack{b=1\\(b,2m)=1}}^{\infty}\frac{\mu(b)}{b^2}+O(x^{1/2}+2^{\omega(m)}x^{1/2}).\end{aligned}$$

The infinite series is no other than $1/\zeta(2)$ with the Euler factors for primes dividing $2m$ removed, hence the result because $2^{\omega(m)}\ll_\epsilon m^\epsilon$. □

11.4. **Proof of the counting result.** We will restrict ourselves to $d>0$ squarefree satisfying $d\equiv 3\,(4)$, in which case $-d$ is a negative fundamental discriminant. Thus, χ_{-d} is the non-principal Dirichlet character associated with the imaginary quadratic field $K_{-d}=\mathbb{Q}(\sqrt{-d})$, and the discriminant of K_{-d} is precisely $-d$.

Under our assumption on d, the character χ_{-d} is the Kronecker symbol $(\frac{-d}{\cdot})$. It has conductor d and is determined by the following conditions on primes: for p odd, $\chi_{-d}(p)$ is the Legendre symbol $(\frac{-d}{p})$, and for $p=2$ we have

$$\chi_{-d}(2)=\begin{cases}1 & \text{if } d\equiv 7\,(8)\\ -1 & \text{if } d\equiv 3\,(8).\end{cases}$$

Equivalently, the values of χ_{-d} at primes are determined by

$$\chi_{-d}(p)=\begin{cases}0 & \text{if } p \text{ ramifies in } K_{-d}\\ 1 & \text{if } p \text{ splits in } K_{-d}\\ -1 & \text{if } p \text{ is inert in } K_{-d}.\end{cases}$$

Proof of Theorem 11.1. Let $S'(D,M,x)$ be the set of positive integers d satisfying conditions (i), (ii), (iii), and (iv) of the statement of Theorem 11.1. For each pair (D,M) and each prime $p|N=DM$, define the numbers

$$\epsilon_p=\epsilon_p(D,M)=\begin{cases}1 & \text{if } p|M\\ -1 & \text{if } p|D\end{cases}$$

and define ϵ_b for all divisors b of N as $\epsilon_b = 0$ if b is not squarefree, and multiplicatively otherwise (using the numbers ϵ_p). Then we have

$$\begin{aligned}
\#S'(D,M,x) &= 2^{-\omega(N)} \sum_{\substack{x<d\le 2x\\ (d,N)=1\\ d\equiv 3\,(4)}} \mu(d)^2 \prod_{p\mid N} (1+\epsilon_p\chi_{-d}(p))\\
&= 2^{-\omega(N)} \sum_{\substack{x<d\le 2x\\ (d,N)=1\\ d\equiv 3\,(4)}} \mu(d)^2 \sum_{b\mid N} \epsilon_b\chi_{-d}(b).
\end{aligned}$$

Writing 1_N for the principal character to the modulus N, we find

$$\#S'(D,M,x) = 2^{-\omega(N)} \sum_{b\mid N} \epsilon_b \sum_{\substack{x<d\le 2x\\ d\equiv 3\,(4)}} \mu^2(d) \left(\frac{-d}{b}\right) \cdot 1_N(d).$$

By Lemma 11.6 the contribution to the previous expression coming from $b=1$ is

$$2^{-\omega(N)} \sum_{\substack{x<d\le 2x\\ (d,N)=1\\ d\equiv 3\,(4)}} \mu^2(d) = \frac{x}{2^{\omega(N)+1}\zeta(2)\prod_{p\mid 2N}\left(1+\frac{1}{p}\right)} + O(x^{1/2}N^{1/4}(\log N)^{1/2}).$$

When $b \neq 1$ is a squarefree divisor of N, the function $d \mapsto (\frac{-d}{b}) \cdot 1_N(d)$ is a Dirichlet character whose modulus divides $4N$, and it is non-principal because b is squarefree. Thus, by Lemma 11.5 we get

$$2^{-\omega(N)} \sum_{\substack{b\neq 1\\ b\mid N}} \epsilon_b \sum_{\substack{x<d\le 2x\\ d\equiv 3\,(4)}} \mu^2(d) \left(\frac{-d}{b}\right) \cdot 1_N(d) \ll x^{1/2}N^{1/4}(\log N)^{1/2}.$$

Therefore we find

$$\#S'(D,M,x) = \frac{x}{2^{\omega(N)+1}\zeta(2)\prod_{p\mid 2N}\left(1+\frac{1}{p}\right)} + O\left(x^{1/2}N^{1/4}(\log N)^{1/2}\right).$$

Finally, by Proposition 11.3 with $\epsilon = 1/2$ and Proposition 11.4 with $\epsilon = \theta/2$ we see that for $x \gg_\theta 1$ we have

$$\#S'(D,M,x) - \#S_\theta(D,M,x) \ll x^{1/2}$$

which concludes the proof, with the constant $\kappa = c_{1/2}$ from Proposition 11.3. □

12. Arakelov degrees

The purpose of this brief section is to introduce some notation related to Arakelov degrees of metrized line bundles. This will be used at various places later in the paper.

12.1. **Metrized line bundles on arithmetic curves.** Let L be a number field and write $S_L = \operatorname{Spec} O_L$. If $\mathscr{M}$ is an invertible sheaf (also called line bundle) on S_L, then $\mathfrak{M} = H^0(S_L, \mathscr{M})$ is a projective O_L-module of rank 1, and since S_L is affine we have $\mathscr{M} = \mathfrak{M}^\sim$. In this way, invertible sheaves on S_L correspond to projective O_L-modules of rank 1.

For every embedding $\sigma : L \to \mathbb{C}$ we let $|-|_\sigma$ be the absolute value on L induced by σ. A metrized line bundle on S_L is an invertible sheaf $\mathscr{M}$ (or equivalently, its associated projective O_L-module $\mathfrak{M}$) together with the following data: for each embedding $\sigma : L \to \mathbb{C}$, a norm $\|-\|_\sigma$ on $M_\sigma := \mathfrak{M} \otimes_\sigma \mathbb{C}$ compatible with the absolute value $|-|_\sigma$. Thus, a metrized invertible sheaf on S_L is a pair $\widehat{\mathscr{M}} = (\mathscr{M}, \{\|-\|_\sigma\}_\sigma)$ with the notation as before.

12.2. **Arakelov degree.** The Arakelov degree $\widehat{\deg}_L \widehat{\mathscr{M}}$ of a metrized line bundle $\widehat{\mathscr{M}}$ on S_L is defined as follows: take any non-zero $\eta \in \mathfrak{M} = H^0(S_L, \mathscr{M})$, then

$$\widehat{\deg}_L \widehat{\mathscr{M}} := \log \# \left(\mathfrak{M}/\langle \eta \rangle\right) - \sum_{\sigma : L \to \mathbb{C}} \log \|\eta\|_\sigma,$$

which is independent of the choice of $\eta \neq 0$. The Arakelov degree $\widehat{\deg}_L$ is additive on tensor products of metrized line bundles, so, it has an obvious extension to metrized $\mathbb{Q}$-line bundles.

We conclude by making two observations that will be useful in later sections of the paper. First, for any choice of $0 \neq \eta \in \mathfrak{M}$ we have

$$\widehat{\deg}_L \widehat{\mathscr{M}} \geq - \sum_{\sigma : L \to \mathbb{C}} \log \|\eta\|_\sigma.$$

Secondly, note that if $\mathscr{N}$ is an invertible sub-sheaf of $\mathscr{M}$, and the metrized line bundle $\widehat{\mathscr{N}}$ is defined by restricting the metrics at infinity of the metrized line bundle $\widehat{\mathscr{M}}$, then we have

$$\widehat{\deg}_L \widehat{\mathscr{N}} \leq \widehat{\deg}_L \widehat{\mathscr{M}}.$$

13. Arakelov height of Heegner points

13.1. **Heegner hypothesis for** (D, M)**.** Let D and M be coprime positive integers with D squarefree and $\omega(D)$ even. We say that a quadratic number field $K/\mathbb{Q}$ satisfies the *Heegner hypothesis for the pair* (D, M) if every prime $p|D$ is inert in K and every prime $p|M$ splits in K. In particular, the primes dividing DM are unramified in K.

If K satisfies the Heegner hypothesis for (D, M), there is an embedding $\psi : K \to B$ (with B the quaternion algebra of discriminant D) which is optimal for the Eichler order $R_0^D(M) \subseteq O_B$ of reduced discriminant M, in the sense that $\psi^{-1}(R_0^D(M)) = O_K$.

Fixing a choice of ψ this leads to a point $\tau_K \in \mathfrak{h}$ and the corresponding point $P_K \in X(K^{ab})$ (cf. Paragraph 4.4) with $X = \varprojlim X_U$ (cf. Paragraph 4.2). Its image $P_{K,D,M} := P_{K,U_0^D(M)}$ in $X_0^D(M)$ has residue field H_K, the Hilbert class field of K.

We call these points (D, M)*-Heegner points.* They are a particular case of the D-Heegner points discussed in Paragraph 4.4.

13.2. **Reduction of Heegner points.** We write $\mathscr{X}_0^D(M) = \mathscr{X}_0^D(M, U_1^D(1))$ for the normal integral model of $X_0^D(M)$, flat, projective over $\mathbb{Z}$, introduced in Paragraph 9.1, and we let $\mathscr{X}_0^D(M)^0 = \mathscr{X}_0^D(M, U_0^D(1))^0$ be the smooth locus of its structure map as in *loc cit.*

Lemma 13.1. *Let K be a quadratic imaginary extension of $\mathbb{Q}$ satisfying the (D, M)-Heegner hypothesis. Let U be be a compact open subgroup of $O_{\mathbb{B}}^\times$ with m_U coprime to DM. Let C be the closure of $P_{K,U_0^D(M)\cap U}$ in the surface $\mathscr{X}_0^D(M, U)$. Then C is contained in $\mathscr{X}_0^D(M, U)^0$.*

Proof. We observe that $\mathscr{X}_0^D(M, U)^0$ is the preimage of $\mathscr{X}_0^D(M)^0$ via the forgetful morphism $\mathscr{X}_0^D(M, U) \to \mathscr{X}_0^D(M)$. Thus, we may assume that $U = U^D(1)$. Furthermore, we only need to study the intersection of C with fibres at p with $p|DM$.

If $p|D$ then $P_{K,U_0^D(M)}$ does not reduce to a supersingular point because p does not ramify in K, and this suffices.

If $p|M$ then $P_{K,U_0^D(M)}$ does not reduce to a supersingular point because p splits in K and by same argument as in p. 256 in [44]. It remains to show that C does not meet a non-reduced component of the fibre at p (this case only occurs when M is not squarefree).

Since K satisfies the Heegner hypothesis for (D, M), the residue field of $P_{K,U_0^D(M)}$ is H_K. As p does not ramify in K, it does not ramify in H_K and we can base change to H_K obtaining an étale cover near the fibre at p. Now the multi-section C is the image of a section C_{H_K} of the structure map to $\operatorname{Spec} O_{H_K}$. Blowing-up the supersingular points of characteristic p we may work on a regular surface, and now Corollary 1.32 in p. 388 of [65] shows that C_{H_K} does not meet a non-reduced fibre. □

We remark that for $D = 1$, this is proved in Proposition (3.1) in [44]. One could also adapt the argument there to analyze the case $p|M$ in the previous proof.

13.3. **Metrized canonical sheaf.** The surface $\mathscr{X}_U = \mathscr{X}_0^D(1, U)$ is semi-stable over $\mathbb{Z}[m_U^{-1}]$, and when U is good enough in the sense of Paragraph 9.1, then $\mathscr{X}_U$ is regular. Let ω_U be the relative dualizing sheaf of $\mathscr{X}_U \to \operatorname{Spec} \mathbb{Z}[m_U^{-1}]$. Then ω_U is an invertible sheaf.

For each inclusion $U \subseteq V$ of open compact subgroups with U and V good enough, the map $\pi_V^U : \mathscr{X}_U \to \mathscr{X}_V$ is étale and

$$(\pi_V^U)^* \omega_V = \omega_U \tag{35}$$

by Ch. 6 of [65], more precisely, Lemma 4.26 and Theorem 2.32 in *loc. cit.*

For each U good enough, the *metrized canonical sheaf* $\widehat{\omega}_U$ on the surface $\mathscr{X}_U$ (over $\mathbb{Z}[m_U^{-1}]$) is defined as the line sheaf ω_U endowed with the following metric $\| - \|_U$ at infinity (defined away from cuspidal points, if any):

The base change of $\mathscr{X}_U$ to $\mathbb{C}$ is X_U^{an} and the relative dualizing sheaf becomes $\Omega^1_{X_U^{an}}$. The decomposition (7) has only one term (because U is good enough), so we can take $g_a = 1$ and drop it from the related notation. The uniformization $\xi_U : \mathfrak{h} \to \tilde{\Gamma}_U \backslash \mathfrak{h}$ is unramified, and the metric on $\Omega^1_{X_U^{an}}$ is defined by

$$\|\alpha_P\|_U = 2|f(\tau)|\Im(\tau) \tag{36}$$

for $P \in \tilde{\Gamma}_U \backslash \mathfrak{h} \subseteq X_U^{an}$, α a regular section of $\Omega^1_{X_U^{an}}$ near P, $\tau \in \mathfrak{h}$ a pre-image of P under ξ_U, and f holomorphic near τ such that $\xi_{U,g_a}^{\bullet} \alpha = f(z)dz$ on an appropriate neighborhood of $\tau \in \mathfrak{h}$.

When U is not good enough, we do not define a metrized canonical sheaf. We observe that the metric that we put on ω_U is not the Arakelov canonical metric, but instead, the hyperbolic metric. When $D = 1$ this metric has singularities at the cusps; otherwise, it is smooth.

At least two other alternative approaches to define metrized canonical bundles on integral models of Shimura curves are available in the literature. In [60] one works on the stack-theoretical integral model of $X_0^D(1)$, while in [114] one proceeds as above with two technical differences: the integral models for U sufficiently small used there come from the theory of integral models of curves of genus $g \geq 2$, and then quotient maps are used to define a version of $\widehat{\omega}_U$ as metrized $\mathbb{Q}$-line bundles even when U is not sufficiently small. The geometric properties are deduced by relating them to integral models of auxiliary Shimura curves. The construction of integral models in [114] has the technical advantage of being available even beyond the case of Shimura curves over $\mathbb{Q}$, where a direct modular interpretation is no longer possible.

We will be interested on the Arakelov height of Heegner points with respect to the metrized line bundles $\widehat{\omega}_U$ (suitably defined in the next paragraph). The three methods for defining a metrized canonical sheaf are in fact equivalent for this purpose, as we will explain.

13.4. **Arakelov height.** Let P be an algebraic point in $X = \varprojlim X_U$. For each U we denote by P_U the image of P in X_U.

We define the Arakelov-theoretical *height of P with respect to the metrized canonical bundles*, denoted by $h_{Ar}(P)$, as follows:

Take any finite collection $\mathscr{U} = \{U_j\}_{j=1}^r$ of good enough open compact subgroups such that the numbers $m_j = m_{U_j}$ satisfy $\gcd(m_1, ..., m_r) = 1$. Let $U = \cap_{j=1}^r U_j$ and note that m_U has the same prime factors as $m_1 \cdots m_r$, and it is good enough too. Let $F_{P,U}$ be a field containing the residue field of P_U and let $S_{P,U} = \operatorname{Spec} O_{F_{P,U}}$. The point P_U extends to a map $s_U : S_{P,U}[m_U^{-1}] \to \mathscr{X}_U$.

Similarly, the points P_{U_j} extend to maps $s_j : S_{P,U}[m_j^{-1}] \to \mathscr{X}_{U_j}$, which are compatible in the sense that

$$s_j|_{S_{P,U}[m_U^{-1}]} = \pi^U_{U_j} \circ s_U.$$

As the U_j are good enough and $\gcd(m_j)_j = 1$, from the previous equation and (35) we deduce that the line sheaves $s_j^* \omega_{U_j}$ (each on $S_{P,U}[m_j^{-1}]$, respectively) glue together, defining a line sheaf on $S_{P,U}$ which we denote by $\omega_{P,U}$. The metrics at infinity induce a metric on $\omega_{P,U}$ for each $\sigma : F_{P,U} \to \mathbb{C}$. Thus, we obtain a metrized projective $O_{F_{P,U}}$-module $\widehat{\mathfrak{M}}$ of rank 1, namely, $\mathfrak{M} = H^0(S_{P,U}, \omega_{P,U})$ with the induced metrics at infinity, which we denote by $\|-\|_{\mathfrak{M},\sigma}$ for each embedding $\sigma : F_{P,U} \to \mathbb{C}$. This allows us to define $h_{Ar}(P)$ as the (normalized) Arakelov degree of $\widehat{\mathfrak{M}}$:

$$h_{Ar}(P) = \frac{\widehat{\deg}_{F_{P,U}} \widehat{\mathfrak{M}}}{[F_{P,U} : \mathbb{Q}]} \tag{37}$$

or more explicitly

$$h_{Ar}(P) = \frac{1}{[F_{P,U} : \mathbb{Q}]} \left(\log \# \left(\mathfrak{M}/\langle \eta \rangle \right) - \sum_{\sigma : F_{P,U} \to \mathbb{C}} \log \|\eta\|_{\mathfrak{M},\sigma} \right) \tag{38}$$

for any non-zero $\eta \in \mathfrak{M}$.

Note that we can always choose the required U_j, for instance, for any $r \geq 2$, we can take $U_j = U_1^D(\ell_j)$ with $\ell_j \geq 5$ distinct primes not dividing D. Furthermore, the number $h_{Ar}(P)$ only depends on P; it is independent of the choice of $\{U_j\}_j$, the choice of field $F_{P,U}$, and the choice of non-zero $\eta \in \mathfrak{M}$.

For Heegner points, one has the following explicit formula:

Theorem 13.2. *Let K be a quadratic imaginary field satisfying the Heegner hypothesis for D. Let P_K be the associated Heegner point in $X = \varprojlim X_U$. Let d_K be the absolute value of the discriminant of K, and let χ_K be the non-trivial primitive Dirichlet character attached to K. Then*

$$h_{Ar}(P_K) = -\frac{L'}{L}(0, \chi_K) + \frac{1}{2} \log \left(d_K^{-1} D \right). \tag{39}$$

Here, $L(s, \chi) = \sum_{n \geq 1} \chi(n) n^{-s}$ (for $\Re(s) > 1$). In the next two paragraphs, we explain how this height formula follows from the existing literature in the case $D > 1$. The case $D = 1$ will not be used in our work, but we remark that the result is still correct in that case, and it can be deduced directly from the Chowla-Selberg formula.

13.5. **The Chowla-Selberg formula, after Gross, Colmez, Kudla-Rapoport-Yang.** By work of Gross [42] and Colmez [19], the classical Chowla-Selberg formula can be understood as a formula for the semi-stable Falting's height of a CM elliptic curve. Kudla, Rapoport and Yang [60, 61] used this fact to give a height formula for Heegner points on Shimura curves with respect to a suitably defined metrized canonical bundle. Keeping track of normalizations, Theorem 13.2 with $D > 1$ can be deduced from the results of Kudla-Rapoport-Yang taking into account that the quantity c in Section 10 of [60] in our case is $c = 1$, because we only consider Heegner points subject to the Heegner hypothesis for D.

For the sake of exposition, let us briefly recall the method of proof in [60]. They work on $\mathfrak{X}_0^D(1)$, the moduli stack over $\mathbb{Z}$ associated to $X_0^D(1)$. First they show that the metrized canonical sheaf on $\mathfrak{X}_0^D(1)$ (the relative dualizing sheaf with metrics coming from the complex uniformization) can be identified, up to an explicit factor in the metrics at infinity, with the metrized Hodge bundle coming from the universal family of fake elliptic curves on $\mathfrak{X}_0^D(1)$ (cf. Section 3 [60]). The Arakelov height of an algebraic point P on $\mathfrak{X}_0^D(1)$ relative to the metrized Hodge bundle coincides with the Faltings height of the fake elliptic curve A_P associated to P, thus, the same holds (up to an explicit factor) for the height relative to the metrized canonical sheaf. On the other hand, when P is a CM point, A_P is isogenous to E_P^2 for certain CM elliptic curve E_P, thus the Faltings height of A_P equals $2h(E_P)$ up to a factor coming from the isogeny, which is made explicit in Theorem 10.7 [60]. Finally, $h(E_P)$ is expressed in terms of the logarithmic derivative of $L(s,\chi)$ by the classical Chowla-Selberg formula, as mentioned before.

The translation to our setting is possible because, upon adding level structure of a good enough U, the corresponding stack is in fact our scheme $\mathscr{X}_U$ over $\mathbb{Z}[m_U^{-1}]$, and the pull-back of the metrized canonical sheaf on $\mathfrak{X}_0^D(1)$ coincides with our $\widehat{\omega}_U$ up to suitable normalization factors on the metrics.

13.6. **The Yuan-Zhang height formula.** Another (more direct) way to deduce Theorem 13.2 from the existing literature is using a recent general result of Yuan and Zhang, namely, Theorem 1.5 in [114], along with their theory of integral models. The Yuan-Zhang theorem works for quaternionic Shimura curves over totally real fields in general, not just over $\mathbb{Q}$.

Using [114], the translation to our setting with $D > 1$ is almost immediate:

The finite parts of our metrized sheaves $\widehat{\omega}_U$ agree with the arithmetic Hodge bundle as defined in [114] when U is good enough, although in *loc. cit.* the definition is given in more generality (cf. Theorem 4.7 (2) *loc.cit.* and equation (35) above). The metrics at infinity in *loc.cit.* also agree (cf. Equation (36) above and Theorem 4.7 (3) *loc.cit.*).

The integral model for X_U over $\mathbb{Z}[m_U^{-1}]$ used in [114], for U small enough, is the minimal regular model. It is unique as X_U has genus $g_U \geq 2$. It can be obtained from our $\mathscr{X}_U$ by repeated blow-up and contraction *away from the smooth locus* $\mathscr{X}_U^0$. By Lemma 13.1 above, if K satisfies the Heegner hypothesis for D (in particular, the discriminant of K is coprime to D as required in [114]) the closure of the associated Heegner point in $\mathscr{X}_0^D(1)$ is contained in $\mathscr{X}_0^D(1)^0$, hence, the closure of $P_{K,U}$ in $\mathscr{X}_U$ is contained in $\mathscr{X}_U^0$. Therefore, this difference on integral models does not affect the height of Heegner points.

At this point, we mention that later, in Section 18, we will directly use the Yuan-Zhang theory of integral models and height formula over totally real fields.

13.7. **Functional equation.** Given an imaginary quadratic field K, the primitive quadratic character χ_K is odd, has conductor d_K, and the functional equation for $L(s,\chi_K)$ is given by $\xi(1-s,\chi_K) = \xi(s,\chi_K)$ where

$$\xi(s,\chi_K) = \left(\frac{d_K}{\pi}\right)^{(s+1)/2}\Gamma\left(\frac{s+1}{2}\right)L(s,\chi_K).$$

Thus,

$$-\frac{L'}{L}(1-s,\chi_K) = \log(d_K/\pi) + \frac{1}{2}\left(\frac{\Gamma'}{\Gamma}\left(\frac{s+1}{2}\right) + \frac{\Gamma'}{\Gamma}\left(\frac{2-s}{2}\right)\right) + \frac{L'}{L}(s,\chi_K)$$

and we see that an equivalent way to state formula (39) is

$$h_{Ar}(P_K) = \frac{L'}{L}(1,\chi_K) + \frac{1}{2}\log(d_K D) - (\gamma + \log(2\pi)) \tag{40}$$

where γ is the Euler-Mascheroni constant. This seems more natural from the point of view of analytic number theory because $\frac{L'}{L}(1,\chi_K)$ is expected to be small as K varies. For instance, from [51] one deduces the following:

Proposition 13.3. *As K varies over quadratic imaginary fields satisfying the Heegner hypothesis for D, if GRH holds for $L(s,\chi_K)$ then we have*

$$h_{Ar}(P_K) = \frac{1}{2}\log(d_K D) + O(\log\log d_K).$$

The implicit constant in the error term can be taken as $2+\epsilon$ for any $\epsilon > 0$ (for $d_K \gg_\epsilon 1$).

See also [52] for further results on the size of $\frac{L'}{L}(1,\chi)$, and see [20] for some related applications of analytic number theory to estimate the height of CM abelian varieties. In *loc. cit.*, however, analytic lower bounds for the height are found, while we need analytic upper bounds, which seems to be a more difficult problem from the point of view of L-functions.

We will not use Proposition 13.3. For our purposes, we will have some freedom to choose the quadratic imaginary field K, and an unconditional estimate for $h_{Ar}(P_K)$ of essentially the same strength can be deduced from Theorem 11.1.

14. Integrality and lower bounds for the L^2-norm

14.1. **Notation and result.** We are now ready to present a key application of our work in the previous sections. As always, D and M stand for coprime positive integers, with D squarefree with an even number of prime factors. Also, we write $N = DM$. In addition, we will assume $D > 1$; in fact, for the results in this section the case $D = 1$ is already known by using methods based on q-expansions, which are not available in the present case $D > 1$.

We will be working with open compact subgroups of the form $U = U_0^D(m) \cap U_1^D(m')$ with m, m' coprime, both coprime to D, in which case $C(U) = (1)$ so that X_U^{an} is connected. Thus, we can choose $g_a = 1$ in the decomposition (7) and write $\tilde{\Gamma}_U = \tilde{\Gamma}_{U,g_a}$. Similarly, with this choice we may drop the subscript g in the notation of the L^2 and supremum norms of Section 8.

For U as above, we write $\xi_U : \mathfrak{h} \to \tilde{\Gamma}_U \backslash \mathfrak{h} = X_U^{an}$ for the complex uniformization. We have an injective map into the space S_U of holomorphic of weight 2 modular forms for U

$$\Psi_U : H^0(X_U, \Omega^1) \to S_U$$

given by the condition that the image of a section α is the modular form $\Psi_U(\alpha) \in S_U$ satisfying that $\xi_U^\bullet \alpha = \Psi_U(\alpha) dz$ with z the complex variable in $\mathfrak{h}$ (cf. Paragraph 4.6).

Recall the normal integral model $\mathscr{X}_0^D(M) = \mathscr{X}_0^D(M, U_1^D(1))$, flat and projective over $\mathbb{Z}$, introduced in Paragraph 9.1. We let

$$\mathscr{S}_2^D(M) = \Psi_{U_0^D(M)}(H^0(\mathscr{X}_0^D(M)^0, \Omega^1_{\mathscr{X}_0^D(M)/\mathbb{Z}})) \subseteq S_2^D(M).$$

Thus, $\mathscr{S}_2^D(M)$ defines a notion of $\mathbb{Z}$-integrality in $S_2^D(M)$.

We note that when $D = 1$ (which we are not considering here), every element of $\mathscr{S}_2^D(M)$ has Fourier expansion (at $i\infty$) with Fourier coefficients in $2\pi i\mathbb{Z}$, but the converse usually fails, see [31] for details.

The main result in this section is:

Theorem 14.1 (Integral forms are not too small)**.** *Given $\epsilon > 0$, if $N \gg_\epsilon 1$ and if $N = DM$ is an admissible factorization with $D > 1$, then for every $f \in \mathscr{S}_2^D(M)$ integral non-zero modular form for $U_0^D(M)$ we have*

$$-\log \|f\|_{U_0^D(M),2} \le \left(\frac{5}{6} + \epsilon\right) \log N + \frac{1}{2} \log M.$$

We remark that in this result either D or M can be small (or even remain bounded) as long as the product $N = DM$ is sufficiently large in terms of ϵ.

14.2. **Lower bound for the height of Heegner points.**

Proposition 14.2. *Let K be a quadratic imaginary field satisfying the Heegner hypothesis for (D, M) and let $P_K \in X(K^{ab})$ be a Heegner point associated to K. Let H be a finite extension of K such that $P_{K,U_0^D(M)}$ is H-rational, and for each $\sigma : H \to \mathbb{C}$ choose $\tau_{K,\sigma} \in \mathfrak{h}$ such that $\xi_{U_0^D(M)}(\tau_{K,\sigma}) = P^\sigma_{K,U_0^D(M)}$.*

Let $\alpha \in H^0(\mathscr{X}_0^D(M)^0, \Omega^1_{\mathscr{X}_0^D(M)/\mathbb{Z}})$ be a non-zero section, write $f = \Psi_{U_0^D(M)}(\alpha)$ and suppose that f does not vanish at the points $\tau_{K,\sigma}$. We have

$$h_{Ar}(P_K) \geq -\log(2M) - \frac{1}{[H:\mathbb{Q}]} \sum_{\sigma: H \to \mathbb{C}} \log\left(|f(\tau_{K,\sigma})| \Im(\tau_{K,\sigma})\right).$$

Proof. Let $\ell_1, \ell_2 \geq 5$ be two distinct primes not dividing $N = DM$. Let $U_j = U_1^D(\ell_j)$ for $j = 1, 2$, let $U = U_1 \cap U_2$, and let H' be a finite extension of H such that $P_{K,U_0^D(M)\cap U}$ is H'-rational. Note that $H_K \subseteq H'$ because $P_{K,U_0^D(M)\cap U}$ maps to $P_{K,U_0^D(M)}$, and similarly, H' contains the residue field of $P_{K,U}$. In the notation of Paragraph 13.4 we let $\mathscr{U} = \{U_1, U_2\}$, $P = P_K$ and $F_{P,U} = H'$, obtaining the metrized $O_{H'}$-module $\mathfrak{M}$ of rank 1 with

$$h_{Ar}(P_K) = \frac{1}{[H':\mathbb{Q}]} \widehat{\deg}_{H'} \mathfrak{M}.$$

We would like to use the section α to construct a non-zero element of $\mathfrak{M}$, so that $h_{Ar}(P_K)$ can be computed as in (38). For this we construct a second metrized $O_{H'}$-module $\mathfrak{N}$ where α canonically induces an element, and such that $\mathfrak{M}$ maps to $\mathfrak{N}$ with controlled torsion cokernel (and respecting the metrics).

Let $S_{H'} = \operatorname{Spec} O_{H'}$. Let $s_U : S_{H'}[(\ell_1\ell_2)^{-1}] \to \mathscr{X}_U$ be the morphism associated to $P_{K,U}$, and for $j = 1, 2$ let $s_j : S_{H'}[\ell_j^{-1}] \to \mathscr{X}_{U_j}$ be the morphism associated to P_{K,U_j}. Similarly, we also have morphisms $s'_U : S_{H'}[(\ell_1\ell_2)^{-1}] \to \mathscr{X}_0^D(M, U)$ and $s'_j : S_{H'}[\ell_j^{-1}] \to \mathscr{X}_0^D(M, U_j)$ induced by the points $P_{K,U_0^D(M)\cap U}$ and $P_{K,U_0^D(M)\cap U_j}$ ($j = 1, 2$) respectively. These are compatible in the obvious way with the forgetful maps among the six surfaces.

Let ω, ω_j, ω', and ω'_j be the sheaves of relative differentials for $\mathscr{X}_U/\mathbb{Z}[(\ell_1\ell_2)^{-1}]$, $\mathscr{X}_{U_j}/\mathbb{Z}[\ell_j^{-1}]$, $\mathscr{X}_0^D(M, U)/\mathbb{Z}[(\ell_1\ell_2)^{-1}]$, and $\mathscr{X}_0^D(M, U_j)/\mathbb{Z}[\ell_j^{-1}]$ (for $j = 1, 2$) respectively. They are not invertible in general, although they are indeed invertible sheaves on the smooth loci of the corresponding structure maps.

The sheaves ${s'_j}^*\omega'_j$ on $S_{H'}[\ell_j^{-1}]$ glue along $s'^*\omega'$ to define a sheaf $\omega'_{P_K,U}$ on $S_{H'}$ in the same way that the line sheaves $s_j^*\omega_j$ determine $\omega_{P_K,U}$ on $S_{H'}$ (cf. Paragraph 13.4). This is because the forgetful maps $\pi^{U_0^D(M)\cap U}_{U_0^D(M)\cap U_j} : \mathscr{X}_0^D(M, U) \to \mathscr{X}_0^D(M, U_j)$ are étale (as U_j is sufficiently small), which can be used instead of (35) in order to check compatibility. Furthermore, $\omega_{P_K,U}$ and $\omega'_{P_K,U}$ are invertible sheaves on $S_{H'}$, by Lemma 13.1.

We define $\mathfrak{N} = H^0(\operatorname{Spec} O_{H'}, \omega'_{P_K,U})$, which is a projective $O_{H'}$-module of rank 1, endowed with the metrics coming from (36) and the complex uniformization of $X_0^D(M, U)^{an}$.

The non-zero global section $\alpha \in H^0(\mathscr{X}_0^D(M)^0, \Omega^1_{\mathscr{X}_0^D(M)/\mathbb{Z}})$ induces (via pull-back) compatible sections on

$$H^0(\mathscr{X}_0^D(M, U)^0, \Omega^1_{\mathscr{X}_0^D(M,U)/\mathbb{Z}[(\ell_1\ell_2)^{-1}]}) = H^0(\mathscr{X}_0^D(M, U)^0, \omega')$$

and

$$H^0(\mathscr{X}_0^D(M, U_j)^0, \Omega^1_{\mathscr{X}_0^D(M,U_j)/\mathbb{Z}[\ell_j^{-1}]}) = H^0(\mathscr{X}_0^D(M, U_j)^0, \omega'_j)$$

($j = 1, 2$) which determine an element $\beta \in \mathfrak{N}$.

Since $P_{K,U_0^D(M)}$ is H-rational, we have for each $\sigma : H' \to \mathbb{C}$ and each $\tau'_{K,\sigma} \in \mathfrak{h}$ mapping to $P^\sigma_{K,U_0^D(M)\cap U}$

$$(41)\qquad \pi^{U_0^D(M)\cap U}_{U_0^D(M)}(\xi_{U_0^D(M)\cap U}(\tau'_{K,\sigma})) = \pi^{U_0^D(M)\cap U}_{U_0^D(M)}(P_{K,U_0^D(M)\cap U})^\sigma = P^\sigma_{K,U_0^D(M)} = \xi_{U_0^D(M)}(\tau_{K,\sigma|_H}).$$

Since f is in the image of $\Psi_{U_0^D(M)}$, we see that condition that f does not vanish at the points $\tau_{K,\sigma}$ for $\sigma : H \to \mathbb{C}$ implies that $\beta \neq 0$.

We observe that the construction of $\mathfrak{M}$ factors through “adding level $U_0^D(M)$” in the sense that

$$s_j^*\omega_j = s_j'^*((\pi_{U_j}^{U_0^D(M)\cap U_j})^*\omega_j) \tag{42}$$

and similarly for $s^*\omega$. Furthermore, on the smooth loci we have exact sequences

$$0 \to (\pi_U^{U_0^D(M)\cap U})^*\omega|_{\mathscr{X}_0^D(M,U)^0} \to \omega'|_{\mathscr{X}_0^D(M,U)^0} \to \mathscr{C} \to 0$$

and

$$0 \to (\pi_{U_j}^{U_0^D(M)\cap U_j})^*\omega_j|_{\mathscr{X}_0^D(M,U_j)^0} \to \omega_j'|_{\mathscr{X}_0^D(M,U_j)^0} \to \mathscr{C}_j \to 0$$

with $\mathscr{C}$, $\mathscr{C}_j$ annihilated by the integer M, thanks to Corollary 9.2.

By (42) and Lemma 13.1, these exact sequences on smooth loci induce a map of $O_{H'}$-modules $\iota : \mathfrak{M} \to \mathfrak{N}$ which is still injective because the maps $\pi_{U_j}^{U_0^D(M)\cap U_j}$ and $\pi_U^{U_0^D(M)\cap U}$ are étale, and also by the non-vanishing assumption on f.

Thus, the cokernel of ι is annihilated by the integer M. Furthermore, the map ι is locally described by pull-back, and the forgetful maps are compatible with the complex uniformization of the relevant curves, so, the map ι respects the metrics at infinity. Thus, ι induces an inclusion $\widehat{\mathfrak{M}} \subseteq \widehat{\mathfrak{N}}$ of metrized $O_{H'}$-modules, whose cokernel is annihilated by M.

So, $M\beta \in \mathfrak{M}$ is a non-zero element, and from (38) we obtain

$$\begin{aligned} h_{Ar}(P_K) &= \frac{1}{[H':\mathbb{Q}]}\left(\log\#\left(\mathfrak{M}/\langle M\beta\rangle\right) - \sum_{\sigma:H'\to\mathbb{C}} \log\|M\beta\|_{\mathfrak{M},\sigma}\right) \\ &\geq \frac{-1}{[H':\mathbb{Q}]}\sum_{\sigma:H'\to\mathbb{C}} \log\|M\beta\|_{\mathfrak{M},\sigma} \\ &= -\log(M) - \frac{1}{[H':\mathbb{Q}]}\sum_{\sigma:H'\to\mathbb{C}} \log\|\beta\|_{\mathfrak{N},\sigma}. \end{aligned}$$

For each $\sigma : H' \to \mathbb{C}$ choose $\tau'_{K,\sigma} \in \mathfrak{h}$ such that $\xi_{U_0^D(M)\cap U}(\tau'_{K,\sigma}) = P^\sigma_{K,U_0^D(M)\cap U}$, then we have that the last expression is

$$-\log(M) - \frac{1}{[H':\mathbb{Q}]}\sum_{\sigma:H'\to\mathbb{C}} \log\left(2\cdot|f(\tau'_{K,\sigma})|\Im(\tau'_{K,\sigma})\right). \tag{43}$$

Also from (41) and the fact that f is in the image of $\Psi_{U_0^D(M)}$, it follows that (43) is equal to

$$-\log(2M) - \frac{1}{[H:\mathbb{Q}]}\sum_{\sigma:H\to\mathbb{C}} \log\left(|f(\tau_{K,\sigma})|\Im(\tau_{K,\sigma})\right)$$

which proves the result. □

14.3. L^2-norm of integral modular forms.

Lemma 14.3. *Let P be an algebraic point of $X_0^D(M)$ (non-cuspidal, as $D > 1$), and let P_j for $j = 1, \dots, r$ be the Galois conjugates of P, with $P_1 = P$, say. Let $\tau_j \in \mathfrak{h}$ be such that $\xi_{U_0^D(M)}(\tau_j) = P_j$ for each $1 \leq j \leq r$. Let $\alpha \in H^0(X_0^D(M), \Omega^1_{X_0^D(M)/\mathbb{Q}})$ and let $f = \Psi_{U_0^D(M)}(\alpha)$ be the associated modular form. Then f vanishes at one of the τ_j if and only if it vanishes at all of them.*

Furthermore, given $\eta > 0$, if $N \gg_\eta 1$ and $N = DM$, then f has at most $N^{1+\eta}$ zeros on $\mathfrak{h}$ up to $\tilde{\Gamma}_{U_0^D(M)}$-equivalence.

Proof. The zeros of f on $\mathfrak{h}$ map via $\xi_{U_0^D(M)}$ to two types of points on $X_0^D(M)$: points in the support of the divisor of α, and the elliptic points on $X_0^D(M)$. The first is Galois-stable, while the second can be seen as the branch locus of

$$\pi^{U_0^D(M)\cap U_1^D(\ell)}_{U_0^D(M)} : X_0^D(M, U_1^D(\ell)) \to X_0^D(M)$$

for any prime $\ell > 3$ coprime to $N = DM$, and this branch locus is also Galois-stable. Hence the first claim.

For the second claim, an upper bound is given by the number of zeros of f up to $\tilde{\Gamma}_{U_0^D(M)\cap U_1^D(\ell)}$-equivalence, and this number is at most the degree of the zero divisor of $\beta = (\pi^{U_0^D(M)\cap U_1^D(\ell)}_{U_0^D(M)})^*\alpha$ on $X_0^D(M, U_1^D(\ell))$ since the complex uniformization $\xi_{U_0^D(M)\cap U_1^D(\ell)}$ is unramified. The degree of the divisor of β is $2g-2$, where g the genus of $X_0^D(M, U_1^D(\ell))$. By standard dimension formulas, the genus satisfies

$$\log g = \log N + O(\log\log\log N) + O(\log \ell).$$

Since it is possible to take $\ell \ll \log N$, we get the result. □

Proof of Theorem 14.1. Fix $\epsilon > 0$. Let $\theta, \delta > 0$ be defined by $\delta = \min\{1/4, \epsilon\}$ and $\theta = \delta/5$.

Take $N \gg_{\theta,\delta} 1$ with the same implicit constant as in Corollary 11.2, and take $N = DM$ an admissible factorization with $D > 1$. We also require $N \gg_\delta 1$ so that the implicit constant is admissible for Lemma 14.3 with $\eta = \delta/5$. After these two conditions, note that we are only requiring that $N \gg_\epsilon 1$.

By Corollary 11.2 with $x = N^{\frac{2}{3}+\delta} > N^{\frac{1}{2}+\delta}$, we have

$$\#S_\theta(D, M, N^{\frac{2}{3}+\delta}) > N^{(\frac{2}{3}+\delta)(1-\delta)}.$$

For each fundamental discriminant $-d$ with $d \in S_\theta(D, M, N^{\frac{2}{3}+\delta})$ note that K_{-d} satisfies the Heegner hypothesis for (D, M). Let $P_{-d} = P_{K_{-d}, U_0^D(M)}$ be the associated Heegner point in $X_0^D(M)$ and note that the number of Galois conjugates of P_{-d} is

$$[H_{K_{-d}} : \mathbb{Q}] = 2[H_{K_{-d}} : K_{-d}] > 2d^{\frac{1}{2}-\theta} > x^{\frac{1}{2}-\theta} = N^{(\frac{2}{3}+\delta)(\frac{1}{2}-\theta)}$$

because the residue field of P_{-d} over K is the Hilbert class field $H_{K_{-d}}$, and by item (v) in the definition of $S_\theta(D, M, x)$ in Theorem 11.1. Hence, the number of points in the set

$$\{P_{-d}^\sigma : d \in S_\theta(D, M, N^{\frac{2}{3}+\delta}), \sigma : H_{K_d} \to \mathbb{C}\}$$

is at least

$$N^{(\frac{2}{3}+\delta)(\frac{1}{2}-\theta)+(\frac{2}{3}+\delta)(1-\delta)} = N^{1+(\frac{5}{6}-\delta)\delta-(\delta+\frac{2}{3})\theta} > N^{1+\frac{1}{2}\delta-\theta} > N^{1+\frac{1}{4}\delta}$$

because $\delta < 1/3$ and $\theta < \delta/4$.

By Lemma 14.3 with $\eta = \delta/5$, we deduce from the previous estimate that there is $d_0 \in S_\theta(D, M, N^{\frac{2}{3}+\delta})$ such that if we let $K = K_{-d_0}$, the Heegner point $P_{K,U_0^D(M)}$ satisfies the non-vanishing condition with respect to f required in Proposition 14.2. Namely, letting $\tau_{K,\sigma} \in \mathfrak{h}$ be a point mapping to $P^\sigma_{K,U_0^D(M)}$ for each $\sigma : H_K \to \mathbb{C}$, we have that f does not vanish at these points.

Thus, Proposition 14.2 gives

$$\begin{aligned} h_{Ar}(P_K) &\geq -\log(2M) - \frac{1}{[H_K : \mathbb{Q}]} \sum_{\sigma : H_K \to \mathbb{C}} \log\left(|f(\tau_{K,\sigma})| \Im(\tau_{K,\sigma})\right) \\ &\geq -\log(2M) - \log \|f\|_{U_0^D(M),\infty}. \end{aligned}$$

By Theorem 8.1 (as $D > 1$) applied to f and the compact open subgroup $U_0^D(M) \cap U_1^D(\ell)$ for some prime $5 \le \ell \le 10 \log N$ coprime to N (cf. Lemma 5.2), we deduce that

$$\begin{aligned}\log \|f\|_{U_0^D(M),\infty} &= \log \|f\|_{U_0^D(M)\cap U_1^D(\ell),\infty}\\ &\le \log \|f\|_{U_0^D(M)\cap U_1^D(\ell),2} + O(1)\\ &= \log \|f\|_{U_0^D(M),2} + O(\log\log N)\end{aligned}$$

with absolute implicit constants. Hence,

$$-\log \|f\|_{U_0^D(M),2} \le \log M + h_{Ar}(P_K) + O(\log\log N)$$

with an absolute implicit constant.

Recall that K has discriminant $-d_0$ with $d_0 \in S_\theta(D, M, N^{\frac{2}{3}+\delta})$. By Theorem 13.2 in its formulation (40), we obtain that for some uniform constant κ as in Theorem 11.1 (where $S_\theta(D, M, x)$ was defined)

$$\begin{aligned}-\log \|f\|_{U_0^D(M),2} &\le \log M + \frac{L'}{L}(1, \chi_K) + \frac{1}{2}\log(d_0 D) + O(\log\log N)\\ &\le \log M + \kappa \log\log d_0 + \frac{1}{2}\log(d_0 D) + O(\log\log N).\end{aligned}$$

As $d_0 \in S_\theta(D, M, N^{\frac{2}{3}+\delta})$ we have $d_0 \le 2N^{\frac{2}{3}+\delta}$, which gives

$$\begin{aligned}-\log \|f\|_{U_0^D(M),2} &\le \log M + \frac{1}{2}\log D + \left(\frac{1}{3} + \frac{\delta}{2}\right)\log N + O(\log\log N)\\ &= \frac{1}{2}\log M + \left(\frac{5}{6} + \frac{\delta}{2}\right)\log N + O(\log\log N)\end{aligned}$$

with an absolute implicit constant, provided that $N \gg_\epsilon 1$. Since $\delta \le \epsilon$, the result follows. □

15. Linear forms in logarithms

15.1. **An application of linear forms in logarithms.** As a preparation for the proof of Theorem 16.7, we prove the following simple consequence of the theory of linear forms in p-adic logarithms.

Proposition 15.1. *Let $\epsilon > 0$. There is a constant $C_\epsilon > 1$ such that for all triples a, b, c of coprime positive integers with $a + b = c$, we have*

$$\frac{d(abc)}{(\log d(abc))^\nu} < C_\epsilon^\nu \nu^{2\nu^2} \mathrm{rad}(abc)^{1+\epsilon\nu}$$

where $\nu = \omega(abc)$ is the number of distinct primer divisors of abc. In particular, if we consider ν as fixed, then for those triples a, b, c we have

$$d(abc) \ll_{\epsilon,\nu} \mathrm{rad}(abc)^{1+\epsilon}.$$

The reader will note that we are actually aiming for a bound of the following sort for abc-triples:

$$d(abc) \ll \mathrm{rad}(abc)^\kappa \tag{44}$$

for some fixed κ. Proposition 15.1 falls short of proving such an estimate because it only applies for fixed (or bounded) value of $\omega(abc)$, but nevertheless, it will be useful to get an improved value of κ. Namely, Proposition 15.1 will be used for abc-triples with at most ν prime factors (for some suitable choice of ν), while the theory developed in previous sections of this paper will be used on the general case of abc triples with more than ν prime factors. We remark that for our purposes, the previous proposition is not really necessary and one can show a version of Theorem 16.7 (i.e. (44) with a slightly worse exponent κ) without it.

Proof. Consider coprime positive integers a, b, c with $a + b = c$. Let $\nu_a = \omega(a)$ be the number of distinct prime factors of a, and let $L_a = \prod_{p|a}(1 + \log p)$. We make analogous definitions for b and c. If p is a prime dividing a, we note that

$$v_p(abc) = v_p(a) = v_p\left(\frac{b}{c} - 1\right).$$

The latter quantity is well-suited for the theory of linear forms in p-adic logarithms. For instance, the corollary in p. 245 in [110] gives

$$v_p(abc) \ll (\nu_b + \nu_c)^{3(\nu_b+\nu_c)} \cdot p \cdot L_b L_c \log(L_b L_c) \log d(bc) \tag{45}$$

where we used the inequality $d(m) \geq \max_{q|m} v_q(m) + 1$ (q varying over primes). Multiplying the analogous bounds for all $p|abc$ we get

$$\begin{aligned} d(abc) &= \prod_{p|abc} (v_p(abc) + 1) \\ &\ll \nu^{6(\nu_a\nu_b+\nu_a\nu_c+\nu_b\nu_c)} \mathrm{rad}(abc)(L_a L_b L_c)^{2\nu} (\log d(abc))^{\nu} \\ &\leq \nu^{2\nu^2} \mathrm{rad}(abc) \cdot \prod_{p|abc} (1 + \log p)^{2\nu} (\log d(abc))^{\nu}. \end{aligned}$$

The result now follows from

$$\prod_{p|m} (1 + \log p) \ll_\epsilon \mathrm{rad}(m)^\epsilon$$

which has an implicit constant that only depends on ϵ. Note that we will take ν-th power of the previous estimate, which explains the term C_ϵ^ν in the final result. □

We also the following estimate for $v_2(abc)$, which also relies on the theory of linear forms in logarithms.

Lemma 15.2. *Let $\epsilon > 0$. There is a constant $C'_\epsilon > 1$ such that for all triples a, b, c of coprime positive integers with $a + b = c$ we have*

$$v_2(abc) < C'_\epsilon \cdot \mathrm{rad}(abc)^\epsilon.$$

Proof. For abc triples with $\omega(abc) = 2$ the result is a consequence of Mihailescu's solution to Catalan's conjecture [72] (this particular case could be addressed by linear forms in logarithms too, cf. [100]).

So we may assume $\omega(abc) \geq 3$. Then the prime $p = 2$ satisfies condition (16) in [95], namely, $p = 2 < \exp((\log \omega(abc))^2)$. Noticing that for abc triples we know [93]

$$\log \log(abc) \leq \log(\mathrm{rad}(abc)^{15}) + O(1) \ll \log \mathrm{rad}(abc),$$

our claim follows from (21), (22) and (23) in [95]. □

15.2. **Heuristics on the applicability of linear forms in logarithms.** The bound (45) is not the sharpest available result in the literature, and it was used because it is simple to state and enough for our purposes. Can one get (44) by using instead the best available bounds on linear forms in p-adic logarithms? We feel skeptical about this, although strictly speaking we don't have a proof that this is not possible. Nevertheless, here is a heuristic justification:

To the best of the author's knowledge, the sharpest improvements to (45) are due to Yu [111], see in particular the quantities C_1 and C_2 given in p.189 *loc. cit.* For coprime positive integers a, b, c with $a + b = c$, let us write $\nu_a = \omega(a)$, $\Lambda_a = \prod_{p|a} \log p$ and similarly for b and c. Combining the best aspects of these two quantities C_1 and C_2, and optimistically ignoring a few factors (which can possibly be problematic!), the main theorem in p. 190 [111] points in the direction that the methods can at best give a bound of the form

$$v_p(abc) = v_p(b/c-1) <_{(?)} e^{\alpha(\nu_b+\nu_c)} \cdot \frac{p}{(\log p)^{\nu_b+\nu_c+2}} \cdot \Lambda_b \cdot \Lambda_c \tag{46}$$

for $p|a$, with $\alpha > 0$ some absolute constant.

For the sake of clarity, note that the factor $e^{\alpha n}$ (as opposed to $n^{\alpha n}$) is the best aspect suggested by C_2, while the denominator on the right hand side of (46) is the best aspect suggested by C_1, but as far as we know, these two improvements are not available simultaneously.

Nevertheless, let us examine the strength of the hypothetical bound (46). Multiplying as p varies and using the analogous bounds for b and c, one would get in this optimistic scenario that

$$\begin{aligned}\prod_{p|abc} v_p(abc) &< e^{2\alpha(\nu_a\nu_b+\nu_a\nu_c+\nu_b\nu_c)} \frac{\mathrm{rad}(abc)}{\Lambda_a^{\nu_b+\nu_c+2}\Lambda_b^{\nu_a+\nu_c+2}\Lambda_c^{\nu_b+\nu_b+2}} \\ &\quad\times (\Lambda_a\Lambda_b)^{\nu_c}(\Lambda_a\Lambda_c)^{\nu_b}(\Lambda_b\Lambda_c)^{\nu_a} \\ &= e^{2\alpha(\nu_a\nu_b+\nu_a\nu_c+\nu_b\nu_c)} \frac{\mathrm{rad}(abc)}{(\Lambda_a\Lambda_b\Lambda_c)^2}.\end{aligned}$$

This bound is not better than

$$\prod_{p|abc} v_p(abc) < e^{2\alpha(n_an_b+n_an_c+n_bn_c)}\mathrm{rad}(abc)^{1/2}.$$

When a, b, c have a comparable number of prime factors (which *a priori* is a possible scenario), this would only give

$$\prod_{p|abc} v_p(abc) < e^{\beta\cdot\omega(abc)^2}\mathrm{rad}(abc)^{1/2} \tag{47}$$

for some constant β. From here it is not clear to the author how to get (44), because

$$\omega(N) = \Omega\left(\frac{\log \mathrm{rad} N}{\log\log \mathrm{rad} N}\right)$$

and in fact, it would already be a problem if for some fixed $\delta > 0$ one has

$$\omega(abc) > (\log \mathrm{rad}(abc))^{\frac{1}{2}+\delta}.$$

In order to make this heuristic more precise, let us describe a *hypothetical* type of abc triples, whose existence would be consistent with (47) and with any bound of the type

$$\log c \ll \mathrm{rad}(abc)^{\kappa} \tag{48}$$

with κ fixed (as the ones obtained by Stewart, Tijdeman, and Yu [93, 94, 95]), yet it would contradict any bound of the form (44).

To simplify notation, write $\nu = \omega(abc)$, $M = abc$ and $R = \mathrm{rad}(abc)$. We require the following:

(i) ν is large,

(ii) the prime factors of M are among the first 2ν primes,

(iii) all the primes $p|M$ satisfy

$$v_p(M) < \exp\left(\frac{\beta \log R}{2\log\log R}\right)$$

with $\beta > 0$ as in (47), and

(iv) a positive proportion of the primes $p|M$, say at least half of them, satisfy

$$v_p(M) > \exp\left((\log\log R)^2\right).$$

Note that by (i) and (ii)

$$\frac{\log R}{\log\log R} < 2\nu. \tag{49}$$

Then by (iii) and (49) we have

$$\log c < \log M \leq \left(\max_{p|M} v_p(M)\right) \log R \leq \exp\left(\frac{\beta \log R}{\log\log R}\right) \ll_\epsilon R^\epsilon$$

which is consistent with (48). Also, observe that by (iii) and (49) we have

$$\prod_{p|M} v_p(M) \leq \left(\max_{p|M} v_p(M)\right)^\nu \leq \exp\left(\frac{\beta\nu \log R}{2\log\log R}\right) \leq e^{\beta\nu^2}$$

which is consistent with (47), even without the factor $\mathrm{rad}(abc)^{1/2}$. Finally, note that by (iv) and (49) we have

$$\prod_{p|M} v_p(M) \geq \exp\left(\frac{n}{2}(\log_2 R)^2\right) \geq \exp\left(\frac{1}{4}(\log R)\log_2 R\right) = R^{(\log_2 R)/4}$$

(here, $\log_2 X = \log\log X$) which is not consistent with (44), for any value of κ.

Of course, such hypothetical *abc*-triples satisfying (i), (ii), (iii), and (iv) *do not exist* because our Theorem 16.7 (cf. Theorem 1.10) actually proves a version of (44). Nevertheless, this heuristic analysis suggests (to the author) that the approach of p-adic linear forms in logarithms has a limitation in this direction. In any case, regardless of the applicability of the theory of linear forms in logarithms in the context of (44), it is worth noticing that the theory in this paper provides a completely new approach to establishing *abc*-type bounds.

16. Bounds for products of valuations

16.1. **A general estimate for elliptic curves.**

Theorem 16.1. *Let S be a finite set of primes and let $\epsilon > 0$. For all but finitely many elliptic curves $E/\mathbb{Q}$ semi-stable away from S, the following holds:*

Let $N = N_E$ be the conductor of E and let Δ_E be the minimal discriminant of E. Consider an admissible factorization $N = DM$ (in particular, D is supported away from S). Then

$$\prod_{p|D} v_p(\Delta_E) < N^{\frac{11}{3}+\epsilon}.$$

Proof. We may assume $D > 1$. From Theorem 6.1, Item (a), we have

$$\log\left(\prod_{p|D} v_p(\Delta_E)\right) \leq \log \delta_{1,N} - \log \delta_{D,M} + \log D + O_S\left(\frac{\log D}{\log\log D}\right). \tag{50}$$

Here, we recall that $\delta_{D,M}$ is the modular degree of the optimal quotient $q_{D,M} : J_0^D(M) \to A_{D,M}$ with $A_{D,M}$ an elliptic curve isogenous to E over $\mathbb{Q}$.

Using the cusp $i\infty$ we have an embedding $j_N : X_0(N) \to J_0(N)$ so that the composite map $\phi_N : X_0(N) \to A_{1,N}$ is a classical optimal modular parameterization and has degree exactly $\delta_{1,N}$. By Frey's formula (5) we get

$$\log \delta_{1,N} = 2\log(2\pi|c_f|) + 2\log(\|f\|_{U_0^1(N),2}) + 2h(A_{1,N}) \tag{51}$$

where c_f is the (positive) Manin constant of the modular parameterization ϕ_N and $f \in S_2(N)$ is the normalized cuspidal Hecke newform associated to E.

From Corollary 5.3, we recall that there is a non-constant morphism $\phi_{D,M} : X_0^D(M) \to A_{D,M}$ degree satisfying

$$\delta_{D,M} \le \deg \phi_{D,M} \le (9 \log N)^2 \delta_{D,M}. \tag{52}$$

Let $\mathscr{A}_{D,M}$ be the Néron model of $A_{D,M}$ over $\mathbb{Z}$, then by the Néron mapping property $\phi_{D,M}$ extends to a $\mathbb{Z}$-morphism of integral models on the smooth locus

$$\phi_{D,M} : \mathscr{X}_0^D(M)^0 \to \mathscr{A}_{D,M}.$$

Let $\omega_{A_{D,M}}$ be a Néron differential of $A_{D,M}$ (unique up to sign) and let

$$\alpha_{D,M} = \phi^{\bullet}_{D,M} \omega_{A_{D,M}} \in H^0(\mathscr{X}_0^D(M)^0, \Omega^1_{\mathscr{X}_0^D(M)/\mathbb{Z}})$$

i.e. the image of $\phi^*_{D,M}\omega_{A_{D,M}}$ under $\phi^*_{D,M}\Omega^1_{\mathscr{A}_{D,M}/\mathbb{Z}} \to \Omega^1_{\mathscr{X}_0^D(M)/\mathbb{Z}}$. Then

$$f_{D,M} = \Psi_{U_0^D(M)}(\alpha_{D,M}) \in \mathscr{S}_2^D(M)$$

is integral and by the same argument as the proof of (5) we get

$$\log \deg \phi_{D,M} = 2 \log(\|f_{D,M}\|_{U_0^D(M),2}) + 2h(A_{D,M}). \tag{53}$$

By (50), (51), (52), and (53) we deduce

$$\begin{aligned} \log \left(\prod_{p|D} v_p(\Delta_E) \right) &= 2 \log |c_f| + 2 \log(\|f\|_{U_0^1(N),2}) - 2 \log(\|f_{D,M}\|_{U_0^D(M),2}) \\ &\quad + 2h(A_{1,N}) - 2h(A_{D,M}) + O(\log \log N) \\ &\quad + \log D + O_S\left(\frac{\log D}{\log \log D} \right). \end{aligned}$$

Since $A_{1,N}$ and $A_{D,M}$ are both isogenous to E, they are connected by an isogeny of degree ≤ 163, so that $2|h(A_{1,N}) - h(A_{D,M})| \le \log 163$. It follows that

$$\begin{aligned} \log \left(\prod_{p|D} v_p(\Delta_E) \right) &= 2 \log |c_f| + 2 \log(\|f\|_{U_0^1(N),2}) - 2 \log(\|f_{D,M}\|_{U_0^D(M),2}) \\ &\quad + \log D + O_S\left(\log \log N + \frac{\log D}{\log \log D} \right). \end{aligned} \tag{54}$$

Since f is a normalized newform for $\Gamma_0(N)$, from [68, 73] we get $\|f\|^2_{U_0^1(N),2} \ll N \log N$ which gives

$$2 \log(\|f\|_{U_0^1(N),2}) \le \log N + O(\log \log N).$$

On the other hand, since $f_{D,M} \in \mathscr{S}_2^D(M)$ is integral and non-zero, by Theorem 14.1 we obtain

$$-2 \log(\|f_{D,M}\|_{U_0^D(M),2}) \le \left(\frac{5}{3} + \frac{\epsilon}{2} \right) \log N + \log M$$

provided that $N \gg_\epsilon 1$. Therefore, for $N \gg_{\epsilon,S} 1$, we obtain

$$\log \left(\prod_{p|D} v_p(\Delta_E) \right) \le 2 \log |c_f| + \left(\frac{8}{3} + \epsilon \right) \log N + \log M + \log D. \tag{55}$$

Finally, by Corollary 10.2 we see that $\log |c_f| \ll_S 1$, hence the result. □

Let us observe that if one only works in the semi-stable case (as in Theorem 16.5 below) then we don't need Corollary 10.2 in the previous proof. The existing literature on the Manin constant in the semi-stable case would suffice.

We also remark that a computation in Section 2.2.1 of [79] also combines the classical Ribet-Takahashi formula with Frey's equation (5), in a way somewhat similar to what we did to derive equation (54) in the previous argument. However, the computation in [79] occurs in a different context (p-integrality of ratios of Petersson norms) and in a less precise form, omitting the contribution of Eisenstein primes and requiring semi-stability. Of course, for our purposes it is crucial to have control on *each* prime, since we aim to prove global estimates. Frey-Hellegouarch curves always have $p = 2$ as an Eisenstein prime, so we cannot ignore this issue.

For later reference, we record here a simple consequence.

Corollary 16.2. *Let S be a finite set of primes and let $\epsilon > 0$. For all but finitely many elliptic curves $E/\mathbb{Q}$ semi-stable away from S and having at least two primes of multiplicative reduction, we have*

$$\prod_{p|N_E^*} v_p(\Delta_E) < N_E^{\frac{11}{2}+\epsilon}$$

where N_E^* is the product of all the primes of multiplicative reduction of E.

Proof. When E has an even number of primes of multiplicative reduction the result follows from Theorem 16.1 with $D = N_E^*$.

When E has an odd number n of primes of multiplicative reduction, necessarily $n \geq 3$ by our assumptions. Call these primes $p_1, \dots, p_n$, then

$$\prod_{p|N_E^*} v_p(\Delta_E) = \left(\prod_{i=1}^{n} \prod_{p|(N_E^*/p_i)} v_p(\Delta_E) \right)^{1/(n-1)}.$$

The result follows from Theorem 16.1 for the various $D = N_E^*/p_i$, since $\frac{11}{3} \cdot \frac{n}{n-1} \leq 11/2$. □

In particular, we obtain the following application.

Corollary 16.3. *Let S be a finite set of primes and let $\epsilon > 0$. For all but finitely many elliptic curves $E/\mathbb{Q}$ semi-stable away from S and having at least two primes of multiplicative reduction, we have*

$$\mathrm{Tam}(E) < N_E^{\frac{11}{2}+\epsilon}.$$

Proof. This follows from Corollary 16.2. In fact, given an elliptic curve E over $\mathbb{Q}$, if E has additive or non-split multiplicative reduction at a prime p then $\mathrm{Tam}_p(E) \leq 4$, so

$$\mathrm{Tam}(E) \leq 4^{\omega(N_E)} \prod_{p|N_E^*} v_p(\Delta_E) \ll_\epsilon N_E^\epsilon \prod_{p|N_E^*} v_p(\Delta_E).$$

□

16.2. **A sharpening of the general estimate.** For the cases on which we are primarily interested, the estimate in Theorem 16.1 can be improved.

Theorem 16.4. *Let $\epsilon > 0$. Let E be an elliptic curve over $\mathbb{Q}$ of conductor $N \gg_\epsilon 1$. Let $N = DM$ be an admissible factorization and suppose that either*

(i) *E is semi-stable and M is not a prime number, or*
(ii) *E is a Frey-Hellegouarch elliptic curve and M is divisible by at least two odd primes.*

Then we have

$$\prod_{p|D} v_p(\Delta) < N^{\frac{8}{3}+\epsilon} M.$$

Proof. The proof is essentially the same as for Theorem 16.1 with the only difference that we use Item (b) instead of Item (a) from Theorem 6.1 (or alternatively, we can directly use Corollary 6.2). This allows us to replace (50) by

$$\log \prod_{p|D} v_p(\Delta) \leq \log \delta_{1,N} - \log \delta_{D,M} + O\left(\frac{\log D}{\log\log D}\right)$$

where the implicit constant is absolute. The rest of the proof continues in the same way, and at the end we can replace (55) by

$$\log\left(\prod_{p|D} v_p(\Delta_E)\right) < 2\log|c_f| + \left(\frac{8}{3}+\epsilon\right)\log N + \log M$$

provided that $N \gg_\epsilon 1$. The necessary bound for the Manin constant is classical in the semi-stable case, and follows from Corollary 10.2 in the case of Frey-Hellegouarch elliptic curves. □

16.3. **The semi-stable case.**

Theorem 16.5. *Let $\epsilon > 0$. There is a number $K_\epsilon > 0$ depending only on ϵ such that the following holds:*

For every semi-stable elliptic curve E over $\mathbb{Q}$ we have

$$\prod_{p|N_E} v_p(\Delta_E) < K_\epsilon \cdot N_E^{\frac{11}{2}+\epsilon}.$$

If moreover $\epsilon > 0$ and E has at least $3 + 11/\epsilon$ places of bad reduction, then we have the stronger estimate

$$\prod_{p|N_E} v_p(\Delta_E) < K_\epsilon \cdot N_E^{\frac{8}{3}+\epsilon}.$$

Furthermore, similar estimates hold for $\mathrm{Tam}(E)$ *instead of* $\prod_{p|N_E} v_p(\Delta_E)$.

Proof. If $N_E = p$ is prime then $v_p(\Delta_E) \leq 5$ (cf. [71]). The first part of the result now follows from Corollary 16.2 with $S = \emptyset$.

For the second part, write $N = p_1 \cdots p_n$ with p_j different primes and note that $n \geq 4$. If n is even then the bound follows from case (i) of Theorem 16.4 with $D = N$ and $M = 1$. If n is odd (thus, $n \geq 5$) we apply the same result with $M = (p_j p_{j+1} p_{j+2})$ and $D = N/M$ for each $j = 1, \ldots, n$ (taking the indices of the p_j modulo n). After multiplying the resulting estimates and taking $(n-3)$-rd roots we get

$$\prod_{p|N} v_p(\Delta_E) < N^{\left(\frac{8}{3}+\epsilon'\right)\frac{n}{n-3}} \cdot N^{\frac{3}{n-3}}$$

for any given $\epsilon' > 0$ and for $N \gg_{\epsilon'} 1$. For $\epsilon > 0$ given, there is a sufficiently small $\epsilon' > 0$ (only depending on ϵ) such that for all integers $n > 11/\epsilon + 3$ we have

$$\left(\frac{8}{3}+\epsilon'\right)\frac{n}{n-3} + \frac{3}{n-3} < \frac{8}{3} + \epsilon,$$

hence the result. The final claim about $\mathrm{Tam}(E)$ follows. □

An immediate consequence is the following upper bound for the number of level-lowering primes (in the sense of Ribet's theory [82]) that a semi-stable elliptic curve can have. For this, we recall from the introduction that for an elliptic curve E over $\mathbb{Q}$ we write

$$L(E) := \{\ell \text{ prime } : \exists p \text{ prime such that } p|N_E \text{ and } \ell|v_p(\Delta_E)\}.$$

Corollary 16.6 (Counting level-lowering primes)**.** *Let $\epsilon > 0$. Then for all semi-stable elliptic curves E over $\mathbb{Q}$ we have*

$$\#L(E) < \frac{(11/2+\epsilon)\log N_E}{\log\log N_E} + O_\epsilon(1).$$

Proof. Let $\Lambda(E)$ be the product of the primes in $L(E)$. Then $\Lambda(E)$ divides $\prod_{p|N_E} v_p(\Delta_E)$ and the previous theorem gives

$$\Lambda(E) \ll_\epsilon N_E^{\frac{11}{2}+\epsilon}.$$

Since $\log\Lambda(E)$ is bigger than or equal to the sum of $\log p$ where p runs over the first $\#L(E)$ prime numbers, the result now follows from the prime number theorem. □

16.4. Products of valuations of *abc* triples.

Theorem 16.7. *Given $\epsilon > 0$, there is a constant $K_\epsilon > 0$ such that the following holds:*

For all coprime positive integers a, b, c with $a + b = c$, we have

$$d(abc) < K_\epsilon \cdot \operatorname{rad}(abc)^{\frac{8}{3}+\epsilon}.$$

In particular, we have

$$\prod_{p|abc} v_p(abc) < K_\epsilon \cdot \operatorname{rad}(abc)^{\frac{8}{3}+\epsilon}.$$

Proof. Let a, b, c be as in the statement, and recall that for a positive integer n the number of positive divisors of n is $d(n) = \prod_{p|n}(v_p(n) + 1)$.

Let $\nu \geq 4$ be arbitrary (we will later take ν large in terms of $\epsilon > 0$). If $\omega(abc) \leq \nu$ we obtain $d(abc) \ll_\nu \operatorname{rad}(abc)^2$ (say) by Proposition 15.1. So we can assume that $n := \omega(abc) > \nu$.

Let E be the Frey-Hellegouarch curve with affine equation $y^2 = x(x-a)(x+b)$ associated to the triple a, b, c. Let Δ be its minimal discriminant and N its conductor. We note that for $p > 2$, the conditions $p|abc$ and $p|N$ are equivalent, and moreover for such a prime p we have

$$v_p(N) = 1 \text{ and } v_p(\Delta) = 2v_p(abc).$$

For $p = 2$, however, we always have $2|abc$, while 2 does not need to divide N, and when it does, its exponent can be larger than 1. Nevertheless, we still have $N \asymp \operatorname{rad}(abc)$, and by Lemma 15.2 we know

$$v_2(abc) \ll_\epsilon \operatorname{rad}(abc)^\epsilon. \tag{56}$$

Write $N = 2^r p_1 \cdot p_m$ where $0 \leq r \leq 8$, $p_i > 2$ are distinct primes, and $m = n$ if $r = 0$, or $m = n - 1$ if $1 \leq r \leq 8$. In either case, $m \geq \nu \geq 4$.

If m is even, we let $D = p_1 \cdots p_m$ and $M = 2^r$. With these choices, Theorem 16.4 gives

$$\prod_{\substack{p|abc\\ p\neq 2}} (v_p(abc) + 1) \leq \prod_{j=1}^{m}(2v_{p_j}(abc)) = \prod_{j=1}^{m} v_{p_j}(\Delta) \ll_\epsilon N^{\frac{8}{3}+\epsilon}.$$

This, together with (56) gives

$$d(abc) \ll_\epsilon N^{\frac{8}{3}+\epsilon}$$

proving the result in the case that m is even.

If m is odd then $m \geq 5$. For any choice of $j_1, j_2, j_3 \in \{1, \dots, m\}$ of three distinct indices, we let $D = p_1 \cdots p_m/(p_{j_1}p_{j_2}p_{j_3})$ and $M = 2^r p_{j_1}p_{j_2}p_{j_3}$. Similarly we obtain

$$\prod_{\substack{1\leq j\leq m\\ j\neq j_1,j_2,j_3}} (2v_{p_j}(abc)) \ll_\epsilon N^{\frac{8}{3}+\epsilon} p_{j_1}p_{j_2}p_{j_3}.$$

Let us take the following cyclic choices: j_1 arbitrary, $j_2 \equiv j_1 + 1 \mod m$, and $j_3 \equiv j_1 + 2 \mod m$. We multiply these m inequalities and then we take $(m-3)$-rd roots to obtain

$$\prod_{\substack{p|abc\\ p\neq 2}} (v_p(abc)+1) \leq \prod_{j=1}^{m} (2v_{p_j}(abc)) \ll_\epsilon N^{(\frac{8}{3}+\epsilon)\frac{m}{m-3}} N^{\frac{3}{m-3}} \leq N^{(\frac{8}{3}+\epsilon)\frac{\nu}{\nu-3}+\frac{3}{\nu-3}}.$$

The result now follows from (56) and the fact that ν can be taken in advance as large as needed. □

17. Counting quadratic extensions of a totally real number field

In this section we give suitable analogues of the results in Section 11 in the setting of totally real number fields.

In this section n will denote the degree of the number field under consideration, and we will write $c_1(n), c_2(n), ...$ for certain *strictly positive* quantities that only depend on the integer n; some $c_i(n)$ will need to be large, while others will be needed small.

For a number field F and a non-zero integral ideal $\mathfrak{a}$ of O_F, the absolute norm of $\mathfrak{a}$ is denoted by $\mathrm{N}\mathfrak{a} = [O_F : \mathfrak{a}]$.

17.1. Auxiliary quadratic extensions.

Lemma 17.1. *Let F be a totally real number field with $[F : \mathbb{Q}] = n$ and discriminant d_F. Let $\mathfrak{I}$ and $\mathfrak{S}$ be non-zero coprime ideals of O_F. There is a totally real quadratic extension L/F satisfying that each prime $\mathfrak{p}$ dividing $\mathfrak{I}$ is inert in O_L, each prime $\mathfrak{p}$ dividing $\mathfrak{S}$ is split in L, and with*

$$\mathrm{N}(\mathrm{Disc}(L/F)) < c_1(n) \cdot (d_F \mathrm{N}(\mathfrak{I}\mathfrak{S}))^{c_2(n)}.$$

Proof. The construction of L without the condition on the size of $\mathrm{N}(\mathrm{Disc}(L/K))$ is classical: One chooses a monic quadratic polynomial $f(x) = x^2 + \alpha x + \beta \in O_F[x]$ which is irreducible modulo $\mathfrak{p}$ for each $\mathfrak{p}|\mathfrak{I}$, is the product of two distinct linear factors modulo $\mathfrak{p}$ for each $\mathfrak{p}|\mathfrak{S}$, and with positive discriminant under each real embedding. (These are simply congruence conditions on the coefficients α, β.) Then any root of $f(x)$ generates a field L over F with the desired properties.

Using geometry of numbers (or more elementary arguments) one can control the size under each real embedding of the coefficients α, β of f in the previous construction. The discriminant of $f(x)$ is divisible by the relative discriminant L/F, and the result follows. □

Given a number field F and quadratic extensions M_1, M_2 of F, we define the quadratic extension $M_3 = M_1 * M_2$ of F as follows: If $M_1 = M_2$ we let $M_3 = M_1$. Otherwise, the compositum M_1M_2 has degree 4 over F and contains three quadratic extensions of F, namely, M_1, M_2 and the third one is defined to be $M_3 = M_1 * M_2$.

Lemma 17.2. *Let F be a totally real number field, let $\mathfrak{I}$ and $\mathfrak{S}$ be non-zero coprime ideals in O_F and let L/F be a totally real quadratic extension such that every prime dividing $\mathfrak{I}$ is inert in O_L and every prime dividing $\mathfrak{S}$ splits in O_L. Let $K/\mathbb{Q}$ be an imaginary quadratic extension such that every rational prime below $\mathfrak{I}\mathfrak{S}$ splits in K. Then the field $M = L * (FK)$ satisfies the following:*

- *M/F is quadratic*
- *M is totally imaginary*
- *every prime of O_F dividing $\mathfrak{I}$ is inert in O_M*

- *every prime of O_F dividing $\mathfrak{S}$ splits in O_M.*

Proof. This follows by observing that any two of L, FK, M generate the compositum LK. □

17.2. **The counting result.**

Theorem 17.3. *Let F be a totally real number field with $[F:\mathbb{Q}] = n$ and discriminant d_F. Let $\mathfrak{I}$ and $\mathfrak{S}$ be non-zero coprime ideals of O_F and let $x > c_3(n) \cdot (d_F \mathrm{N}(\mathfrak{I}\mathfrak{S}))^{c_4(n)}$. The number of (pairwise non-isomorphic) quadratic extensions M/F satisfying*

(i) *M is totally imaginary,*
(ii) *each prime dividing $\mathfrak{I}$ is inert in O_M,*
(iii) *each prime dividing $\mathfrak{S}$ splits in O_M,*
(iv) *$x < \mathrm{N}(\mathrm{Disc}(M/F)) < c_5(n)x$, and*
(v) *$\left|\frac{L'}{L}(1, \chi_M)\right| \le c_6(n)(\log d_F + \log\log x)$ where χ_M is the quadratic Hecke character over F associated to the extension M/F*

is at least $x^{c_7(n)}$.

Proof. We construct the desired fields M as $M = L{*}K$ with L as in Lemma 17.1 (whose discriminant has controlled size) and $K/\mathbb{Q}$ as in Lemma 17.2. Then conditions (i), (ii) and (iii) are satisfied.

Using Corollary 11.2 we can produce enough quadratic extensions $K/\mathbb{Q}$ such that (iv) is also satisfied. Thus, it only remains to show that upon discarding a negligible number of quadratic extensions $K/\mathbb{Q}$, we can also achieve (v).

Given L/F and $K/\mathbb{Q}$ quadratic extensions as above, let ξ and ψ be the corresponding quadratic Hecke characters over F and $\mathbb{Q}$ respectively. Then for $M = L{*}(FK)$, the quadratic Hecke character over F is

$$\chi_M = \xi \cdot \psi_F$$

where $\psi_F = \psi \circ \mathrm{N}_{F/\mathbb{Q}}$ is the base change of ψ from $\mathbb{Q}$ to F. In particular,

$$L(s, \chi_M) = L(s, \xi \otimes \psi_F). \tag{57}$$

The bound (v) is proved for all but a negligible number of choices of K exactly as in [62]. That is, one first proves a version of Proposition 2.3 *loc. cit.* with $k = 1$ for $L(s, \chi_M)$, and then one proceeds as in Corollary 2.5 *loc. cit.*, using the zero density estimate in Proposition A.2 as ψ (hence ψ_F) varies, instead of using Heath-Brown's zero-density from [47] which works over $\mathbb{Q}$. The additional term $\log d_F$ in (v) comes from [108] Lemma 1.11(b).

More precisely, we apply Proposition A.2 over the number field F choosing $d = 1$ and taking π the automorphic representation of $GL_1(\mathbb{A}_F)$ associated to ξ. This produces zero density estimates for L-functions of the form $L(s, \pi \otimes \chi) = L(s, \xi \otimes \chi)$ as χ varies, which is precisely what we need in view of (57). Although Proposition A.2 gives a zero density estimate as χ varies over all finite order Hecke characters (not just for quadratic characters such as ψ_F), this is enough for us since the key feature that we need from the result is the exponent $c \cdot (1 - \sigma) + \epsilon$ for a constant c that in our application only depends on $n = [F : \mathbb{Q}]$. □

Remark 17.4. If one assumes that $F/\mathbb{Q}$ is solvable then it admits automorphic induction (cf. [4, 17]). In this setting, it is not necessary to use the results in the Appendix, because Corollary 1.4 of [63] (by the same authors of the Appendix) suffices for producing the necessary zero-density estimates —in fact, this is how we proceeded in an earlier version of this work. Briefly, the idea is the following: If π_ξ is the automorphic representation of $GL_n(\mathbb{A}_\mathbb{Q})$ induced from ξ, then

$$L(s, \chi_M) = L(s, \xi \otimes \psi_F) = L(s, \pi_\xi \otimes \psi)$$

(cf. [54]). Then one can check that, upon prescribing a few more local conditions on ξ (which can be achieved by adding some additional factors to the ideals $\mathfrak{I}$ and $\mathfrak{S}$) the induced representation π_ξ over $\mathbb{Q}$ is cuspidal, and Corollary 1.4 of [63] can be applied.

18. A modular approach to Szpiro's conjecture over number fields

In this section we introduce some tools that make it possible to approach Szpiro's conjecture over totally real fields using modular parameterizations coming from Shimura curves.

As in the previous section, n will denote the degree of a number field, and we will continue to write $c_i(n)$ for strictly positive quantities that only depend on n. The numeration will be consistent with that of the previous section, although this is only intended to stress the fact that these "constants" (depending only on n) can change from line to line.

Several of the necessary ideas have been already presented in detail over $\mathbb{Q}$ in previous sections of this paper, so, here the discussion will be more concise.

18.1. **Faltings height of elliptic curves over number fields.** In this paragraph we discuss the Faltings height of elliptic curves in more generality than in Section 3.

Let L be a number field and let E be an elliptic curve over L. Let $\mathscr{E}$ be the Néron model of E over O_L. For each embedding $\sigma : L \to \mathbb{C}$ we let $E_\sigma = E \otimes_\sigma \mathbb{C}$ be the complexification of E under the embedding σ. We define the norm $\| - \|_\sigma$ on $H^0(E_\sigma, \Omega^1_{E_\sigma/\mathbb{C}})$ by

$$\|\alpha\|_\sigma^2 := \frac{i}{2}\int_{E_\sigma} \alpha \wedge \overline{\alpha}.$$

The *Faltings height* of E over L, denoted by $h(E)$, is defined as the normalized Arakelov degree of the metrized rank 1 projective module $H^0(\mathscr{E}, \Omega^1_{\mathscr{E}/O_L})$ with the previous metrics at infinity. Namely, taking any non-zero $\beta \in H^0(\mathscr{E}, \Omega^1_{\mathscr{E}/O_L})$ one defines

$$h(E) = \frac{1}{[L:\mathbb{Q}]}\left(\log \#(H^0(\mathscr{E}, \Omega^1_{\mathscr{E}/O_L})/O_L\beta) - \sum_{\sigma : L \to \mathbb{C}} \log \|\beta\|_\sigma\right).$$

Note that this is not the stable Faltings height, and, in general, it can change after enlarging L. However, when A is semi-stable over L then $h(A)$ is invariant under base change to a finite extension of L.

Silverman [88] proved an alternative formula for $h(E)$ that we now recall. The modular j-function and the Ramanujan cusp form Δ are normalized so that

$$j(z) = q^{-1} + 744 + \ldots$$
$$\Delta(z) = q\prod_{n\geq 1}(1-q^n)^{24}, \quad q = e^{2\pi i z}.$$

For E an elliptic curve over L and $\sigma : L \to \mathbb{C}$ and embedding, we choose $\tau_{E,\sigma} \in \mathfrak{h}$ satisfying that $j(\tau_{E,\sigma})$ is the j-invariant of $E \otimes_\sigma \mathbb{C}$. Then Silverman's formula is

$$h(E) = \frac{1}{12[L:\mathbb{Q}]}\left(\log \Delta_E - \sum_{\sigma : L \to \mathbb{C}} \log\left|\Delta(\tau_{E,\sigma}) \cdot \Im(\tau_{E,\sigma})^6\right|\right) - \log(2\pi) \tag{58}$$

where Δ_E is the norm of the minimal discriminant ideal of E over L. (Note that in [88] there is a minor typo in the definition of $\Delta(\tau)$ that gives $+\log(2\pi)$ instead of $-\log(2\pi)$; this has been corrected in a number of places). One deduces:

Lemma 18.1. *With the previous notation,*

$$\frac{1}{[L:\mathbb{Q}]}\log \Delta_E < 12h(E) + 16.$$

We will need another description of $h(E)$. Suppose that E is semi-stable over F and let $\bar{\mathscr{E}}$ be the corresponding semi-stable model over O_L, such that the smooth locus $\mathscr{E}$ of its structure map is the Néron model of E. Let ω be the relative dualizing sheaf of $\bar{\mathscr{E}}$; in particular ω is an invertible sheaf (E is semi-stable) and its restriction to $\mathscr{E}$ is $\Omega^1_{\mathscr{E}/O_L}$.

We make ω into a metrized line bundle $\widehat{\omega}$ with the following metric $\| - \|_\sigma$ associated to an embedding $\sigma : L \to \mathbb{C}$:

Let $x \in E_\sigma$ and let $\lambda \in \Omega^1_{E_\sigma/\mathbb{C}}|_x$. Let $\alpha \in H^0(E_\sigma, \Omega^1_{E_\sigma/\mathbb{C}})$ be the unique invariant differential with $\alpha_x = \lambda$. Then we define

$$\|\lambda\|^2_{\sigma,x} = \frac{i}{2}\int_{E_\sigma} \alpha \wedge \overline{\alpha}.$$

We remark that, in general, the metrized line bundle $\widehat{\omega}$ is *not* the Arakelov canonical metrized line bundle, which one might denote by $\widehat{\omega}^{Ar}$. The metrics of $\widehat{\omega}$ differ from the metrics of $\widehat{\omega}^{Ar}$ by a scalar multiple.

Theorem 18.2. *Let E be a semi-stable elliptic curve over L and keep the previous notation. Let P be an algebraic point of E satisfying that its closure in $\bar{\mathscr{E}}$ is contained in $\mathscr{E}$. Let L'/L be a finite extension over which P is defined and let $S = \operatorname{Spec} O_L$ and $S' = \operatorname{Spec} O_{L'}$. Let $s : S' \to \mathscr{E}$ be the S-map attached to P. Then*

$$\widehat{\deg}_{L'} s^*\widehat{\omega} = [L' : \mathbb{Q}] \cdot h(E).$$

Proof. This is proved in the same way as Proposition 7.2 in [55], which assumes that P is rational and uses $\widehat{\omega}^{Ar}$ instead of $\widehat{\omega}$. The passage from rational to algebraic points of the type considered here is straightforward, provided that in *loc. cit.* one starts with $(P.\widehat{\omega}^{Ar})$ (instead of starting with $(P.P)$ and using adjunction). On the other hand, replacing $\widehat{\omega}^{Ar}$ by $\widehat{\omega}$ modifies the metrics in a way made explicit by Definition 4.1 and Proposition 4.6 in *loc. cit.* Taking this contribution at infinity into account, one obtains the Faltings height of E in the form (58). □

18.2. **Shimura curves.** Let F be a totally real number field of degree n over $\mathbb{Q}$ with $\tau_1, \dots, \tau_n$ its real embeddings. Let $\mathfrak{N}$ be a non-zero ideal in O_F which is the product of ν distinct prime ideals. Suppose that $n + \nu$ is odd and let B be a quaternion F-algebra of discriminant $\mathfrak{N}$ and having τ_1 as its only split place at infinity. Furthermore, when $F = \mathbb{Q}$ we assume $\nu > 0$. Write $\mathbb{B} = B \otimes \hat{\mathbb{Z}}$ and fix a choice of maximal order $O_{\mathbb{B}}$ in $\mathbb{B}$. Let $B^\times_+$ be the set of units in B with totally positive reduced norm.

Associated to this data, for each open compact $U \subseteq \mathbb{B}^\times$ there is a compact Shimura curve X_U defined over F, whose complex points (via τ_1) are given by

$$X^{an}_U = B^\times_+ \backslash \mathfrak{h} \times \mathbb{B}^\times / U.$$

The curve X_U is irreducible over F, although X^{an}_U is not necessarily irreducible and its connected components are parametrized by the class group $C_U = F^\times_+ \backslash \mathbb{A}^\infty_F / \mathrm{rn}(U)$ where rn denotes the reduced norm and $F^\times_+$ is the multiplicative group of totally positive elements of F. We also keep the notation from Paragraph 8.1.

The following expression for the hyperbolic volume of the Shimura curve with $U = O^\times_{\mathbb{B}}$ is a special case of a result of Shimizu [86].

Proposition 18.3. *The number of connected components of $X^{an}_{O^\times_{\mathbb{B}}}$ is h^+_F, the narrow class number of F. Each component has the form $\tilde{\Gamma}_{O^\times_{\mathbb{B}},g} \backslash \mathfrak{h}$ for suitable $g \in \mathbb{B}^\times$, and they have hyperbolic area*

$$Vol\left(\tilde{\Gamma}_{O^\times_{\mathbb{B}},g} \backslash \mathfrak{h}\right) \asymp_n d_F^{3/2} \prod_{\mathfrak{p}|\mathfrak{N}} (\mathrm{N}(\mathfrak{p}) - 1).$$

The Jacobian of X_U over F is denoted by J_U. We denote by $\mathbb{T}^c_U$ the ring of Hecke correspondences on X_U and by $\mathbb{T}_U$ the ring of Hecke operators acting on J_U. They are generated by the Hecke correspondences $T^c_{\mathfrak{n}}$ (resp. Hecke operators $T_{\mathfrak{n}}$) for all $\mathfrak{n}$ integral ideals of O_F coprime to $\mathfrak{N}$ and coprime to the places where U is not maximal. Then $\mathbb{T}_U$ acts also on holomorphic differentials of J_U and of X_U. See [43] for details. Note that the action of $\mathbb{T}^c_{\mathfrak{n}}$ on divisors permutes the components of X_U^{an} according to the action of $\mathfrak{n}$ on $C(U)$.

The Shimura construction associated to a system of Hecke eigenvalues $\chi : \mathbb{T}_U \to \mathbb{C}$ has been carried out in [115] and the theory is similar to that of Shimura curves over $\mathbb{Q}$. In particular, when χ is $\mathbb{Z}$-valued and new, the associated optimal quotient $q : J_U \to A$ satisfies that A is an elliptic curve. We define the modular degree of A arising in this way, as the integer

$$\delta_\chi = qq^\vee \in \mathrm{End}(A).$$

(We remark that δ_χ is not *a priori* the degree of any particular morphism from a Shimura curve to A.) Furthermore, in the special case $U = O_{\mathbb{B}}^\times$ (for instance), results of Carayol [13] give that the conductor ideal of A is precisely $\mathfrak{N}$.

In addition, we define Eisenstein correspondences (cf. Paragraph 5.2) of the form

$$E^c_{U,\mathfrak{n}} = T^c_{\mathfrak{n}} - \sigma_1(\mathfrak{n})\Delta_U$$

where $\sigma_1(\mathfrak{n}) = \sum_{\mathfrak{a}|\mathfrak{n}} \mathrm{N}(\mathfrak{a})$, Δ_U is the diagonal correspondence on X_U, and $\mathfrak{n}$ is required to act as the identity on $C(U)$. In the particular case $U = O_{\mathbb{B}}^\times$ we have that $C(U)$ is the narrow class group of F and we can use $\mathfrak{n}$ coprime to $\mathfrak{N}$, principal and with a totally positive generator, e.g. $\mathfrak{n} = (p)$ with p a rational prime not dividing $\mathrm{N}(\mathfrak{N})$. Such a choice of $\mathfrak{n}$ will ensure that the analogue of condition (*) of Paragraph 5.2 holds for $E^c_{O_{\mathbb{B}}^\times,\mathfrak{n}}$ in our current setting.

Using Eisenstein correspondences as in Section 5 (in the special case $U = O_{\mathbb{B}}^\times$ for simplicity) we obtain:

Theorem 18.4. *Let $X_{O_{\mathbb{B}}^\times}$ be the Shimura curve over F (for $U = O_{\mathbb{B}}^\times$) associated to an indefinite quaternion F-algebra B of discriminant $\mathfrak{N}$ as above. Let χ be a $\mathbb{Z}$-valued new system of Hecke eigenvalues on $\mathbb{T}_{O_{\mathbb{B}}^\times}$ and let $q : J_{O_{\mathbb{B}}^\times} \to A$ be the associated elliptic curve optimal quotient with modular degree δ_χ. There is a map $j : X_{O_{\mathbb{B}}^\times} \to J_{O_{\mathbb{B}}^\times}$ over F such that the composition*

$$\phi = qj : X_{O_{\mathbb{B}}^\times} \to A$$

has degree satisfying

$$h_F^+\delta_\chi \le \deg\phi \le c_8(n)(\log \mathrm{N}(\mathfrak{N}))^{c_9(n)} h_F^+\delta_\chi$$

where h_F^+ is the narrow class number of F.

18.3. **Modular elliptic curves.** We say that an elliptic curve E over a totally real field F is (geometrically) modular if it is isogenous to a factor of the Jacobian J_U of a Shimura curve X_U for some choice of open compact subgroup U in $\mathbb{B}^\times$, and for a suitable choice of $\mathfrak{N}$ (with the same notation as in the previous paragraph).

For technical simplifications, it turns out to be more convenient to require a more restrictive condition. Let us say that E is *modular of Shimura level* 1 if in addition one can choose $\mathfrak{N}$ as the conductor ideal of E and $U = O_{\mathbb{B}}^\times$. In this case E is semi-stable (so, its conductor is squarefree) and the parity of the number of primes of bad reduction of E (i.e. of the prime factors of its conductor) is opposite to the parity of $n = [F : \mathbb{Q}]$. The usual modularity conjecture for elliptic curves over totally real number fields along with the Jacquet-Langlands correspondence, imply that in fact each elliptic curve over F whose conductor satisfies these two conditions, is modular of Shimura level 1 in the sense that we just defined.

If E is modular of Shimura level 1 we simply write $X_1 = X_{O_{\mathbb{B}}^\times}$ for the Shimura curve affording the modular parameterization $X_1 \to E$ of the definition. We observe that in this case E is isogenous to A for an optimal elliptic curve quotient $q : J_1 \to A$, where J_1 is the Jacobian of X_1 over F.

The associated system of Hecke eigenvalues is denoted by χ_E and the modular degree δ_{χ_E} is simply written δ_E.

One would like to control the minimal degree of an isogeny $A \to E$ and to combine this bound with Theorem 18.4. However, a suitable version of the "isogeny theorem" for elliptic curves over number fields of bounded degree has not yet been proved, while we would like some uniformity as the number field varies. It turns out that the bounds for the degree of a minimal isogeny (with controlled field of definition) proved by Gaudron and Rémond [38] are enough for our purposes, and one obtains:

Theorem 18.5. *Let E be an elliptic curve over a totally real number field F and assume that E is modular of Shimura level 1. Then, with the previous notation, there is a non-constant map*

$$\phi_E : X_1 \to E$$

defined over F, whose degree satisfies

$$h_F^+\delta_E \leq \deg \phi_E \leq c_{10}(n) \max\{1, h(E)\}^{c_{11}(n)} h_F^+\delta_E$$

where $h(E)$ denotes the (logarithmic) Faltings height of E.

(Note that the factor $(\log \mathrm{N}(\mathfrak{N}))^{c_9(n)}$ from Theorem 18.4 has been absorbed by the factor $\max\{1, h(E)\}^{c_{11}(n)}$, in view of Lemma 18.1.)

18.4. **Arakelov height of Heegner points after Yuan and Zhang.** In this paragraph we briefly recall some of the main points of the theory developed by Yuan and Zhang in [114].

As U varies over open compact subgroups of $O_{\mathbb{B}}^\times$ (notation as above) one obtains a projective system $\{X_U\}_U$ of curves over F mapping to $X_{O_{\mathbb{B}}^\times}$.

For a positive integer m, write $U(m) = (1 + mO_{\mathbb{B}})^\times$. The next is Proposition 4.1 in [114].

Proposition 18.6. *If $m \geq 3$ and $U \subseteq U(m)$, then for every $g \in \mathbb{B}^\times$ the group $\tilde{\Gamma}_{U,g}$ acts freely on $\mathfrak{h}$, and the genus of every geometric component of X_U is at least 2.*

Write X_m for the curve $X_{U(m)}$, in particular $X_1 = X_{O_{\mathbb{B}}^\times}$ agrees with our previous notation. Note that when $m_1|m_2$ we have a natural map $X_{m_2} \to X_{m_1}$. The next result follows from the first part of Section 4.2 in [114].

Theorem 18.7. *For $m \geq 3$ coprime to $\mathrm{N}(\mathfrak{N})$, there is a canonical regular integral model $\mathscr{X}_m$ for X_m, which is flat and projective over O_F. Furthermore, $\mathscr{X}_m[1/m]$ is semi-stable over $O_F[1/m]$. More precisely, for a prime ideal $\mathfrak{p}$ of O_F not dividing m one has that the special fibre at $\mathfrak{p}$ is*

(i) *relative Mumford, if $\mathfrak{p}|\mathfrak{N}$;*
(ii) *smooth, if $\mathfrak{p} \nmid \mathfrak{N}$.*

For any m_0 coprime to $\mathrm{N}(\mathfrak{N})$ an integral model $\mathscr{X}_{m_0}$ for X_{m_0} is obtained as follows: Choose any $m \geq 3$ coprime to $\mathrm{N}(\mathfrak{N})$ with $m_0|m$, then $\mathscr{X}_{m_0}$ is defined as the quotient of $\mathscr{X}_m$ by the natural action of the finite group $U(m_0)/U(m)$. The scheme $\mathscr{X}_{m_0}$ is independent of the choice of m (up to isomorphism), it is normal, and it is flat and projective over O_F. In particular, this construction applies to X_1.

For $m_1|m_2$ positive integers coprime to $\mathrm{N}(\mathfrak{N})$, the map $X_{m_2} \to X_{m_1}$ extends to an O_F-morphism $\mathscr{X}_{m_2} \to \mathscr{X}_{m_1}$.

In [114] integral models $\mathscr{X}_U$ for X_U are constructed in more generality, but for our purposes the case of X_m with m a positive integer coprime to $\mathrm{N}(\mathfrak{N})$ suffices. In what follows, such an integer m will be called *admissible.*

For each admissible m let $\widehat{\mathscr{L}_m}$ be the metrized Hodge bundle on $\mathscr{X}_m$, as constructed in [114] Section 4.2. This is a metrized $\mathbb{Q}$-line bundle on $\mathscr{X}_m$ in general, and when $m \geq 3$ it is a metrized line bundle on $\mathscr{X}_m$. Its finite part (i.e. forgetting the metrics) is denoted by $\mathscr{L}_m$. The next result follows from Theorem 4.7 [114].

Theorem 18.8. *The metrized Hodge bundles satisfy the following properties:*

(i) *for $m_1|m_2$ admisible integers, the pull-back of $\widehat{\mathscr{L}_{m_1}}$ by $\mathscr{X}_{m_2} \to \mathscr{X}_{m_1}$ is $\widehat{\mathscr{L}_{m_2}}$;*

(ii) *for $m \geq 3$ admissible, we have that $\mathscr{L}_m[1/m]$ is the relative dualizing sheaf of*

$$\mathscr{X}_m[1/m] \to \operatorname{Spec} O_F[1/m];$$

(iii) *For each embedding $\sigma : F \to \mathbb{R} \subseteq \mathbb{C}$, the metric on the restriction of $\mathscr{L}$ to $X_m \otimes_\sigma \mathbb{C}$ is induced via complex uniformization by the metric $|dz| = 2\Im(z)$ on differential forms on $\mathfrak{h}$.*

A totally imaginary quadratic extension K/F is said to satisfy the (generalized) Heegner hypothesis for $\mathfrak{N}$ if every prime $\mathfrak{p}|\mathfrak{N}$ is inert in K. In particular, such an extension K/F has relative discriminant $\mathfrak{d}_{K/F}$ coprime to $\mathfrak{N}$.

If K satisfies the Heegner hypothesis for $\mathfrak{N}$, for each open compact U we have a Heegner point $P_{K,U}$ in X_U. These can be chosen to form a compatible system of algebraic points in the projective system $\{X_U\}_U$. The point $P_K = P_{K,O_{\mathbb{B}}^\times}$ is defined over the Hilbert class field of K, and in general, all the $P_{K,U}$ are defined over abelian extensions of K.

Theorem 1.5 in [114] gives a formula for the Arakelov-theoretical height

$$h_{Ar}(P_K) := \frac{1}{[H_K : F]} \widehat{\deg}_{O_{H_K}} s^* \widehat{\mathscr{L}_1}$$

of P_K on $\mathscr{X}_1$ with respect to $\widehat{\mathscr{L}_1}$, where $s : \operatorname{Spec} O_{H_K} \to \mathscr{X}_1$ is the multi-section attached to P_K. The result is:

Theorem 18.9. *Suppose that F has at least two ramified places in B. Let K/F be a totally imaginary quadratic extension satisfying the Heegner hypothesis for $\mathfrak{N}$. Let χ_K be the quadratic Hecke character of F associated to the extension K/F. Then we have*

$$h_{Ar}(P_K) = -\frac{L'}{L}(0, \chi_K) + \frac{1}{2} \log \frac{\mathrm{N}(\mathfrak{N})}{\mathrm{N}(\mathfrak{d}_{K/F})}.$$

This can be rewritten as

$$h_{Ar}(P_K) = \frac{L'}{L}(1, \chi_K) + \frac{1}{2} \log \mathrm{N}(\mathfrak{d}_{K/F}\mathfrak{N}) + \log d_F - n \cdot (\gamma + \log(2\pi)).$$

The first formula is Theorem 1.5 in [114], while the second is simply a consequence of the functional equation of $L(s, \chi_K)$.

18.5. An approach to Szpiro's conjecture over totally real number fields.

Theorem 18.10. *Let F be a totally real number field of degree n over $\mathbb{Q}$. Let E be an elliptic curve over F and suppose that E is modular of Shimura level 1. Let $\mathfrak{N}$ be the conductor ideal of E, let B be a quaternion F-algebra of discriminant $\mathfrak{N}$ with exactly one split place at infinity, and let X_1 be the associated Shimura curve.*

Let $\psi : X_1 \to E$ be a non-constant morphism over F (which exists, as E is modular of Shimura level 1). Then we have

$$h(E) \leq \frac{1}{2} \log \deg \psi + c_{12}(n) \log(d_F \mathrm{N}(\mathfrak{N}))$$

and

$$\log \Delta_E \leq 6n \log \deg \psi + c_{13}(n) \log(d_F \mathrm{N}(\mathfrak{N})).$$

Proof. For each admissible m, let $\psi_m : X_m \to E$ be the composition of $X_m \to X_1$ with ψ. For $m \geq 3$ admissible, the map ψ_m extends to an $O_F[1/m]$-morphism

$$\psi_m : \mathscr{X}_m[1/m]^\circ \to \mathscr{E}[1/m]$$

by the Néron mapping property, where $\mathscr{E}$ is the Néron model of E and $\mathscr{X}_m[1/m]^\circ$ is the smooth locus of $\mathscr{X}_m[1/m] \to \operatorname{Spec} O_F[1/m]$, obtained from $\mathscr{X}_m[1/m]$ by removing the singular points of the special fibres at primes dividing $\mathfrak{N}$.

Choose two different admissible prime numbers p, q, different from 2 and small in the sense that

$$p, q < 100 \log \mathrm{N}\mathfrak{N}$$

(say), which is possible by a variation of Lemma 5.2. Let $\mathscr{Y}_{pq}$ be the open set of $\mathscr{X}_{pq}$ obtained as the union of the preimages of $\mathscr{X}_p[1/p]^\circ \subseteq \mathscr{X}_p$ and $\mathscr{X}_q[1/q]^\circ \subseteq \mathscr{X}_q$. Then by glueing we obtain an O_F-morphism

$$\psi_{pq} : \mathscr{Y}_{pq} \to \mathscr{E}.$$

Let K/F be a totally imaginary quadratic extension of F satisfying the Heegner hypothesis. Furthermore, assume that the associated Heegner point $P_{K,U(pq)}$ is not a ramification point of ψ_{pq}. Let H be a number field containing K over which $P_{K,U(pq)}$ is defined. Write $S_H = \operatorname{Spec} O_H$ and let $s : S_H \to \mathscr{X}_{pq}$ be the O_F-map obtained from the algebraic point $P_{K,U(pq)}$. Observe that s exists because $\mathscr{X}_{pq}$ is projective over O_F, and it has image contained in $\mathscr{Y}_{pq}$ because all primes dividing $\mathfrak{N}$ are inert in K (cf. p. 242 in [113]).

By a patching argument using ψ_p and ψ_q, we get the canonical injective sheaf morphism (cf. the notation in Paragraphs 18.1 and 18.4)

$$u : \psi_{pq}^*(\omega|_{\mathscr{E}}) \to \mathscr{L}_{pq}|_{\mathscr{Y}_{pq}}$$

which allows us to see the first as a sub-sheaf of the second, on $\mathscr{Y}_{pq}$. The sheaf $\psi_{pq}^*(\omega|_{\mathscr{E}})$ has the norms $\| - \|'_\sigma$ induced from the metrized relative dualizing sheaf $\widehat{\omega}$ of the semi-stable elliptic curve E, while the Hodge bundle has its own norms $\| - \|_\sigma$. We now compare these norms.

Let $\sigma : F \to \mathbb{C}$ be any embedding and take a complex point $x \in X_{pq} \otimes_\sigma \mathbb{C}$. Let $\mu \in \psi_{pq}^*(\Omega^1_{E_\sigma/\mathbb{C}})|_x$ and let $\lambda \in \Omega^1_{E_\sigma/\mathbb{C}}|_{\psi_{pq}(x)}$ be such that $\psi_{pq}^*\lambda = \mu$. Let $\alpha \in H^0(E_\sigma, \Omega^1_{E_\sigma/\mathbb{C}})$ be the invariant differential with $\alpha_{\psi_{pq}(x)} = \lambda$. Then by definition of the pull-back norm on $\psi_{pq}^*(\omega|_{\mathscr{E}})$ we have

$$(59) \qquad \left(\|\mu\|'_{\sigma,x}\right)^2 = \|\lambda\|^2_{\sigma,\psi_{pq}(x)} = \frac{i}{2}\int_{E_\sigma} \alpha \wedge \overline{\alpha}.$$

We now estimate $\|u(\mu)\|_{\sigma,x}$ according to the metrics of the Hodge bundle. Note that

$$u(\mu) = u(\psi_{pq}^*\lambda) = u(\psi_{pq}^*(\alpha_{\psi_{pq}(x)})) = u(\psi_{pq}^*\alpha)_x = (\psi_{pq}^\bullet\alpha)_x$$

and therefore for suitable $g \in \mathbb{B}^\times$ according to the connected component in which x is, we have

$$\|u(\mu)\|_{\sigma,x} \leq 2\|\Psi_{U(pq),g}(\psi_{pq}^\bullet\alpha)\|_{U(pq),g,\infty} \leq c_{14}(n)\|\Psi_{U(pq),g}(\psi_{pq}^\bullet\alpha)\|_{U(pq),g,2}$$

where $\Psi_{U,g}$ is defined analogously to the definition in Paragraph 4.6 (adapting from $\mathbb{Q}$ to F), and the second inequality is by Theorem 8.1.

By pulling back the $(1,1)$-form $\alpha \wedge \overline{\alpha}$ from (59), we now observe that

$$\|\Psi_{U(pq),g}(\psi_{pq}^\bullet\alpha)\|^2_{U(pq),g,2} \leq \deg(\psi_{pq})\|\mu\|^2_{\sigma,x}$$

(this is only a bound rather than an equality because the left hand side just considers one geometric component of $X_{U(pq)}$) which gives the norm comparison

$$(60) \qquad \|u(\mu)\|_{\sigma,x} \leq c_{15}(n)(\deg\psi_{pq})^{1/2}\|\mu\|_{\sigma,x}.$$

Pulling back u by s we get a sheaf morphism on S_H

$$u' : (\psi_{pq}s)^*\omega = s^*\psi_{pq}^*(\omega|_{\mathscr{E}}) \to s^*\mathscr{L}_{pq}|_{\mathscr{Y}_{pq}} = s^*\mathscr{L}_{pq}$$

which still is injective because $P_{K,U(pq)}$ is not in the ramification locus of ψ_{pq}, by assumption. Injectivity, together with the norm comparison (60) gives

$$\widehat{\deg}_{S_H}(\psi_{pq}s)^*\widehat{\omega} \leq \widehat{\deg}_{S_H} s^*\widehat{\mathscr{L}}_{pq} + \frac{[H:\mathbb{Q}]}{2}\log\deg\psi_{pq} + c_{16}(n)[H:\mathbb{Q}].$$

Dividing by $[H:\mathbb{Q}] = [H:F]\cdot n$, recalling Theorem 18.2, the definition of $h_{Ar}(P_K)$, and the fact that the metrized Hodge bundles are compatible with pull-back (Theorem 18.8), one obtains

$$h(E) \leq \frac{1}{n}h_{Ar}(P_K) + \frac{1}{2}\log\deg\psi_{pq} + c_{17}(n).$$

By Theorem 18.9 we get

$$n\cdot h(E) \leq \frac{n}{2}\log\deg\psi_{pq} + \frac{L'}{L}(1,\chi_K) + \frac{1}{2}\log \mathrm{N}(\mathfrak{d}_{K/F}\mathfrak{N}) + \log d_F + c_{18}(n). \tag{61}$$

The number of complex ramification points of ψ_m is at most $2g_m - 2$ where g_m is the sum of the genera the geometric components of X_m. This is at most the total (hyperbolic) volume of X_m divided by 2π, which is at most

$$\frac{1}{2\pi}[U(1):U(m)]\cdot Vol(X_1^{an}) \leq c_{19}(n)(md_F)^{c_{20}(n)}\mathrm{N}(\mathfrak{N})$$

since X_1^{an} has h_F^+ components, and using the volume formula from Proposition 18.3.

Hence, by Theorem 17.3 and recalling that p and q are small, there is some totally imaginary quadratic extension K/F satisfying the Heegner hypothesis for $\mathfrak{N}$, such that $P_{K,U(pq)}$ is not a ramification point of ψ_{pq}, and satisfying the estimates

$$\mathrm{N}(\mathfrak{d}_{K/F}) < c_{21}(n)(d_F\mathrm{N}(\mathfrak{N}))^{c_{22}(n)}$$

and

$$\left|\frac{L'}{L}(1,\chi_K)\right| < c_{23}(n)\left(\log d_F + \log\log \mathrm{N}(\mathfrak{N})\right).$$

From (61) and using the fact that the degree of $X_m \to X_1$ is at most $m^{c_{24}(n)}$ (and that p and q are small), we finally deduce

$$h(E) \leq \frac{1}{2}\log\deg\psi + c_{25}(n)\log(d_F\mathrm{N}(\mathfrak{N})).$$

The estimate for Δ_E follows by Lemma 18.1 □

Theorem 18.10 motivates the following conjecture:

Conjecture 18.11. *Suppose that F is a totally real number field of degree n over $\mathbb{Q}$, and that E/F is an elliptic curve which is modular of Shimura level* 1*. Then*

$$\log\delta_E < \kappa\cdot\log(d_F\mathrm{N}(\mathfrak{N}))$$

for some constant κ that only depends on the degree n.

Note that for a given field F, the conjecture only concerns modular elliptic curves of Shimura level 1 and it involves the canonically defined quantity δ_E instead of using the degree of some arbitrary choice of modular parametrization $X_1 \to E$. Conjecture 18.11 is of interest because it implies Szpiro's conjecture for such elliptic curves, as we prove in the next paragraph.

18.6. **Bounds for δ_E and Szpiro's conjecture.** The purpose of this paragraph is to spell-out the precise relation between Szpiro's conjecture and our proposed conjectural bound for the quantity δ_E, namely, Conjecture 18.11.

First we do this in a particularly convenient case where several technical assumptions can be removed: the case when F is real quadratic. In particular, here one does not need to assume modularity as a hypothesis, because it is proved in the relevant cases.

Theorem 18.12. *Assume Conjecture 18.11 for real quadratic fields and their totally real quadratic extensions. Then there is an absolute constant $c > 0$ such that the following holds:*

For every real quadratic field F and every semi-stable elliptic curve E over F which does not have everywhere good reduction, we have

$$h(E) \le c \cdot \log(d_F N_E) \quad \text{and} \quad \Delta_E \le (d_F N_E)^c.$$

Proof. If E has an odd number of places of bad reduction, then it is modular of Shimura level 1 (according to our definition) by the modularity results from [34] (see also [113, 115] to deduce geometric modularity from automorphy). In this case we have, for the corresponding Shimura curve X_1, a modular parameterization

$$\phi : X_1 \to E$$

afforded by Theorem 18.5, whose degree satisfies

$$\log \deg(\phi) \le \log \delta_E + \log h_F^+ + O_n\left(1 + \log \max\{1, h(E)\}\right).$$

By Theorem 18.10 and bounding h_F^+ in terms of d_F, we get (unconditionally)

$$h(E) \le \frac{1}{2} \log \delta_E + O_n\left(\log \max\{1, h(E)\} + \log(d_F N_E)\right).$$

At this point we apply Conjecture 18.11 to get the result.

When E has a non-zero even number of primes of bad reduction over F, we base-change to a suitable totally real quadratic extension F'/F, such that exactly one prime of bad reduction of E is inert and all the other are split. Since E is semi-stable over F, now it has an odd number of bad places over F' and by [29] it is modular of Shimura level 1. As E/F is semi-stable, its Faltings height is the same after base change. Furthermore, F' can be chosen with $\log d_{F'} \ll \log(d_F N_E)$ by Lemma 17.1. Now the same argument applies. □

Finally, here is a version of the previous result for totally real number fields beyond the quadratic case, under the assumption of modularity.

Theorem 18.13. *Assume Conjecture 18.11. Assume that elliptic curves over totally real number fields are modular (in the sense of* [39]*). Then the following holds:*

Let F be a totally real number field of degree n over $\mathbb{Q}$. Then for every semi-stable elliptic curve E over F which does not have everywhere good reduction, we have

$$h(E) \le \kappa \cdot \log(d_F N_E) \quad \text{and} \quad \Delta_E \le (d_F N_E)^\kappa$$

for some constant κ that only depends on the degree n.

The proof is similar to that of Theorem 18.12. Of course, our methods also show that partial modularity results together with partial progress towards Conjecture 18.11 are enough to give consequences for Szpiro's conjecture. We discuss such an application in the next paragraph.

18.7. **Application: Unconditional exponential bounds.** Finally, we observe that unconditional exponential bounds for δ_E over a totally real field F (and thanks to our results, for Szpiro's conjecture) can be proved by the same methods of Sections 5 and 7. Namely, it is straightforward to extend any of the two proofs of Theorem 5.5 to the totally real setting, and then such an extension is used to prove an analogue of Theorem 7.2. To do the latter, one should use results on effective multiplicity one for GL_2 —such as those in [11, 106, 66]— in order to distinguish systems of Hecke eigenvalues using only few Hecke operators. To count the number of systems of Hecke eigenvalues used in the proof, a crude bound is the genus of $X_{O_{\mathbb{B}}^{\times}}$, which can be estimated by Shimizu's volume formula.

For instance, an unconditional consequence is the following:

Theorem 18.14. *Let F be a totally real number field and let $\epsilon > 0$. For all semi-stable elliptic curves E over F satisfying that the number of places of bad reduction of E has opposite parity to $[F : \mathbb{Q}]$, we have $\log \delta_E \ll_{F,\epsilon} N_E^{1+\epsilon}$, hence*

$$h(E) \ll_{F,\epsilon} N_E^{1+\epsilon} \qquad \textit{and} \qquad \log \Delta_E \ll_{F,\epsilon} N_E^{1+\epsilon}.$$

Indeed, Theorem 5 in [34] gives a finite list of possible j-invariants for non-modular elliptic curves over F. As we are assuming semi-stability, this translates into finitely many F-isomorphism classes of elliptic curves that can fail to be modular in our setting, and they only contribute to a possibly different implicit constant. In all other cases our bounds apply, hence the result.

We note that the list of exceptional j-invariants comes from Faltings theorem for curves and it is in general ineffective. In the case that F is real quadratic the list of exceptional j-invariants is empty [34] hence, the only way in which a real quadratic F contributes to the implicit constants of Theorem 18.14 is by means of the application of effective multiplicity one for GL_2 over varying quadratic number fields.

The problem of proving good bounds for effective multiplicity one on GL_2 over number fields of bounded degree with explicit dependence on the number field (and without the assumption of GRH) seems to be an open problem in analytic number theory.

19. Acknowledgments

Part of this project was carried out while I was a member at the Institute for Advanced Study in 2015-2016, and then continued at Harvard. I greatly benefited from conversations with Enrico Bombieri, Noam Elkies, Nicholas Katz, Barry Mazur, Peter Sarnak, Richard Taylor, and Shou-Wu Zhang, and I sincerely thank them for generously sharing their ideas and knowledge. In particular, the argument in Paragraph 5.6 originates in an idea of R. Taylor in the case of classical modular curves, and the connection between injectivity radius and Lehmer's conjecture used in Section 8 was pointed out to me by P. Sarnak. Feedback from B. Mazur on the topic of the Manin constant was of great help, and I also thank Kestutis Cesnavicius and Bas Edixhoven for some additional observations on this subject. I learned some of the material relevant for this project by attending the joint IAS-Princeton algebraic number theory seminar during my stay at the IAS, and I thank Christopher Skinner and Richard Taylor for organizing it.

Comments from Natalia Garcia-Fritz and Ricardo Menares regarding the presentation of this article are gratefully acknowledged. I also thank Robert Lemke Oliver and Jesse Thorner for the appendix. Finally, I thank Enrico Bombieri and Natalia Garcia-Fritz for their encouragement, which allowed me to push this project further than I initially had in mind.

Appendix A. Zeros of twisted L-functions near $\Re(s) = 1$ (by Robert Lemke Oliver and Jesse Thorner)

Let K be a number field with absolute discriminant discriminant d_K, and let χ be a primitive ray class character defined over K. Our goal is to prove:

Proposition A.1. *Let $Q, T \geq 1$ and $\epsilon > 0$. Suppose that $y = T^{[K:\mathbb{Q}]/2+2+2\epsilon} d_K^{1/2} Q^5$. For any function $b(\mathfrak{p})$ supported on the prime ideals of K with norm greater than y,*

$$\sum_{\mathrm{N}\mathfrak{q} \leq Q} \sideset{}{'}\sum_{\chi \bmod \mathfrak{q}} \int_{-T}^{T} \Big| \sum_{\mathrm{N}\mathfrak{p} > y} \chi(\mathfrak{p}) b(\mathfrak{p}) \mathrm{N}\mathfrak{p}^{-it} \Big|^2 dt \ll_{\epsilon, [K:\mathbb{Q}]} (d_K Q)^{\epsilon} \sum_{\mathrm{N}\mathfrak{p} > y} |b(\mathfrak{p})|^2 \mathrm{N}\mathfrak{p}.$$

Here, $\sideset{}{'}\sum_{\chi \bmod \mathfrak{q}}$ denotes a sum over primitive ray class characters χ of modulus $\mathfrak{q}$ over K.

With Proposition A.1 in hand, one can use the proofs in [63, Sections 3 and 4] to prove a zero density estimate for twisted L-functions. Let $\mathbb{A}_K$ denote the ring of adeles of K, and let π be a cuspidal automorphic representation of $\mathrm{GL}_d(\mathbb{A}_K)$ with unitary central character. We make the implicit assumption that the central character of π is trivial on the product of positive reals when embedded diagonally into the (archimedean places of the) ideles. The standard L-function associated to π is of the form

$$L(s, \pi) = \sum_{\mathfrak{a}} \frac{\lambda_\pi(\mathfrak{a})}{\mathrm{N}\mathfrak{a}^s} = \prod_{\mathfrak{p}} \prod_{j=1}^{d} (1 - \alpha_\pi(j, \mathfrak{p}) \mathrm{N}\mathfrak{p}^{-s})^{-1},$$

where the sum runs over the nonzero integral ideals of K and the product runs over the prime ideals of K. Assume that π satisfies the generalized Ramanujan conjecture, in which case $|\alpha_\pi(j, \mathfrak{p})| \leq 1$ for every j and $\mathfrak{p}$. We now consider the zeros of the twisted L-functions $L(s, \pi \otimes \chi)$. Let $N_{\pi\otimes\chi}(\sigma, T) := \#\{\rho = \beta + i\gamma \colon L(\rho, \pi \otimes \chi) = 0,\ \beta \geq \sigma,\ |\gamma| \leq T\}$.

Proposition A.2. *Let $\epsilon > 0$, let $Q, T \geq 1$, and let $1/2 \leq \sigma \leq 1$. If π satisfies the generalized Ramanujan conjecture, then there exists a constant $c > 0$ (depending only on d an $[K : \mathbb{Q}]$) such that*

$$\sum_{\mathrm{N}\mathfrak{q} \leq Q} \sideset{}{'}\sum_{\chi \bmod \mathfrak{q}} N_{\pi\otimes\chi}(\sigma, T) \ll_{\epsilon, [K:\mathbb{Q}]} (C(\pi) Q T)^{c(1-\sigma)+\epsilon},$$

where $C(\pi)$ is the analytic conductor of π.

The proof of Proposition A.2 proceeds exactly the same as [63, Corollary 1.4]. While the density estimate here is not as strong as [63, Corollary 1.4], the point is that now one can take π and the Hecke characters χ to be defined over number fields other than $\mathbb{Q}$. Since we aim for brevity, Propositions A.1 and A.2 are not the strongest results that the method can produce. A more careful treatment will appear in forthcoming work by R. Lemke Oliver, B. Linowitz, and J. Thorner.

Let $\mathfrak{q}$ be an integral ideal of K, let $I(\mathfrak{q})$ be the group of fractional ideals which are relatively prime to $\mathfrak{q}$, and let $P_{\mathfrak{q}}$ be the subgroup of $I(\mathfrak{q})$ consisting of principal fractional ideals (α) with α totally positive and $\alpha \equiv 1 \bmod^* \mathfrak{q}$. Thus $I(\mathfrak{q})/P_{\mathfrak{q}}$ is the group of ideal classes modulo $\mathfrak{q}$ of K (in the "narrow" sense, which involves no essential loss of generality).

We write $\chi \pmod{\mathfrak{q}}$ to denote a Hecke character of the finite abelian group $I(\mathfrak{q})/P_{\mathfrak{q}}$. If $\mathfrak{q}$ divides $\mathfrak{n}$, then the inclusion map $I(\mathfrak{n}) \to I(\mathfrak{q})$ induces a surjective homomorphism $I(\mathfrak{n})/P_{\mathfrak{n}} \to I(\mathfrak{q})/P_{\mathfrak{q}}$. Composing a character $\chi \pmod{\mathfrak{q}}$ with this map induces a character $\chi' \pmod{\mathfrak{n}}$. We recall that χ is a *primitive character* if the only character which induces χ is χ itself. Given a character $\chi \pmod{\mathfrak{q}}$, the equivalence class of χ contains a unique primitive character $\tilde{\chi} \bmod \mathfrak{f}_\chi$ so that the equivalence class contains precisely those characters which are induced by $\tilde{\chi}$. The integral ideal $\mathfrak{f}_\chi$ is called the *conductor* of χ, and it depends only on the equivalence class of χ.

While the above definition of a Hecke character $\chi \pmod{\mathfrak{q}}$ holds only for those integral ideals which are coprime to $\mathfrak{q}$, we may extend χ to be a completely multiplicative function on the integral ideals of K by setting $\chi(\mathfrak{a}) = 0$ if $\gcd(\mathfrak{a}, \mathfrak{q}) \neq (1)$. Thus we may associate an L-function $L(s, \chi)$ to χ whose Dirichlet series and Euler product are given by

$$L(s,\chi) = \sum_{\mathfrak{a}} \chi(\mathfrak{a})\mathrm{N}\mathfrak{a}^{-s} = \prod_{\mathfrak{p}} (1 - \chi(\mathfrak{p})\mathrm{N}\mathfrak{p}^{-s})^{-1}.$$

The series and product converge absolutely for $\mathrm{Re}(s) > 1$ and can be analytically continued to $\mathbb{C}$ with a functional equation relating s to $1 - s$. (See [108] for further discussion and pertinent references.)

Fix a smooth function ϕ whose support is a compact subset of $(-2, 2)$. Let

$$\hat{\phi}(s) = \int_{\mathbb{R}} \phi(t) e^{st} dt.$$

Thus $\hat{\phi}(s)$ is entire. We repeatedly integrate by parts to see that $\hat{\phi}(\sigma + it) \ll_{\phi,k} e^{2|\sigma|}|\sigma + it|^{-k}$ for any integer $k \geq 0$. Let $T \geq 1$. By Fourier inversion, we find that for any $c, x > 0$

$$\phi(T \log x) = \frac{1}{2\pi i T} \int_{c-i\infty}^{c+i\infty} \hat{\phi}(s/T) x^{-s} ds.$$

Lemma A.3. *Let $\epsilon > 0$ be sufficiently small (with respect to $[K : \mathbb{Q}]$). If $\chi \pmod{\mathfrak{q}}$ is a (possibly non-primitive) Hecke character, then for any $x > 0$ and $T \geq 1$,*

$$\Big| \sum_{\mathfrak{a}} \chi(\mathfrak{a}) \phi\Big(T \log \frac{\mathrm{N}\mathfrak{a}}{x}\Big) - \delta(\chi)\kappa \frac{\varphi(\mathfrak{q})}{\mathrm{N}\mathfrak{q}} x \frac{\hat{\phi}(1/T)}{T} \Big| \ll_{\epsilon,[K:\mathbb{Q}],\phi} (d_K \mathrm{N}\mathfrak{f}_\chi)^{1/4+\epsilon} (\mathrm{N}\mathfrak{q})^{\epsilon} \sqrt{x} T^{[K:\mathbb{Q}]/4+\epsilon},$$

where $\delta(\chi) = 1$ if χ is trivial and $\delta(\chi) = 0$ otherwise, and $\kappa := \mathrm{Res}_{s=1}\zeta_K(s)$.

Proof. The quantity whose absolute value we wish to bound equals

$$\frac{1}{2\pi i} \int_{1/2-i\infty}^{1/2+i\infty} L(s, \tilde{\chi}) \hat{\phi}(s/T) x^s \prod_{\substack{\mathfrak{p}|\mathfrak{q} \\ \mathfrak{p}\nmid\mathfrak{f}_\chi}} (1 - \tilde{\chi}(\mathfrak{p})\mathrm{N}\mathfrak{p}^{-s}) ds.$$

Rademacher [80] proved that if χ is a primitive character and $\epsilon > 0$, then

$$\Big| \Big(\frac{s-1}{s+1}\Big)^{\delta(\chi)} L(s,\chi) \Big| \ll_{\epsilon,[K:\mathbb{Q}]} (d_K \mathrm{N}\mathfrak{f}_\chi (1 + |t|)^{[K:\mathbb{Q}]})^{\frac{1-\sigma+\epsilon}{2}}$$

uniformly in the region $-\epsilon \leq \sigma \leq 1 + \epsilon$. In particular,

$$\kappa = \mathrm{Res}_{s=1}\zeta_K(s) \ll_{\epsilon,[K:\mathbb{Q}]} d_K^{\epsilon}. \tag{62}$$

Thus the above integral is

$$\ll_{\epsilon,[K:\mathbb{Q}]} (d_K \mathrm{N}\mathfrak{f}_\chi)^{1/4+\epsilon/2} 2^{\omega(\mathfrak{q})} \sqrt{x} \int_{-\infty}^{\infty} \hat{\phi}\Big(\frac{1/2 + it}{T}\Big)(1 + |t|)^{(1/4+\epsilon/2)[K:\mathbb{Q}]} dt$$

where ω denotes the number of different prime ideals that divide a non-zero integral ideal. Using our bound on $\hat{\phi}(s)$, the above expression becomes

$$\ll_{\epsilon,[K:\mathbb{Q}],\phi} (d_K \mathrm{N}\mathfrak{f}_\chi)^{1/4+\epsilon/2} 2^{\omega(\mathfrak{q})} \sqrt{x} \int_{-\infty}^{\infty} \min\Big\{1, \frac{T^{[K:\mathbb{Q}]/4+2}}{(1 + |t|)^{[K:\mathbb{Q}]/4+2}}\Big\} (1 + |t|)^{(1/4+\epsilon/2)[K:\mathbb{Q}]} dt.$$

One has $2^{\omega(\mathfrak{q})} \ll_{\epsilon,[K:\mathbb{Q}]} (d_K \mathrm{N}\mathfrak{q})^{\epsilon}$ (cf. Lemma 1.13 in [108]). If ϵ is sufficiently small with respect to $[K : \mathbb{Q}]$, then the claimed bound follows. □

This simple bound is sufficient to establish a weak form of the large sieve inequality for Hecke characters over K, generalizing the classical case over $\mathbb{Q}$.

Proposition A.4. *Let $\epsilon, x > 0$ and $Q, T \geq 1$. For any complex-valued function $b(\mathfrak{a})$ supported on the integral ideals of K, we have that*

$$\sum_{\mathrm{N}\mathfrak{q}\leq Q}\ \sideset{}{'}\sum_{\chi \bmod \mathfrak{q}} \Big|\sum_{x<\mathrm{N}\mathfrak{a}\leq xe^{1/T}} b(\mathfrak{a})\chi(\mathfrak{a})\Big|^2 \ll_{\epsilon,[K:\mathbb{Q}]} (d_KQ)^{\epsilon}\Big(\frac{x}{T}+d_K^{\frac{1}{4}}Q^{\frac{5}{2}}\sqrt{x}T^{\frac{[K:\mathbb{Q}]}{4}+\epsilon}\Big)\sum_{x<\mathrm{N}\mathfrak{a}\leq xe^{1/T}}|b(\mathfrak{a})|^2.$$

Proof. Let $\epsilon, x > 0$ and $Q, T \geq 1$. By a standard application of duality, it suffices to prove that for any sequence of complex numbers b_χ indexed by the primitive Hecke characters χ,

$$\begin{aligned}&\sum_{x<\mathrm{N}\mathfrak{a}\leq xe^{1/T}}\Big|\sum_{\mathrm{N}\mathfrak{q}\leq Q}\ \sideset{}{'}\sum_{\chi \bmod \mathfrak{q}} b_\chi\chi(\mathfrak{a})\Big|^2\\ &\ll_{\epsilon,[K:\mathbb{Q}]} (d_KQ)^{3\epsilon}\Big(\frac{x}{T}+d_K^{1/4}Q^{5/2}\sqrt{x}T^{[K:\mathbb{Q}]/4+\epsilon}\Big)\sum_{\mathrm{N}\mathfrak{q}\leq Q}\ \sideset{}{'}\sum_{\chi \bmod \mathfrak{q}}|b_\chi|^2.\end{aligned}\tag{63}$$

We will prove (63). First, we observe that for an appropriate uniform choice of ϕ, the indicator function $\mathbf{1}_{(x,xe^{1/T}]}(t)$ for the interval $(x, xe^{1/T}]$ is bounded above by $\phi(T\log\frac{t}{x})$. In fact, any smooth ϕ dominating the indicator function of $[0,1]$ with compact support in $(-2,2)$ works, and we fix it once and for all. Thus the left hand side of (63) is bounded by

$$\sum_{\mathfrak{a}}\Big|\sum_{\mathrm{N}\mathfrak{q}\leq Q}\ \sideset{}{'}\sum_{\chi \bmod \mathfrak{q}} b_\chi\chi(\mathfrak{a})\Big|^2\phi\Big(T\log\frac{\mathrm{N}\mathfrak{a}}{x}\Big).\tag{64}$$

Expanding the square and changing the order of summation, we see that (64) equals

$$\begin{aligned}&\sum_{\mathrm{N}\mathfrak{q}_1,\mathrm{N}\mathfrak{q}_2\leq Q}\ \sideset{}{'}\sum_{\substack{\chi_1 \bmod \mathfrak{q}_1\\ \chi_2 \bmod \mathfrak{q}_2}} b_{\chi_1}\overline{b_{\chi_2}}\sum_{\mathfrak{a}}\chi_1(\mathfrak{a})\bar{\chi}_2(\mathfrak{a})\phi\Big(T\log\frac{\mathrm{N}\mathfrak{a}}{x}\Big)\\ &\leq\Big(\max_{\substack{\mathrm{N}\mathfrak{q}_1\leq Q\\ \chi_1 \bmod \mathfrak{q}_1}}\sum_{\mathrm{N}\mathfrak{q}_2\leq Q}\ \sideset{}{'}\sum_{\chi_2 \bmod \mathfrak{q}_2}\Big|\sum_{\mathfrak{a}}\chi_1(\mathfrak{a})\bar{\chi}_2(\mathfrak{a})\phi\Big(T\log\frac{\mathrm{N}\mathfrak{a}}{x}\Big)\Big|\Big)\sum_{\mathrm{N}\mathfrak{q}\leq Q}\ \sideset{}{'}\sum_{\chi \bmod \mathfrak{q}}|b_\chi|^2.\end{aligned}\tag{65}$$

We now apply Lemma A.3 to (65). Since

$$\varphi(\mathfrak{q}) := \mathrm{N}\mathfrak{q}\prod_{\mathfrak{p}\mid\mathfrak{q}}\Big(1-\frac{1}{\mathrm{N}\mathfrak{p}}\Big)\leq\mathrm{N}\mathfrak{q}$$

for any non-zero integral ideal $\mathfrak{q}$ of K, we see that (65) is

$$\ll_{\epsilon,[K:\mathbb{Q}]}\Big(\kappa x\frac{\hat{\phi}(1/T)}{T}+(d_KQ^2)^{1/4+\epsilon}\sqrt{x}T^{[K:\mathbb{Q}]/4+\epsilon}\sum_{\mathrm{N}\mathfrak{q}_2\leq Q}\ \sideset{}{'}\sum_{\chi_2 \bmod \mathfrak{q}_2}1\Big)\sum_{\mathrm{N}\mathfrak{q}\leq Q}\ \sideset{}{'}\sum_{\chi \bmod \mathfrak{q}}|b_\chi|^2.\tag{66}$$

For every $Q \geq 2$ and every $\epsilon > 0$ we have $\sum_{\mathrm{N}\mathfrak{q}_2\leq Q}1 \ll_{[K:\mathbb{Q}]} Q^{1+\epsilon}$ by [108, Lemma 1.12]. Thus we have the trivial bound

$$\sum_{\mathrm{N}\mathfrak{q}_2\leq Q}\ \sideset{}{'}\sum_{\chi_2 \bmod \mathfrak{q}_2}1 \ll_{\epsilon,[K:\mathbb{Q}]} Q^{2+\epsilon}.$$

With this bound as well as (62), we find that (66) is

$$\ll_{\epsilon,[K:\mathbb{Q}]} (d_KQ)^{3\epsilon}\Big(x\frac{\hat{\phi}(1/T)}{T}+d_K^{1/4}Q^{5/2}\sqrt{x}T^{[K:\mathbb{Q}]/4+\epsilon}\Big)\sum_{\mathrm{N}\mathfrak{q}\leq Q}\ \sideset{}{'}\sum_{\chi \bmod \mathfrak{q}}|b_\chi|^2.$$

Since $\hat{\phi}(1/T)\asymp_\phi 1$ for all $T \geq 1$ and ϕ is fixed, we have proved (63) once we re-scale ϵ. □

Proof of Proposition A.1. A result of Gallagher [37, Theorem 1] states that for any sequence of complex numbers a_n and any $T \geq 1$, we have

$$\int_{-T}^{T} \Big| \sum_{n\geq 1} a_n n^{-it} \Big|^2 dt \ll T^2 \int_0^\infty \Big| \sum_{x<n\leq xe^{1/T}} a_n \Big|^2 \frac{dx}{x}.$$

Thus for any function $b(\mathfrak{a})$ supported on the ideals of K,

$$\sum_{\mathrm{N}\mathfrak{q}\leq Q} \sum_{\chi \bmod \mathfrak{q}}' \int_{-T}^{T} \Big| \sum_{\mathfrak{a}} b(\mathfrak{a})\chi(\mathfrak{a})\mathrm{N}\mathfrak{a}^{-it} \Big|^2 dt \ll T^2 \int_0^\infty \sum_{\mathrm{N}\mathfrak{q}\leq Q} \sum_{\chi \bmod \mathfrak{q}}' \Big| \sum_{x<\mathrm{N}\mathfrak{a}\leq xe^{1/T}} b(\mathfrak{a})\chi(\mathfrak{a}) \Big|^2 \frac{dx}{x}$$

By Proposition A.4, we see that the right hand side of the above display is

$$\begin{aligned}
&\ll_{\epsilon,[K:\mathbb{Q}]} (d_K Q)^\epsilon T^2 \int_0^\infty \Big(\frac{x}{T} + d_K^{1/4} Q^{5/2} \sqrt{x} T^{[K:\mathbb{Q}]/4+\epsilon} \Big) \sum_{x<\mathrm{N}\mathfrak{a}\leq xe^{1/T}} |b(\mathfrak{a})|^2 \frac{dx}{x} \\
&= (d_K Q)^\epsilon \sum_{\mathfrak{a}} |b(\mathfrak{a})|^2 \Big(T \int_{e^{-1/T}\mathrm{N}\mathfrak{a}}^{\mathrm{N}\mathfrak{a}} dx + T^{[K:\mathbb{Q}]/4+2+\epsilon} d_K^{1/4} Q^{5/2} \int_{e^{-1/T}\mathrm{N}\mathfrak{a}}^{\mathrm{N}\mathfrak{a}} x^{-1/2} dx \Big) \\
&\ll_{\epsilon,[K:\mathbb{Q}]} (d_K Q)^\epsilon \sum_{\mathfrak{a}} |b(\mathfrak{a})|^2 \mathrm{N}\mathfrak{a} \Big(1 + T^{[K:\mathbb{Q}]/4+1+\epsilon} d_K^{1/4} Q^{5/2} \mathrm{N}\mathfrak{a}^{-1/2} \Big).
\end{aligned}$$

Choose $b(\mathfrak{a})$ to be supported on the prime ideals $\mathfrak{p}$ with $\mathrm{N}\mathfrak{p} > y$. Then the above display is

$$\begin{aligned}
&\ll_{\epsilon,[K:\mathbb{Q}]} (1 + T^{[K:\mathbb{Q}]/4+1+\epsilon} d_K^{1/4} Q^{5/2} y^{-1/2} \Big) (d_K Q)^\epsilon \sum_{\mathrm{N}\mathfrak{p}>y} |b(\mathfrak{p})|^2 \mathrm{N}\mathfrak{p} \\
&\ll_{\epsilon,[K:\mathbb{Q}]} (d_K Q)^\epsilon \sum_{\mathrm{N}\mathfrak{p}>y} |b(\mathfrak{p})|^2 \mathrm{N}\mathfrak{p},
\end{aligned}$$

as desired. □

References

[1] A. Abbes, E. Ullmo, *À propos de la conjecture de Manin pour les courbes elliptiques modulaires.* Compositio Math. 103 (1996), no. 3, 269-286.

[2] A. Agashe, K. Ribet, W. Stein, *The Manin constant.* Pure Appl. Math. Q. 2 (2006), no. 2, Special Issue: In honor of John H. Coates. Part 2, 617-636.

[3] A. Agashe, K. Ribet, W. Stein, *The modular degree, congruence primes, and multiplicity one.* Number theory, analysis and geometry, 19-49, Springer, New York, (2012).

[4] J. Arthur, L. Clozel, *Simple algebras, base change, and the advanced theory of the trace formula.* Annals of Mathematics Studies, 120. Princeton University Press, Princeton, NJ, 1989. xiv+230 pp. ISBN: 0-691-08517-X; 0-691-08518-8

[5] A. Atkin, J. Lehner, *Hecke operators on* $\Gamma_0(N)$. Math. Ann. 185 (1970) 134-160.

[6] M. Bertolini, H. Darmon, *p-adic periods, p-adic L-functions, and the p-adic uniformization of Shimura curves.* Duke Math. J. 98 (1999), no. 2, 305-334.

[7] A. Baker, *Experiments on the abc-conjecture.* Publ. Math. Debrecen 65 (2004), no. 3-4, 253-260.

[8] V. Blomer, R. Holowinsky, *Bounding sup-norms of cusp forms of large level.* Inventiones mathematicae 179.3 (2010): 645-681.

[9] S. Bosch, W. Lütkebohmert, M. Raynaud, *Néron models.* Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], 21. Springer-Verlag, Berlin, 1990. x+325 pp. ISBN: 3-540-50587-3

[10] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over Q: wild 3-adic exercises.* Journal of the American Mathematical Society, 14 (4): 843-939

[11] F. Brumley, *Effective multiplicity one on* GL_N *and narrow zero-free regions for Rankin-Selberg L-functions.* Amer. J. Math. 128 (2006), no. 6, 1455-1474.

[12] K. Buzzard, *Integral models of certain Shimura curves.* Duke Mathematical Journal 87.3 (1997): 591.

[13] H. Carayol, *Sur les représentations l-adiques associées aux formes modulaires de Hilbert.* Annales scientifiques de l'École Normale Supérieure, Série 4 : Volume 19 (1986) no. 3 , p. 409-468

[14] K. Cesnavicius, *A modular description of $\mathscr{X}_0(n)$*. Algebra Number Theory 11 (2017), no. 9, 2001-2089.

[15] K. Cesnavicius, *The Manin-Stevens constant in the semistable case.* Preprint arXiv: 1604.02165 (2016).

[16] K. Cesnavicius, *The Manin constant in the semistable case.* Preprint arXiv: 1703.02951 (2017).

[17] L. Clozel, *Base change for $GL(n)$*. Proceedings of the International Congress of Mathematicians. Vol. 1. (1986).

[18] A. Cojocaru, E. Kani, *The modular degree and the congruence number of a weight 2 cusp form.* Acta Arith. 114 (2004), no. 2, 159-167.

[19] P. Colmez, *Périods des variétés abéliennes à multiplication complex.* Ann. Math., 138 (1993), 625-683.

[20] P. Colmez, *Sur la hauteur de Faltings des variétés abéliennes à multiplication complexe.* Compositio Math. 111 (1998), no. 3, 359-368.

[21] B. Conrad, *Integrality of modular forms via intersection theory.* Appendix to: *p-adic L-functions and the coniveau filtration on Chow groups*, by M. Bertolini, H. Darmon, K. Prasanna, to appear in Crelle.

[22] D. Cox, W. Parry, *Genera of congruence subgroups in $\mathbb{Q}$-quaternion algebras.* J. Reine Angew. Math. 351 (1984), 66-112.

[23] H. Darmon, A. Granville, *On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$*. Bull. London Math. Soc. 27 (1995), no. 6, 513-543.

[24] H. Darmon, L. Merel, *Winding quotients and some variants of Fermat's last theorem.* J. Reine Angew. Math. 490 (1997), 81-100.

[25] S. Das, J. Sengupta, *L^∞ norms of holomorphic modular forms in the case of compact quotient.* Forum Mathematicum. Vol. 27. No. 4. (2015).

[26] P. Deligne, M. Rapoport, *Les schémas de modules de courbes elliptiques.* Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), pp. 143-316. Lecture Notes in Math., Vol. 349, Springer, Berlin, 1973.

[27] F. Diamond J. Im, *Modular forms and modular curves.* Seminar on Fermat's Last Theorem (Toronto, ON, 1993-1994), 39-133, CMS Conf. Proc., 17, Amer. Math. Soc., Providence, RI, 1995.

[28] F. Diamond, K. Kramer, *Modularity of a family of elliptic curves.* Math. Res. Lett. 2 (1995), no. 3, 299-304.

[29] L. Dieulefait, N. Freitas, *Base change for elliptic curves over real quadratic fields.* Comptes Rendus Mathematique 353.1 (2015): 1-4.

[30] B. Edixhoven, *On the Manin constants of modular elliptic curves.* Arithmetic algebraic geometry (Texel, 1989), 25-39, Progr. Math., 89, Birkhäuser Boston, Boston, MA, (1991).

[31] B. Edixhoven, *Comparison of integral structures on spaces of modular forms of weight two, and computation of spaces of forms mod 2 of weight one.* (English, French summary) With appendix A (in French) by Jean-François Mestre and appendix B by Gabor Wiese. J. Inst. Math. Jussieu 5 (2006), no. 1, 1-34.

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

[33] É. Fouvry, M. Nair, G. Tenenbaum, *L'ensemble exceptionnel dans la conjecture de Szpiro.* (French. English, French summary) Bull. Soc. Math. France 120 (1992), no. 4, 485-506.

[34] N. Freitas, B. V. Le Hung, S. Siksek, *Elliptic curves over real quadratic fields are modular.* Inventiones mathematicae 201.1 (2015): 159-206.

[35] G. Freixas i Montplet, *The Jacquet-Langlands correspondence and the arithmetic Riemann-Roch theorem for pointed curves.* Int. J. Number Theory 8 (2012), no. 1, 1-29.

[36] G. Frey, *Links between solutions of A-B=C and elliptic curves.* Number theory (Ulm, 1987), 31-62, Lecture Notes in Math., 1380, Springer, New York, (1989).

[37] P. Gallagher, *A large sieve density estimate near $\sigma = 1$.* Invent. Math. 11 1970 329-339.

[38] É. Gaudron, G. Rémond, *Polarisations et isogénies.* Duke Mathematical Journal 163.11 (2014): 2057-2108.

[39] S. Gelbart, *Elliptic curves and automorphic representations.* Advances in Mathematics 21, no. 3 (1976): 235-292.

[40] A. Ghitza, *Distinguishing Hecke eigenforms.* Int. J. Number Theory 7 (2011), no. 5, 1247-1253.

[41] D. Goldfeld, J. Hoffstein, *On the number of Fourier coefficients that determine a modular form.* A tribute to Emil Grosswald: number theory and related analysis, 385-393, Contemp. Math., 143, Amer. Math. Soc., Providence, RI, (1993).

[42] B. Gross, *Arithmetic on elliptic curves with complex multiplication.* LNM 776, Springer-Verlag, New York, (1980).

[43] B. Gross, *Local orders, root numbers, and modular curves.* Amer. J. Math. 110 (1988), no. 6, 1153-1182.

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

[45] K. Györy, *On the abc conjecture in algebraic number fields.* Acta Arith. 133 (2008), no. 3, 281-295.

[46] E. Halberstadt, A. Kraus, *Courbes de Fermat: résultats et problèmes.* J. Reine Angew. Math. 548 (2002) 167-234.

[47] D. R. Heath-Brown, *A mean value estimate for real character sums.* Acta Arith. 72 (1995), no. 3, 235-275.

[48] D. Helm, *On maps between modular Jacobians and Jacobians of Shimura curves.* Israel J. Math. 160 (2007), 61-117.

[49] M. Hindry, *Why is it difficult to compute the Mordell-Weil group?* Diophantine geometry, 197-219, CRM Series, 4, Ed. Norm., Pisa, 2007.

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

[51] Y. Ihara, *On the Euler-Kronecker constants of global fields and primes with small norms.* Algebraic geometry and number theory, 407-451, Progr. Math., 253, Birkhäuser Boston (2006).

[52] Y. Ihara, K. Murty, M. Shimura, *On the logarithmic derivatives of Dirichlet L-functions at $s = 1$.* Acta Arith. 137 (2009), no. 3, 253-276.

[53] H. Iwaniec, E. Kowalski, *Analytic number theory.* American Mathematical Society Colloquium Publications, 53. American Mathematical Society, Providence, RI, 2004. xii+615 pp. ISBN: 0-8218-3633-1

[54] H. Jacquet, *On the base change problem: after J. Arthur and L. Clozel.* Number theory, trace formulas and discrete groups (Oslo, 1987), 111-124, Academic Press, Boston, MA, 1989.

[55] R. de Jong, *On the Arakelov theory of elliptic curves.* Enseign. Math. (2) 51 (2005), no. 3-4, 179-201.

[56] N. Katz, B. Mazur, *Arithmetic Moduli of Elliptic Curves.* Annals of Mathematics Studies, 108. Princeton University Press, Princeton, NJ, 1985. xiv+514 pp. ISBN: 0-691-08349-5; 0-691-08352-5

[57] R. von Kanel *Integral points on moduli schemes of elliptic curves.* Trans. London Math. Soc. 1 (2014), no. 1, 85-115.

[58] R. von Kanel, B. Matschke, *Solving S-unit, Mordell, Thue, Thue-Mahler and generalized Ramanujan-Nagell equations via Shimura-Taniyama conjecture.* Preprint arXiv:1605.06079 (2016)

[59] M. Kenku, *On the number of $\mathbb{Q}$-isomorphism classes of elliptic curves in each $\mathbb{Q}$-isogeny class.* J. Number Theory 15 (1982), no. 2, 199-202.

[60] S. Kudla, M. Rapoport, T. Yang, *Derivatives of Eisenstein series and Faltings heights.* Compos. Math. 140 (2004), no. 4, 887-951.

[61] S. Kudla, M. Rapoport, T. Yang, *Modular forms and special cycles on Shimura curves.* Annals of Mathematics Studies, 161. Princeton University Press, Princeton, NJ, 2006. x+373 pp. ISBN: 978-0-691-12551-0; 0-691-12551-1

[62] Y. Lamzouri, *The distribution of Euler-Kronecker constants of quadratic fields.* J. Math. Anal. Appl. 432 (2015), no. 2, 632-653.

[63] R. Lemke Oliver, J. Thorner. *Effective log-free zero density estimates for automorphic L-functions and the Sato-Tate conjecture.* International Mathematics Research Notices, (2018) rnx309, `https://doi.org/10.1093/imrn/rnx309`

[64] W. Li, *L-series of Rankin type and their functional equations.* Math. Ann. 244 (1979), no. 2, 135-166.

[65] Q. Liu, *Algebraic geometry and arithmetic curves.* Oxford Graduate Texts in Mathematics, 6. Oxford Science Publications. Oxford University Press, Oxford, 2002. xvi+576 pp. ISBN: 0-19-850284-2

[66] J. Liu, Y. Wang, *A theorem on analytic strong multiplicity one.* J. Number Theory 129 (2009), no. 8, 1874-1882.

[67] C. Maclachlan, A Reid, *The arithmetic of hyperbolic 3-manifolds.* Graduate Texts in Mathematics, 219. Springer-Verlag, New York, 2003. xiv+463 pp. ISBN: 0-387-98386-4

[68] L. Mai, R. Murty, *The Phragmén-Lindelöf theorem and modular elliptic curves.* The Rademacher legacy to mathematics (University Park, PA, 1992), 335-340, Contemp. Math., 166, Amer. Math. Soc., Providence, RI, (1994).

[69] G. Martin, *Dimensions of the spaces of cusp forms and newforms on $\Gamma_0(N)$ and $\Gamma_1(N)$.* J. Number Theory 112 (2005), no. 2, 298-331.

[70] B. Mazur, *Rational isogenies of prime degree* (with an appendix by D. Goldfeld). Invent. Math. 44 (1978), no. 2, 129-162.

[71] J.-F. Mestre, J. Oesterle, *Courbes de Weil semi-stables de discriminant une puissance m-ième.* J. Reine Angew. Math. 400 (1989), 173-184.

[72] P. Mihailescu, *Primary cyclotomic units and a proof of Catalan's conjecture.* J. Reine Angew. Math. 572 (2004), 167-195.

[73] R. Murty, *Bounds for congruence primes.* Automorphic forms, automorphic representations, and arithmetic (Fort Worth, TX, 1996), 177-192, Proc. Sympos. Pure Math., 66, Part 1, Amer. Math. Soc., Providence, RI, (1999).

[74] R. Murty, H. Pasten, *Modular forms and effective Diophantine approximation.* J. Number Theory 133 (2013), no. 11, 3739-3754.

[75] J.-L. Nicolas, G. Robin, *Majorations explicites pour le nombre de diviseurs de N.* Canad. Math. Bull. 26 (1983), no. 4, 485-492.

[76] J. Oesterlé, *Nouvelles approches du "théorème" de Fermat.* Séminaire Bourbaki, Vol. 1987/88. Astérisque No. 161-162 (1988), Exp. No. 694, 4, 165-186 (1989)

[77] M. Papikian, J. Rabinoff, *Optimal quotients of Jacobians with toric reduction and component groups.* Canad. J. Math. 68 (2016), no. 6, 1362-1381.

[78] A. Parshin, *The Bogomolov-Miyaoka-Yau inequality for the arithmetical surfaces and its applications.* Séminaire de Théorie des Nombres, Paris 1986-87, 299-312, Progr. Math., 75, Birkhäuser Boston, Boston, MA, 1988.

[79] K. Prasanna, *Integrality of a ratio of Petersson norms and level-lowering congruences.* Annals of Mathematics, Second Series, Vol. 163, No. 3 (May, 2006), pp. 901-967.

[80] H. Rademacher, *On the Phragmén-Lindelöf theorem and some applications.* Math. Z 72 1959/1960 192-204.

[81] K. Ribet *Congruence relations between modular forms.* Proceedings of the International Congress of Mathematicians, Vol. 1, 2 (Warsaw, 1983), 503-514, PWN, Warsaw, 1984.

[82] K. Ribet, *On modular representations of* $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms.* Invent. Math. 100 (1990), no. 2, 431-476.

[83] K. Ribet, *On the component groups and the Shimura subgroup of* $J_0(N)$. Séminaire de Théorie des Nombres, 1987-1988 (Talence, 1987-1988), Exp. No. 6.

[84] K. Ribet, *On the equation* $a^p + 2^\alpha b^p + c^p = 0$. Acta Arith. 79 (1997), no. 1, 7-16.

[85] K. Ribet, S. Takahashi, *Parametrizations of elliptic curves by Shimura curves and by classical modular curves.* Elliptic curves and modular forms (Washington, DC, 1996). Proc. Nat. Acad. Sci. U.S.A. 94 (1997), no. 21, 11110-11114.

[86] H. Shimizu, *On zeta functions of quaternion algebras.* Ann. of Math. (2) 81 1965 166-193.

[87] G. Shimura, *Construction of class fields and zeta functions of algebraic curves.* Annals of Mathematics, Second Series, Vol. 85, No. 1 (1967), pp. 58-159.

[88] J. Silverman, *Heights and elliptic curves.* Arithmetic geometry (Storrs, Conn., 1984), 253-265, Springer, New York, (1986).

[89] J. Silverman, *The arithmetic of elliptic curves. Second edition.* Graduate Texts in Mathematics, 106. Springer, Dordrecht, 2009. xx+513 pp. ISBN: 978-0-387-09493-9

[90] B. de Smit, *ABC Triples.* `http://www.math.leidenuniv.nl/~desmit/abc/index.php?set=2`

[91] L. Szpiro, *Présentation de la théorie d'Arakélov.* Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985), 279-293, Contemp. Math., 67, Amer. Math. Soc., Providence, RI, 1987.

[92] L. Szpiro, *Discriminant et conducteur des courbes elliptiques.* Séminaire sur les Pinceaux de Courbes Elliptiques (Paris, 1988). Astérisque No. 183 (1990), 7-18.

[93] C. L. Stewart, R. Tijdeman, *On the Oesterlé-Masser conjecture*, Monatsh. Math. 102 (1986), 251-257

[94] C. L. Stewart, K. R. Yu, *On the abc conjecture.* Math. Ann. 291 (1991), no. 2, 225-230.

[95] C. L. Stewart, K. R. Yu, *On the abc conjecture. II.* Duke Math. J. 108 (2001), no. 1, 169-181.

[96] A. Surroca, *Sur l'effectivité du théorème de Siegel et la conjecture abc.* J. Number Theory 124 (2007), no. 2, 267-290.

[97] S. Takahashi, *Degrees of parametrizations of elliptic curves by Shimura curves.* J. Number Theory 90 (2001), no. 1, 74-88.

[98] T. Tatuzawa, *On Siegel's theorem*, Japan. J. Math. 21 (1951), 163-178.

[99] R. Taylor, A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Annals of Mathematics. Second Series, (1995) 141 (3): 553-572.

[100] R. Tijdeman, *On the equation of Catalan.* Acta Arith. 29 (2): 197-209.

[101] E. Ullmo, *Hauteur de Faltings de quotients de* $J_0(N)$*, discriminants d'algèbres de Hecke et congruences entre formes modulaires.* Amer. J. Math. 122 (2000), no. 1, 83-115.

[102] E. Ullmo, *Sur la constante de Hida des courbes modulaires et des courbes de Shimura.* 21st Journées Arithmétiques (Rome, 2001). J. Théor. Nombres Bordeaux 13 (2001), no. 1, 325-337.

[103] P. Vojta, *Diophantine approximations and value distribution theory.* Lecture Notes in Mathematics, 1239. Springer-Verlag, Berlin (1987). x+132 pp. ISBN: 3-540-17551-2

[104] P. Vojta, *Diophantine approximation and Nevanlinna theory.* Arithmetic geometry, 111-224, Lecture Notes in Math., 2009, Springer, Berlin, 2011.

[105] P. Voutier, *An effective lower bound for the height of algebraic numbers.* Acta Arith. 74 (1996), no. 1, 81-95.

[106] Y. Wang, *The analytic strong multiplicity one theorem for* $GL_m(\mathbb{A}_K)$. J. Number Theory 128 (2008), no. 5, 1116-1126.

[107] B. de Weger, $A + B = C$ *and big* Ш*'s.* Quart. J. Math. Oxford Ser. (2) 49 (1998), no. 193, 105-128.

[108] A. Weiss, *The least prime ideal.* J. Reine Angew. Math. 338 (1983), 56-94.

[109] A. Wiles, *Modular elliptic curves and Fermat's last theorem.* Annals of Mathematics. Second Series, (1995) 141 (3): 443-551.

[110] K. R. Yu, *Linear forms in p-adic logarithms. III.* Compositio Math. 91 (1994), no. 3, 241-276.

[111] K. R. Yu, *p-adic logarithmic forms and group varieties. III.* Forum Math. 19 (2007), no. 2, 187-280.

[112] D. Zagier, *Modular parametrizations of elliptic curves.* Canad. Math. Bull. 28 (1985), no. 3, 372-384.

[113] X. Yuan, S.-W. Zhang, W. Zhang, *The Gross-Zagier formula on Shimura curves.* Annals of Mathematics Studies, No. 184, Princeton University Press, 2013.

[114] X. Yuan, S.-W. Zhang, *On the averaged Colmez Conjecture*. On the averaged Colmez conjecture. Ann. of Math. (2) 187 (2018), no. 2, 533-638.
[115] S.-W. Zhang, *Heights of Heegner points on Shimura curves*. Ann. of Math. (2) 153 (2001), no. 1, 27-147.
[116] S.-W. Zhang, *Gross-Schoen cycles and dualising sheaves*. Invent. Math. 179 (2010), no. 1, 1-73.

Department of Mathematics
Harvard University
Science Center
1 Oxford Street
Cambridge, MA 02138, USA
E-mail address, H. Pasten: hpasten@gmail.com