Forum of Mathematics, Sigma (2025), **Vol. 13**:e20 1–82
doi:10.1017/fms.2024.133

CAMBRIDGE
UNIVERSITY PRESS

RESEARCH ARTICLE

Complete verification of strong BSD for many modular abelian surfaces over Q

Timo Keller[1] and Michael Stoll[2]

[1]Rijksuniversiteit Groningen, Bernoulli Institute, Bernoulliborg, Nijenborgh 9, 9747 AG Groningen, The Netherlands; E-mail: t.keller@rug.nl (corresponding author).
[2]Department of Mathematics, Chair of Computer Algebra, Universität Bayreuth, Universitätsstrasse 30, Bayreuth, 95447, Germany; E-mail: Michael.Stoll@uni-bayreuth.de.

Received: 7 January 2024; **Revised:** 8 September 2024; **Accepted:** 10 October 2024

2020 Mathematics Subject Classification: *Primary* – 11G40; *Secondary* – 11G10, 14G05

Abstract

We develop the theory and algorithms necessary to be able to verify the strong Birch–Swinnerton-Dyer Conjecture for absolutely simple modular abelian varieties over **Q**. We apply our methods to all 28 Atkin–Lehner quotients of $X_0(N)$ of genus 2, all 97 genus 2 curves from the LMFDB whose Jacobian is of this type and six further curves originally found by Wang. We are able to verify the strong BSD Conjecture unconditionally and exactly in all these cases; this is the first time that strong BSD has been confirmed for absolutely simple abelian varieties of dimension at least 2. We also give an example where we verify that the order of the Tate–Shafarevich group is 7^2 and agrees with the order predicted by the BSD Conjecture.

Contents

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

1. Introduction

1.1. Background

The *Conjecture of Birch and Swinnerton-Dyer* (‘BSD’ for short), originally formulated based on extensive computations by Birch and Swinnerton-Dyer [8] in the 1960s for elliptic curves over $\mathbf{Q}$, is one of the most important open conjectures in number theory. For example, it is one of the seven ‘Millennium

Problems', for whose solution the Clay Foundation is offering a million dollars each. It relates in a surprising way analytic invariants of an elliptic curve E, which are obtained via its L-series from its local properties (essentially the number of points modulo p on E, for all prime numbers p), to global arithmetic invariants like the rank of the Mordell–Weil group $E(\mathbf{Q})$, its regulator, and the rather mysterious Tate–Shafarevich group $Ш(E/\mathbf{Q})$. The conjecture has been generalized to cover all abelian varieties over all algebraic number fields. It consists of two parts, which we will explain for the case of an abelian variety A of dimension g over $\mathbf{Q}$.

One attaches to A its L-function $L(A/\mathbf{Q}, s)$, which is defined by an Euler product over all prime numbers p. If A is the Jacobian variety of a curve X of genus g, the Euler factor at p for a prime p of good reduction is determined by the number of $\mathbf{F}_{p^n}$-points on the mod p reduction of X for $n \leq g$. It follows from the Weil conjectures for varieties over finite fields that the Euler product converges for $\mathrm{Re}(s) > \frac{3}{2}$ to a holomorphic function. A standard conjecture predicts that $L(A/\mathbf{Q}, s)$ extends to an entire function; this is known when A is *modular* (i.e., occurs as an isogeny factor of the Jacobian $J_0(N)$ of one of the modular curves $X_0(N)$). By the Modularity Theorem of Wiles and others [15, 114, 116], this is always the case when A is an elliptic curve over $\mathbf{Q}$ (this is now a special case of Serre's Modularity Conjecture [61]).

We now introduce the relevant global invariants of A. By the Mordell–Weil Theorem, the abelian group $A(\mathbf{Q})$ of rational points on A is finitely generated, so it splits as $A(\mathbf{Q}) \cong A(\mathbf{Q})_{\mathrm{tors}} \oplus \mathbf{Z}^r$, where $A(\mathbf{Q})_{\mathrm{tors}}$ is the finite *torsion subgroup* and r is a nonnegative integer, the *rank of* $A(\mathbf{Q})$. There is a natural positive definite quadratic form $\hat{h}$ on $A(\mathbf{Q}) \otimes_{\mathbf{Z}} \mathbf{R} \cong \mathbf{R}^r$, the *canonical height*, turning $A(\mathbf{Q})/A(\mathbf{Q})_{\mathrm{tors}}$ into a lattice in a euclidean vector space. The squared covolume of this lattice (equivalently, the determinant of the Gram matrix of $\hat{h}$ with respect to a lattice basis) is the *regulator* $\mathrm{Reg}_{A/\mathbf{Q}}$. The final global arithmetic invariant of A that we need is the *Tate–Shafarevich group* $Ш(A/\mathbf{Q})$. It can be defined as the localization kernel

$$Ш(A/\mathbf{Q}) = \ker\Big(\mathrm{H}^1(\mathbf{Q}, A) \to \bigoplus_v \mathrm{H}^1(\mathbf{Q}_v, A)\Big)$$

in Galois cohomology; here, $\mathbf{Q}_v$ denotes the completion of $\mathbf{Q}$ with respect to a place v, and the direct sum is over all places of $\mathbf{Q}$. Geometrically, $Ш(A/\mathbf{Q})$ is the group of equivalence classes of everywhere locally trivial $A/\mathbf{Q}$-torsors. This group is conjectured to be finite, but this is not known in general; for example, it is not known for a single elliptic curve with (algebraic or analytic) rank at least 2.

We also need some local invariants. To each prime p, one associates the *Tamagawa number* $c_p(A)$; this is the number of connected components of the special fiber at p of the Néron model $\mathscr{A}/\mathbf{Z}$ of A that are fixed by Frobenius and equals 1 for all primes of good reduction. Let $(\omega_1, \dots, \omega_g)$ be the pullback to $\mathrm{H}^0(A, \Omega^1)$ of a basis of the free $\mathbf{Z}$-module $\mathrm{H}^0(\mathscr{A}, \Omega^1)$ of rank g. Then the *real period* of A is the volume of $A(\mathbf{R})$ measured using $|\omega_1 \wedge \cdots \wedge \omega_g|$: $\Omega_A = \int_{A(\mathbf{R})} |\omega_1 \wedge \cdots \wedge \omega_g|$.

The *weak BSD* or *BSD rank conjecture* says that $L(A/\mathbf{Q}, s)$ has an analytic continuation to a neighborhood of $s = 1$ and

$$r_{\mathrm{an}} := \mathrm{ord}_{s=1} L(A/\mathbf{Q}, s) = r.$$

The order of vanishing of $L(A/\mathbf{Q}, s)$ at $s = 1$ is also called the *analytic rank* of $A/\mathbf{Q}$.

We will from now on assume that A is principally polarized – for example, the Jacobian variety of a curve. In particular, $A \cong A^\vee$, where $A^\vee$ is the dual abelian variety. Then the *strong BSD conjecture* says that in addition $Ш(A/\mathbf{Q})$ is finite and

$$L^*(A/\mathbf{Q}, 1) := \lim_{s \to 1} (s-1)^{-r} L(A/\mathbf{Q}, s) = \frac{\Omega_A \prod_p c_p(A) \cdot \mathrm{Reg}_{A/\mathbf{Q}} \, \#Ш(A/\mathbf{Q})}{(\#A(\mathbf{Q})_{\mathrm{tors}})^2}.$$

Since all the other invariants of A can (usually) be computed at least numerically, we define the *analytic order of Sha* to be

$$\#Ш(A/\mathbf{Q})_{\mathrm{an}} := \frac{L^*(A/\mathbf{Q},1)}{\Omega_A \operatorname{Reg}_{A/\mathbf{Q}}} \cdot \frac{(\#A(\mathbf{Q})_{\mathrm{tors}})^2}{\prod_p c_p(A)} .$$

Assuming the BSD rank conjecture, strong BSD can then be phrased as '$Ш(A/\mathbf{Q})$ is finite and $\#Ш(A/\mathbf{Q}) = \#Ш(A/\mathbf{Q})_{\mathrm{an}}$',

Even the weak BSD conjecture for elliptic curves over $\mathbf{Q}$ is wide open in general (this is the Clay Millennium Problem mentioned above). However, the strong BSD conjecture has been verified for many 'small' elliptic curves; see below. In this article, we verify the strong BSD conjecture for the first time in dimension greater than 1 – namely, for a number of abelian *surfaces* $A/\mathbf{Q}$, in a situation where it cannot be reduced to BSD for some elliptic curves. Concretely, this means that A is absolutely simple.

Recall that an abelian variety A of positive dimension over $\mathbf{Q}$ is *absolutely simple* if $A_{\overline{\mathbf{Q}}}$ is not isogenous to a product of at least two abelian varieties of positive dimension. An abelian variety of dimension g whose endomorphism ring $\operatorname{End}_{\mathbf{Q}}(A)$ is isomorphic to an order $\mathcal{O}$ in a totally real number field F of degree $[F : \mathbf{Q}] = g$ is said to have *real multiplication* (RM).

Absolutely simple abelian varieties with real multiplication over $\mathbf{Q}$ are *modular* (see theorem 2.1 for references). This means that A can be obtained as an isogeny factor of some $J_0(N)$, where $J_0(N)$ denotes the Jacobian variety of the modular curve $X_0(N)$. These isogeny factors correspond to (Galois orbits of) newforms in $S_2(\Gamma_0(N))$; see theorem 2.1 below. (Note that we reserve the term 'modular' for GL_2-type abelian varieties here as opposed to the more general property of being 'automorphic'; see [14, §9.1].)

1.2. General results

While the BSD conjecture is wide open in general, there are some cases where parts of it are known to be true. Assume that $A/\mathbf{Q}$ is an absolutely simple abelian variety of dimension g with real multiplication by an order $\mathcal{O}$ in a totally real number field of degree g. Then A is of GL_2-type; in particular, for each prime ideal $\mathfrak{p}$ of $\mathcal{O}$, the common kernel $A[\mathfrak{p}]$ of all elements of $\mathfrak{p}$ acting on A is a 2-dimensional vector space over $\mathcal{O}/\mathfrak{p}$, and hence induces a Galois representation into $\mathrm{GL}_2(\mathcal{O}/\mathfrak{p})$. In this situation, there is a newform f of weight 2 and some level N with q-expansion coefficients that generate an order commensurable with $\mathcal{O}$ and such that A is an isogeny factor of $J_0(N)$; furthermore,

$$L(A/\mathbf{Q},s) = \prod_{\sigma\colon \mathcal{O}\hookrightarrow\mathbf{R}} L(f^\sigma,s),$$

where σ acts on the q-expansion coefficients. Since it is known that $L(f^\sigma,s)$ is an entire function, the same is true for $L(A/\mathbf{Q},s)$. So for $A/\mathbf{Q}$ with RM, we can at least speak of the analytic rank r_{an} and the leading coefficient $L^*(A/\mathbf{Q},1)$ of the L-function at $s=1$. The parity of the order of vanishing of $L(f^\sigma,s)$ at $s=1$ does not depend on σ (it is determined by the eigenvalue ε_N of f^σ under the Fricke involution, which is the same for all f^σ), and the order of vanishing itself does not depend on σ when $\operatorname{ord}_{s=1}L(f^\sigma,s) \le 1$ for some σ, so in this case, we have that $r_{\mathrm{an}} = g\cdot\operatorname{ord}_{s=1}L(f,s)$, where $\operatorname{ord}_{s=1}L(f,s) := \operatorname{ord}_{s=1}L(f^\sigma,s)$ for any σ; see [52, Cor. V.1.3]. We call $\operatorname{ord}_{s=1}L(f,s)$ the *L-rank of A* in this case and abbreviate it as L-rk A. If the BSD rank conjecture holds for A, then the L-rank of A is the same as the rank of $A(\mathbf{Q})$ as an $\mathcal{O}$-module.

Based on work of Gross–Zagier [52] relating the canonical height of Heegner points to $L^{(g)}(A/K,1)$ for suitable imaginary quadratic fields K, Kolyvagin [63] (for modular elliptic curves) and Kolyvagin–Logachëv [64] (for modular abelian varieties in general) were able to show that the BSD rank conjecture holds under the assumption that the L-rank is 0 or 1, that in this case, $Ш(A/\mathbf{Q})$ is finite (this is the only case where we know finiteness), and that $\#Ш(A/\mathbf{Q})_{\mathrm{an}}$ is a rational number.

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

The rational number $\#\text{Ш}(A/\mathbf{Q})_{\text{an}}$ can be computed when A is an elliptic curve, and we show in this paper how to do that when A is a modular abelian surface. To complete the verification of the strong BSD Conjecture for A, it remains to determine $\#\text{Ш}(A/\mathbf{Q})$ and to check that the two numbers agree.

This involves showing that $\text{Ш}(A/\mathbf{Q})[p]$ is trivial for all primes $p \notin S$, where S is an explicit finite set of primes, and then determining $\#\text{Ш}(A/\mathbf{Q})[p^\infty]$ for the finitely many $p \in S$. When A is an elliptic curve, a suitable set S (or even an explicit annihilator of $\text{Ш}(A/\mathbf{Q})$) can be extracted from Kolyvagin's work and subsequent refinements; see below. We show in this paper how to obtain a suitable set S when A is a modular abelian surface.

The remaining task is to determine $\text{Ш}(A/\mathbf{Q})[p^\infty]$ for a given prime p. This is always possible in theory (assuming that $\text{Ш}(A/\mathbf{Q})[p^\infty]$ is finite), since one can compute the p^n-Selmer group of A for $n = 1, 2, \ldots$, which is defined as

$$\mathrm{Sel}_{p^n}(A/\mathbf{Q}) = \ker\Big(\mathrm{H}^1(\mathbf{Q}, A[p^n]) \to \bigoplus_v \mathrm{H}^1(\mathbf{Q}_v, A)\Big)$$

and sits in an exact sequence

$$0 \longrightarrow A(\mathbf{Q})/p^n A(\mathbf{Q}) \longrightarrow \mathrm{Sel}_{p^n}(A/\mathbf{Q}) \longrightarrow \text{Ш}(A/\mathbf{Q})[p^n] \longrightarrow 0\,.$$

Since we know $A(\mathbf{Q})$, this gives us $\text{Ш}(A/\mathbf{Q})[p^n]$, and as soon as $\text{Ш}(A/\mathbf{Q})[p^n] = \text{Ш}(A/\mathbf{Q})[p^{n+1}]$, we have determined $\text{Ш}(A/\mathbf{Q})[p^\infty] = \text{Ш}(A/\mathbf{Q})[p^n]$ (and if $\text{Ш}(A/\mathbf{Q})[p] = 0$, then $\text{Ш}(A/\mathbf{Q})[p^\infty] = 0$ as well). For the computability of the Selmer group in theory, see [110] for elliptic curves and [16] in general. In practice, there are fairly tight limits on p^n, since the computation requires the knowledge of the class and unit groups of number fields of degree growing quickly with p^n, for which no really efficient algorithms are available so far.

If one has a conjecturally tight bound on $\#\text{Ш}(A/\mathbf{Q})[p^\infty]$, then another approach is to try and get a lower bound that agrees with the upper bound. If the upper bound is nontrivial, this involves showing the existence of nontrivial elements of $\text{Ш}(A/\mathbf{Q})$ in some way. One possibility for this is 'visibility', which uses another related abelian variety B, for which one can construct a nontrivial map $B(\mathbf{Q}) \to \mathrm{H}^1(\mathbf{Q}, A)$, whose image one can show to contain nontrivial elements of $\text{Ш}(A/\mathbf{Q})$ under suitable conditions. This is used for the example in Appendix A.

We now give a short overview of what has been done so far regarding the verification of the strong BSD Conjecture in concrete cases.

1.3. *Exact verification of strong BSD for elliptic curves*

In the case of elliptic curves, the various ingredients mentioned above have been worked out, made explicit and been improved to an extent that it was possible to verify the strong BSD conjecture for all elliptic curves E over $\mathbf{Q}$ of rank ≤ 1 and conductor $N < 5000$; see [34, 50, 67, 74, 75].

An explicit finite set S of primes such that $\text{Ш}(E/\mathbf{Q})[p] = 0$ for $p \notin S$ can be obtained using Kolyvagin's work and refinements building on it [23, 56]. The size of $\text{Ш}(E/\mathbf{Q})[p^\infty]$ for $p \in S$ can be obtained by several methods – for example, using Iwasawa theory and p-adic L-functions [109] or by performing descents [16, 27, 28, 29, 31, 33, 34, 75, 93, 110].

1.4. *Numerical verification of strong BSD for higher-dimensional abelian varieties*

Compared to the case of elliptic curves, considerably less has been done regarding the verification of the BSD conjectures for higher-dimensional abelian varieties A over $\mathbf{Q}$. If A is not absolutely simple, then A splits up to isogeny (and possibly after base-change to an algebraic number field) as a product of abelian varieties of lower dimension. Since the validity of strong BSD is invariant under isogenies [113] and Weil restriction [77], this reduces the verification of strong BSD for A to cases of lower dimension. We will therefore assume that A is absolutely simple in the following.

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

In [45], all factors in the BSD formula except for the order of the Tate–Shafarevich group (only its 2-torsion is computed) and the analytic order of Sha are determined exactly in the L-rank 0 cases and numerically to high precision in the L-rank 1 cases for the Jacobian varieties of 29 genus 2 curves over $\mathbf{Q}$ such that the Jacobians are absolutely simple, of GL_2-type and have level $N \leq 200$. This work also includes results on three curves whose Jacobians are Weil restrictions of elliptic curves over $\mathbf{Q}(\sqrt{-3})$.

More recently, van Bommel [11] has done computations similar to those in [45] for various (in general non-modular) Jacobians of hyperelliptic curves of genus ≤ 5. He did not provably compute the regulator or the torsion subgroup, which means that the approximate value of $\#Ш(A)_{\mathrm{an}}$ that he computes may be off by a square rational factor. Van Bommel also provides an algorithm for the computation of the real period, which corrects the version described in [45] in the case when some of the special fibers of a minimal regular model of the curve have multiple components.

However, it was still an open problem to provably compute $\#Ш(A/\mathbf{Q})_{\mathrm{an}}$ as an exact rational number when A has positive rank and to determine $\#Ш(A/\mathbf{Q})$. See, for example, William Stein's blog post [108] for the former.

We now verify the strong BSD Conjecture *unconditionally* and exactly for all the curves in [45] with absolutely simple Jacobian and all genus 2 curves in the LMFDB [68] with absolutely simple modular Jacobian.

1.5. New general results in this paper

We note that, compared to elliptic curves, a number of additional difficulties show up when trying to verify strong BSD for higher-dimensional modular abelian varieties. By the Modularity Theorem, every elliptic curve E over $\mathbf{Q}$ of conductor N is the target of a nontrivial morphism $X_0(N) \to E$. This makes it fairly easy to compute Heegner points on E. Also, elliptic curves are given explicitly by a Weierstrass equation, and a variety of algorithms are available for them. There is no comparable explicit representation of a general (modular) abelian variety of higher dimension. We can, however, work with curves X and their Jacobians. In particular, for hyperelliptic curves, a variety of algorithms exist. However, in general, there is only a dominant homomorphism from $J_0(N)$ to the Jacobian in question and no nontrivial morphism from $X_0(N)$ to the curve X. When there is such a morphism, the relevant computations are much simpler; we have dealt with this case for surfaces first, and the results are described in [59]. In the other cases, the required arguments are much more subtle; for example, it is quite nontrivial to obtain a formula for the canonical height of a Heegner point on the Jacobian J of X from the Gross–Zagier formula.

In this paper, we overcome these difficulties and devise general methods to verify strong BSD exactly for absolutely simple modular Jacobians $J/\mathbf{Q}$ of L-rank 0 and 1 and apply them to several examples. Many of our results and algorithms apply to any dimension or at least to hyperelliptic Jacobians. We note that an abelian variety (assumed to be absolutely simple) is automatically a Jacobian when it is principally polarized and its dimension is 2 or 3.

More specifically, given such a Jacobian J and/or an attached newform f, we do the following. (The numbers link to the corresponding sections.)

(2) We determine the (projective) images of the associated mod-$\mathfrak{p}$ Galois representations for all maximal ideals $\mathfrak{p}$ of the endomorphism ring; in particular, we determine which of them are reducible.

(3) We develop an efficient algorithm for the computation of Heegner points, their canonical heights and Heegner indices. This involves the computation of Petersson norms of newforms of weight 2. We also provide the refined information of the Heegner index as a characteristic ideal of the endomorphism ring.

(4) We derive explicit formulas for $\#Ш(J/\mathbf{Q})_{\mathrm{an}}$ and $\#Ш(J/K)_{\mathrm{an}}$ (where K is a Heegner field). When the L-rank is 1, this involves some fairly nontrivial arguments.

(5) We give an explicit upper bound for the set of primes dividing $\#Ш(J/\mathbf{Q})$ and for the primes dividing $\#Ш(J/K)$, where K is a Heegner field.

(6) We perform $\mathfrak{p}$-isogeny descents in some cases where the mod-$\mathfrak{p}$ Galois representation is reducible to get an upper bound on the $\mathfrak{p}$-Selmer group and thus show that $Ш(J/\mathbf{Q})[\mathfrak{p}] = 0$.
(7) We provide a feasible algorithm for the computation of p-adic L-functions in our setting.
(8) We provide an algorithm that, combining the above algorithms, verifies strong BSD for the Jacobian J (absolutely simple and modular) of a given genus 2 curve X of level N or returns at least a small finite set of primes $\mathfrak{p}$ for which $Ш(J/\mathbf{Q})[\mathfrak{p}^\infty]$ needs to be computed to finish the verification.

We also improve van Bommel's algorithm for the determination of the real period so that it does not rely on a gcd computation with real numbers; see lemma 3.7.

Our methods and algorithms generalize to RM abelian varieties over $\mathbf{Q}$ of arbitrary dimension, provided one can compute Mordell–Weil groups and canonical heights and one has an analogue of algorithm 2.44. In joint work in progress with Pip Goodman and John Voight, we are planning to treat modular abelian varieties over totally real number fields.

We then use the algorithms we developed to verify strong BSD exactly for the first time for a number of absolutely simple abelian surfaces. The specific examples are described below.

1.6. Examples

All computations were carried out with Magma [13]. The code to reproduce our computations can be found at

https://github.com/TimoKellerMath/strongBSDgenus2.

The `README.md` file contains short descriptions of the Magma files and which sections in this paper they belong to.

Using the methods and algorithms developed in this paper, we verified strong BSD completely for the Jacobians of the following genus 2 curves over $\mathbf{Q}$ (whose Jacobians are modular and absolutely simple).

(a) The LMFDB [68] currently (as of September 2024) lists exactly 97 genus 2 curves with absolutely simple Jacobian of GL_2-type; they all have level ≤ 1000. By their completeness statement, this comprises all such examples with absolute value of their discriminant at most 10^6 and 'small' coefficients. We will refer to these as the *LMFDB examples*. Note that there are more newforms of weight 2 with real quadratic coefficients of level ≤ 1000 contained in the LMFDB; our algorithms would at least give an upper bound on the size of the Tate–Shafarevich group of their associated modular abelian variety given a Jacobian in their isogeny class. Some of the examples mentioned below provide such a Jacobian for additional newforms.
(b) The 28 'Hasegawa curves' from [54] that have absolutely simple Jacobian. These are all quotients of $X_0(N)$ by a subgroup of Atkin–Lehner involutions. Because of this, these examples are easier to deal with (compare corollary 3.17, which shows that the computation of Heegner points is simpler in this case), which is why we treated them first, before extending the theory and algorithms to the general case. See [59] for an overview of the results. Note that $X_0(161)/\langle w_7, w_{23}\rangle$ is the only curve on this list whose Jacobian is not isogenous to the Jacobian of one of the LMFDB examples. (We check this by comparing the associated newforms.) Hence, strong BSD for the other 27 Hasegawa curves follows from isogeny invariance and the validity of strong BSD for the LMFDB examples.
(c) The four 'Wang curves' from [45] that are neither Hasegawa curves nor have Jacobian isogenous to that of a curve in the LMFDB. They are the curves labeled 65A, 117B, 125B and 175 in [45].
(d) Sam Frengley's example of a curve with $N = 3200$ and $\#Ш(J/\mathbf{Q}) = 7^2$.

Note that there is some overlap between the first two sets: 21 of the Hasegawa curves are in the LMFDB. In total, the LMFDB, Hasegawa, and Wang examples comprise the Jacobians of 108 isomorphism classes of curves, whose Jacobians fall into 95 distinct isogeny classes. Including the last example, we therefore have verified the strong BSD conjecture completely for 96 isogeny classes of absolutely simple modular abelian surfaces. The distribution of the L-ranks in our examples is as follows:

(a) There are 36 isomorphism classes of L-rank 0 and 61 of L-rank 1. These belong to 31 and 59 isogeny classes, respectively.
(b) There are 6 isomorphism classes of L-rank 0 and 22 of L-rank 1. Out of the 7 Hasegawa non-LMFDB examples, there are 4 isomorphism classes of L-rank 0 and 3 of L-rank 1. The latter include the single isogeny class not represented by LMFDB curves. All these examples belong to distinct isogeny classes. The abundance of L-rank 1 examples is explained by the fact that one often quotients out by the Fricke involution w_N; hence, the sign in the functional equation shows that the L-rank is odd.
(c) All 4 isogeny classes have L-rank 0.

In total, there are 44 isomorphism classes and 35 isogeny classes of L-rank 0 and 64 isomorphism classes and 60 isogeny classes of L-rank 1.

Completeness of our data

We consider all the Hasegawa examples (already contained in [59]) and all Wang-only examples from [45]. The LMFDB examples comprise all absolutely simple modular genus 2 Jacobians of curves with ‘small’ coefficients and of level $N \leq 1000$. The smallest level for which there exists a pair of conjugate newforms that is not related to one of these examples is 43. There is an ongoing project that attempts to produce, for a given weight 2 newform f with real quadratic coefficients, a genus-2 curve over $\mathbf{Q}$ with Jacobian isogenous to A_f. Our code can prove strong BSD for many of these examples automatically, especially by using [60] to skip many descent computations.

1.7. Structure of the paper

We give an overview of the paper; more details are given at the beginning of each section. In Section 2, we give algorithms to determine whether the residual Galois representations attached to f are irreducible or not. In Section 3, we compute (a multiple of) the Heegner index, which is used in the following two sections: In Section 4, we compute $\#Ш(J/\mathbf{Q})_{\mathrm{an}} \in \mathbf{Q}_{>0}$ exactly. In Section 5, we give a description of a finite set S of prime ideals $\mathfrak{p}$ such that $Ш(J/\mathbf{Q})[\mathfrak{p}] = 0$ for $\mathfrak{p} \notin S$; this strongly depends on the determination of the residual Galois representations and the Heegner index. In Section 6, we perform isogeny descents to prove $Ш(J/\mathbf{Q})[\mathfrak{p}] = 0$ for several $\mathfrak{p} \in S$. In Section 7, we show how results from Iwasawa theory and the computation of p-adic L-functions can be used to prove an upper bound on $\#Ш(J/\mathbf{Q})[\mathfrak{p}^\infty]$. In Appendix A, we prove strong BSD for an example of Sam Frengley, where $\#Ш(J/\mathbf{Q}) = 7^2$. In all our other examples, $\#Ш(J/\mathbf{Q}) \in \{1, 2, 4\}$. We also exhibit examples $J/\mathbf{Q}$ for which $p^2 \mid Ш(J/\mathbf{Q})_{\mathrm{an}}$ with $p \in \{3, 5, 7\}$ and prove the ℓ-part of strong BSD for them except for $\ell \in \{2, p\}$, where we only get an upper bound. These examples are obtained as quadratic twists J^K of some of our main examples, where K is a suitable Heegner field.

1.8. Terms and notation

We denote canonical isomorphisms by $\simeq$ and arbitrary, not necessarily canonical isomorphisms by $\cong$. We fix an embedding $\overline{\mathbf{Q}} \hookrightarrow \mathbf{C}$ once and for all.

We use boldface $\boldsymbol{\pi}$ to denote the area of the unit disk to avoid confusion with our use of the letter π to denote an isogeny in most of the paper.

2. Computation of the residual Galois representations

The purpose of this section is to generalize several results on the image of mod-p Galois representations of elliptic curves over $\mathbf{Q}$ (mainly from [98] and [26]) to modular abelian varieties over $\mathbf{Q}$ of higher dimension.

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

Let A be an abelian variety of dimension $g \geq 1$. Let $\mathcal{O}$ be an order in a totally real number field F of degree g over $\mathbf{Q}$. Recall that A has *real multiplication by* $\mathcal{O}$ *over* $\mathbf{Q}$ if $\operatorname{End}_{\mathbf{Q}}(A) \cong \mathcal{O}$, where $\operatorname{End}_{\mathbf{Q}}(A)$ denotes the ring of $\mathbf{Q}$-defined endomorphisms of A. Then A is of GL_2-type in the following sense. Let $\mathfrak{p}$ be a nonzero prime ideal of $\mathcal{O}$ lying above a rational prime p. We denote its finite residue field $\mathcal{O}/\mathfrak{p}$ by $\mathbf{F}_{\mathfrak{p}}$ and call $[\mathbf{F}_{\mathfrak{p}} : \mathbf{F}_p]$ the *degree* $\deg \mathfrak{p}$ of $\mathfrak{p}$; $\mathbf{F}_{\mathfrak{p}}$ is isomorphic to $\mathbf{F}_{p^{\deg \mathfrak{p}}}$. If $\mathfrak{p}$ is *regular* – that is, its local ring is a discrete valuation ring, or equivalently, $\mathfrak{p}$ does not divide the conductor ideal $\mathfrak{f}(\mathcal{O}_F/\mathcal{O}) = \{a \in \mathcal{O} : a\mathcal{O}_F \subseteq \mathcal{O}\}$ of $\mathcal{O}$ in $\mathcal{O}_F$ – then $A[\mathfrak{p}^n](\overline{\mathbf{Q}})$ is free of rank 2 over $\mathcal{O}/\mathfrak{p}^n$ for all $n \geq 1$. We then obtain 2-dimensional Galois representations

$$\rho_{\mathfrak{p}^n,A} \colon \operatorname{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}) \to \operatorname{Aut}_{\mathcal{O}/\mathfrak{p}^n}(A[\mathfrak{p}^n](\overline{\mathbf{Q}})) \cong \mathrm{GL}_2(\mathcal{O}/\mathfrak{p}^n)\,.$$

In a similar way, we have $2g$-dimensional Galois representations

$$\rho_{p^n,A} \colon \operatorname{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}) \to \operatorname{Aut}_{\mathbf{Z}/p^n\mathbf{Z}}(A[p^n](\overline{\mathbf{Q}})) \cong \mathrm{GL}_{2g}(\mathbf{Z}/p^n\mathbf{Z})\,.$$

Since the Galois action preserves the Weil pairing, the image of $\rho_{p,A}$ lies in the general symplectic group $\mathrm{GSp}_{2g}(\mathbf{F}_p)$.

We define the $\mathfrak{p}$*-adic Tate module* $T_{\mathfrak{p}}A := \varprojlim_n A[\mathfrak{p}^n](\overline{\mathbf{Q}})$; it is free of rank 2 over the completion $\mathcal{O}_{\mathfrak{p}}$. We also define $V_{\mathfrak{p}}A = F_{\mathfrak{p}} \otimes_{\mathcal{O}_{\mathfrak{p}}} T_{\mathfrak{p}}A$; this is a 2-dimensional vector space over $F_{\mathfrak{p}}$. There is also the standard p-adic Tate-module T_pA, which is a free module of rank $2g$ over $\mathbf{Z}_p$ and the associated vector space $V_pA = \mathbf{Q}_p \otimes_{\mathbf{Z}_p} T_pA$. We obtain the $\mathfrak{p}$*-adic Galois representation*

$$\rho_{\mathfrak{p}^\infty,A} \colon \operatorname{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}) \to \operatorname{Aut}_{F_{\mathfrak{p}}}(V_{\mathfrak{p}}A) \cong \mathrm{GL}_2(F_{\mathfrak{p}})$$

and the *p-adic Galois representation*

$$\rho_{p^\infty,A} \colon \operatorname{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}) \to \operatorname{Aut}_{\mathbf{Q}_p}(V_pA) \cong \mathrm{GL}_{2g}(\mathbf{Q}_p)\,.$$

As before, the image of $\rho_{p^\infty,A}$ is contained in $\mathrm{GSp}_{2g}(\mathbf{Q}_p)$.

If A is understood, we omit it from the notation and write $\rho_{\mathfrak{p}}$ etc.

We heavily exploit that we can work with 2-dimensional Galois representations instead of $2g$-dimensional ones in the following. For example, there is an easy classification of (maximal) subgroups of $\mathrm{GL}_2(\mathbf{F}_{\mathfrak{p}})$, whereas the subgroups of $\mathrm{GSp}_{2g}(\mathbf{F}_p)$ are more complicated.

The goal of this section is to determine the image $G_{\mathfrak{p}}$ of the mod-$\mathfrak{p}$ Galois representation

$$\rho_{\mathfrak{p}} \colon \operatorname{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}) \to \mathrm{GL}_{\mathcal{O}/\mathfrak{p}}(A[\mathfrak{p}](\overline{\mathbf{Q}})) \cong \mathrm{GL}_2(\mathbf{F}_{\mathfrak{p}})$$

in the case when $g = 2$, so $\mathcal{O}$ is an order in a real quadratic number field. In particular, we want to decide whether $\rho_{\mathfrak{p}}$ is irreducible as an $\mathbf{F}_{\mathfrak{p}}[\operatorname{Gal}(\overline{\mathbf{Q}}|\mathbf{Q})]$- or $\mathbf{F}_p[\operatorname{Gal}(\overline{\mathbf{Q}}|\mathbf{Q})]$-representation and whether its image in $\mathrm{GL}_2(\mathbf{F}_{\mathfrak{p}})$ is as large as allowed by the extra endomorphisms coming from $\mathcal{O}$.

We will state our results for general g if this is easily possible, but in some cases, we assume $g = 2$ to simplify the statements and algorithms.

Let $f \in S_2(\Gamma_0(N))$ be a newform (i.e., a normalized eigenform for the action of the Hecke algebra $\mathbf{T}_{\mathbf{Z}}$ on the new subspace of $S_2(\Gamma_0(N))$). The Fourier coefficients of f generate an order $\mathbf{Z}[f]$ in a totally real number field $\mathbf{Q}(f)$. Let $I_f := \operatorname{Ann}_{\mathbf{T}_{\mathbf{Z}}}(f)$ be the annihilator of f; then $\mathbf{T}_{\mathbf{Z}}/I_f \simeq \mathbf{Z}[f]$, where the Hecke operator T_n is mapped to the Fourier coefficient $a_n(f)$. The Hecke algebra also acts via $\mathbf{Q}$-defined endomorphisms on $J_0(N)$, and so we can define an abelian variety A_f over $\mathbf{Q}$ as $A_f := J_0(N)/I_fJ_0(N)$. Then $\dim A_f = [\mathbf{Q}(f) : \mathbf{Q}]$ and $\operatorname{End}_{\mathbf{Q}}(A_f) \simeq \mathbf{T}_{\mathbf{Z}}/I_f \simeq \mathbf{Z}[f]$. Acting by $\operatorname{Gal}(\overline{\mathbf{Q}}|\mathbf{Q})$ on the Fourier coefficients of f, we obtain a Galois orbit of conjugate newforms f^σ, which has size $[\mathbf{Q}(f) : \mathbf{Q}]$. More generally, if $\alpha \colon \mathbf{Z}[f] \hookrightarrow \mathbf{R}$ is an embedding of $\mathbf{Z}[f]$ into $\mathbf{R}$, then f^α denotes the newform with (real) coefficients $\alpha(a_n(f))$. The abelian variety A_f only depends on the Galois orbit of f.

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

We give a short summary of the contents of this section. After recalling basic results about modular abelian varieties and their Galois representations in Section 2.1, we determine the maximal possible image of $\rho_\mathfrak{p}$ in Section 2.3 and state the classification of its maximal subgroups in Section 2.4. This is eventually used to show that $\rho_\mathfrak{p}$ has maximal image for all $\mathfrak{p}$ outside an explicit finite set by excluding the possibility that the image is contained in one of the maximal subgroups. For fixed $\mathfrak{p}$, we give an algorithm that returns a set of types of maximal subgroups that could contain the image of $\rho_\mathfrak{p}$ in Section 2.5. In Section 2.6, we show how $\rho_\mathfrak{p}$ can be determined explicitly for a given prime ideal $\mathfrak{p}$. We then give some criteria for when the image of the decomposition group at p is contained in a Cartan subgroup in Section 2.7. Together with some results on the image of inertia at primes $\ell \neq p$, which we recall in Section 2.8, this provides the input for an algorithm that determines a (small and explicit) finite set S of prime ideals $\mathfrak{p}$ such that $\rho_\mathfrak{p}$ is irreducible for all $\mathfrak{p} \notin S$ in Section 2.9. To approach the goal of determining an analogous set with respect to $\rho_\mathfrak{p}$ with maximal image, we first describe a method that allows us to eliminate two further types of maximal subgroups (other than Borel subgroups, which correspond to reducible representations) in Section 2.10. To deal with maximal images, we need to exclude that the given newform f has complex multiplication, so we provide an algorithm that checks that in Section 2.11. We then derive an algorithm that computes a small explicit finite set of prime ideals $\mathfrak{p}$ such that $\rho_\mathfrak{p}$ has maximal image for all $\mathfrak{p}$ not in this set in Section 2.12. Finally, we provide a table giving the types of all representations $\rho_\mathfrak{p}$ attached to our LMFDB examples.

2.1. Preliminaries

We begin by stating the correspondence between (absolutely simple) abelian varieties with real multiplication over $\mathbf{Q}$ and weight-2 newforms for $\Gamma_0(N)$.

Recall that $L(A/\mathbf{Q}, s)$ denotes the L-series of A and $L(f, s)$ denotes the L-series of f and that $L(A/\mathbf{Q}, s)$ is defined as

$$L(A/\mathbf{Q}, s) = \prod_p \frac{1}{\det(1 - \mathrm{Frob}_p^{-1}\, p^{-s} \mid \mathrm{H}^1_{\text{ét}}(A \otimes \overline{\mathbf{Q}}, \mathbf{Q}_\ell)^{I_p})},$$

where for each Euler factor at p, one chooses a prime $\ell \neq p$ for the ℓ-adic cohomology group; this is well-defined because the Euler factors are independent of ℓ. The product converges for $\mathrm{Re}(s) > \frac{3}{2}$ to a holomorphic function. The L-function associated to $f = \sum_n a_n q^n$ with coefficients $a_n \in \mathbf{C}$ is

$$L(f, s) = \sum_{n \geq 1} \frac{a_n}{n^s} = \prod_p \frac{1}{1 - a_p p^{-s} + \varepsilon(p) p^{1-2s}},$$

where $\varepsilon(p)$ is 1 if $p \nmid N$ and 0 otherwise. Since $L(f, s)$ is the Mellin transform of f and f is a cusp form, $L(f, s)$ is holomorphic on the whole complex plane.

Theorem 2.1 (Characterization of modular abelian varieties over $\mathbf{Q}$). *Let $A/\mathbf{Q}$ be an absolutely simple abelian variety. The following are equivalent.*

(i) *A has real multiplication over $\mathbf{Q}$.*
(ii) *There is some N such that A is an isogeny factor of $J_0(N)$.*
(iii) *There is some N and a newform $f \in S_2(\Gamma_0(N))$ such that*

$$L(A/\mathbf{Q}, s) = \prod_{\alpha\colon \mathbf{Z}[f] \hookrightarrow \mathbf{R}} L(f^\alpha, s)\,.$$

The number N in (iii) is uniquely determined; we call it the level N_A of $A/\mathbf{Q}$. The statement in (ii) holds for the same N and its multiples. If these equivalences hold, then $\mathrm{End}^0_{\mathbf{Q}}(A) := \mathrm{End}_{\mathbf{Q}}(A) \otimes_{\mathbf{Z}} \mathbf{Q}$ is isomorphic to $\mathbf{Q}(f)$ and the conductor of $A/\mathbf{Q}$ equals $N_A^{\dim A}$. Furthermore, A is of GL_2-type (i.e., the p-adic Tate modules $V_p A$ are free modules of rank 2 over the completion of $\mathbf{Q}(f)$ at p); if $\mathfrak{p}$ is a prime

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

ideal of $\mathbf{Q}(f)$ *above the rational prime* p, *then* $V_{\mathfrak{p}}A$ *is a vector space of dimension* 2 *over the completion* $\mathbf{Q}(f)_{\mathfrak{p}}$, *a local field.*

Proof. The equivalence of (ii) and (iii) is a well-known characterization of modular abelian varieties following from the Eichler–Shimura relation and Faltings' Isogeny Theorem. The equivalence of (i) and (ii) can be found as [97, Thm. 5] as a consequence of Serre's Modularity Conjecture for absolutely simple 2-dimensional residual odd Galois representations (which is formulated in the same paper); this conjecture is now a theorem [61]. See also [91]. The remaining statements are well-known. □

We will use these equivalences tacitly. Note that in the literature, sometimes more general modular abelian varieties are considered, which are quotients of $J_1(N)$ and which can have complex multiplication.

However, when A is an *absolutely simple* abelian surface with CM, then A cannot be of GL_2-type over $\mathbf{Q}$, as the following result shows. We thank Pip Goodman for pointing it out to us.

Proposition 2.2. *Let* $A/\mathbf{Q}$ *be an absolutely simple abelian surface with CM. Then* $\mathrm{End}^0_{\mathbf{Q}}(A) = \mathbf{Q}$*; in particular,* $A/\mathbf{Q}$ *is not of* GL_2*-type.*

Proof. Let $E = \mathrm{End}^0_{\overline{\mathbf{Q}}}(A) = \mathrm{End}_{\overline{\mathbf{Q}}}(A) \otimes_{\mathbf{Z}} \mathbf{Q}$ be the geometric endomorphism algebra of A. By [101, Proposition 30], the minimal field over which the endomorphisms of A are defined is E^*, the reflex field of E (note that the base field is just $\mathbf{Q}$ here). In particular, $E^*|\mathbf{Q}$ is Galois, and the absolute Galois group $\mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q})$ acts on $\mathrm{End}^0_{\overline{\mathbf{Q}}}(A)$ through $\mathrm{Gal}(E^*|\mathbf{Q})$, so we obtain an embedding

$$i\colon\ \mathrm{Gal}(E^*|\mathbf{Q}) \hookrightarrow \mathrm{Aut}(\mathrm{End}^0_{\overline{\mathbf{Q}}}(A))\,.$$

We now consult Examples 8.4 (2) in *loc. cit.* In Example (C), there the reflex field is not Galois, and in Example (A), the CM-type is not primitive, which means that A is not absolutely simple. So both these cases cannot occur, and by Example (B), it follows that $E^* = E$; in particular, the map i above is an isomorphism. This finally implies that

$$\mathrm{End}^0_{\mathbf{Q}}(A) = \mathrm{End}^0_{\overline{\mathbf{Q}}}(A)^{\mathrm{Gal}(E^*/\mathbf{Q})} = E^{\mathrm{Gal}(E/\mathbf{Q})} = \mathbf{Q}\,.$$

□

Remark 2.3. In the situation of theorem 2.1, A is isogenous to A_f (by Faltings' Isogeny Theorem), and therefore, the Galois representations on $V_{\mathfrak{p}}A$ and on $V_{\mathfrak{p}}A_f$ are isomorphic (similarly for V_pA and V_pA_f). When A and/or f are clear from the context, we write $\rho_{\mathfrak{p}^\infty}$ and ρ_{p^∞} for these representations, which depend only on the Galois orbit of f. The fact that A and A_f are isogenous also implies that the semi-simplifications of $\rho_{\mathfrak{p},A}$ and of $\rho_{\mathfrak{p},f} := \rho_{\mathfrak{p},A_f}$ are isomorphic when $\mathfrak{p}$ is a regular prime of both $\mathbf{Z}[f] \simeq \mathrm{End}_{\mathbf{Q}}(A_f)$ and $\mathrm{End}_{\mathbf{Q}}(A)$ (and similarly for $\rho_{p,A}$ and $\rho_{p,f}$).

Note that the canonical isomorphism $\mathbf{Z}[f] \simeq \mathbf{T}_{\mathbf{Z}}/I_f \simeq \mathrm{End}_{\mathbf{Q}}(A_f)$ induces a canonical identification of $\mathbf{Q}(f)$ with $\mathrm{End}^0_{\mathbf{Q}}(A_f)$, which in turn is isomorphic to $\mathrm{End}^0_{\mathbf{Q}}(A)$ via the isogeny between A and A_f. Fixing the isogeny, this identifies $\mathcal{O} = \mathrm{End}_{\mathbf{Q}}(A)$ with an order in the totally real number field $\mathbf{Q}(f)$. If $\mathbf{Z}[f]$ is contained in $\mathcal{O}$ under this identification (e.g., when $\mathcal{O}$ is the maximal order), then the Fourier coefficient a_n of f, which is the image of the Hecke operator $T_n \in \mathbf{T}_{\mathbf{Z}}$ in $\mathbf{Z}[f]$, can be interpreted as an element of $\mathcal{O}$ (i.e., an endomorphism of A). We make use of this to get the correct identifications of σ-isotypic components when dealing with the Gross–Zagier formula for the height of a Heegner point in Section 3.7.

Write $F = \mathbf{Q}(f)$ and $\mathcal{O}_F$ for the maximal order of F, and let $\mathcal{O} \subseteq \mathcal{O}_F$ be any order in F. Recall the conductor ideal of $\mathcal{O}$ in $\mathcal{O}_F$,

$$\mathfrak{f}(\mathcal{O}_F/\mathcal{O}) = \{a \in \mathcal{O} : a\mathcal{O}_F \subseteq \mathcal{O}\}\,;$$

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

it is the largest ideal of $\mathcal{O}$ that is also an ideal of $\mathcal{O}_F$. If A is an abelian variety such that $\mathrm{End}_{\mathbf{Q}}(A) \cong \mathcal{O}$, then one can check that the isogenous abelian variety $A' := A/A[\mathfrak{f}(\mathcal{O}_F/\mathcal{O})]$ has $\mathrm{End}_{\mathbf{Q}}(A') \cong \mathcal{O}_F$. So by working with A' instead of with A (or A_f), we can assume that the endomorphism ring is the maximal order.

Definition 2.4. Let p be a prime. We write

$$\chi_{p^n}\colon \mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}) \longrightarrow \mathrm{Aut}(\mu_{p^n}(\overline{\mathbf{Q}})) \simeq (\mathbf{Z}/p^n\mathbf{Z})^\times$$

for the mod-p^n cyclotomic character and

$$\chi_{p^\infty}\colon \mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}) \longrightarrow \mathrm{Aut}(\mu_{p^\infty}(\overline{\mathbf{Q}})) \simeq \mathbf{Z}_p^\times$$

for the p-adic cyclotomic character.

Definition 2.5. If $\mathfrak{p}$ is a maximal ideal in an order $\mathcal{O}$ of a number field, we write $p(\mathfrak{p})$ for the characteristic of the finite field $\mathbf{F}_\mathfrak{p} = \mathcal{O}/\mathfrak{p}$.

Theorem 2.6 (Characteristic polynomials of Frobenii of a modular Galois representation). *Let $f \in S_2(\Gamma_0(N))$ be a newform with Fourier coefficients a_ℓ and coefficient field $\mathbf{Q}(f)$ a totally real field of degree g.*

Associated to f, there is a strictly compatible system of $\mathfrak{p}$-adic Galois representations $\rho_{\mathfrak{p}^\infty}$, unramified outside $Np(\mathfrak{p})$. For all $\ell \nmid Np(\mathfrak{p})$, the characteristic polynomial of $\rho_{\mathfrak{p}^\infty}(\mathrm{Frob}_\ell)$ equals

$$\mathrm{charpol}(f, \ell; T) := \det\bigl(T - \rho_{\mathfrak{p}^\infty}(\mathrm{Frob}_\ell)\bigr) = T^2 - a_\ell T + \ell \in \mathbf{Z}[f][T]\,.$$

One has

$$\det \circ \rho_{\mathfrak{p}^\infty} = \chi_{p^\infty}$$

for $\mathfrak{p} \nmid N$. In particular, $\rho_{\mathfrak{p}^\infty}$ is odd. The determinant of the p-adic Galois representation

$$\rho_{p^\infty}\colon \mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}) \to \mathrm{GL}_{2g}(\mathbf{Z}_p)$$

is $\chi_{p^\infty}^g$.

Proof. This is well-known and shown more generally for weight $k \geq 2$ in [37] (and for weight 2 earlier by Shimura). □

If $\mathfrak{p}$ is a regular prime of $\mathbf{Z}[f]$ (or $\mathcal{O}$) not dividing $N\ell$, then we write $\mathrm{charpol}(f, \ell, \mathfrak{p}; T)$ for the characteristic polynomial of the image of Frob_ℓ under $\rho_{\mathfrak{p},f}$ (or $\rho_{\mathfrak{p},A}$); it is the image of $\mathrm{charpol}(f, \ell; T)$ in $\mathbf{F}_\mathfrak{p}[T]$.

Magma can compute the Fourier coefficients a_ℓ of a newform f and its coefficient ring $\mathbf{Z}[f]$ efficiently. This will be crucial for computing the image of $\rho_\mathfrak{p}$, because the only access to elements of the absolute Galois group of $\mathbf{Q}$ we have is via Frobenius elements, and we can reconstruct the characteristic polynomials of the Frobenii acting on $A[\mathfrak{p}](\mathbf{Q})$, which uniquely determine their semi-simple part. The fact that we know only the characteristic polynomials also means that we do not have direct access to the unipotent part of $\rho_p(\mathrm{Frob}_\ell)$ via a_ℓ alone.

Let p be a prime. We fix an embedding of $\overline{\mathbf{Q}}$ into $\overline{\mathbf{Q}}_p$; this determines a decomposition group $D_p = \mathrm{Gal}(\overline{\mathbf{Q}}_p|\mathbf{Q}_p) \hookrightarrow \mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q})$ and its inertia subgroup $I_p = \mathrm{Gal}(\overline{\mathbf{Q}}_p|\mathbf{Q}_p^{\mathrm{nr}})$. The inertia subgroup has a descending filtration by its (normal) higher ramification subgroups, the first of which is the wild ramification subgroup I_p^{w}, the unique (hence normal) Sylow pro-p subgroup of I_p. The quotient I_p/I_p^{w}

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

is the tame inertia group I_p^{t}, which is canonically isomorphic to the pro-cyclic p'-group

$$\varprojlim_{\mathbf{N}_{\mathbf{F}|}} \mathbf{F}^\times \cong \hat{\mathbf{Z}}^{(p')}(1) \simeq \prod_{\ell \neq p} \mathbf{Z}_\ell(1),$$

where the limit is taken over all finite fields $\mathbf{F}$ of characteristic p, the transition maps in the projective limit are the field norms and $\mathbf{Z}_\ell(1)$ is the Galois module $\varprojlim_n \mu_{\ell^n}(\overline{\mathbf{Q}}_p)$. (See [98, §1.3]. Note that Serre uses I_p to denote I_p^{w}, I_t to denote I_p^{t} and I to denote I_p.)

Lemma 2.7. *The absolute Galois group of the residue field $\mathbf{F}_p$, which is canonically isomorphic to $\hat{\mathbf{Z}}\,\mathrm{Frob}_p$, acts on I_p^{t} via conjugation. One has*

$$\mathrm{Frob}_p\, x\, \mathrm{Frob}_p^{-1} = x^p \quad \textit{for } x \in I_p^{\mathrm{t}}\,.$$

Note that we have written I_p^{t} multiplicatively here.

Proof. See [81, Theorem 7.5.3]. □

See [98, §1.7] for the following definition.

Definition 2.8. Let $k \geq 1$. We define the character ψ_k of I_p^{t} via the canonical projection from the projective limit as

$$\psi_k \colon I_p^{\mathrm{t}} \xrightarrow{\sim} \varprojlim_{\mathbf{N}_{\mathbf{F}|}} \mathbf{F}^\times \twoheadrightarrow \mathbf{F}_{p^k}^\times\,.$$

One has $\mathbf{N}_{\mathbf{F}_{p^k}|\mathbf{F}_p} \circ \psi_k = \psi_1 = \chi_p$.

The k *fundamental characters of level* k are the powers $\psi_k^{p^n}$ for $0 \leq n < k$ (equivalently, ψ_k followed by the k automorphisms of $\mathbf{F}_{p^k}$).

2.2. General set-up and notation

In the following, f will always denote a newform of weight 2, level N and trivial nebentypus. We let $\mathcal{N}(N)$ denote the set of such newforms; $\mathcal{N}(N, g)$ denotes the subset consisting of forms whose Galois orbit has size g. The Fourier coefficients of f will be denoted a_n (or $a_n(f)$ if we want to make the dependence on f explicit); they generate the coefficient ring $\mathbf{Z}[f]$, which is an order in a totally real number field $F = \mathbf{Q}(f)$ (of degree g when $f \in \mathcal{N}(N, g)$).

Further, A will denote an abelian variety over $\mathbf{Q}$ that is $\mathbf{Q}$-isogenous to A_f (e.g., $A = A_f$ or $A = A' = A_f / A_f[\mathfrak{f}(\mathcal{O}_F/\mathbf{Z}[f])]$ as in remark 2.3) and has endomorphism ring $\mathcal{O}$. Let $\mathfrak{p}$ be a regular prime ideal of $\mathcal{O}$; then $\mathfrak{p}$ is a maximal ideal of $\mathcal{O}$; we write $\mathbf{F}_\mathfrak{p} = \mathcal{O}/\mathfrak{p}$ for its residue class field and $p(\mathfrak{p})$ for the residue characteristic (i.e., the characteristic of $\mathbf{F}_\mathfrak{p}$). Then $\rho_\mathfrak{p} = \rho_{\mathfrak{p},A}$ is the Galois representation on $A[\mathfrak{p}]$; its semi-simplification $\rho_\mathfrak{p}^{\mathrm{ss}}$ is independent of the choice of A (as long as $\mathfrak{p}$ is regular). Since we are mostly interested in determining when $\rho_\mathfrak{p}$ is irreducible (or has maximal image), knowing $\rho_\mathfrak{p}^{\mathrm{ss}}$ is usually enough, and so we suppress the dependency on A in the notation. (Note that when $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_F$ that does not correspond to a regular prime ideal of $\mathcal{O}$, then $\rho_{\mathfrak{p},A'}$ will be reducible, since there is an isogeny $A' \longrightarrow A$ whose kernel has nontrivial intersection with $A'[\mathfrak{p}]$.)

2.3. Determination of the maximal image

One of our goals is to show that the image of $\rho_\mathfrak{p}$ is as large as possible for all but finitely many prime ideals $\mathfrak{p}$ (with a small explicit set of possible exceptions). The first step is to determine what this maximal image is. Then we will show that it suffices to consider the image in $\mathrm{PGL}_2(\mathbf{F}_\mathfrak{p})$.

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

To show that the projective image is maximal, we have to exclude the possibility that it is contained in one of the maximal subgroups of the maximal projective image, so we need a classification of these maximal subgroups. This will be done in Section 2.4 below.

Definition 2.9. We write $G_\mathfrak{p} := \rho_\mathfrak{p}(\mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q})) \subseteq \mathrm{GL}_2(\mathbf{F}_\mathfrak{p})$ for the image of $\rho_\mathfrak{p}$. theorem 2.6 implies that $\det(G_\mathfrak{p}) = \mathbf{F}_p^\times$, since $\det \circ \rho_\mathfrak{p}$ is the mod-p cyclotomic character. We set

$$G_\mathfrak{p}^{\max} := \{M \in \mathrm{GL}_2(\mathbf{F}_\mathfrak{p}) : \det(M) \in \mathbf{F}_p^\times\} ;$$

then $G_\mathfrak{p} \subseteq G_\mathfrak{p}^{\max}$.

Definition 2.10. We write $\mathbf{P}\colon \mathrm{GL}_2(\mathbf{F}_\mathfrak{p}) \to \mathrm{PGL}_2(\mathbf{F}_\mathfrak{p})$ for the canonical surjection. For a subgroup G of $\mathrm{GL}_2(\mathbf{F}_\mathfrak{p})$, we write $\mathbf{P}G$ for its image in $\mathrm{PGL}_2(\mathbf{F}_\mathfrak{p})$. We call $\mathbf{P}G$ the *projective image of* G. We also say that $\mathbf{P}G_\mathfrak{p}$ is the *projective image of* $\rho_\mathfrak{p}$. We write $\overline{\det}\colon\ \mathrm{PGL}_2(\mathbf{F}_\mathfrak{p}) \to \mathbf{F}_\mathfrak{p}^\times/\mathbf{F}_\mathfrak{p}^{\times 2}$ for the homomorphism induced by the determinant.

We write $\mathrm{PSL}_2(\mathbf{F}_\mathfrak{p}) := \mathbf{P}\mathrm{SL}_2(\mathbf{F}_\mathfrak{p})$ for the quotient of $\mathrm{SL}_2(\mathbf{F}_\mathfrak{p})$ by its center $\{\pm I_2\}$. Note that this is not the same as the group of $\mathbf{F}_\mathfrak{p}$-points of the algebraic group PSL_2. When p is odd, $\mathrm{PSL}_2(\mathbf{F}_\mathfrak{p})$ has index 2 in $\mathrm{PGL}_2(\mathbf{F}_\mathfrak{p})$ and is the kernel of $\overline{\det}$.

Lemma 2.11. *We have that* $\mathbf{P}G_\mathfrak{p}^{\max} = \mathrm{PGL}_2(\mathbf{F}_\mathfrak{p})$ *when* $\deg \mathfrak{p}$ *is odd and* $\mathbf{P}G_\mathfrak{p}^{\max} = \mathrm{PSL}_2(\mathbf{F}_\mathfrak{p})$ *when* $\deg \mathfrak{p}$ *is even.*

Proof. The image of $G_\mathfrak{p}^{\max}$ in $\mathrm{PGL}_2(\mathbf{F}_\mathfrak{p})$ consists of the elements $\gamma \in \mathrm{PGL}_2(\mathbf{F}_\mathfrak{p})$ such that $\overline{\det}(\gamma)$ is in the image of $\mathbf{F}_p^\times$. The latter is trivial if and only if $\deg \mathfrak{p}$ is even (or $p = 2$, in which case $\mathrm{PSL}_2(\mathbf{F}_\mathfrak{p}) = \mathrm{PGL}_2(\mathbf{F}_\mathfrak{p})$). (See also [89, §5.2].) □

Proposition 2.12. *Let* $G \le G_\mathfrak{p}^{\max}$ *be a subgroup such that* $\det(G) = \mathbf{F}_p^\times$ *and* $\mathbf{P}G = \mathbf{P}G_\mathfrak{p}^{\max}$. *Then* $G = G_\mathfrak{p}^{\max}$.

Proof. First assume that $\#\mathbf{F}_\mathfrak{p} > 3$ and let $\mathscr{D}H$ denote the derived subgroup of a group H. Since the center of $\mathrm{GL}_2(\mathbf{F}_\mathfrak{p})$ is abelian, the assumption $\mathbf{P}G = \mathbf{P}G_\mathfrak{p}^{\max}$ implies that $\mathscr{D}G = \mathscr{D}G_\mathfrak{p}^{\max} = \mathrm{SL}_2(\mathbf{F}_\mathfrak{p})$, so $\mathrm{SL}_2(\mathbf{F}_\mathfrak{p}) \le G$. The second equality follows from

$$\mathrm{SL}_2(\mathbf{F}_\mathfrak{p}) = \mathscr{D}\,\mathrm{SL}_2(\mathbf{F}_\mathfrak{p}) \le \mathscr{D}G_\mathfrak{p}^{\max} \le \mathscr{D}\mathrm{GL}_2(\mathbf{F}_\mathfrak{p}) \le \mathrm{SL}_2(\mathbf{F}_\mathfrak{p}),$$

where the first equality follows from the fact that $\mathrm{PSL}_2(\mathbf{F}_\mathfrak{p})$ is nonsolvable simple (since nonabelian when $\#\mathbf{F}_\mathfrak{p} > 3$) by [65, Theorem 8.4]. Since both groups map onto $\mathbf{F}_p^\times$ under the determinant, we then have exact sequences

$$1 \to \mathrm{SL}_2(\mathbf{F}_\mathfrak{p}) \to G \overset{\det}{\to} \mathbf{F}_p^\times \to 1 \quad \text{and} \quad 1 \to \mathrm{SL}_2(\mathbf{F}_\mathfrak{p}) \to G_\mathfrak{p}^{\max} \overset{\det}{\to} \mathbf{F}_p^\times \to 1,$$

so $\#G = \#\mathrm{SL}_2(\mathbf{F}_\mathfrak{p})\#\mathbf{F}_p^\times = \#G_\mathfrak{p}^{\max}$, whence the claim.

The two cases $\mathbf{F}_\mathfrak{p} = \mathbf{F}_2$ or $\mathbf{F}_3$ can be checked by an easy computation. □

2.4. *Classification of the maximal subgroups of* $\mathbf{P}G_\mathfrak{p}^{\max}$

By lemma 2.11, $\mathbf{P}G_\mathfrak{p}^{\max} = \mathrm{PGL}_2(\mathbf{F}_\mathfrak{p})$ when $\deg \mathfrak{p}$ is odd, and $\mathbf{P}G_\mathfrak{p}^{\max} = \mathrm{PSL}_2(\mathbf{F}_\mathfrak{p})$ when $\deg \mathfrak{p}$ is even. By proposition 2.12, we know that $G_\mathfrak{p} = G_\mathfrak{p}^{\max}$ if and only if $\mathbf{P}G_\mathfrak{p} = \mathbf{P}G_\mathfrak{p}^{\max}$, which is equivalent to $\mathbf{P}G_\mathfrak{p} \not\subseteq \Gamma$ for every maximal subgroup Γ of $\mathbf{P}G_\mathfrak{p}^{\max}$. In this section, we recall the classification of these maximal subgroups.

We begin with the case $\deg \mathfrak{p}$ even, where $\mathbf{P}G_\mathfrak{p}^{\max} = \mathrm{PSL}_2(\mathbf{F}_\mathfrak{p})$.

Theorem 2.13 (Maximal subgroups of $\mathbf{P}G_\mathfrak{p}^{\max}$, $\deg \mathfrak{p}$ even). *Let p be a prime and let $q = p^{2e}$ be an even power of p. The maximal subgroups of* $\mathrm{PSL}_2(\mathbf{F}_q)$ *are as follows.*

(i) *(Borel) The stabilizer of a point of* $\mathbf{P}^1(\mathbf{F}_q)$*. It has order* $q(q-1)/2$ *when* q *is odd and* $q(q-1)$ *when* q *is even.*
(ii) *(Sub-line) The stabilizer* $\mathrm{PGL}_2(\mathbf{F}_{q'}) \cap \mathrm{PSL}_2(\mathbf{F}_q)$ *of a sub-line* $\mathbf{P}^1(\mathbf{F}_{q'})$*, where* $q = q'^{\ell}$ *with a prime* ℓ *(in particular,* $\ell \mid 2e$*).*
(iii) *(Dihedral) Stabilizers of a pair of points in* $\mathbf{P}^1(\mathbf{F}_q)$ *(normalizer of a split Cartan subgroup, order* $q-1$ *for* $q \neq 9$ *odd and* $2(q-1)$ *for* q *even) or of a pair of* $\mathbf{F}_q$*-conjugate points in* $\mathbf{P}^1(\mathbf{F}_{q^2})$ *(normalizer of a nonsplit Cartan subgroup, order* $q+1$ *for* $q \neq 9$ *odd and* $2(q+1)$ *for* q *even).*
(iv) *(Exceptional) Subgroups isomorphic to* S_4 *(when* $e = 1$ *and* $3 < p \equiv \pm 3 \bmod 8$*), or* A_5 *(when* $e = 1$ *and* $p \equiv \pm 3 \bmod 10$*).*

Proof. See [62, Corollary 2.2], taking into account that q is an even power of p. □

When $q = 4$, the sub-line and normalizer of a split Cartan case are in the same conjugacy class. When $q = 9$, the normalizers of split Cartan subgroups are contained in exceptional subgroups of type A_5, and the normalizers of nonsplit Cartan subgroups are contained in sub-line stabilizers.

When $\deg \mathfrak{p}$ is odd, we have $\mathbf{P}G_{\mathfrak{p}}^{\max} = \mathrm{PGL}_2(\mathbf{F}_{\mathfrak{p}})$. Since $\det(G_{\mathfrak{p}}) = \mathbf{F}_p^{\times}$ contains elements of $\mathbf{F}_{\mathfrak{p}}^{\times}$ that are non-squares in this case, we also know that $\mathbf{P}G_{\mathfrak{p}}$ is not contained in $\mathrm{PSL}_2(\mathbf{F}_{\mathfrak{p}})$.

Theorem 2.14 (Maximal subgroups of $\mathbf{P}G_{\mathfrak{p}}^{\max}$, $\deg \mathfrak{p}$ odd). *Let* $p \neq 2$ *be a prime and let* $q = p^{2e+1}$ *be an odd power of* p*. The maximal subgroups of* $\mathrm{PGL}_2(\mathbf{F}_q)$ *different from* $\mathrm{PSL}_2(\mathbf{F}_q)$ *are as follows.*

(i) *(Borel) The stabilizer of a point of* $\mathbf{P}^1(\mathbf{F}_q)$*. It has order* $q(q-1)$*.*
(ii) *(Sub-line) The stabilizer* $\mathrm{PGL}_2(\mathbf{F}_{q'})$ *of a sub-line* $\mathbf{P}^1(\mathbf{F}_{q'})$*, where* $q = q'^{\ell}$ *with a prime* ℓ *(in particular,* $\ell \mid 2e+1$*).*
(iii) *(Dihedral) Stabilizers of a pair of points in* $\mathbf{P}^1(\mathbf{F}_q)$ *(normalizer of a split Cartan subgroup, order* $2(q-1)$*, when* $q > 5$*) or of a pair of* $\mathbf{F}_q$*-conjugate points in* $\mathbf{P}^1(\mathbf{F}_{q^2})$ *(normalizer of a nonsplit Cartan subgroup, order* $2(q+1)$*).*
(iv) *(Exceptional) Subgroups isomorphic to* S_4 *(when* $e = 0$ *and* $3 < p \equiv \pm 3 \bmod 8$*), and if* $q = 3$*,* A_4*.*

Proof. See [62, Corollary 2.3], which excludes $q = 3$. For $q = 3$, Magma computes that $\mathrm{PGL}_2(\mathbf{F}_3) \cong S_4$ has 3 maximal subgroups, S_3, D_4, A_4, which correspond to the Borel, normalizer of nonsplit Cartan and exceptional maximal subgroup case, respectively. □

Definition 2.15. We say that $\rho_{\mathfrak{p}}$ or $G_{\mathfrak{p}}$ is *Borel*, *sub-line*, *dihedral* or *exceptional* when $\mathbf{P}G_{\mathfrak{p}}$ is contained in a maximal subgroup of $\mathbf{P}G_{\mathfrak{p}}^{\max}$ of the corresponding type. In the dihedral case, we distinguish between *split* and *nonsplit*, according to the Cartan subgroup involved. We say that $\rho_{\mathfrak{p}}$ or $G_{\mathfrak{p}}$ is *reducible* or *irreducible* if the action of $G_{\mathfrak{p}}$ on $\mathbf{F}_{\mathfrak{p}}^2$ is, and we say that it is *maximal* if $G_{\mathfrak{p}} = G_{\mathfrak{p}}^{\max}$.

The action of $G_{\mathfrak{p}}$ is reducible if and only if $\rho_{\mathfrak{p}}$ is Borel. In the sub-line case, the invariant sub-line can be the image of a nontrivial invariant subspace of $A[\mathfrak{p}]$ considered as an $\mathbf{F}_p$-vector space. In this case (if $\rho_{\mathfrak{p}}$ is not also Borel), $\rho_{\mathfrak{p}}$ is irreducible as a 2-dimensional $\mathbf{F}_{\mathfrak{p}}$-representation, but reducible as a $2(\deg \mathfrak{p})$-dimensional $\mathbf{F}_p$-representation. See Section 2.10 below for a more detailed discussion.

2.5. Irreducibility and maximality criteria for fixed $\mathfrak{p}$

In this section, we collect some criteria that allow us to verify that $\rho_{\mathfrak{p}}$ is irreducible or maximal for a given prime ideal $\mathfrak{p}$, using information from the characteristic polynomials of $\rho_{\mathfrak{p}}(\mathrm{Frob}_{\ell})$ for $\ell \nmid Np$. Recall from theorem 2.6 that the characteristic polynomial of $\rho_{\mathfrak{p}}(\mathrm{Frob}_{\ell})$ has the form

$$T^2 - \bar{a}_{\ell} T + \bar{\ell},$$

where $x \mapsto \bar{x}$ denotes the reduction homomorphism $\mathbf{Z}[f] \to \mathbf{F}_{\mathfrak{p}}$.

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

We define some invariants associated to elements of $\mathrm{PGL}_2(\mathbf{F}_\mathfrak{p})$; see [98, §2]. For $\mathbf{F}$ a finite field of odd characteristic, we define the Legendre symbol for $a \in \mathbf{F}$ as usual:

$$\left(\frac{a}{\mathbf{F}}\right) = \begin{cases} 0 & \text{if } a = 0, \\ 1 & \text{if } a = b^2 \text{ for some } b \in \mathbf{F}^\times, \\ -1 & \text{otherwise.} \end{cases}$$

Lemma 2.16. *Let* $\mathbf{F}$ *be a finite field.*

(1) *The function*

$$\mathrm{GL}_2(\mathbf{F}) \longrightarrow \mathbf{F}, \quad M \longmapsto \frac{\mathrm{Tr}(M)^2}{\det(M)}$$

descends to a function $u\colon\ \mathrm{PGL}_2(\mathbf{F}) \longrightarrow \mathbf{F}$.

(2) *Assume that* $\mathbf{F}$ *has characteristic* $p \neq 2$. *The function*

$$\mathrm{GL}_2(\mathbf{F}) \longrightarrow \{0, 1, -1\}, \quad M \longmapsto \left(\frac{\mathrm{Tr}(M)^2 - 4\det(M)}{\mathbf{F}}\right)$$

descends to $\Delta\colon\ \mathrm{PGL}_2(\mathbf{F}) \longrightarrow \{0, 1, -1\}$.

Proof. Since Tr^2 and det are both homogeneous of degree 2 and $\det(M) \neq 0$, the existence of u follows. Similarly, $\mathrm{Tr}(M)^2 - 4\det(M)$ is well-defined up to multiplication with a nonzero square, so the Legendre symbol is well-defined. □

We now assume that the characteristic of $\mathbf{F}$ is odd.

If $u(g) \neq 0$ (equivalently, $\mathrm{Tr}(M) \neq 0$, where M is a lift of g to $\mathrm{GL}_2(\mathbf{F})$), then $\Delta(g) = \left(\frac{u(g)(u(g)-4)}{\mathbf{F}}\right)$. If $u(g) = 0$, then $\Delta(g) = \left(\frac{-\det(M)}{\mathbf{F}}\right) \neq 0$, so $\Delta(g) = 0$ is equivalent to $u(g) = 4$.

We note that $\Delta(g)$ gives the square class of the discriminant of the characteristic polynomial of any lift M of g to $\mathrm{GL}_2(\mathbf{F})$. This implies that $\Delta(g) \neq 0$ if and only if M has distinct eigenvalues (and hence is semi-simple). The eigenvalues are in $\mathbf{F}$ when $\Delta(g) = 1$ and in the quadratic extension of $\mathbf{F}$ and conjugate when $\Delta(g) = -1$. It follows that the elements of any Borel subgroup of $\mathrm{PGL}_2(\mathbf{F})$ have $\Delta \neq -1$. We therefore obtain the following.

Corollary 2.17. *Let* $\mathfrak{p}$ *be a prime ideal of odd residue characteristic. If* $\Delta(g) = -1$ *for some* $g \in \mathbf{P}G_\mathfrak{p}$, *then* $\rho_\mathfrak{p}$ *is irreducible.*

Proof. If $\rho_\mathfrak{p}$ were reducible, then $\mathbf{P}G_\mathfrak{p}$ would be contained in a Borel subgroup, and so $\Delta(\mathbf{P}G_\mathfrak{p}) \subseteq \{0, 1\}$, contradicting the assumption. □

This gives a method to prove the irreducibility of $\rho_\mathfrak{p}$ by computing

$$\Delta(\mathbf{P}\rho_\mathfrak{p}(\mathrm{Frob}_\ell)) = \left(\frac{a_\ell^2 - 4\ell}{\mathbf{F}_\mathfrak{p}}\right)$$

for a number of primes $\ell \nmid Np(\mathfrak{p})$. If we obtain the value -1 for one such ℓ, this shows that $\rho_\mathfrak{p}$ is irreducible.

We can use the invariant $u(g)$ to obtain information on the order of g. (See [98, §2.6 iii].)

Proposition 2.18. *Let* $\mathbf{F}$ *be a finite field of characteristic* p *and let* $g \in \mathrm{PGL}_2(\mathbf{F})$.

(1) g *is unipotent* $\iff u(g) = 4 \iff \Delta(g) = 0$.
(2) *If* $p \neq 2$*:* $\mathrm{ord}(g) = 2 \iff u(g) = 0$.
(3) *If* $p \neq 3$*:* $\mathrm{ord}(g) = 3 \iff u(g) = 1$.

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

(4) *If* $p \neq 2$*:* $\operatorname{ord}(g) = 4 \iff u(g) = 2$.
(5) *If* $p \neq 5$*:* $\operatorname{ord}(g) = 5 \iff u(g)^2 - 3u(g) + 1 = 0$.

Proof. Let $g = \mathbf{P}M$ for some $M \in \mathrm{GL}_2(\mathbf{F})$. If $\Delta(g) \neq 0$ (equivalently, $u(g) \neq 4$), then M is semi-simple by the discussion above, and so, up to scaling, we can diagonalize M over $\bar{\mathbf{F}}$ as $M \sim \operatorname{diag}(1, \zeta)$, where ζ is some root of unity of order $\operatorname{ord}(g)$. Then $u(g) = (1+\zeta)^2/\zeta = \zeta + 2 + \zeta^{-1}$. Two values of u agree if and only if the corresponding values of ζ are either equal or inverses of each other. Claim (1) follows from the discussion above, and the others follow by observing that the condition on p ensures that the corresponding $u(g)$ is not equal to 4 and by matching roots of unity ζ with u: $\zeta = -1 \iff u = 0$, $\operatorname{ord}(\zeta) = 3 \iff \zeta + \zeta^{-1} = -1 \iff u = 1$, $\operatorname{ord}(\zeta) = 4 \iff \zeta + \zeta^{-1} = 0 \iff u = 2$, and the two values of $\zeta + 2 + \zeta^{-1}$ for a fifth root of unity ζ are the roots of $u^2 - 3u + 1$. □

We can use this to show that $\rho_{\mathfrak{p}}$ is not exceptional since the elements of S_4 have order at most 4 and the elements of A_5 have order 5 or at most 3. So if we can find an element $g \in \mathbf{P}G_{\mathfrak{p}}$ of order at least 5, then $\mathbf{P}G_{\mathfrak{p}} \not\subseteq S_4$, and if we can find an element of order 4 or at least 6, then $\mathbf{P}G_{\mathfrak{p}} \not\subseteq A_5$.

We now want to rule out the other possible maximal subgroups.

If $\rho_{\mathfrak{p}}$ is dihedral, then $\mathbf{P}G_{\mathfrak{p}}$ is contained in the normalizer $N(C)$ either of a split or of a nonsplit Cartan subgroup C. The elements of $N(C) \setminus C$ have order 2; hence, $u = 0$. If C is split, then the nontrivial elements of C have $\Delta = 1$; if C is nonsplit, its nontrivial elements have $\Delta = -1$. So if we find elements in $\mathbf{P}G_{\mathfrak{p}}$ with $\Delta = 1$ and $u \neq 0$ and also elements with $\Delta = -1$ and $u \neq 0$, then $\mathbf{P}G_{\mathfrak{p}}$ cannot be dihedral.

For the sub-line case, we restrict to $\deg \mathfrak{p} \leq 2$. If $\rho_{\mathfrak{p}}$ is sub-line, we must then have $\deg \mathfrak{p} = 2$, and $\mathbf{P}G_{\mathfrak{p}} \subseteq \mathrm{PGL}_2(\mathbf{F}_p)$ (up to conjugation in $\mathrm{PGL}_2(\mathbf{F}_{\mathfrak{p}})$). Since clearly $u(g) \in \mathbf{F}_p$ for each element $g \in \mathrm{PGL}_2(\mathbf{F}_p) \subset \mathrm{PSL}_2(\mathbf{F}_{\mathfrak{p}})$, we can exclude the sub-line case when we find an element $g \in \mathbf{P}G_{\mathfrak{p}}$ such that $u(g) \in \mathbf{F}_{\mathfrak{p}} \setminus \mathbf{F}_p$. Without the restriction on $\deg \mathfrak{p}$, we can similarly exclude the sub-line case when we find $g \in \mathbf{P}G_{\mathfrak{p}}$ such that $\mathbf{F}_p(u(g)) = \mathbf{F}_{\mathfrak{p}}$. It is also the case that the discriminant of the characteristic polynomial of any element is in $\mathbf{F}_p$ (up to squares in $\mathbf{F}_{\mathfrak{p}}^\times$) and therefore a square in $\mathbf{F}_{\mathfrak{p}}$, so that $\Delta \in \{0, 1\}$. So, similar to the Borel case, this case can also be ruled out as soon as we find an element with $\Delta = -1$. (This last argument is specific to $\deg \mathfrak{p} = 2^n$ for some n.)

Assuming that we already know that the image is not exceptional, we can therefore prove that it is maximal by considering primes $\ell \nmid Np$, computing

$$\Delta(\ell) := \Delta(\mathbf{P}\rho_{\mathfrak{p}}(\mathrm{Frob}_\ell)) = \left(\frac{a_\ell^2 - 4\ell}{\mathbf{F}_{\mathfrak{p}}}\right)$$

until we have found one ℓ such that $\Delta(\ell) = -1$ and $\mathfrak{p} \nmid a_\ell$ and another ℓ such that $\Delta(\ell) = 1$ and $\mathfrak{p} \nmid a_\ell$. (Recall that $u(\mathbf{P}\rho_{\mathfrak{p}}(\mathrm{Frob}_\ell)) \neq 0 \iff \mathfrak{p} \nmid a_\ell$).

We obtain the following algorithm that returns a set of possible types of subgroups of $\mathbf{P}G_{\mathfrak{p}}^{\max}$ that can contain $\mathbf{P}G_{\mathfrak{p}}$. If this set is empty, then $\rho_{\mathfrak{p}}$ has maximal image. We assume $g = 2$ here since the discussion of the sub-line case above was assuming $\deg \mathfrak{p} \leq 2$, and $g = 2$ is our main case of interest. The algorithm can be modified to work for general g if desired.

We use the symbols S_4 and A_5 to denote subgroups isomorphic to the respective groups, R ('reducible') for a Borel subgroup, L for a sub-line stabilizer, and N_s and N_{ns} for the normalizers of a split or nonsplit Cartan subgroup.

Algorithm 2.19.

Input: A newform $f \in \mathcal{N}(N, 2)$. A prime ideal $\mathfrak{p}$ of the maximal order $\mathcal{O}$ of $\mathbf{Z}[f]$. A bound B.
Output: A subset of $\{R, L, N_s, N_{ns}, S_4, A_5\}$ such that if a type is not in the set, then $\mathbf{P}G_{\mathfrak{p}}$ is not contained in a maximal subgroup of $\mathbf{P}G_{\mathfrak{p}}^{\max}$ of this type.

```
1. [Initialize] Set $S := \{R, L, N_s, N_{ns}, S_4, A_5\}$. Set $p := p(\mathfrak{p})$.
2. [Degree 1] If $\deg \mathfrak{p} = 1$:
```

   a. Remove L and A_5 from S.
   b. If $p \in \{2, 3\}$, then remove N_s and S_4 from S.

3. [Degree 2] If $\deg \mathfrak{p} = 2$:
   a. If $p = 2$, then remove N_s, S_4 and A_5 from S.
   b. If $p = 3$, then remove N_s, N_{ns} and S_4 from S.
   c. If $p \geq 5$ and $p^2 \nmid N$, then remove N_{ns} from S.
   d. If $p \not\equiv \pm 3 \bmod 10$, then remove A_5 from S.
4. [S_4 possible?] If $p \not\equiv \pm 3 \bmod 8$, then remove S_4 from S.
5. [Loop over primes] For each prime $\ell \leq B$ such that $\ell \nmid Np$:
   a. Compute the image $u(\ell)$ of a_ℓ^2/ℓ in $\mathbf{F}_\mathfrak{p}$.
   b. If $p \neq 2$, then compute $\Delta(\ell) := \left(\frac{a_\ell^2 - 4\ell}{\mathbf{F}_\mathfrak{p}}\right)$.
   c. If $u(\ell) \notin \{0, 1, 2, 4\}$, then remove S_4 from S.
   d. If $u(\ell) \notin \{0, 1, 4\}$ and $u(\ell)^2 - 3u(\ell) + 1 \neq 0$, then remove A_5 from S.
   e. If $\deg \mathfrak{p} = 2$ and $u(\ell) \notin \mathbf{F}_p$, then remove L from S.
   f. If $p = 2$, $\deg \mathfrak{p} = 1$ and $u(\ell) = 1$, then remove R from S.
   g. If $p = 2$ and $\deg \mathfrak{p} = 2$, then remove R from S.
      If in addition $u(\ell) = 1$, then remove N_{ns} from S.
   h. If $p \neq 2$ and $\Delta(\ell) = -1$, then remove R and L from S.
      If in addition $u(\ell) \neq 0$, then remove N_s from S.
   i. If $p \neq 2$, $\Delta(\ell) = 1$ and $u(\ell) \neq 0$, then remove N_{ns} from S.
   j. If $S = \emptyset$, then return $\emptyset$.
6. Return S.

The correctness of the algorithm follows from the classification results in Section 2.4 and the discussion in this section. The fact that N_{ns} can be excluded when $\deg \mathfrak{p} = 2$ in Step 3c follows from corollary 2.24 below.

If the image is indeed maximal, then $\mathbf{P}G_\mathfrak{p} = \mathbf{P}G_\mathfrak{p}^{\max}$ contains elements with $u \neq 0$ and $\Delta = 1$, with $u \neq 0$ and $\Delta = -1$, of order ≥ 6 (when $p \geq 5$) and of order 4. Chebotarëv's density theorem then guarantees that suitable primes ℓ exist to rule out all the possible types. Using an effective version of the density theorem would give an explicit bound B for the primes ℓ that have to be considered in the algorithm to be able to decide whether $\rho_\mathfrak{p}$ has maximal image. This bound will be too large to be useful in practice, however.

2.6. *Explicit computation*

When algorithm 2.19 returns a nonempty set of types, we can try to determine the image explicitly as follows. We assume that we have given a curve X of genus 2 over $\mathbf{Q}$ whose Jacobian J is isogenous to A_f; we will determine the image of $\rho_{J,\mathfrak{p}}$ (which has the same semi-simplification as $\rho_{\mathfrak{p},f}$), assuming that $\mathfrak{p}$ is a regular prime of $\mathrm{End}_\mathbf{Q}(J)$.

We compute (using Magma, say) the big period matrix associated to J, which allows us to write $J(\mathbf{C}) = \mathbf{C}^2/\Lambda$ for some (numerically) explicit lattice Λ. We can also determine the action of $\mathrm{End}(J)$ on $\mathbf{C}^2$, and so we can approximate numerically the points in $J(\mathbf{C})[\mathfrak{p}]$. We represent these points by (numerical) divisors on X, which we then recognize as divisors supported in algebraic points (this will work when the precision is sufficiently large). We then verify that the algebraic points on J we obtain are indeed in $J[\mathfrak{p}]$. Knowing the points explicitly as algebraic points allows us to determine the Galois action.

Since Magma can easily determine the torsion subgroup of $J(\mathbf{Q})$ using the algorithm described in [111, §11], we can at least deduce that the representation associated to some prime ideal $\mathfrak{p}$ with $p(\mathfrak{p}) = p$ is reducible if $J(\mathbf{Q})[p]$ is nontrivial.

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

Examples 2.20. We give two examples for such an explicit computation.

(1) $A = J_0(125)^+$ with endomorphism ring the maximal order of $\mathbf{Q}(\sqrt{5})$. The representation $\rho_{\langle\sqrt{5}\rangle}$ is reducible. $A[\sqrt{5}]$ has constituents $\mu_5^{\otimes 2}$ and $\mu_5^{\otimes 3}$. In this case, $5 \nmid [\mathbf{Q}(A[\sqrt{5}]) : \mathbf{Q}]$, so

$$A[\sqrt{5}] \cong \mu_5^{\otimes 2} \oplus \mu_5^{\otimes 3}.$$

(2) $A = J_0(147)^{\langle w_3, w_{49}\rangle}$ with endomorphism ring the maximal order of $\mathbf{Q}(\sqrt{2})$. There is a prime $\mathfrak{p} \mid 7$ in $\operatorname{End}(A)$ such that $\rho_{\mathfrak{p}}$ is reducible. We find that its irreducible constituents are $\mu_7^{\otimes 3}$ and $\mu_7^{\otimes 4}$. As $[\mathbf{Q}(A[\mathfrak{p}]) : \mathbf{Q}] = 7 \cdot (7-1)$ and $A[7](\mathbf{Q}(\sqrt{-7})) = A[7](\mathbf{Q}(\mu_7^{\otimes 3})) = 0$, one has a nonsplit short exact sequence of Galois modules

$$0 \to \mu_7^{\otimes 4} \to A[\mathfrak{p}] \to \mu_7^{\otimes 3} \to 0.$$

2.7. *The image of inertia at p*

Our next goal will be to prove that $\rho_{\mathfrak{p}}$ is irreducible (or even maximal) for all but finitely many $\mathfrak{p}$, with a small explicit set of possible exceptions. To this end, we need to study the representations $\rho_{\mathfrak{p}}$ more carefully, so that we can extract some uniform statements. We begin by considering the action of the inertia group at the prime p. Recall the definitions and the notations I_p, I_p^{w}, I_p^{t} from Section 2.1. Also recall the fundamental characters ψ_k from definition 2.8. In the following, g is arbitrary again.

We now consider $\rho_{\mathfrak{p}}|_{I_p}$, where $p = p(\mathfrak{p})$ is the residue characteristic of $\mathfrak{p}$. We have the following result.

Theorem 2.21. *Assume $p^2 \nmid N$. Exactly one of the following two statements is true.*

(i) *$\rho_{\mathfrak{p}}|_{I_p}$ has, up to conjugation, the form*

$$\begin{pmatrix} \chi_p^n & * \\ 0 & \chi_p^{1-n} \end{pmatrix}$$

for some $n \in \{0, 1\}$.

(ii) *After extending to the quadratic extension of $\mathbf{F}_{\mathfrak{p}}$ when $\deg \mathfrak{p}$ is odd, $\rho_{\mathfrak{p}}|_{I_p}$ has, up to conjugation, the form*

$$\begin{pmatrix} \psi_2 & 0 \\ 0 & \psi_2^p \end{pmatrix}.$$

Proof. By [97, Prop. 1], the claim is true up to the exponents of the characters. (Note that according to *loc. cit.*, fundamental characters of level > 2 cannot occur.) By [87, Cor. 3.4.4], as extended via [66, Lemma 4.9] to the semistable case, the characters must be among χ_p^0 and χ_p^1 in the first case, and among $\psi_2^0, \psi_2^1, \psi_2^p$ and ψ_2^{p+1} in the second case. The condition that $\det \circ \rho_{\mathfrak{p}} = \chi_p = \psi_2^{p+1}$, together with the fact that the characters are conjugate in the second case, then fixes the exponents. See also [69, Thm. 3.6]. □

Definition 2.22. In case (i), we say that $\rho_{\mathfrak{p}}|_{I_p}$ has *level 1*, and in case (ii), $\rho_{\mathfrak{p}}|_{I_p}$ has *level 2*.

Corollary 2.23. *Assume $p^2 \nmid N$. When $\rho_{\mathfrak{p}}|_{I_p}$ has level 1, then $\mathbf{P}\rho_{\mathfrak{p}}(I_p)$ contains a cyclic subgroup of order $p-1$ of a split Cartan subgroup. In the case of level 2, $\mathbf{P}\rho_{\mathfrak{p}}(I_p)$ is cyclic of order $p+1$.*

Proof. This follows immediately from theorem 2.21. □

Corollary 2.24. *If $\deg \mathfrak{p}$ is even and $p > 3$ with $p^2 \nmid N$, then $\mathbf{P}G_{\mathfrak{p}}$ cannot be contained in the normalizer of a nonsplit Cartan subgroup.*

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

Proof. By corollary 2.23, $\mathbf{P}G_{\mathfrak{p}}$ contains elements of order $\geq p-1 > 2$. Since $\deg \mathfrak{p}$ is even, no quadratic extension is necessary in theorem 2.21 in the level 2 case, so in all cases, we find elements of order > 2 in a *split* Cartan subgroup. Since such elements lie in a unique Cartan subgroup (which is the centralizer of the element) and the normalizer of a nonsplit Cartan subgroup contains only one Cartan subgroup, the claim follows. □

Lemma 2.25. *Let* $\chi \colon \operatorname{Gal}(\overline{\mathbf{Q}}_p|\mathbf{Q}_p) \to \mathbf{F}^\times$ *be a one-dimensional character of order prime to p. Then* $\chi|_{I_p}$ *is a power of* χ_p.

Proof. Since χ has order prime to p and I_p^{w} is a pro-p group, its image under χ must be trivial, so χ is at most tamely ramified. Since $\mathbf{Q}_p^{\mathrm{nr}}(\mu_p)$ is the maximal abelian tamely ramified extension of $\mathbf{Q}_p^{\mathrm{nr}}$, $\chi|_{I_p}$ must factor through $I_p \to I_p^{\mathrm{t}} \to \mathbf{F}_p^\times$, which implies the claim. □

Corollary 2.26. *Let* $\mathfrak{p}$ *be a regular prime of* $\mathbf{Z}[f]$ *of residue characteristic p and assume that* $\rho_{\mathfrak{p}}$ *is reducible and* $p^2 \nmid N$. *Then there is a character* ε *of* $\operatorname{Gal}(\overline{\mathbf{Q}}|\mathbf{Q})$ *with values in* $\mathbf{F}_{\mathfrak{p}}^\times$ *and conductor d such that* $d^2 \mid N$ *and (with respect to a suitable basis)*

$$\rho_{\mathfrak{p}} = \begin{pmatrix} \varepsilon\chi_p^n & * \\ 0 & \varepsilon^{-1}\chi_p^{1-n} \end{pmatrix}$$

with $n = 0$ *or* $n = 1$.

Proof. The semi-simplification of $\rho_{\mathfrak{p}}$ splits as a direct sum $\pi_1 \oplus \pi_2$ of one-dimensional characters $\pi_1, \pi_2 \colon \operatorname{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}) \to \mathbf{F}_{\mathfrak{p}}^\times$. By lemma 2.25, $\pi_1|_{I_p} = \chi_p^n$ for some n, and so $\pi_2|_{I_p} = \chi_p^{1-n}$. We can therefore write $\pi_1 = \varepsilon\chi_p^n$ with some character ε that is unramified at p. Since $\chi_p = \det \circ \rho_{\mathfrak{p}} = \pi_1 \cdot \pi_2$, it follows that $\pi_2 = \varepsilon^{-1}\chi_p^{1-n}$. We then have

$$d^2 = \operatorname{cond}(\varepsilon)\operatorname{cond}(\varepsilon^{-1}) \mid \operatorname{cond}(\rho_{\mathfrak{p}}) \mid N\,.$$

Since $p^2 \nmid N$, we have $n \in \{0, 1\}$ by theorem 2.21. □

Remark 2.27. One can use this to refine algorithm 2.19 by potentially eliminating type R in more cases. For each prime $\ell \nmid Np$, compare the reduction of $a_\ell \bmod \mathfrak{p}$ with all elements of the form $\varepsilon(\ell)\ell^n + \varepsilon(\ell)^{-1}\ell^{1-n}$ for the finitely many possible characters ε and $n \in \{0, 1\}$, and let S_ℓ be the set of compatible pairs (ε, n). Then one takes the intersection of the sets S_ℓ for several ℓ. If the intersection is empty, then $\rho_{\mathfrak{p}}$ must be irreducible.

Examples 2.28. We give two examples that illustrate corollary 2.26. In order to determine whether $G_{\mathfrak{p}}$ has a nontrivial unipotent part, we determine explicit generators of $A[\mathfrak{p}](\overline{\mathbf{Q}})$, which allows us to find $[\mathbf{Q}(A[\mathfrak{p}]) : \mathbf{Q}]$ (and, in fact, to determine the Galois action); see Section 2.6.

(1) $A = J_0(39)^{w_{13}}$ with endomorphism ring the maximal order of $\mathbf{Q}(\sqrt{2})$. There is exactly one prime $\mathfrak{p} \mid 7$ such that $\rho_{\mathfrak{p}}$ is reducible. Since 39 is squarefree, $\rho_{\mathfrak{p}}^{\mathrm{ss}} \cong 1 \oplus \chi_7$. We find that $A[\mathfrak{p}](\mathbf{Q}) \cong \mathbf{Z}/7\mathbf{Z}$, so we have a short exact sequence

$$0 \to \mathbf{Z}/7\mathbf{Z} \to A[\mathfrak{p}] \to \mu_7 \to 0,$$

which turns out to be nonsplit since $[\mathbf{Q}(A[\mathfrak{p}]) : \mathbf{Q}]$ is divisible by 7.

(2) $A = J_0(87)^{w_{29}}$ with endomorphism ring the maximal order of $\mathbf{Q}(\sqrt{5})$. The representation $\rho_{\langle\sqrt{5}\rangle}$ is reducible. Similarly as in Example (1), the constituents are $\mathbf{Z}/5\mathbf{Z}$ and μ_5. Since $A[\sqrt{5}](\mathbf{Q}) \cong \mathbf{Z}/5\mathbf{Z}$, we have the exact sequence

$$0 \to \mathbf{Z}/5\mathbf{Z} \to A[\mathfrak{p}] \to \mu_5 \to 0,$$

which is again nonsplit.

We now consider the case that $\rho_{\mathfrak{p}}(\mathrm{Gal}(\overline{\mathbf{Q}}_p|\mathbf{Q}_p))$ is contained in the normalizer of a Cartan subgroup of $\mathrm{GL}_2(\mathbf{F}_{\mathfrak{p}})$.

Lemma 2.29. *Assume $\mathfrak{p}$ is a regular prime ideal lying above a rational prime $p > 3$ such that $p^2 \nmid N$ and that $\rho_{\mathfrak{p}}(\mathrm{Gal}(\overline{\mathbf{Q}}_p|\mathbf{Q}_p))$ is contained in the normalizer $N(C)$ of a Cartan subgroup C of $\mathrm{GL}_2(\mathbf{F}_{\mathfrak{p}})$. Then the following are equivalent:*

(i) *$\rho_{\mathfrak{p}}|_{I_p}$ has level 1.*
(ii) *$\rho_{\mathfrak{p}}(\mathrm{Gal}(\overline{\mathbf{Q}}_p|\mathbf{Q}_p)) \subseteq C$.*
(iii) *$\mathbf{P}\rho_{\mathfrak{p}}(\mathrm{Gal}(\overline{\mathbf{Q}}_p|\mathbf{Q}_p)) \subseteq \mathbf{P}C$ has order $p-1$ and C is split.*

Proof. Clearly, (iii) implies (ii) (since $\mathbf{P}^{-1}(\mathbf{P}C) = C$). If (ii) holds, then $\rho_{\mathfrak{p}}(\mathrm{Gal}(\overline{\mathbf{Q}}_p|\mathbf{Q}_p))$ is abelian of order prime to p, so lemma 2.25 implies that $\rho_{\mathfrak{p}}|_{I_p}$ has level 1.

To show that (i) implies (iii), first note that the image of the wild inertia group I_p^{w} must be trivial since I_p^{w} is a pro-p group and the order of $N(C)$ is prime to p (since $p > 2$). So $\rho_{\mathfrak{p}}|_{I_p}$ factors through I_p^{t}, which is pro-cyclic, and hence, $\rho_{\mathfrak{p}}(I_p)$ is a cyclic group, which has order $p-1$ since $\rho_{\mathfrak{p}}|_{I_p}$ has level 1 and $p^2 \nmid N$. Let Frob_p be any lift of the p-Frobenius on $\overline{\mathbf{F}}_p$ to $\mathrm{Gal}(\overline{\mathbf{Q}}_p|\mathbf{Q}_p)$. lemma 2.7 implies that conjugating by $\rho_{\mathfrak{p}}(\mathrm{Frob}_p)$ has the effect of taking pth powers on $\rho_{\mathfrak{p}}(I_p)$. Since $p \equiv 1 \bmod \#\rho_{\mathfrak{p}}(I_p)$, this action is trivial, so the image of Frob_p commutes with the image of I_p. This shows that $\rho_{\mathfrak{p}}(\mathrm{Gal}(\overline{\mathbf{Q}}_p|\mathbf{Q}_p))$ is abelian. Since $\#\rho_{\mathfrak{p}}(\mathrm{Gal}(\overline{\mathbf{Q}}_p|\mathbf{Q}_p))$ contains elements of order $p-1 > 3$, this implies that $\rho_{\mathfrak{p}}(\mathrm{Gal}(\overline{\mathbf{Q}}_p|\mathbf{Q}_p)) \leq C$. (This is where we use that $\rho_{\mathfrak{p}}(\mathrm{Gal}(\overline{\mathbf{Q}}_p|\mathbf{Q}_p)) \leq N(C)$: all the abelian subgroups of $N(C)$ containing elements of order ≥ 3 are contained in C.) From the discussion above, it follows that $\mathbf{P}\rho_{\mathfrak{p}}(I_p)$ has order $p-1$; both statements together imply (iii). □

Corollary 2.30. *Assume $\mathfrak{p}$ is a regular prime ideal lying above a rational prime $p > 3$ such that $p^2 \nmid N$ and that $G_{\mathfrak{p}}$ is contained in a Cartan subgroup C. Then C is split; in particular, $\rho_{\mathfrak{p}}$ is reducible.*

Proof. The assumption implies that $\rho_{\mathfrak{p}}(\mathrm{Gal}(\overline{\mathbf{Q}}_p|\mathbf{Q}_p)) \subseteq G_{\mathfrak{p}} \subseteq C$. The claim then follows from the implication '(ii) $\Rightarrow$ (iii)' in lemma 2.29. □

Corollary 2.31. *Assume $p > 3$ and $p^2 \nmid N$. If $\mathbf{P}G_{\mathfrak{p}}$ is dihedral, then $\mathbf{P}\rho_{\mathfrak{p}}(I_p)$ is cyclic and contained in the corresponding Cartan subgroup C.*

Proof. The first statement follows as in the proof of lemma 2.29. The second statement follows from the classification of $\rho_{\mathfrak{p}}(I_p)$. □

2.8. *The image of inertia at a prime $\ell \neq p$*

We now consider the image $\rho_{\mathfrak{p}}(I_\ell)$ of the inertia subgroup at a prime $\ell \neq p$.

Lemma 2.32. *Let $\mathfrak{p}$ be a regular prime ideal of $\mathbf{Z}[f]$ of residue characteristic p and let $\ell \neq p$ be a prime. If $\ell^2 \nmid N$, then the image $\rho_{\mathfrak{p}}(I_\ell)$ of the inertia subgroup at ℓ consists of unipotent elements.*

Proof. If $\ell \nmid N$, then $\rho_{\mathfrak{p}}$ is unramified at ℓ, and so the image of inertia is trivial. Otherwise, since the prime-to-p part of the Artin conductor of $\rho_{\mathfrak{p}}$ divides the prime-to-p part of N, it follows from $v_\ell(N) = 1$ that the image of wild inertia is trivial and that the image of inertia has a one-dimensional fixed subspace; see [97, p. 181]. So

$$\rho_{\mathfrak{p}}|_{I_\ell} \sim \begin{pmatrix} 1 & * \\ 0 & \chi_p \end{pmatrix}.$$

Since χ_p is unramified at ℓ, this implies that $\rho_{\mathfrak{p}}(I_\ell)$ is unipotent. (See also [90, Section 2]; note that the definition of the conductor is purely local.) □

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

Corollary 2.33. *Let $\mathfrak{p}$ be a regular prime ideal of $\mathbf{Z}[f]$ of residue characteristic p and assume that $G_\mathfrak{p}$ is contained in the normalizer $N(C)$ of a Cartan subgroup C. Then $\rho_\mathfrak{p}$ is unramified at all primes $\ell \neq p$ such that $\ell^2 \nmid N$.*

Proof. This follows from lemma 2.32 since $N(C)$ contains no nontrivial unipotent elements. □

Corollary 2.34. *Let $\mathfrak{p}$ be a regular prime ideal of $\mathbf{Z}[f]$ of residue characteristic $p > 3$ and assume that $G_\mathfrak{p}$ is contained in the normalizer $N(C)$ of a Cartan subgroup C. Since C has index 2 in $N(C)$, we obtain a quadratic character (which can be trivial)*

$$\varepsilon_\mathfrak{p} \colon \mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}) \xrightarrow{\rho_\mathfrak{p}} N(C) \to N(C)/C \simeq \{\pm 1\};$$

let d be its conductor. Then the odd part of d^2 divides N. Moreover, if $4 \nmid N$, then $d^2 \mid N$.

Proof. Note that the odd part of d is squarefree. Let $\ell \neq p$ be an odd prime. If $\ell^2 \nmid N$, then $\rho_\mathfrak{p}$ is unramified at ℓ by corollary 2.33, and so $\ell \nmid d$. This shows the claim except for powers of 2 or p. If $p^2 \nmid N$, then $\rho_\mathfrak{p}(I_p) \subseteq C$ by corollary 2.31 (here, we use $p > 3$), and so $\varepsilon_\mathfrak{p}$ is unramified at p. This takes care of the power of p. If $4 \nmid N$, corollary 2.33 applies as well to show that $2 \nmid d$. This completes the proof. □

Question 2.35. Can the stronger statement be extended to the case $4 \mid N$?

Corollary 2.36. *Let $p > 2$ be prime and let $K|\mathbf{Q}$ be an imaginary quadratic extension such that N and D_K are coprime and K is not equal to $\mathbf{Q}(\sqrt{-1})$, $\mathbf{Q}(\sqrt{-2})$, or $\mathbf{Q}(\sqrt{-3})$. If $\rho_\mathfrak{p}$ is irreducible, then the restriction $\rho_\mathfrak{p}|_{G_K}$ is still irreducible.*

Proof. Suppose that $\rho_\mathfrak{p}$ is irreducible, but $\rho_\mathfrak{p}|_{G_K}$ is reducible. Then the quadratic character on $G_\mathbf{Q}$ associated to $K|\mathbf{Q}$ induces a nontrivial quadratic character ε on the image of $\rho_\mathfrak{p}$: G_K fixes a one-dimensional subspace V, and ε is given by the action on $\{V, \rho_\mathfrak{p}(\sigma)V\}$ for $\sigma \in G_\mathbf{Q} \setminus G_K$. Since $\rho_\mathfrak{p}$ is ramified only at primes dividing Np and $K|\mathbf{Q}$ is ramified exactly at the primes dividing D_K, it follows from the condition that N and D_K are coprime that the conductor $|D_K|$ of ε is a power of p. Since $D_K \neq -3, -4, -8$, we must have $p > 3$ and $D_K = -p$.

Since $\rho_\mathfrak{p}$ fixes an unordered pair of complementary one-dimensional subspaces but does not fix the two subspaces individually, it must be dihedral (compare theorems 2.13 and 2.14). Then ε is the character as in corollary 2.34, so corollary 2.34 implies that $|D_K|^2 = p^2 \mid N$ (here, we use that $p > 3$), contradicting again the coprimality of N and D_K. □

2.9. *Explicit irreducibility for almost all $\mathfrak{p}$*

It is known that $\rho_\mathfrak{p}$ is irreducible for all but finitely many $\mathfrak{p}$. Lombardo [69, Thm. 1.4] gives an explicit (but very large) bound for the reducible primes (actually, for the primes such that the image is not maximal). What we need, however, is to determine as exactly as possible the finite set of primes $\mathfrak{p}$ such that $\rho_\mathfrak{p}$ is reducible in each concrete case.

In view of corollary 2.26, we make the following definition.

Definition 2.37. We write $d_{\max}$ for the largest positive integer d such that $d^2 \mid N$.

We then obtain the following criterion. (Compare [38, §3.1], where similar criteria are used to show that the mod-p Galois representations associated to an abelian surface with minimal endomorphism ring are maximal for almost all primes p.)

Proposition 2.38. *Let $\ell \nmid N$ be a prime and let $m(\ell)$ be the order of ℓ in $(\mathbf{Z}/d_{\max}\mathbf{Z})^\times$. Let $\mathfrak{p}$ be a regular prime of $\mathbf{Z}[f]$ of residue characteristic p. If $p^2 \nmid N$ and*

$$\mathfrak{p} \nmid \ell \cdot \mathrm{res}_T(T^2 - a_\ell T + \ell, T^{m(\ell)} - 1) \in \mathbf{Z}[f],$$

then $\rho_\mathfrak{p}$ is irreducible.

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

We note that when $\varphi(d_{\max}) = 1$ (which is the case, for example, when N is squarefree) or $\ell \equiv 1 \bmod d_{\max}$, the resultant simplifies to $\ell + 1 - a_\ell$.

Proof. Let us prove the contrapositive. Thus, suppose that $\rho_\mathfrak{p}$ is reducible. Let ε be the character in corollary 2.26. It can be considered as a Dirichlet character of conductor $d \mid d_{\max}$ with values in $\mathbf{F}_\mathfrak{p}^\times$. Since $p^2 \nmid N$, we have $n = 0$ or $n = 1$ in corollary 2.26, and by symmetry (and since what we do depends only on the semi-simplification of $\rho_\mathfrak{p}$), we can assume $n = 0$. If $\ell = p$, then $\mathfrak{p} \mid \ell$, and we are done. Hence, suppose $\ell \nmid Np$. Then $\rho_\mathfrak{p}(\mathrm{Frob}_\ell)$ is well-defined and has $\varepsilon(\ell)$ as an eigenvalue, which is also a root of unity of order dividing $m(\ell)$. So the characteristic polynomial $T^2 - \bar{a}_\ell T + \bar{\ell} \in \mathbf{F}_\mathfrak{p}[T]$ of $\rho_\mathfrak{p}(\mathrm{Frob}_\ell)$ has at least one root in common with $T^{m(\ell)} - 1$. This is equivalent to

$$\mathrm{res}_T\,(T^2 - \bar{a}_\ell T + \bar{\ell}, T^{m(\ell)} - 1) = 0\,.$$

Since the resultant is compatible with ring homomorphisms, this implies that $\mathfrak{p}$ divides the resultant in the statement. □

Remark 2.39. One can alternatively consider the condition

$$p \mid \ell \cdot \mathrm{res}_T\left(\mathrm{charpol}(\rho_{p^\infty}(\mathrm{Frob}_\ell))(T), T^{m(\ell)} - 1\right) \in \mathbf{Z}$$

with the same $m(\ell)$ as above. Using the fact that the resultant is the product of all differences of roots of the first and of the second polynomial, together with the Weil conjectures for the characteristic polynomial of Frob_ℓ on T_pA, we see that the resultant above is an integer R satisfying

$$0 < (\sqrt{\ell} - 1)^{2gm(\ell)} < R < (\sqrt{\ell} + 1)^{2gm(\ell)}\,.$$

In particular, it is nonzero, so taking just one $\ell \nmid N$ gives a relatively small bound for the set of primes p such that $\rho_\mathfrak{p}$ is reducible for some $\mathfrak{p} \mid p$. In practice, one takes several ℓ and uses the gcd of the resultants to obtain reasonably sharp bounds.

This leads to the following algorithm. Recall the notation $p(\mathfrak{p})$ for the residue characteristic of the prime ideal $\mathfrak{p}$.

Algorithm 2.40.

Input: A newform $f \in \mathcal{N}(N, g)$. A bound B.
Output: A finite set S of primes of the maximal order $\mathcal{O}$ of $\mathbf{Z}[f]$ such that $\rho_\mathfrak{p}$ is irreducible for all $\mathfrak{p} \notin S$, or 'failure'.

```
1. [Maximal conductor] Compute $d_{\max} := \prod_{p|N} p^{\lfloor v_p(N)/2 \rfloor}$.
2. [Initialization] Let $I := \langle 0 \rangle$ as an ideal of $\mathcal{O}$.
3. [Loop over primes] For all primes $\ell \leq B$ such that $\ell \nmid N$:
   a. Compute the order $m(\ell)$ of $\ell$ in $(\mathbf{Z}/d_{\max}\mathbf{Z})^\times$.
   b. Set $I := I + \langle \ell \cdot \mathrm{res}_T\,(T^2 - a_\ell T + \ell, T^{m(\ell)} - 1) \rangle$.
4. [Result] If $I = \langle 0 \rangle$, then output 'failure', else output $\{\mathfrak{p} : \mathfrak{p} \mid I \mathrm{or} p(\mathfrak{p})^2 \mid N\}$.
```

We can then use algorithm 2.19 on the regular odd primes in S to try to show that $\rho_\mathfrak{p}$ is irreducible even though algorithm 2.40 was unable to prove that. One can also use the idea from remark 2.27.

Remark 2.41. If we take B sufficiently large in algorithm 2.40, then by the Chebotarëv density theorem, the set S that the algorithm returns will contain only the prime ideals $\mathfrak{p}$ such that $p(\mathfrak{p})^2 \mid N$ or that the image of $\rho_\mathfrak{p}$ consists of elements with one eigenvalue in the image of a character of conductor dividing $d_{\max}$. This is compatible with the image being contained in the normalizer of a split Cartan subgroup (but not in the Cartan subgroup itself).

Example 2.42. Let $A = J_0(35)^{w_7}$ be the Jacobian of the modular curve quotient $X_0(35)/\langle w_7 \rangle$, where w_7 denotes the Atkin–Lehner involution. A corresponds to the Galois orbit of size 2 of newforms of level 35, weight 2 and trivial nebentypus. Let$f$ be one of these two newforms. Then $\mathbf{Z}[f]$ is the maximal order of $\mathbf{Q}(\sqrt{17})$. Since the level $N = 35$ is squarefree, $d_{\max} = 1$.

Let $\beta = (1 + \sqrt{17})/2$ be a generator of $\mathbf{Z}[f]$. We then have $a_2 = -\beta$ (for one of the two conjugate newforms), so the resultant is

$$\operatorname{res}_T(T^2 + \beta T + 2, T - 1) = 3 + \beta,$$

which is an element of norm 2^3. This shows that $\rho_{\mathfrak{p}}$ is irreducible for all prime ideals $\mathfrak{p}$ with odd residue characteristic. We also have $a_3 = \beta - 1$, and the corresponding resultant is

$$\operatorname{res}_T(T^2 - (\beta - 1)T + 3, T - 1) = 5 - \beta,$$

whose norm is 2^4 and which is not divisible by 2, so it generates a power of one of the two prime ideals above 2 in $\mathbf{Z}[f]$; explicitly,

$$\langle 5 - \beta \rangle = \langle \beta + 1 \rangle^4 = \mathfrak{p}^4 .$$

Write $\langle 2 \rangle = \mathfrak{p}\mathfrak{p}'$. Then we can deduce that $\rho_{\mathfrak{p}'}$ is irreducible.

Magma computes that $A(\mathbf{Q})_{\text{tors}} \cong \mathbf{Z}/16\mathbf{Z}$. This shows that $\rho_{\mathfrak{p}}$ must be reducible (and that it is nontrivial since $A[\mathfrak{p}](\mathbf{Q}) \cong \mathbf{Z}/2\mathbf{Z}$ and not $(\mathbf{Z}/2\mathbf{Z})^2$).

Example 2.43. We now consider $A = J_0(125)^+$, which corresponds to a Galois orbit of newforms with coefficient ring the maximal order of $\mathbf{Q}(\sqrt{5})$. Let $\alpha = (1+\sqrt{5})/2$. Then we can pick one of the newforms f such that $a_2 = -\alpha$ and $a_3 = \alpha - 2$. Here, $d_{\max} = 5$ and so $m(2) = m(3) = 4$. We find that

$$\begin{aligned} r_2 &:= \operatorname{res}_T(T^2 + \alpha T + 2, T^4 - 1) &&= 15 + 5\alpha \quad \text{and} \\ r_3 &:= \operatorname{res}_T(T^2 - (\alpha - 2)T + 3, T^4 - 1) &&= 90 - 15\alpha\,. \end{aligned}$$

The ideal of $\mathbf{Z}[f]$ generated by $2r_2$ and $3r_3$ has norm 5^2. So the algorithm shows that $\rho_{\mathfrak{p}}$ is irreducible for all primes $\mathfrak{p} \neq \langle \sqrt{5} \rangle$. An explicit computation shows that $\rho_{\langle \sqrt{5} \rangle}$ is reducible; see example 2.20, (1).

2.10. Excluding the sub-line and exceptional cases for almost all $\mathfrak{p}$

In the following, we require that the coefficient field of the newform is of degree 2, and so $\dim A = 2$ as well. This simplifies the discussion of the sub-line case.

Our next goal will be to show that $\rho_{\mathfrak{p}}$ has maximal image for all $\mathfrak{p}$ outside a small explicit finite set. Starting from the result of the previous subsection, it remains to show that for all but a few explicit $\mathfrak{p}$, $\mathbf{P}G_{\mathfrak{p}}$ is not contained in the stabilizer of a sub-line (when $\deg \mathfrak{p} = 2$), in a maximal subgroup of type S_4 or A_5, or in the normalizer of a Cartan subgroup.

We begin with the sub-line case and assume that $\rho_{\mathfrak{p}}$ is irreducible and $p(\mathfrak{p})$ is odd. In this case, $G_{\mathfrak{p}} \subseteq \mathbf{P}^{-1}(\mathrm{PGL}_2(\mathbf{F}_p)) \cap G_{\mathfrak{p}}^{\max}$, which is a group containing $\mathrm{GL}_2(\mathbf{F}_p)$ with index 2. More precisely, let $\alpha \in \mathbf{F}_{\mathfrak{p}}^\times \setminus \mathbf{F}_p^\times$ be such that $\alpha^2 \in \mathbf{F}_p^\times$; then the group is the union of $\mathrm{GL}_2(\mathbf{F}_p)$ and $\alpha\mathrm{GL}_2(\mathbf{F}_p)$. So $G_{\mathfrak{p}}$ stabilizes the union of a 2-dimensional $\mathbf{F}_p$-subspace U (that is not a 1-dimensional $\mathbf{F}_{\mathfrak{p}}$-subspace) of $A[p]$ and αU. If $G_{\mathfrak{p}} \subseteq \mathrm{GL}_2(\mathbf{F}_p)$ (for some choice of $\mathbf{F}_{\mathfrak{p}}$-basis of $A[p]$), then these two $\mathbf{F}_p$-subspaces are fixed individually, and so ρ_p is the direct sum of two copies of a 2-dimensional $\mathrm{Gal}(\bar{\mathbf{Q}}|\mathbf{Q})$-representation over $\mathbf{F}_p$; in particular, ρ_p is reducible. Conversely, if ρ_p is reducible (but $\rho_{\mathfrak{p}}$ is not), then $\mathbf{P}G_{\mathfrak{p}}$ must be contained in the stabilizer of the sub-line that is the image of a 2-dimensional $\mathbf{F}_p$-subspace fixed by $G_{\mathfrak{p}}$. So, by showing that $\rho_{\mathfrak{p}}$ is irreducible and $\mathbf{P}G_{\mathfrak{p}}$ is not contained in the stabilizer of a sub-line, we also show that A has no nontrivial isogenies of degree a power of p.

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

In any case, we know from the discussion in Section 2.5 that the element $u(\mathbf{P}\rho_{\mathfrak{p}}(\mathrm{Frob}_\ell)) = a_\ell^2/\ell \in \mathbf{F}_{\mathfrak{p}}$ must be in $\mathbf{F}_p$ for all $\ell \nmid Np$ if $\mathbf{P}G_{\mathfrak{p}}$ is contained in the stabilizer of a sub-line. This is equivalent to $p \mid a_\ell^2 - a_\ell^{\sigma 2}$, where σ denotes the nontrivial automorphism of $\mathbf{Z}[f]$. Since in our setting, there always are $\mathfrak{p}$ of degree 2 such that $\mathbf{P}G_{\mathfrak{p}}$ does not consist entirely of elements g such that $u(g) \in \mathbf{F}_p$, there will be a set of primes $\ell \nmid N$ of positive density such that $a_\ell^2 \neq a_\ell^{\sigma 2}$. (If f has an inner twist by a quadratic character, then $a_\ell = \pm a_\ell^\sigma$ for almost all ℓ. But in this case, A_f is isogenous to the Weil restriction of an elliptic curve over the quadratic field associated to the character, and so A_f is not absolutely simple.) We can replace $a_\ell^2 - a_\ell^{\sigma 2}$ by $(a_\ell^2 - a_\ell^{\sigma 2})/\sqrt{\mathrm{disc}(\mathbf{Z}[f])} \in \mathbf{Z}$ (note that the prime divisors of $\mathrm{disc}(\mathbf{Z}[f])$ are always ramified, so the corresponding primes of $\mathbf{Z}[f]$ have degree 1). This leads to the following algorithm.

Algorithm 2.44.

Input: A newform $f \in \mathcal{N}(N, 2)$. A bound B.
Output: A finite set S of prime ideals of the maximal order $\mathcal{O}$ of $\mathbf{Z}[f]$ such that $\mathbf{P}G_{\mathfrak{p}}$ is not contained in the stabilizer of a sub-line for all $\mathfrak{p} \notin S$, or ‘failure’.

```
1. [Initialize] Set $R := 0 \in \mathbf{Z}$.
2. [Loop over primes] For all primes $\ell \leq B$ such that $\ell \nmid N$:
   a. Set $R := \gcd(R, \ell \cdot (a_\ell^2 - a_\ell^{\sigma 2})/\sqrt{\mathrm{disc}(\mathbf{Z}[f])})$.
   b. If $R = 1$, then exit the loop.
3. [Result] If $R = 0$, then return ‘failure’,
   else return $\{\mathfrak{p} : p(\mathfrak{p}) \mid R \text{ and } \deg \mathfrak{p} = 2\}$.
```

By the discussion above, the algorithm will not return ‘failure’ when B is sufficiently large.

We now consider the case of exceptional image. Our analysis of the projective image of the inertia group I_p allows us to find elements of order at least 6 in $\mathbf{P}\rho_{\mathfrak{p}}(I_p) \leq \mathbf{P}G_{\mathfrak{p}}$ in most cases, which implies that $\mathbf{P}G_{\mathfrak{p}}$ is not contained in S_4 or A_5.

Proposition 2.45. *If $p \geq 7$ is a prime such that $p^2 \nmid N$, then $\mathbf{P}G_{\mathfrak{p}}$ is not exceptional for all $\mathfrak{p} \mid p$.*

Proof. Since we assume $p^2 \nmid N$, it follows from corollary 2.23 that $\mathbf{P}G_{\mathfrak{p}}$ contains elements of order $p-1$ or $p+1$. So if $p \geq 7$, there are always elements of order at least 6 in $\mathbf{P}G_{\mathfrak{p}}$, which implies that $\mathbf{P}G_{\mathfrak{p}}$ cannot be contained in a group isomorphic to S_4 or to A_5. □

So we only have to consider prime ideals $\mathfrak{p}$ of residue characteristic p such that $p \leq 5$ or $p^2 \mid N$. By the classification in Section 2.4, we can also exclude $p = 3$ when $\deg \mathfrak{p} = 1$ and $p = 2$. We can then run algorithm 2.19 on these finitely many $\mathfrak{p}$ to reduce the set of possibly exceptional primes further.

2.11. Proving non-CM

Recall that our goal is to show that $G_{\mathfrak{p}} = G_{\mathfrak{p}}^{\max}$ for all $\mathfrak{p}$ outside an explicit small finite set. Now if f has CM, then $G_{\mathfrak{p}}$ will *always* be contained in the normalizer of a Cartan subgroup, so in this case, our task is impossible. Note that by proposition 2.2, in our case of interest when $g = 2$, if the associated abelian surface is absolutely simple, f cannot have CM. However, since it may be of interest in other situations, we describe a suitable algorithm.

We recall the relevant definition (see [88, §3], specialized to the case of interest).

Definition 2.46. Let f be a newform of weight 2, level N and trivial nebentypus, and let ε be a Dirichlet character. We say that f has *CM by* ε, if $f \otimes \varepsilon = f$. We say that f *has CM*, if f has CM by some nontrivial Dirichlet character ε.

Remark 2.47. The Dirichlet character ε is then necessarily quadratic: Since f has totally real coefficients, ε has to take real values.

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

If f has CM by ε, then $\varepsilon(\ell)a_\ell = a_\ell$ for all $\ell \nmid N \operatorname{cond}(\varepsilon)$, so $a_\ell = 0$ whenever $\varepsilon(\ell) = -1$. This can be used to show that f does *not* have CM by ε, by exhibiting a prime $\ell \nmid N$ such that $\varepsilon(\ell) = -1$ and $a_\ell \neq 0$.

The idea is then to first determine a finite set of possibilities for the conductor D of ε and then to check for each of the finitely many possible characters ε of conductor D that f does not have CM by ε using this approach.

Theorem 2.48. *Let f be a newform of weight 2, level N and trivial nebentypus, and let ε be a quadratic Dirichlet character of conductor D. Then the twist $f \otimes \varepsilon$ of f by ε is a normalized eigenform of level dividing $\operatorname{lcm}(N, D^2)$ and trivial nebentypus.*

Proof. See [102, Proposition 3.64], using that ε^2 is trivial. □

Proposition 2.49. *If f is a CM form of level N, it is the newform associated to a Hecke character ψ of some conductor $\mathfrak{m}$ of an imaginary quadratic number field K of discriminant $-\Delta_K$. One has $N = \Delta_K M$ with M the absolute norm $\mathcal{N}(\mathfrak{m}) := \#\mathcal{O}_K/\mathfrak{m}$ and $\langle \Delta_K \rangle \mid \mathfrak{m}$. In particular, $\Delta_K^2 \mid N$.*

Proof. [96, Theorem 1.4 and Corollary 1.5] □

In the situation of proposition 2.49, the CM character ε is the quadratic character associated to K. This leads to the following algorithm.

Algorithm 2.50.

```
Input: A newform $f$ of weight 2, level $N$ and trivial nebentypus. A bound $B$.
Output: ‘non-CM’ or ‘no result’.
1. Let $S$ be the set of all negative fundamental discriminants $-\Delta$ such that $\Delta^2 \mid N$.
2. For each $\Delta \in S$, do the following.
   a. For all primes $\ell \leq B$ such that $\ell$ is inert in $\mathbf{Q}(\sqrt{-\Delta})$, do:
      (i) if $a_\ell \neq 0$, then continue with the next $\Delta$.
   b. Return ‘no result’.
3. Return ‘non-CM’.
```

Remark 2.51. If f does have CM, then this algorithm will eventually return ‘no result’. Then one has a candidate character ε (the character associated to $-\Delta$), and one can try to verify that $f \otimes \varepsilon = f$ (this is a finite computation, as the space of cusp forms of weight 2, level $\operatorname{lcm}(N, \Delta^2)$ and trivial nebentypus is of finite dimension and can be computed).

The following result guarantees that there will be enough primes ℓ as above when f has no CM.

Theorem 2.52. *Let f be a non-CM form. The set of primes ℓ such that $a_\ell = 0$ has density* 0.

Proof. See [99, p. 174]. □

Example 2.53. If N is squarefree, then proposition 2.49 implies that f has no CM since the only possible value of Δ would lead to $-\Delta_K = -1$, which is not a discriminant of an imaginary quadratic number field.

Remark 2.54. The newforms of weight 2, level 800, trivial nebentypus and with coefficients in $\mathbf{Q}(\sqrt{5})$ in the Galois orbit with LMFDB label 800.2.a.j have CM by $\mathbf{Q}(\sqrt{-5})$. Computing its endomorphism ring using Magma, we see that it has nontrivial idempotents, so A_f is not absolutely simple as predicted by proposition 2.2.

2.12. *Maximal image for almost all* $\mathfrak{p}$

Let f as usual be a newform of weight 2, level N and trivial nebentypus. We now assume that f does not have CM. In this section, we will describe an algorithm inspired by [26] that finds a small finite set of primes $\mathfrak{p}$ such that for all $\mathfrak{p} \notin S$, the representation $\rho_\mathfrak{p}$ has maximal image.

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

Using the algorithms we have described so far (and assuming $g = 2$, as that is required for some of these algorithms), we can determine a finite set S of prime ideals such that for all $\mathfrak{p} \notin S$, the representation $\rho_{\mathfrak{p}}$ is either maximal or irreducible and dihedral. So if $\mathbf{P}G_{\mathfrak{p}}$ is not maximal for $\mathfrak{p} \notin S$, it is contained in the normalizer $N(C)$ of a Cartan subgroup C. It therefore remains to find a finite set of prime ideals such that $\mathbf{P}G_{\mathfrak{p}}$ is not dihedral for $\mathfrak{p}$ outside this set.

So assume that $\rho_{\mathfrak{p}}$ is irreducible and dihedral, with $\mathbf{P}G_{\mathfrak{p}} \subseteq N(C)$ as above. We can also assume that $p^2 \nmid N$, as this excludes only finitely many p, which we can consider separately. By corollary 2.30, $\mathbf{P}G_{\mathfrak{p}}$ is not contained in C. So the character $\varepsilon_{\mathfrak{p}}$ defined in corollary 2.34 is nontrivial.

Proposition 2.55. *If N is squarefree, the residue characteristic of $\mathfrak{p}$ is not 2 and $\rho_{\mathfrak{p}}$ is irreducible, then $\rho_{\mathfrak{p}}$ is not dihedral.*

Proof. Let us prove the contrapositive. Thus, suppose that $\rho_{\mathfrak{p}}$ is dihedral. Then by the discussion above, $\varepsilon_{\mathfrak{p}}$ is nontrivial. By Corollary 2.34, the conductor $d > 1$ of $\epsilon_{\mathfrak{p}}$ satisfies $d^2 \,|\, N$. Thus, N is not squarefree. □

So in the semi-stable case, we already know that $\rho_{\mathfrak{p}}$ is maximal for all $\mathfrak{p} \notin S$. If N is not squarefree, then corollary 2.34 provides us with a finite set of possibilities for $\varepsilon_{\mathfrak{p}}$, and we can try to rule each of them out for all prime ideals outside a finite set.

Lemma 2.56. *Assume that $\mathfrak{p}$ has odd residue characteristic p and that $\rho_{\mathfrak{p}}$ is dihedral, with associated character $\varepsilon_{\mathfrak{p}}$. If $\ell \nmid Np$ is a prime such that $\varepsilon_{\mathfrak{p}}(\ell) = -1$, then $\mathfrak{p} \mid a_\ell$.*

Proof. Since $\varepsilon_{\mathfrak{p}}(\ell) = -1$ by assumption, we have $\rho_{\mathfrak{p}}(\mathrm{Frob}_\ell) \in N(C) \setminus C$. Then $\mathbf{P}\rho_{\mathfrak{p}}(\mathrm{Frob}_\ell)$ has order 2, which implies that $a_\ell \equiv \mathrm{Tr}(\rho_{\mathfrak{p}}(\mathrm{Frob}_\ell)) = 0 \bmod \mathfrak{p}$. □

We make use of this as follows. For each quadratic character ε of conductor d such that $d^2 \mid N$ (or $d \mid 8d_0$ with d_0 odd such that $d_0^2 \mid N$ if $4 \mid N$), find some prime $\ell = \ell(\varepsilon) \nmid N$ such that $a_\ell \neq 0$ and $\varepsilon(\ell) = -1$ (there are many such primes by theorem 2.52). Then for all $\mathfrak{p}$ such that $\mathfrak{p} \nmid \ell a_\ell$ (which are all but finitely many), it follows that $\varepsilon_{\mathfrak{p}} \neq \varepsilon$. (In practice, it makes sense to use several such primes ℓ to cut the set of possible exceptions down further.) So replacing S by the union of S with the finitely many finite sets $S_\varepsilon = \{\mathfrak{p} : \mathfrak{p} \mid \ell a_{\ell(\varepsilon)}\}$, we obtain the desired finite set S of prime ideals such that for $\mathfrak{p} \notin S$, $\rho_{\mathfrak{p}}$ has maximal image.

Algorithm 2.57.

Input: A non-CM newform $f \in \mathcal{N}(N, 2)$. A bound B.
Output: A finite set S of prime ideals of the maximal order $\mathcal{O}$ of $\mathbf{Z}[f]$ such that for all $\mathfrak{p} \notin S$, $\rho_{\mathfrak{p}}$ has maximal image, or 'failure'.

```
1. [Initialize] Let $S$ be the union of
       $\{\mathfrak{p} : p(\mathfrak{p}) \in \{2,3,5\} \text{ or } p(\mathfrak{p})^2 \mid N\}$
   and the finite sets returned by algorithms 2.40 and 2.44 (run on $f$ with the bound $B$).
   Return 'failure' when one of these algorithms failed.
2. [Possible conductors] Set $\mathcal{D} := \{d \in \mathbf{Z}_{>0} : d^2 \mid N \text{ and } 2 \nmid d\}$.
   If $4 \mid N$, set $\mathcal{D} := \mathcal{D} \cup \{4d : d \in \mathcal{D}\} \cup \{8d : d \in \mathcal{D}\}$.
3. [Loop over characters] For each $d \in \mathcal{D}$ and each quadratic Dirichlet character $\varepsilon$ of conductor $d$, do:
   a. [Initialize] Set $I := \langle 0 \rangle$ as an ideal in $\mathcal{O}$.
   b. [Loop over primes] For each prime $\ell \leq B$ such that $\ell \nmid N$ and $\varepsilon(\ell) = -1$, set $I := I + \langle \ell a_\ell \rangle$.
   c. [Failure] If $I = \langle 0 \rangle$, then return 'failure'.
   d. [Record prime ideals] Set $S := S \cup \{\mathfrak{p} : I \subseteq \mathfrak{p}\}$.
4. [Refine] Run algorithm 2.19 on each $\mathfrak{p} \in S$ and remove $\mathfrak{p}$ from $S$ when the result is the empty set.
5. Return $S$.
```

If B is sufficiently large, then the algorithm will not return 'failure', and by the discussion above, S will satisfy the specification.

We can use the information obtained from the various algorithms to provide a list of possible types of maximal subgroups that could contain $G_\mathfrak{p}$ for those primes $\mathfrak{p}$ that are in the set returned by algorithm 2.57.

2.13. The image of the $\mathfrak{p}$-adic Galois representation

For theorem 7.7, we also need information about the image of $\rho_{\mathfrak{p}^\infty}|_{\mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}(\mu_{p^\infty}))}$, and for theorem 5.10, about the image of $\rho_{\mathfrak{p}^\infty}$.

Proposition 2.58. *Let $\mathcal{O}$ be the ring of integers of an unramified extension of $\mathbf{Z}_p$. Let $G \subseteq \mathrm{SL}_2(\mathcal{O})$ be a closed subgroup.*

(i) *If $p > 3$ and G surjects onto $\mathrm{SL}_2(\mathcal{O}/p)$, then $G = \mathrm{SL}_2(\mathcal{O})$.*
(ii) *If $p = 3$ and G surjects onto $\mathrm{SL}_2(\mathcal{O}/3^2)$, then $G = \mathrm{SL}_2(\mathcal{O})$.*

Proof. See [100, Lemma IV.23.3], noting that the proof works for $\mathcal{O}$ instead of $\mathbf{Z}_p$; for $p = 3$, our claim follows from the proof given there. □

Proposition 2.59. *Assume that $\mathcal{O}/3 \in \{\mathbf{F}_3, \mathbf{F}_{3^2}\}$. Let $\rho\colon \mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}) \to \mathrm{GL}_2(\mathcal{O})$ be a continuous homomorphism with mod-3^n reduction ρ_{3^n}. If ρ_3 is surjective and the number of characteristic polynomials of elements of $\rho_{3^2}(\mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}))$ with constant term 1 is larger than the number of characteristic polynomials of elements of $\rho_3(\mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}))$ with constant term 1, then ρ_{3^2} is surjective.*

Proof. This is a Magma computation, looping over all subgroups of $\mathrm{SL}_2(\mathcal{O}/3^2)$ that surject onto $\mathrm{SL}_2(\mathcal{O}/3)$ and computing characteristic polynomials. □

Proposition 2.60. *Let $\mathcal{O}$ be the ring of integers of an unramified extension of $\mathbf{Z}_p$. Let*

$$G \subseteq G_{\mathfrak{p}^\infty}^{\max} := \{M \in \mathrm{GL}_2(\mathcal{O}) : \det(M) \in \mathbf{Z}_p^\times\}$$

be a closed subgroup with $\det(G) = \mathbf{Z}_p^\times$.

If $p > 3$ and the image of G in $\mathrm{GL}_2(\mathbf{F}_\mathfrak{p})$ contains $\mathrm{SL}_2(\mathbf{F}_p)$, then $G = G_{\mathfrak{p}^\infty}^{\max}$.

Proof. This follows from the proof of [69, Theorem 4.22]. □

We do not need proposition 2.60 for the examples in this article, but it is useful for further examples.

2.14. Examples

The following table contains the result of running our algorithms on all absolutely simple Jacobians with real multiplication of genus 2 curves over $\mathbf{Q}$ that are contained in the LMFDB. (The genus 2 curves in the LMFDB have discriminant bounded by 10^6; since the conductor of the Jacobian is the square of the level N and divides the discriminant, this implies that $N \leq 1000$.) We add information on the isogeny classes coming from Hasegawa or Wang curves that are not also represented by an LMFDB curve.

The entry 'N' gives the level and the letter x of the isogeny class of the curve in the LMFDB (the LMFDB label of the isogeny class is then $N^2.x\ldots$). For the Hasegawa and Wang curves not representing an isogeny class of an LMFDB curve, we use the label from [45]. The entry '$p^2 \mid N$' lists the primes at which the Jacobian does not have semi-stable reduction. The third entry 'disc$(\mathcal{O})$' gives the discriminant of the endomorphism ring of the Jacobian. The next entry lists the prime ideals $\mathfrak{p}$ such that $\rho_\mathfrak{p}$ is reducible and gives the splitting of $\rho_\mathfrak{p}^{\mathrm{ss}}$ into characters. We use ε_d to denote the quadratic character associated to the quadratic extension of discriminant d. Since $\rho_\mathfrak{p}^{\mathrm{ss}}$ is the same for isogenous Jacobians, we list each isogeny class only once. The primes are given as 'p' when $\mathfrak{p} = \langle p \rangle$ is of degree 2, as '$\mathfrak{p}_p'$' or '$\mathfrak{p}_p''$' when $p = p(\mathfrak{p})$ is split and as '$\mathfrak{p}_p$' when p is ramified. The last entry lists the prime

N	$p^2 \mid N$	$\mathrm{disc}(\mathcal{O})$	reducible $\rho_\mathfrak{p}$	irreducible non-maximal $\rho_\mathfrak{p}$
23a		5	$\mathfrak{p}'_{11}$: $\mathbf{1} \oplus \chi_{11}$	3: A_5
29a		8	$\mathfrak{p}'_7$: $\mathbf{1} \oplus \chi_7$	$\mathfrak{p}_2$: $N(C_{ns})$
31a		20	$\mathfrak{p}_5$: $\mathbf{1} \oplus \chi_5$	
35a		17	$\mathfrak{p}'_2$: $\mathbf{1} \oplus \chi_2$	$\mathfrak{p}''_2$: $N(C_{ns})$
39a		8	$\mathfrak{p}_2$: $\mathbf{1} \oplus \chi_2$; $\mathfrak{p}'_7$: $\mathbf{1} \oplus \chi_7$	
51a		17	$\mathfrak{p}'_2$: $\mathbf{1} \oplus \chi_2$	$\mathfrak{p}''_2$: $N(C_{ns})$; 3: A_5
65a		12	$\mathfrak{p}_2$: $\mathbf{1} \oplus \chi_2$; $\mathfrak{p}_3$: $\mathbf{1} \oplus \chi_3$	
67a		5		3: A_4
67c		5	$\mathfrak{p}'_{11}$: $\mathbf{1} \oplus \chi_{11}$	
73a		13	$\mathfrak{p}'_3$: $\mathbf{1} \oplus \chi_3$	
73b		5		3: A_4
77b		5	2: $\mathbf{1} \oplus \chi_2$	
85a		8	$\mathfrak{p}_2$: $\mathbf{1} \oplus \chi_2$	
85b		12	$\mathfrak{p}_2$: $\mathbf{1} \oplus \chi_2$; $\mathfrak{p}_3$: $\mathbf{1} \oplus \chi_3$	
87a		5	$\mathfrak{p}_5$: $\mathbf{1} \oplus \chi_5$	
88b	[2]	17	$\mathfrak{p}'_2$: $\mathbf{1} \oplus \chi_2$	$\mathfrak{p}''_2$: $N(C_{ns})$
93a		5		3: A_5
103a		5		3: A_4
107a		5		3: A_5
115b		5		3: A_5
123b		8	$\mathfrak{p}'_7$: $\mathbf{1} \oplus \chi_7$	$\mathfrak{p}_2$: $N(C_{ns})$; 3: A_5
125a	[5]	5	$\mathfrak{p}_5$: $\chi_5^2 \oplus \chi_5^3$	3: A_5
129a		8		$\mathfrak{p}_2$: $N(C_{ns})$; 3: A_5
133c		5		3: A_4
133d		13	$\mathfrak{p}'_3$: $\mathbf{1} \oplus \chi_3$	
133e		5	$\mathfrak{p}_5$: $\mathbf{1} \oplus \chi_5$	
135c	[3]	52	$\mathfrak{p}'_3$: $\mathbf{1} \oplus \chi_3$	
147a	[7]	8	$\mathfrak{p}_2$: $\mathbf{1} \oplus \chi_2$; $\mathfrak{p}'_7$: $\chi_7^3 \oplus \chi_7^4$	
165a		8	$\mathfrak{p}_2$: $\mathbf{1} \oplus \chi_2$	
167a		5		
176a	[2]	17	$\mathfrak{p}'_2$: $\mathbf{1} \oplus \chi_2$	$\mathfrak{p}''_2$: $N(C_{ns})$
177a		5		3: A_5
188a	[2]	5		2: $N(C_{ns})$; 3: A_5
191a		5		3: A_5
193a		5		3: A_4
205a		5		3: A_5
207b	[3]	8	$\mathfrak{p}_2$: $\mathbf{1} \oplus \chi_2$	3: A_5
209a		8		$\mathfrak{p}_2$: $N(C_{ns})$
211a		5	$\mathfrak{p}_5$: $\mathbf{1} \oplus \chi_5$	3: A_5
213a		5		3: A_5
221a		5		3: A_5
223a		8		$\mathfrak{p}_2$: $N(C_{ns})$
227a		5		2: $N(C_{ns})$
245a	[7]	8	$\mathfrak{p}'_7$: $\chi_7^3 \oplus \chi_7^4$	$\mathfrak{p}_2$: $N(C_{ns})$; 3: sub-line
250a	[5]	5	$\mathfrak{p}_5$: $\chi_5^2 \oplus \chi_5^3$	2: $N(C_{ns})$
261c	[3]	20		
275a	[5]	5	$\mathfrak{p}_5$: $\mathbf{1} \oplus \chi_5$	3: A_5
275b	[5]	13	$\mathfrak{p}'_3$: $\varepsilon_5 \oplus \varepsilon_{-3\cdot 5}$	
287a		5		
289a	[17]	13	$\mathfrak{p}'_3$: $\varepsilon_{17} \oplus \varepsilon_{-3\cdot 17}$; $\mathfrak{p}'_{17}$: $\chi_{17}^3 \oplus \chi_{17}^{14}$	
299a		5		
303a		8		$\mathfrak{p}_2$: $N(C_{ns})$
313a		5		
321a		5		
334a		5		
357a		8		$\mathfrak{p}_2$: $N(C_{ns})$
358a		5	$\mathfrak{p}_5$: $\mathbf{1} \oplus \chi_5$	
375a	[5]	5	$\mathfrak{p}_5$: $\chi_5^2 \oplus \chi_5^3$	3: A_5
376b	[2]	5		2: $N(C_{ns})$
376e	[2]	5		2: $N(C_{ns})$
383a		5		3: A_5
389a		8		$\mathfrak{p}_2$: $N(C_{ns})$
457a		5		
461a		5		3: A_5

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

N	$p^2 \mid N$	disc$(\mathcal{O})$	reducible $\rho_\mathfrak{p}$	irreducible non-maximal $\rho_\mathfrak{p}$
491a		5		
499a		5		3: A_5
523a		5		3: A_4
533a		8		$\mathfrak{p}_2$: $N(C_{ns})$
599a		5		
621a	[3]	8		$\mathfrak{p}_2$: $N(C_{ns})$; 3: A_5
621c	[3]	5		3: A_5
637a	[7]	5		3: A_4
640a	[2]	5	2: $\mathbf{1} \oplus \chi_2$	
640b	[2]	5	2: $\mathbf{1} \oplus \chi_2$	
647a		5		3: A_5
677a		5		3: A_5
683a		5		2: $N(C_{ns})$
689a		5		2: $N(C_{ns})$
752a	[2]	5		2: $N(C_{ns})$; 3: A_5
752f	[2]	5		2: $N(C_{ns})$
752j	[2]	5		2: $N(C_{ns})$
783a	[3]	5		
799a		5		3: A_5
809a		5		
837b	[3]	8		$\mathfrak{p}_2$: $N(C_{ns})$
841a	[29]	5	$\mathfrak{p}'_{29}$: $\chi_{29}^5 \oplus \chi_{29}^{24}$	
845a	[13]	5		3: A_5
877a		5		2: $N(C_{ns})$
887a		5		3: A_5
929a		5		3: A_5
Hasegawa curve isogeny class not in the LMFDB				
161		5		3: A_5
‘Wang only’ curve isogeny classes not in the LMFDB				
65A		8	$\mathfrak{p}_2$: $\mathbf{1} \oplus \mathbf{1}$; $\mathfrak{p}'_7$: $\mathbf{1} \oplus \chi_7$	3: A_5
117B	[3]	8	$\mathfrak{p}_2$: $\mathbf{1} \oplus \chi_2$	
125B	[5]	5	$\mathfrak{p}_5$: $\mathbf{1} \oplus \chi_5$	3: A_5
175	[5]	5	$\mathfrak{p}_5$: $\mathbf{1} \oplus \chi_5$	

ideals $\mathfrak{p}$ such that $\rho_\mathfrak{p}$ is irreducible, but algorithm 2.57 does not prove that $\rho_\mathfrak{p}$ is maximal. In these cases, we have determined the isomorphism type of $\mathbf{P}G_\mathfrak{p}$ by a direct computation; we give it in the table.

3. Computation of Heegner points and the Heegner index

For this section, we fix the following setup. Let $f \in \mathcal{N}(N, g)$ be a newform of level N with Galois orbit of size g, so that its coefficient ring $\mathbf{Z}[f]$ is an order in the totally real number field $\mathbf{Q}(f)$ of degree g. Its Fourier coefficients are $a_n = a_n(f) \in \mathbf{Z}[f]$. We denote the set of embeddings $\mathbf{Q}(f) \hookrightarrow \mathbf{R}$ by Σ, and we write f^σ for the modular form with real coefficients obtained from f by applying $\sigma \in \Sigma$ to its coefficients. Recall that I_f denotes the annihilator of f in the integral Hecke algebra $\mathbf{T}$, and that we have morphisms of abelian varieties

$$A_f^\vee = J_0(N)[I_f] \overset{\iota_f}{\hookrightarrow} J_0(N) \overset{\pi_f}{\twoheadrightarrow} J_0(N)/I_f J_0(N) = A_f\ ;$$

the composition $\lambda_f = \pi_f \circ \iota_f : A_f^\vee \longrightarrow A_f$ is a polarization of $A_f^\vee$; it is the polarization induced by the canonical principal polarization of $J_0(N)$ as the Jacobian of $X_0(N)$. (If $\lambda\colon A \longrightarrow A^\vee$ is the polarization coming from $L \in \mathrm{NS}(A)$ and $\varphi\colon B \subseteq A$ is an abelian subvariety, then $\varphi^\vee \circ \lambda \circ \varphi\colon B \longrightarrow B^\vee$ is the polarization on B coming from $\varphi^* L$. See [9, Cor. 2.4.6 (d)].) Note that ι_f is the composition of $\pi_f^\vee$ with the inverse of the canonical polarization of $J_0(N)$. We write

$$d_f := d_1 \cdots d_g, \tag{3.1}$$

where $(d_1, \dots, d_g)$ is the type of λ_f; then $\deg \lambda_f = d_f^2$ (see [9, Thm. 3.6.1 and Cor. 3.6.2]). The number d_f is sometimes called the *modular degree* of A_f; see, for example, [3, §3.3].

We further assume that we are given a (nice) curve X whose Jacobian J is isogenous to A_f via an isogeny $\pi\colon A_f \to J$. We denote $\mathrm{End}_{\mathbf{Q}}(J)$ by $\mathcal{O}$. The isogeny π induces an isomorphism of endomorphism algebras (where $\mathrm{End}^0_{\mathbf{Q}}(A) := \mathrm{End}_{\mathbf{Q}}(A) \otimes_{\mathbf{Z}} \mathbf{Q}$)

$$\pi^0_*\colon \mathbf{Q}(f) = \mathrm{End}^0_{\mathbf{Q}}(A_f) \xrightarrow{\simeq} \mathrm{End}^0_{\mathbf{Q}}(J) = \mathrm{Frac}(\mathcal{O}), \qquad \varphi \longmapsto \pi\varphi\pi^{-1}, \tag{3.2}$$

which we use to identify $\mathrm{End}^0_{\mathbf{Q}}(J) = \mathbf{Q}(f)$. In particular, $\mathcal{O}$ is identified with an order of $\mathbf{Q}(f)$. Then for any $\gamma \in \mathbf{Z}[f] \cap \mathcal{O}$, it follows that

$$\pi \circ \gamma = \gamma \circ \pi. \tag{3.3}$$

We write $\pi_J = \pi \circ \pi_f : J_0(N) \to J$. We then have a commutative diagram

$$\begin{tikzcd} J_0(N) \arrow[r, two heads, "\pi_f"'] \arrow[rr, bend left, "\pi_J"] \arrow[d, equal] & A_f \arrow[r, "\pi"'] & J \\ J_0(N)^\vee & A_f^\vee \arrow[l, hook', "\pi_f^\vee"'] \arrow[u, "\lambda_f"'] & J^\vee \pi_J^\vee \arrow[l, "\pi^\vee"'] \arrow[u, "\lambda"'] \arrow[ll, bend left] \end{tikzcd} \tag{3.4}$$

with a polarization $\lambda = \pi \circ \lambda_f \circ \pi^\vee = \pi_J \circ \pi_J^\vee$ of $J^\vee$. Then by pre-composing λ with the canonical principal polarization λ_J of J, we obtain an element

$$\alpha := \lambda \circ \lambda_J = \pi \circ \lambda_f \circ \pi^\vee \circ \lambda_J \in \mathcal{O} \subseteq \mathbf{Q}(f). \tag{3.5}$$

By [76, Prop. 12.12], $(\deg \pi)^2 (\deg \lambda_f) = \deg \alpha = \mathbf{N}(\alpha)^2$, which implies that

$$\mathbf{N}(\alpha) = d_f \cdot \deg \pi. \tag{3.6}$$

In practice, we start with the curve X of genus g, and we know that its Jacobian J has real multiplication (and is absolutely simple). We then need to find the corresponding newform $f \in \mathcal{N}(N, g)$. We first determine N. When X is a quotient of $X_0(N)$, then we know N by construction. In general, we find N as the square root of the conductor of J, which can be computed up to finitely many choices of power of 2 at worst; in our LMFDB examples, the conductor has been determined exactly and is available in the LMFDB. Given N, we then compare the traces of the Fourier coefficients at primes $\ell \nmid N$ of the various candidate f with the corresponding coefficient of the L-function of J. This quickly leaves only one candidate, which must then be the correct f (up to the Galois action). We now assume that f is fixed.

One of the ingredients we need in order to prove that $Ш(J/\mathbf{Q})[\mathfrak{p}] = 0$ for all except an explicit finite set of prime ideals $\mathfrak{p}$ of $\mathcal{O}$ is the *Heegner index*, whose definition we now recall. (See Sections 4 and 5 below for why the Heegner index is important.) Let K be a *Heegner field* for f; this is an imaginary quadratic field such that all prime divisors of N split in K and such that the L-series $L(f/K, s) = L(f, s)L(f \otimes \varepsilon_K, s)$ (with ε_K the quadratic character corresponding to K) vanishes to first order at $s = 1$. The first condition implies that $\mathcal{O}_K$ contains ideals $\mathfrak{n}$ of norm N such that $\mathcal{O}_K/\mathfrak{n}$ is a cyclic group of order N. Then the natural map $\mathbf{C}/\mathcal{O}_K \to \mathbf{C}/\mathfrak{n}^{-1}$ corresponds to a cyclic isogeny of degree N between two elliptic curves with CM by $\mathcal{O}_K$ and so defines a point in $X_0(N)$, which is known to be defined over the Hilbert class field H of K. More generally, let $\mathfrak{a}$ be some ideal of $\mathcal{O}$; then we can consider $\mathbf{C}/\mathfrak{a} \to \mathbf{C}/\mathfrak{a}\mathfrak{n}^{-1}$. We obtain h_K points $x_{[\mathfrak{a}]} \in X_0(N)(H)$ in this way, where h_K denotes the class number of K and the point depends only on the ideal class of $\mathfrak{a}$. These points form an orbit under $\mathrm{Gal}(H|K)$; their formal sum $\mathbf{x}_K$ is the *Heegner cycle* on $X_0(N)$ associated to K and $\mathfrak{n}$; it is defined over K. Let $\infty \in X_0(N)(\mathbf{Q})$ denote the cusp at infinity. Then $y_K = [\mathbf{x}_K - h_K \cdot (\infty)] \in J_0(N)(K)$ is a *Heegner*

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

point associated to K. By varying $\mathfrak{n}$ in the construction, we may get different Heegner points, but they all agree up to sign and adding a torsion point. (See also [51].) So in the following, we will consider Heegner points up to sign and modulo torsion.

We then obtain a point $y_{K,\pi} = \pi_J(y_K) \in J(K)$. By [52], the $\mathcal{O}$-span of $y_{K,\pi} \in J(K)$ is a rank $g = \dim J$ subgroup of finite index of $J(K)$ (which does not depend on the choice of the Heegner point). This index is the *Heegner index*; we denote it by

$$I_{K,\pi} := (J(K) : \mathcal{O} \cdot y_{K,\pi}). \tag{3.7}$$

Considering the characteristic ideal $\mathcal{I}_{K,\pi} := \mathrm{Char}_{\mathcal{O}}(J(K)/\mathcal{O}y_{K,\pi})$ gives refined information; this refinement is helpful for our intended application because we can study the summands of $\text{Ш}(J/\mathbf{Q})[p^\infty] = \bigoplus_{\mathfrak{p}|p} \text{Ш}(J/\mathbf{Q})[\mathfrak{p}^\infty]$ individually. In the same way, we have $y_{K,A_f} = \pi_f(y_K) \in A_f(K)$, and we set $I_K := (A_f(K) : \mathbf{Z}[f]y_{K,A_f})$ and $\mathcal{I}_K := \mathrm{Char}_{\mathbf{Z}[f]}(A_f(K)/\mathbf{Z}[f]y_{K,A_f})$.

For an abelian variety $A/\mathbf{Q}$ and a quadratic number field K, we denote the quadratic twist of A by the quadratic character associated to K by A^K. Then A^K is isomorphic to A over K. The natural map $A(\mathbf{Q}) \times A^K(\mathbf{Q}) \to A(K)$ has finite kernel and cokernel killed by 2: The kernel is the diagonally embedded $A(\mathbf{Q})[2]$, and the image contains $2A(K)$.

When $L\text{-rk}\, J = 0$, then $J(K)$ is essentially $J^K(\mathbf{Q})$; more precisely, the image of $J^K(\mathbf{Q})$ in $J(K)$ contains $2J(K)$ up to torsion, and so we can identify $2y_{K,\pi}$ up to torsion with a rational point on J^K. When $L\text{-rk}\, J = 1$, then $2J(K)$ is contained in $J(\mathbf{Q})$ up to torsion, and we can identify $2y_{K,\pi}$ up to torsion with a rational point on J. (See also [73, Lemma 2.1].) This simplifies the computations since certain algorithms (for example, computing canonical heights on J) are so far only implemented when the base field is $\mathbf{Q}$.

The aim of this section is to explain how we can compute the Heegner index $I_{K,\pi}$ (or the corresponding ideal $\mathcal{I}_{K,\pi}$).

The first step is to determine a Heegner field K. This is explained in Section 3.2. In order to determine the $\mathcal{O}$-span of $y_{K,\pi}$, we need to determine $\mathcal{O} = \mathrm{End}_{\mathbf{Q}}(J)$ and its action on $J(K)$ (we can determine generators of $J(K)$ from generators of $J(\mathbf{Q})$ and of $J^K(\mathbf{Q})$, which Magma can usually compute). Section 3.3 explains how to do that. Then, of course, we need to find the Heegner point $y_{K,\pi}$ on J.

One approach is to compute the j-invariant morphism $X_0(N) \to \mathbf{P}^1_{\mathbf{Q}}$ given by sending the point representing an isogeny $E \to E'$ to $j(E)$ as an algebraic map. Then, given the h_K different j-invariants of elliptic curves with CM by $\mathcal{O}_K$, we can lift them to the corresponding points in $X_0(N)(H)$ and thus get an algebraic description of the Heegner cycle. However, this turns out to be too slow even for moderately large N. Therefore, we do not give more details here.

Instead, we use an analytic approach. We start with the h_K reduced integral binary quadratic forms whose roots with positive imaginary part map to the points in the support of the Heegner cycle on $X_0(N)$ under the uniformization map $\mathbf{H} \to X_0(N)(\mathbf{C})$, where $\mathbf{H}$ denotes the upper half plane. These quadratic forms can easily be determined using the built-in Magma function `HeegnerForms`. Via the uniformization map $\mathbf{H} \to X_0(N)(\mathbf{C})$, we obtain the set of h_K points in the Heegner cycle. If the curve X is a quotient of $X_0(N)$, we can then map the Heegner cycle directly to X and try to recognize it as a divisor defined over K. We can then obtain the point on J given by the Heegner cycle. If X is not a quotient of $X_0(N)$, we do the following. We first use the Abel–Jacobi map $X_0(N)(\mathbf{C}) \to J_0(N)(\mathbf{C})$ and the map $\pi_{f,\mathbf{C}} \colon J_0(N)(\mathbf{C}) \to A_f(\mathbf{C}) \cong \mathbf{C}/\Lambda_f$ to map the Heegner cycle to $A_f(\mathbf{C})$. We then compute the point $y_K \in A_f(\mathbf{C})$ (by taking a sum in $\mathbf{C}/\Lambda_f$). Then we use an explicit numerical representation of the isogeny $\pi_{\mathbf{C}} \colon A_f(\mathbf{C}) \to J(\mathbf{C})$ to map the Heegner point from $A_f(\mathbf{C})$ to $J(\mathbf{C})$. Finally, we recognize the image as a point defined over the Heegner field K. This is explained in Section 3.4. However, $J(K) \subset J(\mathbf{C})$ is dense. Hence, we must prove that we have found the correct point. We do this by determining its canonical height (which is well-defined since it does not change when adding a torsion point or changing the sign) via the Gross–Zagier formula. Since there are only finitely many points with bounded height, knowing the height is sufficient to cut the possibilities down to finitely many candidates up to sign and torsion; in practice, there is only one candidate. So we check that the point we have computed has the correct height and that no other point (up to sign and torsion) has the same height up to the numerical precision used in the computation. In principle, we could use this approach to bypass the analytic computation of the Heegner point altogether and just recognize it from its height, but using both approaches provides an additional level of confirmation that our results are correct. A further benefit of computing the Heegner point (and its image under a generator of the endomorphism ring of J) is that this provides us with generators of a finite-index subgroup of $J(K)$. So in order to determine $J(K)$ (which is necessary for the computation of the Heegner index $I_{K,\pi}$), it then suffices to saturate the known subgroup, which means that we do not have to search for points first. This can save a considerable amount of time.

Since the Gross–Zagier formula involves the Petersson norm of f^σ for the various embeddings $\sigma\colon \mathbf{Z}[f] \hookrightarrow \mathbf{R}$, we need a way to compute these Petersson norms; see Section 3.5. To apply the Gross–Zagier formula, we project y_K, viewed as an element of $J_0(N)(K) \otimes_{\mathbf{Z}} \mathbf{R}$, to its various σ-components $y_{K,\sigma}$ (which have the property that $\mathbf{Q}(f)$ acts on them via the embedding σ). The formula then gives an expression for $\hat{h}(y_{K,\sigma})$, where $\hat{h}\colon J_0(N)(K) \otimes_{\mathbf{Z}} \mathbf{R} \to \mathbf{R}$ is the normalized canonical height on $J_0(N)$ associated to twice the theta divisor. This is discussed in Section 3.7. Finally, we have to relate the height $\hat{h}_J(y_{K,\pi})$ with respect to twice the theta divisor on J to the heights $\hat{h}(y_{K,\sigma})$; this is done in Section 3.8.

3.1. Computational representation of Diagram (3.4)

For our computations, we need to represent $A_f^\vee, A_f, J$ as complex tori and the isogenies between them. This is done as follows.

Definition 3.1. Let A be an arbitrary abelian variety over $\mathbf{C}$, of dimension g. Associated to a $\mathbf{C}$-basis $\underline{\omega} = (\omega_1, \ldots, \omega_g)$ of $\mathrm{H}^0(A, \Omega^1)$ and a $\mathbf{Z}$-basis $\underline{\gamma} = (\gamma_1 \; \ldots, \gamma_{2g})$ of the integral homology $\mathrm{H}_1(A(\mathbf{C}), \mathbf{Z})$, there is the *period matrix*

$$\Pi_A := \Pi_{A,\underline{\omega},\underline{\gamma}} := \Big(\int_{\gamma_j} \omega_i\Big)_{i,j} \in \mathbf{C}^{g\times 2g}.$$

Its $2g$ columns generate a lattice Λ, and $A(\mathbf{C}) \cong \mathbf{C}/\Lambda$ via $x \mapsto \big(\int_0^x \omega_i\big)_i + \Lambda$. We also write Λ_A for Λ to indicate the associated abelian variety.

Definition 3.2. Let A and B be two abelian varieties over $\mathbf{C}$ of the same dimension g, and let Π_A and Π_B be associated period matrices. If $\varphi\colon\ A \longrightarrow B$ is an isogeny, then there are uniquely determined matrices $\alpha_\varphi \in \mathrm{GL}_g(\mathbf{C})$ and $M_\varphi \in \mathbf{Z}^{2g\times 2g}$ such that

$$\alpha_\varphi \cdot \Pi_A = \Pi_B \cdot M_\varphi.$$

We call $(\alpha_\varphi, M_\varphi)$ the *pair of matrices associated to* φ.

We observe that, given Π_A and Π_B, each of M_φ and α_φ can be determined from the other.

Note that α_φ is the matrix of the $\mathbf{C}$-linear map $\omega \mapsto \varphi^*\omega$ with respect to the bases of the spaces of holomorphic differentials used for Π_A and Π_B, and M_φ is the matrix of the $\mathbf{Z}$-linear map $\gamma \mapsto \varphi_*\gamma$ on the homology bases.

If A, B and φ are defined over $\mathbf{Q}$ and we use $\mathbf{Q}$-bases of $\mathrm{H}^0(A, \Omega^1)$ and $\mathrm{H}^0(B, \Omega^1)$, then $\alpha_\varphi \in \mathrm{GL}_g(\mathbf{Q})$ (since φ^* is a $\mathbf{Q}$-linear map). Similarly, if we use $\mathbf{Z}$-bases of $\mathrm{H}^0(\mathscr{A}, \Omega^1)$ and $\mathrm{H}^0(\mathscr{B}, \Omega^1)$, where $\mathscr{A}$ and $\mathscr{B}$ are the Néron models of A and B over $\mathbf{Z}$, then $\alpha_\varphi \in \mathbf{Z}^{g\times g} \cap \mathrm{GL}_g(\mathbf{Q})$.

Definition 3.3. Let A and B be abelian varieties defined over $\mathbf{Q}$, with Néron models $\mathscr{A}$ and $\mathscr{B}$ over $\mathbf{Z}$, respectively. Let $\varphi\colon\ A \longrightarrow B$ be an isogeny defined over $\mathbf{Q}$. Then we set

$$c_\varphi := \big(\mathrm{H}^0(\mathscr{A}, \Omega^1) : \varphi^*\mathrm{H}^0(\mathscr{B}, \Omega^1)\big) \in \mathbf{Z}_{\geq 1}.$$

If Π_A and Π_B are computed using $\mathbf{Z}$-bases of $\mathrm{H}^0(\mathscr{A}, \Omega^1)$ and $\mathrm{H}^0(\mathscr{B}, \Omega^1)$, then $c_\varphi = |\det \alpha_\varphi|$.

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

Definition 3.4. Let $f \in \mathcal{N}(N, g)$. We define $S_2(f, \mathbf{Z})$ to be the $\mathbf{Z}$-sublattice of the $\mathbf{C}$-span of f and its Galois conjugates in $S_2(\Gamma_0(N))$ that consists of forms whose q-expansions have integral coefficients. Under the natural identification of $S_2(\Gamma_0(N))$ with $\mathrm{H}^0(X_0(N), \Omega^1) \simeq \mathrm{H}^0(J_0(N), \Omega^1)$, the image of $S_2(f, \mathbf{Z})$ contains $\pi_f^* \mathrm{H}^0(\mathscr{A}_f, \Omega^1)$ (where $\mathscr{A}_f$ is the Néron model of A_f over $\mathbf{Z}$). The index

$$c_f := \big(S_2(f, \mathbf{Z}) : \pi_f^* \mathrm{H}^0(\mathscr{A}_f, \Omega^1)\big) \in \mathbf{Z}_{\geq 1}$$

is the *Manin constant* of π_f.

See [1, Def. 3.3 and Thm. 3.4].

Proposition 3.5. *The Manin constant c_f is divisible only by primes p such that $p^2 \mid N$ or $p = 2$, and the conductor of $\mathbf{Z}[f]$ is even.*

In particular, $c_f = 1$ if N is squarefree and the conductor of $\mathbf{Z}[f]$ is odd.

Proof. This is [1, Cor. 3.7] for odd primes and [22, Thm. 5.19] for $p = 2$. □

It has been conjectured (see [22, Conj. 5.2] and the text preceding it) that c_f is always 1, but [22, Thm. 5.10] gives a counterexample in dimension 24 (with $N = 431$ odd and $2 \mid c_f$).

Magma can compute a period matrix $\Pi_{A_f^\vee}$ of $A_f^\vee$ with respect to a $\mathbf{Z}$-basis of $S_2(f, \mathbf{Z})$ and some homology basis. Magma also computes the matrix I of the intersection pairing (inside the homology of $J_0(N)(\mathbf{C})$) on the first homology of $A_f^\vee(\mathbf{C})$. Then $\Pi_{A_f} := \Pi_{A_f^\vee} \cdot I^{-1}$ is a period matrix for A_f (with respect to the same basis of $S_2(f, \mathbf{Z})$), and (I_g, I) is the pair of matrices associated to the polarization λ_f. Let now J be the Jacobian of a curve of genus 2 over $\mathbf{Q}$ such that there is an isogeny $\pi\colon A_f \to J$ as in (3.4). Magma can compute a period matrix Π_J for J with respect to a certain $\mathbf{Q}$-basis B of $\mathrm{H}^0(J, \Omega^1)$ (if J is the Jacobian of a genus 2 curve $y^2 = f(x)$, then B corresponds to the differentials dx/y and $x\,dx/y$ on the curve) and a symplectic homology basis. We can then find the associated pair of matrices (α_π, M_π). The algorithm [11, Algorithm 13] determines the ‘compensation factor’ (called W in *loc. cit.*)

$$C = \big(\mathrm{H}^0(\mathscr{J}, \Omega^1) : \langle B \rangle_{\mathbf{Z}}\big) \tag{3.8}$$

(where $\mathscr{J}$ is the Néron model of J over $\mathbf{Z}$ and the index of two commensurable $\mathbf{Z}$-lattices in $\mathrm{H}^0(J, \Omega^1)$ is in general a positive rational number). Combining these computations gives the following.

Lemma 3.6.

$$c_f \cdot c_\pi = C \cdot |\det \alpha_\pi|.$$

In our LMFDB examples, the compensation factor C (with respect to a minimal Weierstrass model) is always 1, and $c_f c_\pi$ divides the degree of the isogeny π.

For later applications, we want to compute the sizes of the kernel and cokernel of the map $\pi_{\mathbf{R}}\colon A_f(\mathbf{R}) \to J(\mathbf{R})$ induced by the isogeny π on the groups of real points. We note that we can obtain the action of complex conjugation τ on $A(\mathbf{C}) \cong \mathrm{H}_1(A(\mathbf{C}), \mathbf{Z}) \otimes \mathbf{R}/\mathbf{Z}$ by solving $\overline{\Pi_A} = \Pi_A \cdot M_{A,\tau}$ for $M_{A,\tau} \in \mathbf{Z}^{2g \times 2g}$. We obtain $\ker\pi \cong M_\pi^{-1}\mathbf{Z}^{2g}/\mathbf{Z}^{2g} \simeq \mathbf{Z}^{2g}/M_\pi \mathbf{Z}^{2g}$, and we can find its τ-invariant part $\ker\pi_{\mathbf{R}}$ using $M_{A_f,\tau}$. The group $\pi_0(J(\mathbf{R}))$ of connected components of $J(\mathbf{R})$ is isomorphic to

$$\ker(1 + \tau \mid \Lambda_J)/(1 - \tau)\Lambda_J \cong \ker(I_{2g} + M_{J,\tau} \mid \mathbf{Z}^{2g})/(I_{2g} - M_{J,\tau})\mathbf{Z}^{2g}$$

and similarly for A_f, so

$$\operatorname{coker}\pi_{\mathbf{R}} \cong \frac{\ker(I_{2g} + M_{J,\tau} \mid \mathbf{Z}^{2g})}{(I_{2g} - M_{J,\tau})\mathbf{Z}^{2g} + \ker(I_{2g} + M_{J,\tau} \mid M_\pi \mathbf{Z}^{2g})}.$$

When considering the quadratic twist π^K for an imaginary quadratic field K, then we have to replace $M_{J,\tau}$ by $-M_{J,\tau}$ to obtain the twisted action of τ on $J^K(\mathbf{C}) \cong J(\mathbf{C})$.

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

We can use a similar idea to compute Ω_J from the period matrix Π_J and the compensation factor C from (3.8), as follows.

Lemma 3.7. *Let $T \in \mathrm{GL}_{2g}(\mathbf{Z})$ be such that $(M_{J,\tau} + I_{2g}) \cdot T = (\tilde{M} \mid 0)$ with $\tilde{M} \in \mathbf{Z}^{2g\times g}$. Then*

$$\Omega_J = C \cdot |\det(\Pi_J \cdot \tilde{M})|.$$

Proof. It is well-known that Ω_J is the covolume of the lattice given by integrating a Néron basis over the $\mathbf{C}|\mathbf{R}$-trace of $\mathrm{H}_1(X(\mathbf{C}), \mathbf{Z})$ (see [45, §3.5] or [11, Def. 11]). The $\mathbf{Z}$-lattice generated by the columns of the matrix $M_{J,\tau} + I_{2g}$ corresponds to the $\mathbf{C}|\mathbf{R}$-trace of $\mathrm{H}_1(X(\mathbf{C}), \mathbf{Z})$ (w.r.t. the homology basis used to compute Π_J). This lattice is known to have rank g, so there exists a unimodular matrix T as in the statement, and multiplying on the right by T preserves the lattice. So the columns of $\tilde{M}$ give a basis of the $\mathbf{C}|\mathbf{R}$-trace of $\mathrm{H}_1(X(\mathbf{C}), \mathbf{Z})$, and the result follows (taking into account the factor C arising from changing the basis of differentials used in the computation of Π_J to a Néron basis). □

This improves over the method currently implemented in Magma (which is based on [11, Algorithm 13]) in that it uses an exact computation to find the correct integral linear combination of $g \times g$ minors of Π_J instead of relying on a ‘real gcd’ computation with numerical approximations. (The approximation step is in the computation of $M_{J,\tau}$, but here we know that the entries are integers, so we can simply round.)

We now want to determine the endomorphism $\alpha \in \mathcal{O} = \mathrm{End} J$ that was defined in (3.5). Since Π_J is computed with respect to a symplectic homology basis, we obtain the M-matrix of the canonical polarization of J as the matrix I' of the standard symplectic pairing. Then $M := M_\pi \cdot I \cdot M_\pi^\top \cdot I'$ gives the action of $\alpha \in \mathcal{O}$ on the lattice associated to J, and its action on the tangent space can be recovered from that. (Recall that I denotes the matrix of the intersection pairing for $A_f^\vee(\mathbf{C})$.) We can (and do) ‘optimize’ α by post-composing π with an automorphism $\varepsilon \in \mathrm{End}_{\mathbf{Q}}(J)^\times$ (this has the effect of multiplying α by ε^2) in the sense that we minimize the images $\alpha^\sigma \in \mathbf{R}_{>0}$ under the real embeddings of $\mathcal{O}$ (in practice, we minimize the trace of α). This leads to potentially smaller Heegner points on J, which simplifies some of the computations.

3.2. *Determining Heegner fields*

To be able to use the results of [52] and some other results that require the discriminant of the Heegner field to be odd, we restrict to odd discriminants in the following.

We find a Heegner field K by enumerating the odd discriminants $-D$ of imaginary quadratic number fields with the property that all prime divisors of N split completely in $\mathcal{O}_K$ (this can be checked easily by computing Legendre symbols). The condition $\mathrm{ord}_{s=1} L(f/K, s) = 1$ is equivalent to $L(f \otimes \varepsilon_K, 1) \neq 0$ when L-rk $J = 1$ and to $L'(f \otimes \varepsilon_K, 1) \neq 0$ when L-rk $J = 0$. Using modular symbols as described in [31, §2.8], we can decide whether $L(f \otimes \varepsilon_K, 1) = 0$ or not. The nonvanishing of $L'(f \otimes \varepsilon_K, 1)$ can be proved by computing it to a high enough precision using Dokchitser’s Magma implementation [40]. Alternatively and in practice (because the evaluation of the twisted L-value can take fairly long when N is large), we can compute the Heegner point for a given K; if it is non-torsion, then K is a suitable Heegner field.

3.3. *Computing the endomorphism ring and its action on Mordell–Weil groups*

We need to determine the endomorphism ring $\mathcal{O}$ of the Jacobian J and how it acts on the Mordell–Weil group $J(\mathbf{Q})$ or $J^K(\mathbf{Q})$, or, more generally, on $J(L)$ for some number field L. For this, we compute a numerical approximation to the big period matrix as in Section 3.1; potential endomorphisms can be guessed from this information. To verify that the presumed endomorphism ring is the correct one, we can use data from the LMFDB [68]. (Alternatively, one could use [70].) This shows that the numerical endomorphisms are close to actual endomorphisms and thus gives us a representation of $\mathcal{O}$ as a subring

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

of a matrix algebra over $\mathbf{Z}$, together with its action on the complex torus $\mathbf{C}^2/\Lambda \cong J(\mathbf{C})$. To compute the action of $\mathcal{O}$ on $J(L)$, we use an improved version of Magma's `(To/From)AnalyticJacobian` to convert between points in $J(\mathbf{C})$ in Mumford representation and representatives in $\mathbf{C}^2$. (The improvement also handles points at infinity and Weierstrass points.) For a generator γ of $\mathcal{O}$ and each generator x of $J(L)$, we map x to $\mathbf{C}^2/\Lambda$, apply γ to the image, and map back to $J(\mathbf{C})$. We then recognize the coefficients of the Mumford representation as elements of L using Magma's `MinimalPolynomial` and check that the coefficients we recognize really define a point in $J(L)$. We then write the resulting point as a linear combination of the generators of $J(L)$. In this way, we obtain a matrix giving the action of γ on $J(L)$ with respect to the chosen generators. We can bound the height of $\gamma \cdot x$ by $\max_\sigma |\gamma^\sigma|^2$ times the height of x, so there are only finitely many candidates for $\gamma \cdot x$, which allows us to determine $\gamma \cdot x$ exactly by computing with sufficient precision. As an additional check, we verify that the matrix we obtain has the same minimal polynomial as γ.

3.4. Computing Heegner points analytically

Recall that π denotes the isogeny $A_f \to J$ and that we want to compute the Heegner point

$$y_{K,\pi} = \pi_J(y_K) = \pi(y_{K,A_f}) \in J(K).$$

In this section, we explain how to find $y_{K,\pi}$ explicitly. Also recall that $\boldsymbol{\pi}$ denotes the real number giving the area of the unit disk, to avoid confusion with the isogeny π.

We obtain a computational representation of the isogeny $\pi \colon A_f \to J$ as described in Section 3.1. Since we know that an isogeny has to exist, we can be sure that what we obtain indeed describes an actual isogeny.

To find the Heegner point on J, we first determine the integral binary quadratic 'Heegner forms' associated to K and N. These are representatives of the h_K classes of positive definite binary quadratic forms of discriminant D_K such that their roots $\tau \in \mathbf{H}$ map to the points in the Heegner cycle $\mathbf{x}_K$. Let $(f_1, \ldots, f_g)$ be the $\mathbf{Z}$-basis of $S_2(f, \mathbf{Z})$ that is used for the computation of the big period matrix of A_f (it can be obtained via the Magma function `qIntegralBasis`). We then compute the period integrals

$$P(\tau, j) := 2\boldsymbol{\pi} i \int_{i\infty}^{\tau} f_j(z)\,dz = \int_0^{e^{2\boldsymbol{\pi} i\tau}} \sum_{n\geq 1} a_n(f_j) q^n \frac{dq}{q} = \sum_{n\geq 1} \frac{a_n(f_j)}{n} e^{2\boldsymbol{\pi} i\tau n} \in \mathbf{C}$$

for each of these roots τ and each $1 \leq j \leq g$ to the desired precision. (We pick our Heegner forms in such a way that τ has imaginary part as large as possible. We can use the bound $|a_n^\sigma| \leq \sqrt{3}n$ (see [50, Lemma 2.9], where a bound $|a_n^\sigma| \leq n$ is claimed, but their argument bounding $|a_{p^m}^\sigma|$ is not correct for powers of 2 or 3) and the representation of f_j as a linear combination of the f^σ to determine the number of terms we need. The points $y_\tau = \big(P(\tau, j)\big)_j \in \mathbf{C}^g/\Lambda_f \simeq A_f(\mathbf{C})$ then are of the form $[x_\tau - (\infty)]$ projected to A_f, where ∞ is the cusp at infinity and x_τ runs through the points in the support of the Heegner cycle $\mathbf{x}_K$. In particular, we have $\sum_\tau y_\tau = y_{K,A_f}$.

We then use the matrix α_π associated to the isogeny π to map y_K or all the points y_τ to $\mathbf{C}^g/\Lambda \cong J(\mathbf{C})$. We apply the numerical inverse of the Abel–Jacobi map to find the Mumford representation of this or these points as points on J. We then try to recognize the coefficients in the Mumford representation as elements of K (for $\pi(y_{K,A_f}) = y_{K,\pi}$) or of H (for $\pi(y_\tau)$) and check that this really gives rise to a point in $J(K)$ or $J(H)$.

Using the action of $\mathcal{O}$ on $J(K)$ that we have determined in Section 3.3, we can then determine the $\mathcal{O}$-span of $y_{K,\pi}$ and from it the ideal

$$\mathcal{I}_{K,\pi} = \mathrm{Char}_{\mathcal{O}}(J(K)/\mathcal{O}y_{K,\pi})$$

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

and the index $I_{K,\pi} = (J(K) : \mathcal{O}y_{K,\pi})$. The corresponding index for A_f is $I_K = (A_f(K) : \mathbf{Z}[f]\cdot y_{K,A_f})$. We can express it in terms of $I_{K,\pi}$ via

$$I_K = \frac{(\mathcal{O}_{\mathbf{Q}(f)} : \mathbf{Z}[f])}{(\mathcal{O}_{\mathbf{Q}(f)} : \mathcal{O})} \cdot \frac{\#A_f[\pi](K)}{\#\big(J(K)/\pi(A_f(K))\big)} \cdot I_{K,\pi}.$$

The first factor on the right takes care of the fact that $\mathbf{Z}[f]$ and $\mathcal{O} = \operatorname{End}_{\mathbf{Q}}(J)$ can be different orders in $\mathbf{Q}(f)$; it can be computed easily as $\sqrt{\operatorname{disc}\mathbf{Z}[f]/\operatorname{disc}\mathcal{O}}$. The second factor captures the effect of the isogeny π. Note that the second factor can be multiplicatively bounded from above by $\#A_f[\pi](K) \mid \deg\pi$, which gives a multiplicative upper bound for I_K as well. (We may get a better bound than $\deg\pi$ from bounding $\#A_f(K)_{\mathrm{tors}}$ using the coefficients of the L-series of A_f/K.)

We will need $I_{K,\pi}$ in Section 4.4 for the computation of $Ш(J/\mathbf{Q})_{\mathrm{an}}$ when L-rk $J = 1$ and in Section 5.2 for the determination of an explicit finite support of $Ш(J/\mathbf{Q})$. We will need (a multiplicative upper bound for) I_K in Section 7.

3.5. Computing the Petersson norm of a newform

Let $\sigma\colon \mathbf{Q}(f) \hookrightarrow \mathbf{R}$ be an embedding. For the Gross–Zagier formula, we need the Petersson norms of the conjugates f^σ for the various possible σ. We identify $X_0(N)(\mathbf{C})$ with $\Gamma_0(N)\backslash\mathbf{H}^*$ (where $\mathbf{H}^* = \mathbf{H}\cup\mathbf{P}^1(\mathbf{Q})$ is the upper half-plane together with the cusps) and use the normalization

$$\|f^\sigma\|^2 = \int_{X_0(N)(\mathbf{C})} |f^\sigma(x+yi)|^2\, dx \wedge dy$$

for the Petersson norm of $f^\sigma \in S_2(\Gamma_0(N), \mathbf{C})$ as in [52, (5.1)]. (Sometimes this is normalized differently by dividing by the volume $\mu(X_0(N)(\mathbf{C}))$ to make it independent of the choice of N.) We compute the Petersson norm by relating it to the *symmetric square L-function* $L(\operatorname{Sym}^2 f^\sigma, s)$.

If an L-function $L(\mathcal{X}, s)$ has an Euler product expansion, we write it as

$$L(\mathcal{X}, s) = \prod_\ell L_\ell(\mathcal{X}, \ell^{-s})^{-1},$$

where $L_\ell(\mathcal{X}, T) \in R[T]$ (with R the coefficient ring of the L-function) is the Euler polynomial at ℓ.

We define the symmetric square L-function $L(\operatorname{Sym}^2 f, s)$ as the L-function associated to the strictly compatible system $(\operatorname{Sym}^2 \rho_{\mathfrak{p}^\infty, f})$ of $\mathfrak{p}$-adic Galois representations. For a prime $\ell \nmid N$, write

$$L_\ell(f, T) = 1 - a_\ell T + \ell T^2 = (1-\alpha_\ell T)(1-\beta_\ell T)\,;$$

then

$$\begin{aligned} L_\ell(\operatorname{Sym}^2 f, T) &= (1-\alpha_\ell^2 T)(1-\alpha_\ell\beta_\ell T)(1-\beta_\ell^2 T) \\ &= (1-\ell T)\big((1+\ell T)^2 - a_\ell^2 T\big). \end{aligned} \tag{3.9}$$

We define the *imprimitive symmetric square L-function* $\tilde{L}(\operatorname{Sym}^2 f, s)$ by this formula for the Euler polynomial at *all* primes (then we take $\alpha_\ell = a_\ell$ and $\beta_\ell = 0$ when $\ell \mid N$); compare [24, p. 110]. (The difference is whether we take I_ℓ-coinvariants before ($\tilde{L}(\operatorname{Sym}^2 f, s)$) or after ($L(\operatorname{Sym}^2 f, s)$) applying Sym^2 when defining the Euler polynomials.) This imprimitive version is what Shimura denotes $D(s)$ in [103].

We thank user334725 on MathOverflow [115] for pointers to the relevant literature.

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

Proposition 3.8. *Let $f \in S_2(\Gamma_0(N), \mathbf{C})$ be a normalized eigenform. Then the Petersson norm of f is given by*

$$\|f\|^2 = \frac{N}{8\pi^3} \cdot \tilde{L}(\operatorname{Sym}^2 f, 2).$$

Proof. Denote the Fourier coefficients of f by a_n. We set

$$D(f, s) := \sum_{n \geq 1} \frac{a_n^2}{n^s}.$$

By [83, Satz 6] (and taking into account the different normalization (compare also [104, Eq. (2.5)])),

$$\begin{aligned} \|f\|^2 &= [\Gamma(1) : \Gamma_0(N)] \frac{\pi}{3} \frac{1}{(4\pi)^2} \operatorname{res}_{s=2} D(f, s) \\ &= N \prod_{\ell \mid N} \left(1 + \frac{1}{\ell}\right) \frac{1}{48\pi} \operatorname{res}_{s=2} D(f, s). \end{aligned} \tag{3.10}$$

By [103, Eq. (0.4)] (see [104, Lemma 1] for the relation between the Euler factors), we have the following equality, where the superscript N means that we leave out the Euler factors coming from prime divisors of N.

$$D(f, s) = \frac{\zeta^N(s-1)}{\zeta^N(2s-2)} \tilde{L}(\operatorname{Sym}^2 f, s).$$

Taking the residue at $s = 2$ on both sides, we obtain

$$\operatorname{res}_{s=2} D(f, s) = \frac{6}{\pi^2} \prod_{\ell \mid N} \left(1 + \frac{1}{\ell}\right)^{-1} \tilde{L}(\operatorname{Sym}^2 f, 2),$$

which gives the desired result when used in (3.10). □

So we need to compute $\tilde{L}(\operatorname{Sym}^2 f, 2)$. However, we cannot directly do that since $\tilde{L}(\operatorname{Sym}^2 f, 2)$ does not in general satisfy a suitable functional equation (which is needed to obtain a reasonably fast converging series for the value via a Mellin transform). We can, however, compute $L(\operatorname{Sym}^2 f, 2)$ if we know its Euler factors at primes dividing N. So we need to determine these Euler factors; combining this with (3.9) will also tell us what the correction factor $\tilde{L}(\operatorname{Sym}^2 f, 2)/L(\operatorname{Sym}^2 f, 2)$ is.

For a prime ℓ, we set

$$C_\ell := \frac{L_\ell(\operatorname{Sym}^2 f, \ell^{-2})}{\tilde{L}_\ell(\operatorname{Sym}^2 f, \ell^{-2})}.$$

Corollary 3.9. *Let f and C_ℓ be as above. Then*

$$\|f\|^2 = \frac{N}{8\pi^3} \prod_{\ell^2 \mid N} C_\ell \cdot L(\operatorname{Sym}^2 f, 2).$$

In particular,

$$\|f\|^2 = \frac{N}{8\pi^3} \cdot L(\operatorname{Sym}^2 f, 2)$$

when the level N is squarefree.

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

Proof. This follows from proposition 3.8 and the definition of C_ℓ, together with the fact that $C_\ell = 1$ unless $\ell^2 \mid N$, which will be shown in lemma 3.10 below. □

Alternative algorithms for computing the Petersson inner product are described in [25] and have been implemented in Pari.

Using the formula in corollary 3.9, we can compute $\|f^\sigma\|^2$ using [40] for all $\sigma \in \Sigma$ if we can determine the Euler factors $L_\ell(\operatorname{Sym}^2 f, T)$ for the primes $\ell \mid N$. We will do that in the following subsection.

3.6. *Euler factors of the symmetric square L-function*

In this section, we explain how to find the Euler factors of $L(\operatorname{Sym}^2 f, s)$ at primes ℓ dividing the level N of f. In [24, §1], analogous statements are shown for the L-function of an elliptic curve, and [94] has similar results stated in a somewhat different language.

Recall that when $\ell \nmid N$, $L_\ell(\operatorname{Sym}^2 f, T) = \tilde{L}_\ell(\operatorname{Sym}^2 f, T)$ (and hence $C_\ell = 1$), and we can write down $\tilde{L}_\ell(\operatorname{Sym}^2 f, T)$ easily in terms of $L_\ell(f, T)$. We now consider the case $v_\ell(N) = 1$.

Lemma 3.10. *Assume that* $v_\ell(N) = 1$. *Then*

$$L_\ell(\operatorname{Sym}^2 f, T) = \tilde{L}_\ell(\operatorname{Sym}^2 f, T) = 1 - T.$$

In particular, $C_\ell = 1$ *whenever* $\ell^2 \nmid N$.

Proof. Fix some $\mathfrak{p} \nmid N\ell$ and set $p = p(\mathfrak{p})$ and $V_\mathfrak{p} = V_\mathfrak{p}(A_f)$. Since $v_\ell(N) = 1$, $V_\mathfrak{p}$ has a one-dimensional quotient of I_ℓ-coinvariants. Since $\chi_{p^\infty} = \det \circ \rho_{\mathfrak{p}^\infty}$ is trivial on I_ℓ, it follows that $\rho_{\mathfrak{p}^\infty}(I_\ell)$ lands in a unipotent subgroup (compare lemma 2.32). The image is nontrivial, since otherwise, $\ell \nmid N$. Since $\ell \neq p$ and the unipotent subgroups of $\mathrm{GL}_2(\mathbf{Q}(f)_\mathfrak{p})$ are pro-p groups, whereas the wild inertia at ℓ is a pro-ℓ group, it follows that $\rho_{\mathfrak{p}^\infty}|_{I_\ell}$ factors through the tame inertia group I_ℓ^{t}. By lemma 2.7, conjugating by any lift Frob_ℓ of the Frobenius automorphism to I_ℓ^{t} has the effect of raising to the ℓth power. Using that $\det \rho_{\mathfrak{p}^\infty}(\mathrm{Frob}_\ell) = \chi_{p^\infty}(\mathrm{Frob}_\ell) = \ell$, it follows that (with respect to a suitable $\mathbf{Q}(f)_\mathfrak{p}$-basis), $\rho_{\mathfrak{p}^\infty}(\mathrm{Frob}_\ell) = \pm\left(\begin{smallmatrix} \ell & 0 \\ 0 & 1 \end{smallmatrix}\right)$and $\rho_{\mathfrak{p}^\infty}|_{I_\ell} \subseteq \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$. This implies that $L_\ell(f, T) = 1 \mp T$, and so $\tilde{L}_\ell(\operatorname{Sym}^2 f, T) = 1 - T$. We also see that

$$\operatorname{Sym}^2 \rho_{\mathfrak{p}^\infty}|_{\mathrm{Gal}(\overline{\mathbf{Q}}_\ell|\mathbf{Q}_\ell)} = \begin{pmatrix} \chi_{p^\infty}^2 & * & * \\ 0 & \chi_{p^\infty} & * \\ 0 & 0 & 1 \end{pmatrix}$$

with a one-dimensional I_ℓ-coinvariant quotient, on which Frob_ℓ acts trivially. This shows that $L_\ell(\operatorname{Sym}^2 f, T) = 1 - T$ as well. (This is analogous to [24, Lemma 1.2].)

In particular, $C_\ell = 1$, which, together with the discussion preceding this lemma, gives the last claim. □

We now consider the case $\ell^2 \mid N$. We first note that $L(\operatorname{Sym}^2 f, s)$ does not change under quadratic twists.

Lemma 3.11. *Let* $\tilde{f}$ *be a quadratic twist of* f. *Then*

$$L(\operatorname{Sym}^2 \tilde{f}, s) = L(\operatorname{Sym}^2 f, s).$$

Proof. We consider the Euler factor at ℓ. Fix some $\mathfrak{p} \nmid N\ell$ and set $p = p(\mathfrak{p})$ and $V_\mathfrak{p} = V_\mathfrak{p}(A_f)$. Let ε be the quadratic character such that $\tilde{f} = f \otimes \varepsilon$. Since the canonical group homomorphism $\mathrm{GL}(V_\mathfrak{p}) \to \mathrm{GL}(\operatorname{Sym}^2 V_\mathfrak{p})$ is trivial on ±id, it follows that $\operatorname{Sym}^2(\rho_{\mathfrak{p}^\infty} \otimes \varepsilon) = \operatorname{Sym}^2 \rho_{\mathfrak{p}^\infty}$, which, upon restricting to $\mathrm{Gal}(\overline{\mathbf{Q}}_\ell|\mathbf{Q}_\ell)$, directly translates into $L_\ell(\operatorname{Sym}^2 \tilde{f}, T) = L_\ell(\operatorname{Sym}^2 f, T)$. The claim follows. □

The argument in the proof together with the fact that $\rho_{\mathfrak{p}^\infty}(I_\ell) \subseteq \mathrm{SL}(V_\mathfrak{p})$ shows that the action of I_ℓ on $\mathrm{Sym}^2 V_\mathfrak{p}$ depends only on the projective image $\mathbf{P}\rho_{\mathfrak{p}^\infty}(I_\ell) \subseteq \mathrm{PSL}(V_\mathfrak{p})$. We will see that the dimension of the I_ℓ-coinvariants of $\mathrm{Sym}^2 V_\mathfrak{p}$ depends on whether this projective image is abelian or not.

Lemma 3.12. *Let k be a field of characteristic zero and let V be a two-dimensional k-vector space. Let $G \subseteq \mathrm{SL}(V)$ be such that $\mathbf{P}G$ is not unipotent.*

(1) *If $\mathrm{Sym}^2 V$ has a nontrivial G-invariant quotient, then G is abelian.*
(2) *If $\mathbf{P}G$ is abelian, then $\bar{V} := V \otimes_k \bar{k}$ has a basis e_1, e_2 consisting of simultaneous eigenvectors for the elements of G. The G-coinvariant space of $\mathrm{Sym}^2 \bar{V} = \langle e_1^2, e_1e_2, e_2^2\rangle$ is one-dimensional and is isomorphic to the direct summand $\bar{k} \cdot e_1e_2$.*

Proof. We can assume without loss of generality that k is algebraically closed.

(1) If $\mathrm{Sym}^2 V$ has a nontrivial G-invariant quotient, then $\mathrm{Sym}^2 V^*$ has a nonzero G-invariant element, which is a quadratic form q on V. Then G must fix the zero set of q in $\mathbf{P}^1(k)$. This zero set can have either one or two elements.

In the first case, G fixes a point in $\mathbf{P}^1$, and hence is contained in a Borel subgroup, so, after fixing a suitable basis, the associated representation ρ has the form $\left(\begin{smallmatrix}\chi & \alpha \\ 0 & \chi^{-1}\end{smallmatrix}\right)$ with a character χ such that $\chi^2 \neq \mathbf{1}$ (recall that $\mathbf{P}G$ is not unipotent). Then (with the columns giving the action on X^2, XY, Y^2, when X, Y is the given basis with $\rho(g)X = \chi(g)X$, $\rho(g)Y = \alpha(g)X + \chi^{-1}(g)Y$)

$$\mathrm{Sym}^2 \rho = \begin{pmatrix}\chi^2 & \alpha\chi & \alpha^2 \\ 0 & \mathbf{1} & 2\alpha\chi^{-1} \\ 0 & 0 & \chi^{-2}\end{pmatrix},$$

and this has nontrivial G-coinvariants only when $\alpha = 0$, which implies that G is abelian.

In the second case, G is contained in the normalizer of a Cartan subgroup, so its elements are (with respect to a suitable basis (e_1, e_2)) either of the form $\left(\begin{smallmatrix}a & 0 \\ 0 & a^{-1}\end{smallmatrix}\right)$ (which fix $e_1 \cdot e_2$) or of the form $\left(\begin{smallmatrix}0 & -a \\ a^{-1} & 0\end{smallmatrix}\right)$. However, the elements of the second form send $e_1 \cdot e_2$ to its negative, so (noting that there must be elements of the first form with $a^2 \neq 1$, again since $\mathbf{P}G$ is not unipotent, so that neither e_1^2 nor e_2^2 can be fixed by G) such elements cannot be present in G, which again implies that G is abelian.

(2) If $\mathbf{P}G$ is abelian, then so is G. The representation on V then splits as a sum of two characters χ and χ^{-1} such that $\chi^2 \neq 1$. Let e_1 and e_2 be corresponding eigenvectors. Then $\mathrm{Sym}^2 V$ splits as $\chi^2 \oplus \mathbf{1} \oplus \chi^{-2}$, with the G-action on e_1e_2 being trivial. This shows the claim.

□

This leads to the following classification.

Lemma 3.13. *Let ℓ be a prime such that $\ell^2 \mid N$. Then $\tilde{L}_\ell(\mathrm{Sym}^2 f, T) = 1$. Let $\tilde{f}$ be a quadratic twist of f whose level $\tilde{N}$ is (multiplicatively) minimal. Fix a regular prime ideal $\mathfrak{p} \nmid N\ell$ of $\mathbf{Z}[f]$.*

(1) *$\mathbf{P}\rho_{\mathfrak{p}^\infty}(I_\ell)$ is trivial if and only if $\ell \nmid \tilde{N}$. In particular, using (3.9),*

$$C_\ell = \frac{(\ell-1)((\ell+1)^2 - a_\ell(\tilde{f})^2)}{\ell^3}.$$

(2) *$\mathbf{P}\rho_{\mathfrak{p}^\infty}(I_\ell)$ is nontrivial and unipotent if and only if $v_\ell(\tilde{N}) = 1$. In this case, $L_\ell(\mathrm{Sym}^2 f, T) = 1 - T$ and the conductor exponent of $\mathrm{Sym}^2 f$ at ℓ is 2. In particular, $C_\ell = \frac{\ell^2-1}{\ell^2}$.*
(3) *$\mathbf{P}\rho_{\mathfrak{p}^\infty}(I_\ell)$ is abelian and not unipotent if and only if $v_\ell(\tilde{N}) = 2$. In this case, $L_\ell(\mathrm{Sym}^2 f, T) = 1 \mp \ell T$, with the negative sign if and only if $\rho_{\mathfrak{p}^\infty}(\mathrm{Gal}(\overline{\mathbf{Q}}_\ell|\mathbf{Q}_\ell))$ is abelian, and the conductor exponent of $\mathrm{Sym}^2 f$ at ℓ is 2. In particular, $C_\ell = \frac{\ell\mp1}{\ell}$ (with the same sign).*

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

(4) $\mathbf{P}\rho_{\mathfrak{p}^\infty}(I_\ell)$ *is nonabelian if and only if* $v_\ell(\tilde{N}) \geq 3$. *In this case, we have* $L_\ell(\mathrm{Sym}^2 f, T) = 1$, *and the conductor exponent of* $\mathrm{Sym}^2 f$ *at* ℓ *is at least* 4 *and at most* $2v_\ell(\tilde{N}) - 1$. *In particular,* $C_\ell = 1$.

Proof. When $\ell^2 \mid N$, then the space of I_ℓ-coinvariants is trivial, and hence, so is its symmetric square. This means that $\tilde{L}_\ell(\mathrm{Sym}^2 f, T) = 1$. By lemma 3.11, we have that $L(\mathrm{Sym}^2 f, s) = L(\mathrm{Sym}^2 \tilde{f}, s)$. It suffices to show the 'only if' direction of the equivalences at the beginning of each statement since the consequences exhaust all possibilities disjointly.

(1) If $\mathbf{P}\rho_{\mathfrak{p}^\infty}(I_\ell)$ is trivial, then $\rho_{\mathfrak{p}^\infty}|_{I_\ell}$ is of the form $(\mathbf{1} \oplus \mathbf{1}) \otimes \varepsilon$ with a quadratic character ε. Twisting by ε makes the representation unramified at ℓ, so $\ell \nmid \tilde{N}$ (using that $\tilde{N}$ is minimal). The statement on C_ℓ then follows.

(2) If the projective image is nontrivial and unipotent, then there is a quadratic character ε such that $\rho_{\mathfrak{p}^\infty} \otimes \varepsilon|_{I_\ell}$ is unipotent and nontrivial, which implies that $v_\ell(\tilde{N}) = 1$. The statement on the Euler factor then follows from lemma 3.10.

(3) We assume that $\mathbf{P}\rho_{\mathfrak{p}^\infty}(I_\ell)$ is abelian, but not unipotent. By lemma 3.12, $\mathrm{Sym}^2 V_{\mathfrak{p}}$ has a one-dimensional I_ℓ-coinvariant space. Also, because $\rho_{\mathfrak{p}^\infty}|_{I_\ell}$ is a sum of two characters of order coprime to ℓ, the representation factors through the tame inertia group, and hence, there is no wild part in the conductor. This shows that $v_\ell(\tilde{N}) = 2$ and that the conductor exponent of $\mathrm{Sym}^2 f = \mathrm{Sym}^2 \tilde{f}$ is $3 - 1 = 2$. Also by lemma 3.12, the coinvariant space corresponds to the tensor product of the two one-dimensional representations in the splitting of $V_{\mathfrak{p}}$. Frobenius either fixes each of these two one-dimensional spaces, in which case its action on the tensor product is by $\det(\rho_{\mathfrak{p}^\infty}(\mathrm{Frob}_\ell)) = \ell$; then $L_\ell(\mathrm{Sym}^2 f, T) = 1 - \ell T$, and $\rho_{\mathfrak{p}^\infty}(\mathrm{Gal}(\overline{\mathbf{Q}}_\ell|\mathbf{Q}_\ell))$ is abelian. Or else Frob_ℓ swaps the two spaces; then it acts by the negative of the determinant (compare the proof of lemma 3.12), so $L_\ell(\mathrm{Sym}^2 f, T) = 1 + \ell T$, and $\rho_{\mathfrak{p}^\infty}(\mathrm{Gal}(\overline{\mathbf{Q}}_\ell|\mathbf{Q}_\ell))$ is nonabelian.

(4) We assume that $\mathbf{P}\rho_{\mathfrak{p}^\infty}(I_\ell)$ is nonabelian. This implies that it is not unipotent. By lemma 3.12, the I_ℓ-coinvariant space of $\mathrm{Sym}^2 V_{\mathfrak{p}}$ is trivial. This shows that $L_\ell(\mathrm{Sym}^2 f, T) = 1$. Also, $\mathbf{P}\rho_{\mathfrak{p}^\infty}|_{I_\ell}$ cannot factor through the tame inertia group since the latter is abelian. So there must be wild ramification at ℓ both in $\mathbf{P}\rho_{\mathfrak{p}^\infty}$ and in $\mathrm{Sym}^2 \rho_{\mathfrak{p}_\infty}$. As the tame parts of the conductor exponents of these two are given by $\dim V_{\mathfrak{p}} = 2$ and $\dim \mathrm{Sym}^2 V_{\mathfrak{p}} = 3$, respectively, it follows that $\ell^3 \mid \tilde{N}$ and the conductor exponent c of $\mathrm{Sym}^2 f$ is at least 4. To obtain the claimed upper bound, we observe that when $\rho\colon G \longrightarrow \mathrm{GL}(V)$ is a 2-dimensional representation, then the codimension of the invariant subspace of $\mathrm{Sym}^2 \rho$ is at most twice the codimension of the invariant subspace of ρ. Then [97, Eq. (1.2.1)] implies that the wild part $c - 3$ of c is at most twice the wild part $v_\ell(\tilde{N}) - 2$ of the conductor exponent of $\tilde{f}$. This gives the desired bound. □

Given f, a choice of $\tilde{f}$ can be obtained from the LMFDB. Alternatively, the conductor d of the twisting character ε must satisfy $d^2 \mid N$, so we can check the finitely many possibilities for ε and compare the resulting levels to find $\tilde{f}$.

Which of the two possibilities for the Euler factor in case (3) is correct and what the correct choice of conductor exponent is in case (4) can be checked by trying all possibilities and determining which one is compatible with the functional equation. Using the function `SymmetricPower` that Magma provides for constructing symmetric power L-functions seems to result in fairly slow code. Instead, we compute the relevant number of coefficients ourselves and use this coefficient sequence when constructing the L-series, which is then used for testing the functional equation and evaluating at $s = 2$.

3.7. *Computing the height of a Heegner point using the Gross–Zagier formula*

To state the Gross–Zagier formula, we need to introduce some more notation. Let K be a Heegner field for f. Recall that H denotes the Hilbert class field of K. The Heegner cycle $\mathbf{x}_K$ on $X_0(N)$ and the Heegner point $y_K = [\mathbf{x}_K - h_K \cdot (\infty)] \in J_0(N)(K)$ have been defined in the introduction to this section. Recall that $I_f = \mathrm{Ann}_{\mathbf{T}}(f)$.

The action of $\mathbf{T}$ (or its quotient $\mathrm{End}_{\mathbf{Q}}(J_0(N))$) on $J_0(N)(K)$ extends to a linear action on the real vector space $J_0(N)(K) \otimes_{\mathbf{Z}} \mathbf{R}$. Since the center Z of $\mathrm{End}_{\mathbf{Q}}(J_0(N))$ is an order in a totally real étale

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

$\mathbf{Q}$-algebra, we obtain a canonical decomposition

$$J_0(N)(K) \otimes_{\mathbf{Z}} \mathbf{R} = \bigoplus_{\sigma\colon Z \hookrightarrow \mathbf{R}} J_0(N)(K)_\sigma$$

into isotypical linear subspaces. If σ factors through $\mathbf{Z}[f]$, then

$$J_0(N)(K)_\sigma \subseteq A_f^\vee(K) \otimes_{\mathbf{Z}} \mathbf{R} = J_0(N)(K)[I_f] \otimes_{\mathbf{Z}} \mathbf{R},$$

and by the Heegner hypothesis (which implies that $A_f^\vee(K)$ has rank 1 as a $\mathbf{Z}[f]$-module), it follows that $\dim J_0(N)(K)_\sigma = 1$. We will abuse notation slightly and also write $J_0(N)(K)_\sigma$ when $\sigma \in \Sigma$, implicitly pre-composing with the projection $Z \longrightarrow \mathbf{Z}[f]$. We write $y_{K,\sigma} \in J_0(N)(K)_\sigma$ for the components of y_K with respect to this composition and set

$$y_K^f := \sum_{\sigma \in \Sigma} y_{K,\sigma} \in A_f^\vee(K) \otimes_{\mathbf{Z}} \mathbf{R};$$

Then $\lambda_f(y_K^f) = y_{K,A_f}$; compare the diagram (3.4). Note that $\omega \in \mathbf{Q}(f)$ acts on $y_{K,\sigma}$ as $\omega \cdot y_{K,\sigma} = \omega^\sigma y_{K,\sigma}$. Explicitly, when $(b_j)_{1\le j\le g}$ is a $\mathbf{Z}$-basis of $\mathbf{Z}[f]$ and $(b_j^*)_{1\le j\le g}$ is its dual basis in $\mathbf{Z}[f] \otimes_{\mathbf{Z}} \mathbf{R}$ with respect to the trace form, we have

$$y_{K,\sigma} = \sum_{j=1}^{g} (b_j \cdot y_K) \otimes b_j^{*\,\sigma}. \tag{3.11}$$

The normalized canonical height on $J_0(N)(K)$ (with respect to twice the theta divisor) induces a positive definite quadratic form on $J_0(N)(K) \otimes_{\mathbf{Z}} \mathbf{R}$, which (by abuse of notation) we also denote $\hat{h}$. Since the endomorphisms are self-adjoint with respect to the height pairing (this is because they are fixed under the Rosati involution; see [9, Section 5.5] and recall that the endomorphism ring is totally real), it follows that the σ-components are pairwise orthogonal under the height pairing.

Recall that we write $L(f/K, s)$ for the L-function of f base-changed to K. This is the same as $L(f, \mathbf{1}, s)$ for the trivial character $\mathbf{1}\colon \mathrm{Gal}(H|K) \to \mathbf{C}^\times$ in the notation of [52].

Theorem 3.14 (Gross–Zagier formula). *With the notation introduced above and assuming that D_K is odd, we have*

$$\hat{h}(y_{K,\sigma}) = L'(f^\sigma/K, 1)\frac{u_K^2\sqrt{-D_K}}{16\pi^2\|f^\sigma\|^2}.$$

Here, $u_K := \#\mathcal{O}_K^\times/\mathbf{Z}^\times$, which equals 1 for $D_K < -4$, 2 for $D_K = -4$ and 3 for $D_K = -3$.

Proof. This is a reformulation of [52, Theorem I.6.3], taking into account that our $\hat{h}$ is $1/2h_K$ times the height used there (see [52, Eq. (I.6.4)]), where h_K is the class number of K. Note that Gross and Zagier assume that the Heegner discriminant is odd; see [52, §I.3]. □

To evaluate this formula, we need the Petersson norm from 3.5, and we need to evaluate $L'(f^\sigma/K, 1)$. By the Artin formalism of L-functions,

$$L(f/K, s) = L(f, s)L(f \otimes \varepsilon_K, s)$$

with $f \otimes \varepsilon_K$ the twist of f by (the Kronecker character associated to) K. Its first derivative at $s = 1$ is

$$L'(f/K, 1) = L(f, 1)L'(f \otimes \varepsilon_K, 1) + L'(f, 1)L(f \otimes \varepsilon_K, 1).$$

Since K is a Heegner field by assumption, $L(f/K, s)$ vanishes to first order at $s = 1$. This implies that exactly one of the two terms in the sum is nonzero; which one it is can be decided by considering the

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

action of the Fricke involution w_N on f: if $w_N \cdot f = f$, then $L(f, 1) = 0$; otherwise, $w_N \cdot f = -f$, and $L'(f, 1) = 0$. The special values of the L-functions of newforms and their derivatives can be computed to arbitrary precision using Tim Dokchitser's Magma implementation [40]. It provides a `TensorProduct` function for L-functions, which, however, tends to be slow in our use case. So we construct the tensor product L-function $L(f \otimes \varepsilon_K, s)$ 'by hand' for performance reasons, explicitly giving the Euler factors.

We finally obtain a formula for $\hat{h}(y_K^f)$.

Corollary 3.15. *Let K be a Heegner field for f and let $y_K^f \in A_f(K)^\vee$ be an associated Heegner point. Then*

$$\hat{h}(y_K^f) = \frac{u_K^2 \sqrt{-D_K}\pi}{2N \prod_{\ell^2 | N} C_\ell} \sum_{\sigma \in \Sigma} \frac{L'(f^\sigma/K, 1)}{L(\mathrm{Sym}^2 f^\sigma, 2)}.$$

Proof. Since the $y_{K,\sigma}$ are orthogonal with respect to the height pairing, we have $\hat{h}(y_K^f) = \sum_\sigma \hat{h}(y_{K,\sigma})$. Now combine theorem 3.14 and corollary 3.9. □

3.8. Comparing canonical heights

Our goal in this section is to determine $\hat{h}_J(y_{K,\pi})$ (so that we can either use that to identify $y_{K,\pi}$ up to a sign and adding torsion assuming there is an essentially unique point of that height, or to verify that our computation of $y_{K,\pi}$ is correct). Recall the diagram (3.4) –in particular, the endomorphism α of J defined in (3.5). Note that $\lambda = \pi_J \circ \pi_J^\vee$ equals α composed with the inverse of the canonical polarization λ_J of J induced by the theta divisor.

We freely use standard facts about height pairings on abelian varieties; see, for example, [10, §9]. We denote by $\langle -, - \rangle_J$ the height pairing on J (such that $\hat{h}_J(x) = \langle x, x \rangle_J$). By [10, Prop. 9.3.6] (noting that our $\hat{h}_J$ is twice their $\hat{h}_\theta$), it satisfies

$$\langle x, x' \rangle_J = \hat{h}_{\mathscr{P}}(\lambda_J(x), x'),$$

where $\hat{h}_{\mathscr{P}}(-)$ is the canonical height on $J^\vee \times J$ associated to the Poincaré bundle $\mathscr{P}$. Similarly, we obtain the canonical height associated to a polarization $\lambda \colon J^\vee \to J$ as $\hat{h}_\lambda(x) = \hat{h}_{\mathscr{P}}(x, \lambda(x))$. If $\varphi \colon A \to J$ is a homomorphism and $\lambda_{A^\vee} \colon A^\vee \to A$ is a polarization such that

$$\lambda = \varphi^{\vee *}\lambda_{A^\vee} = \varphi \circ \lambda_{A^\vee} \circ \varphi^\vee = \alpha \circ \lambda_J^{-1}$$

with $\alpha \in \mathrm{End}_{\mathbf{Q}}(J)$, then by functoriality of heights, we have for $x \in J(\overline{\mathbf{Q}})$

$$\begin{aligned}\hat{h}_{\lambda_{A^\vee}}(\varphi^\vee(\lambda_J(x))) &= \hat{h}_{\varphi^{\vee *}\lambda_{A^\vee}}(\lambda_J(x)) = \hat{h}_\lambda(\lambda_J(x)) = \hat{h}_{\mathscr{P}}(\lambda_J(x), \lambda(\lambda_J(x))) \\ &= \hat{h}_{\mathscr{P}}(\lambda_J(x), \alpha(x)) = \langle x, \alpha(x) \rangle_J.\end{aligned}$$

Proposition 3.16. *For each $\sigma \in \Sigma$, write $y_{K,\pi,\sigma} = \pi_J(y_{K,\sigma}) \in J(K) \otimes_{\mathbf{Z}} \mathbf{R}$ for the σ-component of $y_{K,\pi}$. Then $\hat{h}_J(y_{K,\pi,\sigma}) = \alpha^\sigma \hat{h}(y_{K,\sigma})$, and so*

$$\hat{h}_J(y_{K,\pi}) = \sum_{\sigma \in \Sigma} \alpha^\sigma \hat{h}(y_{K,\sigma}).$$

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

Proof. Chasing $y_{K,\sigma}$ through the diagram (3.4) and taking into account the definition of $\alpha \in \mathcal{O} \subseteq \mathbf{Q}(f)$, we see that (identifying $A_f^\vee(K)$ with its image under the inclusion ι_f)

$$\begin{aligned}\pi^\vee\big(\lambda_J(y_{K,\pi,\sigma})\big) &= \pi^\vee\big((\lambda_J \circ \pi_J)(y_{K,\sigma})\big) = \pi_J^\vee\big((\lambda_J \circ \pi_J)(y_{K,\sigma})\big)\\ &= \alpha \cdot y_{K,\sigma} = \alpha^\sigma y_{K,\sigma}.\end{aligned}$$

By the discussion preceding the proposition, we have

$$\begin{aligned}\hat{h}\big(\pi^\vee\big(\lambda_J(y_{K,\pi,\sigma})\big)\big) &= \langle y_{K,\pi,\sigma}, \alpha \cdot y_{K,\pi,\sigma}\rangle_J = \langle y_{K,\pi,\sigma}, \alpha^\sigma y_{K,\pi,\sigma}\rangle_J\\ &= \alpha^\sigma \langle y_{K,\pi,\sigma}, y_{K,\pi,\sigma}\rangle_J = \alpha^\sigma \hat{h}_J(y_{K,\pi,\sigma}).\end{aligned}$$

Therefore,

$$\hat{h}_J(y_{K,\pi,\sigma}) = \frac{\hat{h}\big(\pi^\vee\big(\lambda_J(y_{K,\pi,\sigma})\big)\big)}{\alpha^\sigma} = \frac{\hat{h}(\alpha^\sigma y_{K,\sigma})}{\alpha^\sigma} = \alpha^\sigma \hat{h}(y_{K,\sigma}).$$

□

When X is a quotient of $X_0(N)$, this gives a particularly simple formula.

Corollary 3.17. *Assume that $\pi_X \colon X_0(N) \longrightarrow X$ is a finite covering of curves of degree n and that $\pi_J \colon J_0(N) \longrightarrow J$ is induced by π_X via Albanese functoriality. Then*

$$\hat{h}_J(y_{K,\pi}) = n\hat{h}\left(y_K^f\right).$$

Proof. In this case, $\alpha = \lambda_J \circ \pi_J \circ \pi_J^\vee$ is multiplication by $\deg \pi_X = n$, so $\alpha^\sigma = n$ for all $\sigma \in \Sigma$. Now use proposition 3.16. □

In the general case, we can determine α as described in Section 3.1. We record the final general formula for the height of $y_{K,\pi}$.

Corollary 3.18. *With the notation introduced so far, we have*

$$\hat{h}_J(y_{K,\pi}) = \frac{u_K^2\sqrt{-D_K}\pi}{2N\prod_{\ell^2 \mid N} C_\ell} \sum_{\sigma\in\Sigma} \alpha^\sigma \frac{L'(f^\sigma/K, 1)}{L(\mathrm{Sym}^2 f^\sigma, 2)}.$$

Proof. Combine theorem 3.14 and proposition 3.16. □

Remark 3.19. In a similar way as in the proof of proposition 3.16, we obtain the formula

$$\langle \beta \cdot y_{K,\pi}, \gamma \cdot y_{K,\pi}\rangle_J = \sum_{\sigma\in\Sigma} \alpha^\sigma \beta^\sigma \gamma^\sigma \hat{h}(y_{K,\sigma})$$

for arbitrary $\beta, \gamma \in \mathcal{O}$. This allows us to compute the height pairing matrix M for a $\mathbf{Z}$-basis of $\mathcal{O}y_{K,\pi}$ and from this the regulator $\mathrm{Reg}_{\mathcal{O}y_{K,\pi}} = \det M$. Then the Heegner index is given by

$$I_{K,\pi} = \#J(K)_{\mathrm{tors}}\sqrt{\frac{\mathrm{Reg}_{\mathcal{O}y_{K,\pi}}}{\mathrm{Reg}_{J(K)}}}.$$

4. Computing the analytic order of Ш

Recall that J is an absolutely simple and principally polarized abelian variety over $\mathbf{Q}$ of dimension g of GL_2-type with associated newform $f \in S_2(\Gamma_0(N))$, and A_f is the modular abelian variety associated to f. In particular, A_f and J are isogenous.

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

For an abelian variety J over a number field F, we define the *Tamagawa product* to be

$$\mathrm{Tam}(J/F) := \prod_v c_v(J/F),$$

where v runs through the finite places of F. When J is the Jacobian variety of an explicitly given curve, the Tamagawa numbers $c_v(C/F)$ (which are 1 for all places of good reduction) and hence the Tamagawa product $\mathrm{Tam}(J/F)$ can be computed. For Jacobians of genus 2 curves in the LMFDB [68], this information is also available in the LMFDB. For the Tamagawa number at 2 in the example in Appendix A, we compute a regular model by hand.

We now describe how to compute the *analytic order of the Tate–Shafarevich group*

$$\#\text{Ш}(J/\mathbf{Q})_{\mathrm{an}} := \frac{L^{(r)}(J/\mathbf{Q},1)}{r!\,\Omega_J\,\mathrm{Reg}_{J/\mathbf{Q}}} \cdot \frac{(\#J(\mathbf{Q})_{\mathrm{tors}})^2}{\mathrm{Tam}(J/\mathbf{Q})} \tag{4.1}$$

as an exact positive rational number, assuming that L-rk $J \in \{0,1\}$.

Note that we can provably verify that L-rk $J \in \{0,1\}$ and determine L-rk J in this case. The Fricke involution w_N sends f to f or $-f$. In the first case, the analytic order of $L(f,s)$ is odd, and in the second case, it is even. In the even case, we can show that $L(f,1) \neq 0$, and in the odd case that $L'(f,1) \neq 0$ by computing the respective value numerically to a high enough precision.

4.1. Comparing the real periods of A_f and J

Let A be an abelian variety over $\mathbf{Q}$ of dimension g with Néron model $\mathscr{A}$ over $\mathbf{Z}$. We say that a $\mathbf{Q}$-basis of $\mathrm{H}^0(A,\Omega^1)$ is a *Néron basis* for A if it is a $\mathbf{Z}$ basis of the image of $\mathrm{H}^0(\mathscr{A},\Omega^1_{\mathscr{A}/\mathbf{Z}})$. Let $(\omega_1,\dots,\omega_g)$ be a Néron basis for A. Then $\omega_A := \omega_1 \wedge \cdots \wedge \omega_g$ is a generator of the free $\mathbf{Z}$-module of rank $1\mathrm{H}^0(\mathscr{A},\Omega^g_{\mathscr{A}/\mathbf{Z}})$. Recall that the *real period* of A is

$$\Omega_A := \int_{A(\mathbf{R})} |\omega_A| = \left|\int_{A(\mathbf{R})} \omega_A\right|.$$

Let B be another abelian variety over $\mathbf{Q}$ of dimension g with Néron model $\mathscr{B}$ over $\mathbf{Z}$, and let $\pi\colon A \longrightarrow B$ be an isogeny. Since by the Néron mapping property, π uniquely extends to the Néron models, one has $\pi^*\omega_B = n_\pi \cdot \omega_A$ with an integer n_π. By the above, $|n_\pi| = c_\pi$, where c_π is defined in definition 3.3. We now compare Ω_A and Ω_B.

Lemma 4.1. *Let $\pi\colon A \longrightarrow B$ be an isogeny of abelian varieties of dimension g over $\mathbf{Q}$. Denote by $\pi_{\mathbf{R}}$ the induced morphism $A(\mathbf{R}) \longrightarrow B(\mathbf{R})$ on the real Lie groups. Then*

$$\frac{\Omega_B}{\Omega_A} = \frac{\#\operatorname{coker}\pi_{\mathbf{R}} \cdot c_\pi}{\#\ker\pi_{\mathbf{R}}} \in \mathbf{Q}_{>0}.$$

Here, c_π divides $e(\pi)^g$, where $e(\pi)$ is the exponent of $\ker\pi$, $\#\ker\pi_{\mathbf{R}}$ *divides* $\deg\pi$, *and* $\#\operatorname{coker}\pi_{\mathbf{R}}$ *divides the number $\#\pi_0(B(\mathbf{R}))$ of connected components of $B(\mathbf{R})$, which divides 2^g.*

Proof. The isogeny π induces a short exact sequence of real Lie groups

$$0 \longrightarrow (\ker\pi)(\mathbf{R}) \longrightarrow A(\mathbf{R}) \xrightarrow{\pi_{\mathbf{R}}} \pi(A(\mathbf{R})) \longrightarrow 0.$$

This gives, for $\omega \in \mathrm{H}^0(B,\Omega^g)$,

$$\int_{A(\mathbf{R})} \pi^*\omega = \#\ker\pi_{\mathbf{R}} \cdot \int_{\mathrm{im}(\pi_{\mathbf{R}})} \omega = \frac{\#\ker\pi_{\mathbf{R}}}{\#\operatorname{coker}\pi_{\mathbf{R}}} \int_{B(\mathbf{R})} \omega,$$

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

where the second equality uses that ω is translation-invariant (compare [57, Lemma 5.13]). Hence,

$$\frac{\Omega_B}{\Omega_A} = \frac{\int_{B(\mathbf{R})} |\omega_B|}{\int_{A(\mathbf{R})} |\omega_A|} = \frac{c_\pi \cdot \int_{B(\mathbf{R})} |\omega_B|}{\int_{A(\mathbf{R})} |\pi^*\omega_B|}$$
$$= \frac{c_\pi \cdot \#\operatorname{coker}\pi_{\mathbf{R}} \cdot \int_{B(\mathbf{R})} |\omega_B|}{\#\ker\pi_{\mathbf{R}} \cdot \int_{B(\mathbf{R})} |\omega_B|} = \frac{c_\pi \cdot \#\operatorname{coker}\pi_{\mathbf{R}}}{\#\ker\pi_{\mathbf{R}}}.$$

One has $\#\ker\pi_{\mathbf{R}} \mid \deg\pi$ because $\ker\pi_{\mathbf{R}} \subseteq \ker\pi$. Let $\pi' \colon B \xrightarrow{\sim} A/\ker\pi \to A/A[e(\pi)] \xrightarrow{\sim} A$ be the isogeny such that $\pi' \circ \pi$ is multiplication by $e(\pi)$. Then

$$n_{\pi'} n_\pi \cdot \omega_A = n_{\pi'} \cdot \pi^*\omega_B = \pi^*(n_{\pi'} \cdot \omega_B) = \pi^*\pi'^*\omega_A = (\pi' \circ \pi)^*\omega_A = [e(\pi)]^*\omega_A = e(\pi)^g \cdot \omega_A,$$

so $c_\pi = |n_\pi|$ divides $e(\pi)^g$. $\pi_{\mathbf{R}}$ is a topological covering map, so its image is open and closed (i.e., a union of connected components). This implies that $\#\operatorname{coker}\pi_{\mathbf{R}}$ divides $\#\pi_0(B(\mathbf{R}))$. Since the trace map $B(\mathbf{C}) \to B(\mathbf{R})$ has image the connected component $B(\mathbf{R})^0$ of the origin, it follows that $\pi_0(B(\mathbf{R}))$ is killed by 2. This implies that $\pi_0(B(\mathbf{R}))$ is isomorphic to $B(\mathbf{R})[2]/B(\mathbf{R})^0[2]$ of order dividing $4^g/2^g = 2^g$ [92, proof of Lemma 3.10]. □

Note that we can determine $\#\ker\pi_{\mathbf{R}}$ and $\#\operatorname{coker}\pi_{\mathbf{R}}$ explicitly if we have a suitable computational representation of the isogeny π; see Section 3.1.

Remark 4.2. See [57, Lemma 5.13] for a similar statement over arbitrary completions of global fields.

4.2. Computing $L(J/\mathbf{Q}, 1)/\Omega_J$

We now consider the isogeny $\pi \colon A_f \to J$. The formula for $\#Ш(J/\mathbf{Q})_{\text{an}}$ in the case of L-rank 0 contains the factor $L(J/\mathbf{Q}, 1)/\Omega_J$. In this section, we explain how this quotient can be computed as a rational number. We will then also use this later applied to a rank 0 quadratic twist of J when dealing with the L-rank 1 case. By lemma 4.1, we have

$$\frac{L(J/\mathbf{Q}, 1)}{\Omega_J} = \frac{L(A_f/\mathbf{Q}, 1)}{\Omega_{A_f}} \cdot \frac{\Omega_{A_f}}{\Omega_J} = \frac{L(A_f/\mathbf{Q}, 1)}{\Omega_{A_f}} \cdot \frac{1}{c_\pi} \cdot \frac{\#\ker\pi_{\mathbf{R}}}{\#\operatorname{coker}\pi_{\mathbf{R}}},$$

and $\Omega_{A_f} = c_f \cdot \Omega'_{A_f}$, where Ω'_{A_f} is the volume computed with respect to a $\mathbf{Z}$-basis of $S_2(f, \mathbf{Z})$ instead of a Néron basis. This gives

$$\frac{L(J/\mathbf{Q}, 1)}{\Omega_J} = \frac{L(A_f/\mathbf{Q}, 1)}{\Omega'_{A_f}} \cdot \frac{1}{c_f c_\pi} \cdot \frac{\#\ker\pi_{\mathbf{R}}}{\#\operatorname{coker}\pi_{\mathbf{R}}}. \tag{4.2}$$

The quotient $LR(A_f) := L(A_f/\mathbf{Q}, 1)/\Omega'_{A_f}$ is what Magma calls the `LRatio` of A_f. This Magma function computes $LR(A_f) \in \mathbf{Q}_{\geq 0}$ directly using modular symbols, but this computation is very slow and needs lots of memory when the level N of f is not very small (this seems to be caused by a computation of an integral homology basis of the ambient modular symbols space). The computation runs in reasonable time for $N \leq 1000$, which is enough for the L-rank zero case, but becomes infeasible for example when $N = 67 \cdot 7^2$, which is the first relevant level of a suitable quadratic twist in the L-rank one case.

So we use a numerical method instead. We compute numerical approximations to $L(A_f/\mathbf{Q}, 1)$ and to Ω'_{A_f} or Ω_J and recognize the quotient as a rational number of small height. (See [117] for a similar approach in the context of elliptic curves.) To do that reliably, we need a bound for the denominator of this quotient.

Proposition 4.3.

$$LR(A_f) = \frac{m}{\#\pi_0(A_f(\mathbf{R})) \cdot \#A_f(\mathbf{Q})_{\mathrm{tors}}} \qquad \textit{for some } m \in \mathbf{Z}_{\geq 0}.$$

Proof. By [3, Prop. 4.6], the denominator of $\#\pi_0(A_f(\mathbf{R})) \cdot LR(A_f)$ divides the order n of the image in A_f of the difference of the cusps represented by 0 and ∞. This image is a rational torsion point, so $n \mid \#A_f(\mathbf{Q})_{\mathrm{tors}}$. □

Corollary 4.4. *Let g denote the dimension of A_f and of J. Then*

$$\frac{L(J/\mathbf{Q}, 1)}{\Omega_J} = \frac{m}{4^g \cdot c_f c_\pi \cdot \#J(\mathbf{Q})_{\mathrm{tors}}} \qquad \textit{for some } m \in \mathbf{Z}_{\geq 0}.$$

Proof. Note that $\#A_f(\mathbf{Q})_{\mathrm{tors}}$ divides $\#\ker\pi_{\mathbf{R}} \cdot \#J(\mathbf{Q})_{\mathrm{tors}}$ and that $\#\pi_0(A_f(\mathbf{R}))$ and $\#\mathrm{coker}\pi_{\mathbf{R}}$ both divide 2^g. The claim then follows from (4.2) and proposition 4.3. □

Since we can determine $\#J(\mathbf{Q})_{\mathrm{tors}}$ (an upper bound obtained from the L-series coefficients as in [3, §3.5] would be enough) and we can compute $c_f c_\pi$ by lemma 3.6, it suffices to compute $L(J/\mathbf{Q}, 1)$ and Ω_J to sufficient precision so that the resulting approximation to $4^g \cdot c_f c_\pi \cdot \#J(\mathbf{Q})_{\mathrm{tors}} \cdot L(J/\mathbf{Q}, 1)/\Omega_J$ has error $< 1/2$. We then round to the nearest integer to obtain the numerator m in corollary 4.4. In practice, we use higher precision and check that the error is as small as can be expected.

4.3. *The case of L-rank* 0

We obtain the following formula.

Proposition 4.5. *Assume that $L(f, 1) \neq 0$. Then*

$$\#\text{Ш}(J/\mathbf{Q})_{\mathrm{an}} = \frac{L(J/\mathbf{Q}, 1)}{\Omega_J} \cdot \frac{(\#J(\mathbf{Q})_{\mathrm{tors}})^2}{\mathrm{Tam}(J/\mathbf{Q})} \in \mathbf{Q}_{>0}.$$

Proof. This is (4.1) for $r = 0$. □

Note that all quantities in the formula in theorem 4.5 can be computed explicitly: for the first factor, see Section 4.2, for the torsion subgroup, see [111, §11], and for the Tamagawa product, see the beginning of this section.

4.4. *The case of L-rank* 1*: Computing* $\#\text{Ш}(J/K)_{\mathrm{an}}$

In the following, we keep assuming that J is a Jacobian. In particular, J is principally polarized.

When the L-rank is 1, we first find a Heegner field K and compute the analytic order of Ш for J/K exactly from the BSD formula

$$L^*(J/K, 1) = \#\text{Ш}(J/K) \cdot \frac{\Omega_{J/K}\, \mathrm{Reg}'_{J/K}}{\sqrt{|D_K|}^g} \cdot \frac{\mathrm{Tam}(J/K)}{(\#J(K)_{\mathrm{tors}})^2}.$$

Here, the period $\Omega_{J/K}$ is defined as

$$\Omega_{J/K} = \int_{J(\mathbf{C})} |\omega \wedge \overline{\omega}|, \tag{4.3}$$

where ω is a generator of the free rank $1\mathbf{Z}$-module of top Néron differentials on J (this works since J/K is base-changed from an abelian variety over $\mathbf{Q}$). Note that this is 2^g times the covolume of the period

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

lattice (which is generated by the columns of the big period matrix Π_J, if it is computed with respect to a Néron basis of the invariant 1-forms).

The regulator $\mathrm{Reg}'_{J/K}$ is computed with respect to heights over K. We will write $\mathrm{Reg}_{J/K}$ to denote the regulator with respect to the normalized height; we then have that $\mathrm{Reg}'_{J/K} = [K : \mathbf{Q}]^{\mathrm{rk}\, J(K)} \cdot \mathrm{Reg}_{J/K}$. See [113]. (In the literature, the formula is often stated without making precise what 'the regulator' and 'the period' are, which can lead to confusion. See the answers to the Math Overflow question at [41] and [32] for a discussion.) We deduce that

$$\#\text{Ш}(J/K)_{\mathrm{an}} = \frac{(\#J(K)_{\mathrm{tors}})^2}{\mathrm{Tam}(J/K)} \cdot \frac{L^*(J/K,1)\sqrt{|D_K|}^{\,g}}{\Omega_{J/K}\,[K:\mathbf{Q}]^{\mathrm{rk}\, J(K)}\,\mathrm{Reg}_{J/K}} \tag{4.4}$$

$$= \frac{(\#J(K)_{\mathrm{tors}})^2}{\mathrm{Tam}(J/K)\cdot u_K^{2g}} \cdot \frac{\prod_\sigma 8\pi^2 \|f^\sigma\|^2}{\Omega_{J/K}} \cdot \frac{\prod_\sigma \hat{h}(y_{K,\sigma})}{\mathrm{Reg}_{J/K}}, \tag{4.5}$$

where σ runs through the g embeddings $\sigma\colon \mathbf{Q}(f) \hookrightarrow \mathbf{R}$. The second equality follows from the Gross–Zagier formula theorem 3.14 with

$$L^*(J/K,1) = \frac{L^{(g)}(J/K,1)}{g!} = \prod_\sigma L'(f/K^\sigma, 1),$$

where $L(f/K^\sigma, s) = L(f^\sigma, s)L(f^\sigma \otimes \varepsilon_K, s)$ with the quadratic character ε_K associated to $K|\mathbf{Q}$.

Note that all primes p of bad reduction for $J/\mathbf{Q}$ split as $\mathfrak{p}\bar{\mathfrak{p}}$ in K by the Heegner condition. This implies that $K_\mathfrak{p} \simeq \mathbf{Q}_p \simeq K_{\bar{\mathfrak{p}}}$ and so in particular that $c_\mathfrak{p}(J/K) = c_p(J/\mathbf{Q}) = c_{\bar{\mathfrak{p}}}(J/K)$. Therefore, the Tamagawa product over K is the square of the Tamagawa product over $\mathbf{Q}$,

$$\mathrm{Tam}(J/K) = \mathrm{Tam}(J/\mathbf{Q})^2. \tag{4.6}$$

We now describe in a series of lemmas how to determine the last two factors in (4.5). Combining the results gives the explicit formula in Corollary 4.13.

Lemma 4.6. *Let $f \in \mathcal{N}(N,g)$. Then the Petersson norm $\|f\|^2$ satisfies*

$$8\pi^2\|f\|^2 = \|\omega_f\|^2 := \int_{X_0(N)(\mathbf{C})} \omega_f \wedge \overline{i\omega_f}$$

with $\omega_f = 2\pi i f(z)\,dz$.

Proof. See [52, §1.6]. □

We now want to relate the product of the Petersson norms to the complex period of A_f. Extending diagram (3.4) to the left, we obtain the following diagram, where $B_f = I_f J_0(N)$ is the kernel of π_f:

$$\begin{tikzcd}
B_f \arrow[r, hook, "\iota_f"] \arrow[d, "\lambda'_f"'] & J_0(N) \arrow[r, two heads, "\pi_f"] \arrow[d, equal] & A_f \\
B_f^\vee & J_0(N)^\vee \arrow[l, two heads, "\iota_f^\vee"'] & A_f^\vee \arrow[l, hook', "\pi_f^\vee"'] \arrow[u, "\lambda_f"']
\end{tikzcd} \tag{4.7}$$

Also recall the definition of d_f from (3.1).

Lemma 4.7. *Let W_g be the image of $\mathrm{Sym}^g X_0(N)$ in $J_0(N)$ (with respect to some base divisor of degree g). Let $B_f = I_f J_0(N) = \ker \pi_f$. Then the intersection number $W_g \cdot B_f$ equals d_f.*

We thank Jakob Stix and Yusuf Mustopa for help with the proof.

Proof. Let $m := \dim J_0(N) = g(X_0(N))$. By [4, Thm. V.1.3] (with $(r, d, n) \leftarrow (0, g, m)$), the class of W_g is $1/(m-g)! \cdot \theta^{m-g}$, where θ is the class of the theta divisor on $J_0(N)$. We write d'_f for the product $d'_1 \cdots d'_g$, where $(d'_1, \dots, d'_g)$ is the type of λ'_f in diagram (4.7) above. Then

$$d'_f{}^2 = \deg \lambda'_f = \#(B_f \cap \ker \iota_f^\vee) = \#(\ker \pi_f \cap A_f^\vee) = \deg \lambda_f = d_f^2,$$

so $d'_f = d_f$. This implies that the intersection number is (compare [9, Thm. 3.6.3])

$$W_g \cdot B_f = \frac{\theta|_{B_f}^{m-g}}{(m-g)!} = \frac{(m-g)! \cdot d'_f}{(m-g)!} = d'_f = d_f.$$

□

We denote the Abel–Jacobi morphism $X_0(N) \hookrightarrow J_0(N)$ with respect to the cusp ∞ by ι. Since $\iota^*\colon \mathrm{H}^0(J_0(N), \Omega^1) \xrightarrow{\sim} \mathrm{H}^0(X_0(N), \Omega^1)$ is an isomorphism, we can identify the differentials ω_{f^σ} with holomorphic (hence invariant) 1-forms on $J_0(N)$, which we also denote by ω_{f^σ}. The map $\pi_f : J_0(N) \to A_f$ induces an injective homomorphism $\pi_f^* : \mathrm{H}^0(A_f(\mathbf{C}), \Omega^1) \to \mathrm{H}^0(J_0(N)(\mathbf{C}), \Omega^1)$ whose image is the subspace spanned by the ω_{f^σ}. We write $\omega_{A_f,\sigma}$ for the uniquely determined preimage of ω_{f^σ} under this map.

Lemma 4.8. *With the notation introduced so far,*

$$\prod_\sigma \|\omega_{f^\sigma}\|^2 = d_f \cdot \int_{A_f(\mathbf{C})} \bigwedge_\sigma (\omega_{A_f,\sigma} \wedge \overline{i\omega_{A_f,\sigma}}).$$

Proof. To simplify notation, fix a numbering $\sigma_1, \dots, \sigma_g$ of the embeddings $\sigma\colon \mathbf{Q}(f) \hookrightarrow \mathbf{R}$ and write ω_j for $\omega_{f^{\sigma_j}}$.

We first show that

$$\prod_\sigma \|\omega_{f^\sigma}\|^2 = \int_{W_g(\mathbf{C})} \omega_1 \wedge \overline{i\omega_1} \wedge \cdots \wedge \omega_g \wedge \overline{i\omega_g},$$

where W_g is as in theorem 4.7 with base divisor $g \cdot \infty$. Consider the composition $X_0(N)^g \xrightarrow{\iota^g} J_0(N)^g \xrightarrow{s} J_0(N)$ with the first morphism $\iota \times \ldots \times \iota$ and s the summation morphism. This morphism has degree $g!$ above its image W_g since it factors through the g-fold symmetric power of $X_0(N)$, which is birational to W_g via s. This gives

$$\int_{W_g(\mathbf{C})} \omega_1 \wedge \overline{i\omega_1} \wedge \ldots \wedge \omega_g \wedge \overline{i\omega_g} = \frac{1}{g!} \int_{X_0(N)(\mathbf{C})^g} (\iota^g)^* s^* (\omega_1 \wedge \overline{i\omega_1} \wedge \cdots \wedge \omega_g \wedge \overline{i\omega_g}).$$

Now for any invariant 1-form ω on an abelian variety, we have that $s^*\omega = \sum_{k=1}^g \mathrm{pr}_k^* \omega$ with pr_k the kth projection $J_0(N)^g \to J_0(N)$; see [9, §1.5 (9)]. This implies

$$(\iota^g)^* s^* \left(\bigwedge_{j=1}^g \omega_j \wedge \overline{i\omega_j} \right) = (\iota^g)^* \left(\bigwedge_{j=1}^g \left(\sum_{k=1}^g \mathrm{pr}_k^* \omega_j \right) \wedge \left(\sum_{k=1}^g \mathrm{pr}_k^* \overline{i\omega_j} \right) \right).$$

We expand the right-hand side. Terms containing two factors $\mathrm{pr}_k^* \omega_j$ or two factors $\mathrm{pr}_k^* \overline{i\omega_j}$ with the same k vanish since the wedge product of two holomorphic differentials on a curve vanishes. So we are left with a sum of terms of the form

$$\pm\frac{1}{g!}\int_{X_0(N)(\mathbf{C})^g}\mathrm{pr}_1^*(\omega_{j_1}\wedge\overline{i\omega_{j_1'}})\wedge\cdots\wedge\mathrm{pr}_g^*(\omega_{j_g}\wedge\overline{i\omega_{j_g'}})=\pm\frac{1}{g!}\prod_{k=1}^{g}\int_{X_0(N)(\mathbf{C})}\omega_{j_k}\wedge\overline{i\omega_{j_k'}}$$

with $\{j_1,\dots,j_g\}=\{j_1',\dots,j_g'\}=\{1,\dots,g\}$. Now when $j_k\neq j_k'$ for some k, then the corresponding integral vanishes since the f^σ are pairwise orthogonal with respect to the Petersson inner product. All the remaining terms have a positive sign (all relevant permutations are even) and differ only in the ordering of the factors; in particular, there are exactly $g!$ such terms. So we obtain

$$\begin{aligned}\int_{W_g(\mathbf{C})}\bigwedge_\sigma(\omega_{f^\sigma}\wedge\overline{i\omega_{f^\sigma}})&=\int_{W_g(\mathbf{C})}\omega_1\wedge\overline{i\omega_1}\wedge\cdots\wedge\omega_g\wedge\overline{i\omega_g}\\&=\prod_{j=1}^{g}\int_{X_0(N)(\mathbf{C})}\omega_j\wedge\overline{i\omega_j}=\prod_\sigma\|\omega_{f^\sigma}\|^2,\end{aligned}$$

as desired.

We now consider $\pi_f|_{W_g}: W_g\longrightarrow A_f$. Since $\dim W_g=\dim A_f=g$ and by theorem 4.7, W_g meets generic cosets of $B_f=\ker\pi_f$ transversally in $W_g\cdot B_f=d_f$ points, we finally obtain that

$$\begin{aligned}\prod_\sigma\|\omega_{f^\sigma}\|^2&=\int_{W_g(\mathbf{C})}\omega_1\wedge\overline{i\omega_1}\wedge\cdots\wedge\omega_g\wedge\overline{i\omega_g}\\&=\int_{W_g(\mathbf{C})}\bigwedge_\sigma(\pi_f^*\omega_{A_f,\sigma}\wedge\overline{i\pi_f^*\omega_{A_f,\sigma}})\\&=d_f\cdot\int_{A_f(\mathbf{C})}\bigwedge_\sigma(\omega_{A_f,\sigma}\wedge\overline{i\omega_{A_f,\sigma}}).\end{aligned}$$

□

We now relate the integral on the right-hand side in lemma 4.8 to the period $\Omega_{A_f/K}$.

Lemma 4.9. *One has*

$$\begin{aligned}\int_{A_f(\mathbf{C})}\bigwedge_\sigma(\omega_{A_f,\sigma}\wedge\overline{i\omega_{A_f,\sigma}})&=\frac{\operatorname{disc}\mathbf{Z}[f]}{c_f^2}\cdot\int_{A_f(\mathbf{C})}|\omega_{A_f}\wedge\overline{\omega_{A_f}}|\\&=\frac{\operatorname{disc}\mathbf{Z}[f]}{c_f^2}\cdot\Omega_{A_f/K},\end{aligned}$$

where ω_{A_f} is a top Néron differential on A_f, that is, a generator of $\mathrm{H}^0(\mathscr{A}_f,\Omega^g)$ with $\mathscr{A}_f/\mathbf{Z}$ the Néron model of A_f, $\Omega_{A_f/K}:=\int_{A_f(\mathbf{C})}|\omega_{A_f}\wedge\overline{\omega_{A_f}}|$, and c_f is the Manin constant from definition 3.4.

Over $\mathbf{R}$, one has

$$\int_{A_f(\mathbf{R})}\bigwedge_\sigma\omega_{A_f,\sigma}=\pm\frac{\sqrt{\operatorname{disc}\mathbf{Z}[f]}}{c_f}\cdot\Omega_{A_f/\mathbf{Q}}.$$

Proof. Let $(f_j)_{j=1}^g$ be a $\mathbf{Z}$-basis of $S_2(f,\mathbf{Z})$. Then $f=\sum_j b_jf_j$ for some $b_j\in\mathbf{Z}[f]$, which form a $\mathbf{Z}$-basis of $\mathbf{Z}[f]=\mathbf{Z}[a_n(f):n\geq1]$. The matrix $A=(b_j^\sigma)_{\sigma,j}$ then is such that $A\cdot(f_j)_j^\top=(f^\sigma)_\sigma^\top$, and it satisfies

$$\det(A)^2=\det(b_i^\sigma)_{i,\sigma}^2=\operatorname{disc}\mathbf{Z}[f].$$

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

By the definition of c_f, we have that

$$|\pi_f^* \omega_{A_f}| = c_f \cdot |\omega_{f_1} \wedge \cdots \wedge \omega_{f_g}|,$$

so

$$|\omega_{A_f} \wedge \overline{\omega_{A,f}}| = c_f^2 \cdot \Big|\bigwedge_j (\omega_{A,j} \wedge \overline{i\omega_{A,j}})\Big|,$$

where $\pi_f^* \omega_{A,j} = \omega_{f_j}$. We also have that

$$\bigwedge_\sigma (\omega_{A_f,\sigma} \wedge \overline{i\omega_{A_f,\sigma}}) = (\det A)^2 \bigwedge_j (\omega_{A,j} \wedge \overline{i\omega_{A,j}}).$$

Combining these gives the result.

The formula for $A_f(\mathbf{R})$ follows in the same way, the only difference being that we do not take wedge products with conjugate differentials; hence, we get the square root of the factor. □

We need to compare the periods $\Omega_{J/K}$ and $\Omega_{A_f/K}$.

Lemma 4.10. *One has*

$$\frac{\Omega_{J/K}}{\Omega_{A_f/K}} = \frac{c_\pi^2}{\deg \pi},$$

where c_π is as in definition 3.3.

Proof. Note that the top Néron differentials ω_{A_f} and ω_J on A_f and J are related by $\pi^*\omega_J = \pm c_\pi \cdot \omega_{A_f}$. Hence,

$$\begin{aligned}\Omega_{J/K} &= \int_{J(\mathbf{C})} |\omega_J \wedge \overline{\omega_J}| = \frac{1}{\deg \pi} \int_{A_f(\mathbf{C})} |\pi^*(\omega_J \wedge \overline{\omega_J})| \\ &= \frac{1}{\deg \pi} \int_{A_f(\mathbf{C})} |(c_\pi \cdot \omega_{A_f}) \wedge \overline{(c_\pi \cdot \omega_{A_f})}| = \frac{c_\pi^2}{\deg \pi} \Omega_{A_f/K}.\end{aligned}$$

□

Combining Lemmata 4.6 and 4.8 to 4.10 yields the following explicit expression for the second factor in (4.5).

Corollary 4.11. *One has*

$$\frac{\prod_\sigma 8\boldsymbol{\pi}^2 \|f^\sigma\|^2}{\Omega_{J/K}} = \frac{\deg \pi \cdot d_f \cdot \operatorname{disc} \mathbf{Z}[f]}{(c_f c_\pi)^2} \in \mathbf{Q}_{>0}.$$

We now consider the third (and last) factor in (4.5).

Lemma 4.12. *One has*

$$\frac{\prod_\sigma \hat{h}(y_{K,\sigma})}{\operatorname{Reg}_{J/K}} = \frac{I_{K,\pi}^2}{(\#J(K)_{\mathrm{tors}})^2 \cdot \mathbf{N}(\alpha) \cdot \operatorname{disc} \operatorname{End}_{\mathbf{Q}}(J)} \in \mathbf{Q}_{>0},$$

where $\alpha \in \operatorname{End}_{\mathbf{Q}} J$ is defined in (3.5) and $I_{K,\pi}$ is the Heegner index of J with respect to the chosen isogeny $\pi \colon A_f \to J$; see (3.7).

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

Proof. Since $\alpha^\sigma \hat{h}(y_{K,\sigma}) = \hat{h}_J((\pi \circ \lambda_f)(y_{K,\sigma}))$ (see proposition 3.16),

$$\mathbf{N}(\alpha) \prod_\sigma \hat{h}(y_{K,\sigma}) = \prod_\sigma \alpha^\sigma \hat{h}(y_{K,\sigma}) = \prod_\sigma \hat{h}_J((\pi \circ \lambda_f)(y_{K,\sigma})).$$

Here, σ runs through the embeddings $\mathrm{End}_{\mathbf{Q}}(J) \hookrightarrow \mathbf{R}$. Now

$$\mathrm{Reg}_J(\mathrm{End}_{\mathbf{Q}}(J) \cdot y_{K,\pi}) = \det(\langle b_i \cdot y_{K,\pi}, b_j \cdot y_{K,\pi}\rangle_J)$$

with $(b_i)_{i=1}^g$ a $\mathbf{Z}$-basis of $\mathrm{End}_{\mathbf{Q}}(J)$.

But $(\pi \circ \lambda_f)(y_{K,\sigma}) = \sum_{j=1}^g b_j \cdot y_{K,\pi} \otimes b_j^{*,\sigma}$, where $(b_j^*)_{j=1}^g$ is the dual basis of $\mathrm{End}_{\mathbf{Q}}(J) \otimes_{\mathbf{Z}} \mathbf{R}$ with respect to the trace pairing $(a, b) \mapsto \mathrm{Tr}_{\mathrm{End}_{\mathbf{Q}}(J)/\mathbf{Z}}(ab)$ of $\mathrm{End}_{\mathbf{Q}}(J)$; see (3.11). Using this and the fact that the $(\pi \circ \lambda_f)(y_{K,\sigma})$ are orthogonal in pairs with respect to the height pairing, we find that

$$\begin{aligned}\prod_\sigma \hat{h}_J((\pi \circ \lambda_f)(y_{K,\sigma})) &= \det(\langle(\pi \circ \lambda_f)(y_{K,\sigma_1}), (\pi \circ \lambda_f)(y_{K,\sigma_2})\rangle_J)\\ &= \mathrm{Reg}_J(\mathrm{End}_{\mathbf{Q}}(J) \cdot y_{K,\pi}) \cdot \det(b_j^{*,\sigma})^2\\ &= \mathrm{Reg}_J(\mathrm{End}_{\mathbf{Q}}(J) \cdot y_{K,\pi}) \cdot \det(b_j^{\sigma})^{-2}\\ &= \mathrm{Reg}_J(\mathrm{End}_{\mathbf{Q}}(J) \cdot y_{K,\pi}) \cdot (\operatorname{disc} \mathrm{End}_{\mathbf{Q}}(J))^{-1}.\end{aligned}$$

Using that $\mathrm{Reg}_J(\mathrm{End}_{\mathbf{Q}}(J) \cdot y_{K,\pi}) = I_{K,\pi}^2 \,\mathrm{Reg}_{J/K}/(\#J(K)_{\mathrm{tors}})^2$, we finally obtain

$$\begin{aligned}\frac{\prod_\sigma \hat{h}(y_{K,\sigma})}{\mathrm{Reg}_{J/K}} = \frac{\prod_\sigma \hat{h}_J((\pi \circ \lambda_f)(y_{K,\sigma}))}{\mathbf{N}(\alpha) \cdot \mathrm{Reg}_{J/K}} &= \frac{\mathrm{Reg}_J(\mathrm{End}_{\mathbf{Q}}(J) \cdot y_{K,\pi})}{\mathbf{N}(\alpha) \cdot \mathrm{Reg}_{J/K} \cdot \operatorname{disc} \mathrm{End}_{\mathbf{Q}}(J)}\\ &= \frac{I_{K,\pi}^2}{(\#J(K)_{\mathrm{tors}})^2 \cdot \mathbf{N}(\alpha) \cdot \operatorname{disc} \mathrm{End}_{\mathbf{Q}}(J)}.\end{aligned}$$

□

We can now compute $\#Ш(J/K)_{\mathrm{an}} \in \mathbf{Q}_{>0}$ exactly, as follows.

Corollary 4.13.

$$\#Ш(J/K)_{\mathrm{an}} = \frac{1}{(c_f c_\pi)^2} \cdot \frac{\operatorname{disc} \mathbf{Z}[f]}{\operatorname{disc} \mathrm{End}_{\mathbf{Q}}(J)} \cdot \left(\frac{I_{K,\pi}}{\mathrm{Tam}(J/\mathbf{Q}) \cdot u_K^g}\right)^2.$$

Proof. This follows from using corollary 4.11 and lemma 4.12 in (4.5), noting that $\mathbf{N}(\alpha) = d_f \cdot \deg \pi$ by (3.6). □

Since $\mathbf{Z}[f]$ and $\mathrm{End}_{\mathbf{Q}}(J)$ both are sub-orders of the ring of integers of $\mathbf{Q}(f)$, the quotient of their discriminants is a square. So $\#Ш(J/K)_{\mathrm{an}}$ is a square; this is consistent with the fact that J over K is even in the sense of [86] since the only bad places are primes that split in K, and the curve J is the Jacobian of is simultaneously deficient or not at both places above a bad prime p of J over $\mathbf{Q}$.

Remark 4.14. Assuming $\mathbf{Z}[f] = \mathrm{End}_{\mathbf{Q}}(J)$ and $u_K = 1$, all invariants on the right-hand side of Corollary 4.13 are orders of finite $\mathcal{O}$-modules in a natural way. It is natural to ask for a refined BSD formula over $\mathcal{O}$ – namely, whether the element in the Grothendieck group of finite $\mathcal{O}$-modules corresponding to the right-hand side of Corollary 4.13 equals that defined by $Ш(J/K)$.

4.5. Periods of quadratic twists

In order to compute $\#Ш(J/\mathbf{Q})_{\mathrm{an}}$ in the L-rank 1 case, we also need to compute $\#Ш(J^K/\mathbf{Q})_{\mathrm{an}}$. We can do this as described in Section 4.3. This requires the computation of the quotient $L(J^K/\mathbf{Q}, 1)/\Omega_{J^K}$.

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

We do that as explained in Section 4.2. The computation of Ω_{J^K} requires the period matrix of J^K. We explain in this section how we can obtain this period matrix easily from that of J. See corollary 4.17 below for a slightly more general version. We also need to determine $c_{f^K} c_{\pi^K}$ to obtain the bound for the denominator. We show in corollary 4.20 that it is the same as $c_f c_\pi$.

The following result is a generalization of [82, Lemma 3.1 and Cor. 2.6] from elliptic curves to more general abelian varieties. We first state a local version. We will frequently use the embedding

$$\mathrm{H}^0(\mathscr{A}^K, \Omega^1) \hookrightarrow \mathrm{H}^0(A^K, \Omega^1) \hookrightarrow \mathrm{H}^0(A_K, \Omega^1)$$

induced by the isomorphism $A^K_K \simeq A_K$, where $\mathscr{A}^K$ is a Néron model of the quadratic twist A^K.

Lemma 4.15. *Let A be an abelian variety over $\mathbf{Q}_p$, where p is an odd prime; assume that A has good reduction. Let $K|\mathbf{Q}_p$ be a ramified quadratic extension, given as $K = \mathbf{Q}_p(\varpi)$ with $\varpi^2 = up$, where $u \in \mathbf{Z}_p^\times$. Let $\mathscr{A}$ and $\mathscr{A}^K$ denote the Néron models of A and of its quadratic twist A^K over $\mathbf{Z}_p$.*

Then the image of $\mathrm{H}^0(\mathscr{A}^K, \Omega^1)$ in $\mathrm{H}^0(A_K, \Omega^1)$ is $1/\varpi$ times the image of $\mathrm{H}^0(\mathscr{A}, \Omega^1)$.

We thank Kęstutis Česnavicius for help with the proof.

Proof. We consider the images of $\mathrm{H}^0(\mathscr{A}, \Omega^1)$ and of $\mathrm{H}^0(\mathscr{A}^K, \Omega^1)$ in $V := \mathrm{H}^0(A_K, \Omega^1)$, respectively; they are free $\mathbf{Z}_p$-submodules of V of rank $g = \dim_K V = \dim A$. The first image is the $\mathbf{Z}_p$-dual of $L := \mathrm{Lie}(\mathscr{A}) \hookrightarrow \mathrm{Lie}(A_K)$ (i.e., it consists of the differentials ω such that $\langle \lambda, \omega \rangle \in \mathbf{Z}_p$ for all $\lambda \in L$ under the natural pairing between the Lie algebra (the tangent space at the origin) and V (its dual)), and similarly for $L^K := \mathrm{Lie}(\mathscr{A}^K) \hookrightarrow \mathrm{Lie}(A_K)$ and the second image. To see this, note first that $\mathrm{H}^0(\mathscr{A}, \Omega^1_{\mathscr{A}})$ is identified with $\mathrm{H}^0(\mathrm{Spec}\mathbf{Z}_p, \varepsilon^*\Omega^1_{\mathscr{A}})$, where ε is the zero section of $\mathscr{A}$; see [12, §4.2, Prop. 1]. Then by [12, §2.2, Prop. 7(b)], $\varepsilon^*\Omega^1_{\mathscr{A}} = \mathcal{I}/\mathcal{I}^2$, where $\mathcal{I}$ is the ideal sheaf of the zero section of $\mathscr{A}$. The functor of points definition of the Lie algebra then gives that $\mathrm{Lie}(\mathscr{A})$ is the $\mathbf{Z}_p$-dual of $\mathcal{I}/\mathcal{I}^2$. These identifications are all compatible with base change to $\mathbf{Q}_p$, so the duality is compatible with what is happening on the generic fiber.

It therefore suffices to show that $L^K = \varpi \cdot L$. By our assumptions, $K|\mathbf{Q}_p$ is tamely ramified. By [42, Thm. 4.2], the natural map induces an isomorphism of $\mathscr{A}^K$ with the subscheme of the restriction of scalars $R_{\mathbf{Z}_p[\varpi]/\mathbf{Z}_p}\mathscr{A}_{\mathbf{Z}_p[\varpi]}$ fixed by the twisted action of $\mathrm{Gal}(K|\mathbf{Q}_p)$. Taking the invariants under this action commutes with forming the Lie algebra, so we obtain that L^K is obtained by taking the invariants under this twisted action on $\mathrm{Lie}(\mathscr{A}_{\mathbf{Z}_p[\varpi]}) = L \otimes_{\mathbf{Z}_p} \mathbf{Z}_p[\varpi]$; this invariant space is exactly $\varpi \cdot L$. □

Corollary 4.16. *Let A be an abelian variety over $\mathbf{Q}$ and let K be a quadratic number field of odd discriminant D_K such that all primes of bad reduction for A are unramified in K. Let $\mathscr{A}$ and $\mathscr{A}^K$ denote the Néron models of A and of its quadratic twist A^K over $\mathbf{Z}$. Then the image of $\mathrm{H}^0(\mathscr{A}^K, \Omega^1)$ in $\mathrm{H}^0(A_K, \Omega^1)$ is $1/\sqrt{D_K}$ times the image of $\mathrm{H}^0(\mathscr{A}, \Omega^1)$.*

Proof. Fix a Néron basis $(\omega_1, \ldots, \omega_g)$ for A, where $g = \dim A$. Identifying invariant 1-forms on A and on A^K with their images on A_K, we see that $(\sqrt{D_K}^{-1}\omega_1, \ldots, \sqrt{D_K}^{-1}\omega_g)$ is a $\mathbf{Q}$-basis of the space of invariant 1-forms on A^K. Since $K|\mathbf{Q}$ is unramified at all places of bad reduction of A, these 1-forms will form a local Néron basis at all these places, and also at all places of good reduction for A at which $K|\mathbf{Q}$ is unramified. Finally, lemma 4.15 (with $\varpi \leftarrow \sqrt{D_K}$) shows that they also form a local Néron basis at all places where $K|\mathbf{Q}$ is ramified. So we have obtained a (global) Néron basis for A^K, and the claim follows. □

Corollary 4.17. *Let A be an abelian variety over $\mathbf{Q}$ and let K be a quadratic number field of odd discriminant such that all primes of bad reduction for A are unramified in K. Let Π_A be a big period matrix for A with respect to a Néron basis of $\mathrm{H}^0(A, \Omega^1)$. Then $\sqrt{D_K}^{-1}\Pi_A$ is a big period matrix for the quadratic twist A^K with respect to a Néron basis of $\mathrm{H}^0(A^K, \Omega^1)$.*

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

Proof. We use the Néron bases described in the proof of corollary 4.16. Fixing an embedding $K \hookrightarrow \mathbf{C}$ and a symplectic basis of $\mathrm{H}_1(A(\mathbf{C}), \mathbf{Z})$, we see for the resulting period matrices that $\Pi_{A^K} = \sqrt{D_K}^{-1}\Pi_A$. □

We can use this result, together with the following elementary statement about abelian groups with an involution, to relate the period of A/K to the real periods of $A/\mathbf{Q}$ and $A^K/\mathbf{Q}$ when K is an imaginary quadratic field.

Lemma 4.18.

(1) *Let V be a finite dimensional $\mathbf{F}_2$-vector space and let $\iota \in \mathrm{GL}(V)$ with $\iota^2 = \mathrm{id}_V$. Then*

$$(V : (\mathrm{id} + \iota)(V)) = \#V^{\langle\iota\rangle}.$$

(2) *Let G be a finitely generated abelian group and let $\iota \in \mathrm{Aut}(G)$ with $\iota^2 = \mathrm{id}_G$. Let $G_1 = \{g + \iota(g) : g \in G\}$ and $G_2 = \{g - \iota(g) : g \in G\}$. Then*

$$(G : G_1 + G_2) = \#\Big(\frac{G}{2G}\Big)^{\langle\iota\rangle}.$$

Proof.

(1) The map $\varphi := \mathrm{id} + \iota = \mathrm{id} - \iota$ has kernel $V^{\langle\iota\rangle}$. Since V is finite, we have

$$(V : (\mathrm{id} + \iota)(V)) = \#\operatorname{coker}\varphi = \#\ker\varphi = \#V^{\langle\iota\rangle}.$$

(2) Since for each $g \in G$, $2g = (g+\iota(g)) + (g-\iota(g)) \in G_1 + G_2$, we have that $2G \subseteq G_1 + G_2$. Therefore, using part (1),

$$(G : G_1 + G_2) = \Big(\frac{G}{2G} : \frac{G_1 + G_2}{2G}\Big) = \Big(\frac{G}{2G} : (\mathrm{id} + \iota)\Big(\frac{G}{2G}\Big)\Big) = \#\Big(\frac{G}{2G}\Big)^{\langle\iota\rangle}.$$

□

Corollary 4.19. *Let A and K be as in corollary 4.17, with $D_K < 0$. Then*

$$\frac{\Omega_{A/\mathbf{Q}}\Omega_{A^K/\mathbf{Q}}\sqrt{|D_K|}^g}{\Omega_{A/K}} = \frac{\#A(\mathbf{R})[2]}{2^g} = \#\pi_0(A(\mathbf{R})).$$

Proof. We use Π_A and Π_{A^K} to denote big period matrices of A and A^K with respect to a Néron basis of the invariant 1-forms. The period $\Omega_{A/K}$ is 2^g times the covolume of the lattice $\Lambda \subseteq \mathbf{C}^g$ (where, as usual, $g = \dim A$) generated by the columns of Π_A (a Néron basis of $\mathrm{H}^0(A/\mathbf{Q}, \Omega^1)$ gives a Néron basis of $\mathrm{H}^0(A/K, \Omega^1)$), since at the bad places of A, $K|\mathbf{Q}$ is unramified and Néron models are preserved by unramified base extension). The real periods $\Omega_{A/\mathbf{Q}}$ and $\Omega_{A^K/\mathbf{Q}}$ are the covolumes of the lattices in $\mathbf{R}^g$ generated by the $\mathbf{C}|\mathbf{R}$-traces of the columns of Π_A and Π_{A^K}, respectively. The first lattice is $\Lambda_1 = \{\lambda + \bar{\lambda} : \lambda \in \Lambda\}$. By corollary 4.17, $\Pi_{A^K} = D_K^{-1/2}\Pi_A$ (using suitable bases), which together with $D_K < 0$ implies that $\Omega_{A^K/\mathbf{Q}}$ is $\sqrt{|D_K|}^{-g}$ times the covolume of the lattice in $\mathbf{R}^g$ generated by the $\mathbf{C}|\mathbf{R}$-traces of the columns of $\sqrt{-1} \cdot \Pi_A$. This is the same as the covolume of $\Lambda_2 \subseteq \sqrt{-1}\,\mathbf{R}^g$, where $\Lambda_2 = \{\lambda - \bar{\lambda} : \lambda \in \Lambda\}$. So $\Omega_{A/\mathbf{Q}}\Omega_{A^K/\mathbf{Q}}\sqrt{|D_K|}^g$ is the covolume of $\Lambda_1 + \Lambda_2 \subseteq \mathbf{C}^g$. Applying lemma 4.18 (2) with $G = \Lambda$ and ι the restriction of complex conjugation, we finally obtain

$$\frac{\Omega_{A/\mathbf{Q}}\Omega_{A^K/\mathbf{Q}}\sqrt{|D_K|}^g}{\Omega_{A/K}} = \frac{(\Lambda : \Lambda_1 + \Lambda_2)}{2^g} = \frac{\#(\Lambda/2\Lambda)^+}{2^g} = \frac{\#A(\mathbf{R})[2]}{2^g},$$

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

where $(\Lambda/2\Lambda)^+$ denotes the subgroup fixed under the induced action of complex conjugation. (Note that $A(\mathbf{C})[2] \simeq \frac{1}{2}\Lambda/\Lambda \simeq \Lambda/2\Lambda$ as a $\mathrm{Gal}(\mathbf{C}|\mathbf{R})$-module.) The last equality comes from the fact that $\#A(\mathbf{R})^0[2] = 2^g$ since the connected component of the identity is a g-dimensional real torus. □

Corollary 4.20. *Let $f \in \mathcal{N}(N, g)$ and let K be a quadratic number field such that D_K is coprime with $2N$. Let further $\pi\colon A_f \to J$ be an isogeny defined over $\mathbf{Q}$. We write f^K and π^K for the corresponding quadratic twists of f and π, respectively. Then $c_{f^K} c_{\pi^K} = c_f c_\pi$.*

Proof. The map $\pi_f : J_0(N) \to A_f$ is geometrically defined, so π_{f^K} is the same as the quadratic twist π_f^K of π_f. Note that c_f is the index of $\pi_f^* \mathrm{H}^0(\mathscr{A}_f, \Omega^1_{\mathscr{A}_f/\mathbf{Z}})$ in $\pi_f^*(A_f, \Omega^1) \cap \mathrm{H}^0(\mathscr{J}_0(N), \Omega^1_{\mathscr{J}_0(N)/\mathbf{Z}})$ (where, as usual, $\mathscr{A}_f$ and $\mathscr{J}_0(N)$ denote the Néron models of A_f and $J_0(N)$ over $\mathbf{Z}$). Applying corollary 4.16, we see that, considered inside $\mathrm{H}^0(J_0(N)_K, \Omega^1)$, the images of both spaces are multiplied by $1/\sqrt{D_K}$ by twisting, so the index stays the same. This shows that $c_{f^K} = c_f$. An analogous argument shows that $c_{\pi^K} = c_\pi$. □

4.6. *The case of L-rank* 1*: Computing* $\#Ш(J/\mathbf{Q})_{\mathrm{an}}$

We now show how we can compute $\#Ш(J/\mathbf{Q})_{\mathrm{an}}$ from $\#Ш(J/K)_{\mathrm{an}}$ as determined in Section 4.4 and $\#Ш(J^K/\mathbf{Q})_{\mathrm{an}}$, which we can compute as in Section 4.3 (and using Section 4.5 to make the computation of the 'L-ratio' for the quadratic twist feasible, which would otherwise be quite slow, as the level of the twisted newform tends to be fairly large) since the L-rank of J^K is zero by the Heegner hypothesis.

From the induction formula $L(J/K, s) = L(J/\mathbf{Q}, s)L(J^K/\mathbf{Q}, s)$, we obtain

$$L^{(g)}(J/K, 1) = L^{(g)}(J/\mathbf{Q}, 1)L(J^K/\mathbf{Q}, 1).$$

Then one computes $\#Ш(J/\mathbf{Q})_{\mathrm{an}}$ from the relation

$$\begin{aligned}\#Ш(J/K)_{\mathrm{an}} &= \#Ш(J/\mathbf{Q})_{\mathrm{an}} \cdot \#Ш(J^K/\mathbf{Q})_{\mathrm{an}} \\ &\quad \cdot \frac{(\#J(K)_{\mathrm{tors}})^2}{(\#J(\mathbf{Q})_{\mathrm{tors}})^2(\#J^K(\mathbf{Q})_{\mathrm{tors}})^2} \\ &\quad \cdot \frac{\mathrm{Tam}(J/\mathbf{Q})\,\mathrm{Tam}(J^K/\mathbf{Q})}{\mathrm{Tam}(J/K)} \cdot \frac{\mathrm{Reg}_{J/\mathbf{Q}}}{2^g\,\mathrm{Reg}_{J/K}} \cdot \frac{\Omega_J \Omega_{J^K} \sqrt{|D_K|}^g}{\Omega_{J/K}}\end{aligned} \tag{4.8}$$

that we obtain from (4.4) and its analogues for $J/\mathbf{Q}$ and $J^K/\mathbf{Q}$.

As discussed at the beginning of Section 4.4, both regulators are defined in terms of the normalized canonical height. This implies that

$$\frac{\mathrm{Reg}_{J/\mathbf{Q}}}{(\#J(\mathbf{Q})_{\mathrm{tors}})^2} \cdot \frac{(\#J(K)_{\mathrm{tors}})^2}{\mathrm{Reg}_{J/K}} = (J(K) : J(\mathbf{Q}))^2.$$

Since we have computed $J(K)$ already, we can easily determine this index. By corollary 4.19, the last factor is $\#J(\mathbf{R})[2]/2^g$, assuming D_K is odd.

We can evaluate the factor involving Tamagawa numbers using the following result. This is not used in the proof of the formula in corollary 4.22 below but will be useful for the example in Appendix A.

Lemma 4.21. *We have*

$$\mathrm{Tam}(J^K/\mathbf{Q}) = \mathrm{Tam}(J/\mathbf{Q}) \cdot \prod_{p | D_K} c_p(J^K/\mathbf{Q}),$$

and hence,

$$\frac{\operatorname{Tam}(J/\mathbf{Q})\operatorname{Tam}(J^K/\mathbf{Q})}{\operatorname{Tam}(J/K)} = \prod_{p \mid D_K} c_p(J^K/\mathbf{Q}),$$

where $c_p(J^K/\mathbf{Q}) = \#J(\mathbf{F}_p)[2]$ *when* $p \mid D_K$ *is an odd prime.*

Proof. Since all bad primes p of J split in K, the Tamagawa numbers of J^K at these primes are the same as those of J and also agree with the two Tamagawa numbers of J/K at the primes dividing p. Since the only further primes of bad reduction for J^K are those dividing D_K, we obtain the stated equalities.

The last claim follows from the fact that J^K has totally unipotent reduction at p, which implies that there is no 2-torsion in $\mathcal{J}^K(\mathbf{F}_p)^0$ (where $\mathcal{J}^K$ is the Néron model of J^K), together with the fact that the component group is killed by 2 since J^K obtains good reduction after a quadratic extension (see [53, Cor. 5.3.3.2]). This gives an isomorphism between $J(\mathbf{F}_p)[2] \simeq \mathcal{J}^K(\mathbf{F}_p)[2]$ and the $\mathbf{F}_p$-points of the component group. □

Recall that $\operatorname{Tam}(J/K) = \operatorname{Tam}(J/\mathbf{Q})^2$ by (4.6). We then obtain the following.

Corollary 4.22. *Keep the notations and assumptions introduced so far. If* D_K *is odd, then*

$$\#\text{Ш}(J/\mathbf{Q})_{\text{an}} = \frac{\operatorname{disc}\mathbf{Z}[f]}{\operatorname{disc}\operatorname{End}_{\mathbf{Q}}(J)} \cdot \frac{4^g}{\#J(\mathbf{R})[2]\cdot\operatorname{Tam}(J/\mathbf{Q})} \cdot \left(\frac{I_{K,\pi}}{(J(K):J(\mathbf{Q}))\cdot u_K^g}\right)^2 \cdot \left(\frac{L(J^K/\mathbf{Q},1)}{\Omega_{J^K}}\right)^{-1}.$$

Proof. Combine (4.8) with the remarks after it and with Corollary 4.13 and theorem 4.5, applied to J^K. □

5. Bounding the support of the Tate–Shafarevich group

Let $A/\mathbf{Q}$ be an absolutely simple GL_2-type abelian variety with associated newform f. In this section, we obtain an explicit bound on the support of the Tate–Shafarevich group coming from the Heegner point Euler system. This leads to an explicit description of a finite set of (regular) prime ideals $\mathfrak{p}$ of $\mathbf{Z}[f]$ such that $\text{Ш}(A/\mathbf{Q})[\mathfrak{p}] = 0$ for all $\mathfrak{p}$ not in this set. In the L-rank 0 case, we make the results of Kolyvagin–Logachëv [64] explicit and in the L-rank 1 case those of Nekovář [80]. We first prove a result on the vanishing of the first Galois cohomology group for irreducible $\rho_{\mathfrak{p}}$ in Section 5.1. Specializing to the case where $A = J$ is a Jacobian for simplicity (so we do not have to deal with polarizations), we derive the explicit finite support for $\text{Ш}(J/\mathbf{Q})$ in Section 5.2; see theorems 5.6, 5.7 and 5.10.

In the following subsection, F will be a general number field and does not denote $\operatorname{Frac}\mathbf{Z}[f]$.

5.1. Vanishing of $\mathrm{H}^1(F(A[\mathfrak{p}])|F, A[\mathfrak{p}])$

We assume that $\mathfrak{p}$ is a regular prime ideal of $\mathbf{Z}[f]$ and set $p = p(\mathfrak{p})$. The goal of this section is to show that the Galois cohomology group $\mathrm{H}^1(F(A[\mathfrak{p}])|F, A[\mathfrak{p}])$ vanishes when the mod $\mathfrak{p}$ Galois representation is irreducible (and $p > 2$); see proposition 5.4. The vanishing of this group is an important input for [64, Proposition 5.10].

Let F be a number field. (This level of generality is needed later on and is also useful for further applications – for example, in our forthcoming work on the BSD conjecture over totally real fields with Pip Goodman.) Let $G := \operatorname{Gal}(F(A[\mathfrak{p}])|F) \hookrightarrow G_{\mathfrak{p}}^{\max}$ with $G_{\mathfrak{p}}^{\max}$ defined as in definition 2.9.

The main idea is that $\mathrm{H}^1(G, A[\mathfrak{p}]) = 0$ if G contains a nontrivial homothety. Our arguments are purely group cohomological, without much arithmetic input.

Definition 5.1. A *homothety* in the automorphism group of a vector space V over a field K is a map of the form $v \mapsto \lambda v$ with $\lambda \in K^\times$. It is *nontrivial* if $\lambda \neq 1$.

Lemma 5.2. *Let V be a finite-dimensional vector space over a finite field* $\mathbf{F}$ *and let G be a subgroup of* $\mathrm{GL}(V)$. *If G contains a nontrivial homothety, then* $\mathrm{H}^1(G, V) = 0$.

Proof. (Compare [67, Lemma 3].) Let $g \in G$ be a nontrivial homothety; note that $\langle g \rangle$ is a normal subgroup of G. Consider the associated inflation-restriction exact sequence:

$$0 \longrightarrow \mathrm{H}^1(G/\langle g \rangle, V^{\langle g \rangle}) \xrightarrow{\text{inf}} \mathrm{H}^1(G, V) \xrightarrow{\text{res}} \mathrm{H}^1(\langle g \rangle, V)$$

The left-hand group is trivial since $V^{\langle g \rangle} = 0$ (a nontrivial scalar matrix fixes no nontrivial element of a vector space), and the right-hand group is trivial because $\#\langle g \rangle \mid \#\mathbf{F}^\times$ and $\#V = \#\mathbf{F}^{\dim V}$ are coprime. So the middle group must be trivial as well. □

Lemma 5.3. *Let* $\mathbf{F}$ *be a finite field of characteristic $p \geq 3$ and let $G \subseteq \mathrm{GL}_2(\mathbf{F})$ be such that G does not fix a unique line in* $\mathbf{F}^2$. *Then*

$$\mathrm{H}^1(G, \mathbf{F}^2) = 0.$$

Proof. We proceed in a number of steps.

(1) If N is a normal subgroup in G and N fixes a unique line, then so does G. This is because G acts on the lines fixed by N.
(2) If N is a normal subgroup in G of index prime to p, then (by inflation-restriction and since $\mathrm{H}^1(G/N, V) = 0$ for $V = (\mathbf{F}^2)^N$) $\mathrm{H}^1(N, \mathbf{F}^2) = 0$ implies $\mathrm{H}^1(G, \mathbf{F}^2) = 0$.
(3) By (1) and (2), we can restrict to subgroups of $\mathrm{SL}_2(\mathbf{F})$, observing that $G \cap \mathrm{SL}_2(\mathbf{F})$ is a normal subgroup of G of index dividing $\#\mathbf{F}^\times$.
(4) If $\#G$ is prime to p, then $\mathrm{H}^1(G, \mathbf{F}^2) = 0$. We can therefore assume that p divides $\#G$ and therefore also $\#\mathbf{P}G$.
(5) If G contains $-I$ (the unique nontrivial homothety in $\mathrm{SL}_2(\mathbf{F})$; note $p \geq 3$), then $\mathrm{H}^1(G, \mathbf{F}^2) = 0$ by lemma 5.2. Since $-I$ is the unique element of order 2 in $\mathrm{SL}_2(\mathbf{F})$, this is the case whenever $\#G$ is even, so in particular when $\#\mathbf{P}G$ is even.
(6) We consult [62, Thm. 2.1], which lists all subgroups of $\mathrm{PSL}_2(\mathbf{F})$. In cases (f), (i), (p) and (u), $p = 2$. In cases (b)–(e), (g), (h), (j) and (k), p does not divide $\#\mathbf{P}G$. In cases (n), (o), (q)–(t) and (v), $\#\mathbf{P}G$ is even. In the remaining cases (a), (l) and (m), $\mathbf{P}G$ is contained in a Borel subgroup and has order divisible by p, so G fixes a unique line. In each case, either the assumptions are violated, or we can conclude using (4) or (5). □

Proposition 5.4 (Irreducible implies trivial cohomology). *Let A be an absolutely simple abelian variety over* $\mathbf{Q}$ *of* GL_2*-type and let $\mathfrak{p}$ be a regular prime ideal of* $\mathrm{End}_{\mathbf{Q}}(A)$. *Let F be a number field that is a Galois extension of* $\mathbf{Q}$. *We assume that $p(\mathfrak{p}) \geq 3$ and that $\rho_{\mathfrak{p}}|_{G_F}$ is irreducible. Then*

$$\mathrm{H}^1(F(A[\mathfrak{p}])|F, A[\mathfrak{p}]) = 0.$$

Proof. Let G be the image of $\rho_{\mathfrak{p}}$ and let $G' := \rho_{\mathfrak{p}}(G_F)$, which is a normal subgroup of G. Since $\rho_{\mathfrak{p}}$ is irreducible, G does not fix a unique line; by part (1) of the proof of lemma 5.3, this implies that G' also does not fix a unique line. Then lemma 5.3 says that

$$\mathrm{H}^1(F(A[\mathfrak{p}])|F, A[\mathfrak{p}]) = \mathrm{H}^1(G', \mathbf{F}_{\mathfrak{p}}^2) = 0.$$

□

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

5.2. *Bounding the support of* $Ш(A/\mathbf{Q})$

Using our computations of $G_{\mathfrak{p}}$ from Section 2 and the Heegner index from Section 3, we can improve [64] and [80] to give an explicit finite bound for the support of $Ш(A/\mathbf{Q})$ considered as a $\mathbf{Z}$- or an $\mathcal{O}$-module.

We do not repeat the full proof; we only explain how to make the arguments explicit.

Assumption 5.5. Let A be a modular abelian variety of level N. We write $\mathcal{O} := \mathrm{End}_{\mathbf{Q}}(A)$ and assume that $\mathcal{O}$ is the maximal order of $\mathbf{Q}(f)$ (via an isomorphism as in (3.2)). This is no essential restriction; compare remark 2.3 and note that the truth of the strong BSD Conjecture is an isogeny invariant by [78, Theorem I.7.3]. (However, the support of Ш can change under isogenies.) Let K be a Heegner field of odd *Heegner discriminant* $D_K \neq -3$ (in particular, $D_K \notin \{-3, -4, -8\}$) (i.e., K is an imaginary quadratic field such that all primes dividing the level N split completely in K). Then $y_{K,\pi} \in A(K)$ is a *Heegner point*, and we assume that L-rk$(A/K) = 1$ (i.e., $y_{K,\pi}$ is non-torsion by the Gross–Zagier formula). Note that $y_{K,\pi}$ satisfies the Euler system relations from [64, §2] because the isogeny π is equivariant with respect to the action of $\mathbf{Z}[f] \subseteq \mathcal{O}$; see (3.3).

For several curves among our LMFDB examples, the endomorphism ring of the Jacobian is not maximal. However, in all these cases, there is another curve in the database whose Jacobian is isogenous with endomorphism ring the maximal order; it then suffices to consider these other curves.

In Table 1, we collect the most important objects and constants in [64]. We specialize to the case that A is the Jacobian J of a curve with its canonical principal polarization. In particular, since J has RM, the Rosati involution associated to the polarization is the identity on $\mathrm{End}_{\mathbf{Q}}(J) \otimes_{\mathbf{Z}} \mathbf{R}$, which we need to use the results in [64, §2.1]. This implies that the polarization φ_Λ in Table 1 is principal. Recall that $\mathrm{Tam}(J/\mathbf{Q}) = \prod_\ell c_\ell(J/\mathbf{Q})$ is the Tamagawa product of J. The component group $\pi_0(\mathcal{J})$ of the Néron model $\mathcal{J}/\mathbf{Z}$ of $J/\mathbf{Q}$ is an $\mathcal{O}$-module. This allows us to consider its order $\mathrm{Tam}(J/\mathbf{Q})$ as the corresponding characteristic ideal in $\mathcal{O}$ in the following.

Theorem 5.6 (Explicit finite support of Ш in the L-rank 0 case). *Assume L-rk $J = 0$. Suppose that $\mathfrak{p}$ is a maximal ideal of $\mathcal{O}$ such that $\rho_{\mathfrak{p}}$ is irreducible and*

$$\mathfrak{p} \nmid 2 \cdot \mathrm{Tam}(J/\mathbf{Q}) \cdot \underset{K}{\gcd}(\mathcal{I}_{K,\pi}),$$

Table 1. *The constants $m_k = m_k(\mathfrak{p}^n)$ and important objects occurring in the proof of [64]. The notation '$[m]$' denotes m when $p(\mathfrak{p}) = 2$ and 0 otherwise.*

symbol	definition	properties
m_1	$\mathfrak{p}^{m_1} \cdot \mathrm{Sel}_{\mathfrak{p}^\infty}(J/\mathbf{Q}) = 0$	$m_1 = m_3 + m_{10} + 2(m_9 + m_{11}) + m_{13}$
m_2	$\mathrm{ord}_{\mathfrak{p}}(\mathrm{Ann}_{\mathcal{O}}(\ker \varphi_\Lambda))$	0 if φ_Λ principal polarization
A	$\prod_v \mathrm{Ann}_{\mathcal{O}}(\mathrm{H}^1(K_v^{\mathrm{nr}} \vert K_v, J))$	divides $\mathrm{Tam}(J/K) = \mathrm{Tam}(J/\mathbf{Q})^2$
B	$\mathrm{ord}(h_K \cdot \lambda(j(\pi(0))))$	divides $\#J(K)_{\mathrm{tors}}$
x	$ABy_{K,\pi} \bmod \mathfrak{p}^n J(K)$	
m_4	$[1]$	0 if $\mathfrak{p} \nmid 2$
m_6	$[3g] + m_2/2$	0 if $\deg \varphi_\Lambda = 1$ and $\mathfrak{p} \nmid 2$
m_7	$gm_4 + m_6$	0 if $\deg \varphi_\Lambda = 1$ and $\mathfrak{p} \nmid 2$
m_3	$[2] + 3m_7 + m_4 + m_2$	
	$= [12g + 3] + 5m_2/2$	0 if $\deg \varphi_\Lambda = 1$ and $\mathfrak{p} \nmid 2$
m_9	Lemma 5.9 in [64]	0 if $\mathfrak{p} \nmid 2$ and $\rho_{\mathfrak{p}}$ is irreducible
m_{10}	$\mathfrak{p}^{m_{10}} \mathrm{H}^1(K \vert \mathbf{Q}, J[\mathfrak{p}^n](K)) = 0$	0 if $\mathfrak{p} \nmid 2$
V	$K(J[\mathfrak{p}^{n+m_2(\mathfrak{p})}])$	
m_{11}	$\mathfrak{p}^{m_{11}} \mathrm{H}^1(V \vert K, J[\mathfrak{p}^n]) = 0$	0 if $\rho_{\mathfrak{p}}$ irreducible
m_{13}	$r \cdot x \in \mathfrak{p}^n J(K) \implies r \in \mathfrak{p}^{n-m_{13}} \mathcal{O}$	0 if $\mathfrak{p} \nmid ABI_{K,\pi}$

where K runs through the Heegner fields for $J/\mathbf{Q}$. Then

$$Ш(J/\mathbf{Q})[\mathfrak{p}] = 0.$$

Proof. Note that the arguments in [64] (there for a prime ℓ) also work for prime ideals $\mathfrak{p}$; this is explained in [39, §7.1]: annihilation of modules under $\mathcal{O}$ by p is translated to the annihilation under $\mathfrak{p} \mid p$ using the Chinese remainder theorem $\mathcal{O}/p \xrightarrow{\sim} \bigoplus_{\mathfrak{p}|p} \mathcal{O}/\mathfrak{p}^{e_\mathfrak{p}}$. We set $p := p(\mathfrak{p})$.

Looking at Table 1, all constants m_i are 0 for $\mathfrak{p}$ satisfying our hypotheses.

(i) $m_3 = 0$ because $\mathfrak{p} \nmid 2$ and the polarization is principal.

(ii) If $\mathfrak{p} \nmid \mathrm{Tam}(J/\mathbf{Q})$, then $\mathfrak{p} \nmid A$: Let $p = p(\mathfrak{p})$. Let $v \nmid p$ be a finite prime of K with residue field $\mathbf{F}_v$. Let $\mathcal{J}$ be the Néron model of J/K. By [78, Proposition I.3.8],[1]

$$\begin{aligned}\mathrm{H}^1_{\mathrm{nr}}(K_v, J) &\simeq \mathrm{H}^1(\mathbf{F}_v, \pi_0(\mathcal{J})(\overline{\mathbf{F}}_v))\\ &\simeq \varinjlim_n \mathrm{H}^1(\mathbf{F}_{v^n}|\mathbf{F}_v, \pi_0(\mathcal{J})(\mathbf{F}_{v^n}))\end{aligned}$$

as $\mathcal{O}$-modules. The last module is a subquotient of $\pi_0(\mathcal{J})(\mathbf{F}_{v^n})$ since $\mathbf{F}_{v^n}|\mathbf{F}_v$ is cyclic [81, Proposition 1.7.1]. (Note that conjecturally, $\mathrm{Tam}(J/\mathbf{Q})$ divides all Heegner indices [52, Conjecture V.(2.2)]; see also Corollary 4.13.)

(iii) If $\mathfrak{p} \mid B$, then $J(\mathbf{Q})[\mathfrak{p}] \neq 0$, so $\rho_\mathfrak{p}$ is reducible.

(iv) $m_9 = 0$ if $\mathfrak{p} \nmid 2$ and $\rho_\mathfrak{p}$ is irreducible because the irreducibility implies that the p-isogeny graph is reduced to a point; see [64, Lemma 5.9].

(v) $\mathfrak{p} \nmid 2$ implies that $m_{10} = 0$ since $\#\mathrm{Gal}(K|\mathbf{Q}) = 2$ is prime to $\#A[\mathfrak{p}]$.

(vi) $\rho_\mathfrak{p}$ irreducible implies $m_{11} = 0$ by proposition 5.4 with $F = K$.

(vii) One can take m_{13} to be

$$v_\mathfrak{p}(\mathcal{I}_{K,\pi}) = v_\mathfrak{p}\big(\mathrm{Char}_\mathcal{O}(J(K)/\mathcal{O}y_K)\big).$$

This is because this choice of $m_{13} = m_{13}(\mathfrak{p}^\infty)$ satisfies [64, Proposition 5.12].

Hence, $m_1 = 0$, so $\mathrm{Sel}_{\mathfrak{p}^\infty}(J/\mathbf{Q}) = 0$. □

To simplify notation below, we write $\mathcal{K}_\mathfrak{p}(f)$ for the set of all Heegner fields K such that $a_n(f) \not\equiv \varepsilon_K(n)a_n(f) (\mathrm{mod}\ \mathfrak{p})$ for some n coprime to N, where ε_K is the nontrivial quadratic Dirichlet character associated with $K|\mathbf{Q}$. In practice, we find a Heegner field K such that $K \in \mathcal{K}_\mathfrak{p}(f)$ for *all* $\mathfrak{p} \nmid 2$ by checking that for some small bound B the ideal

$$\big\langle a_n(f) - \varepsilon_K(n)a_n(f) : (n, ND_K) = 1,\ n \le B\big\rangle$$

of $\mathbf{Z}[f]$ has norm a power of 2 (note that the norm is always divisible by 2). Note that this ideal is nonzero if f does not have CM by ε_K in the terminology of definition 2.46.

Theorem 5.7 (Explicit finite support of Ш in the L-rank 1 case). *Assume that L-rk $J = 1$ and $J/\mathbf{Q}$ is simple and does not have CM. Suppose that $\mathfrak{p}$ is a maximal ideal of $\mathcal{O}$ such that $\rho_\mathfrak{p}$ is irreducible, $K \in \mathcal{K}_\mathfrak{p}(f)$ and*

$$\mathfrak{p} \nmid 2 \cdot \mathrm{Tam}(J/\mathbf{Q}) \cdot \mathcal{I}_{K,\pi}.$$

Then

$$Ш(J/\mathbf{Q})[\mathfrak{p}] = Ш(J/K)[\mathfrak{p}] = 0.$$

[1] Note the erratum at https://jmilne.org/math/Books/index.html.

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

Proof. In the setting of [80], $F = \mathbf{Q}$, K is a Heegner field for $J/\mathbf{Q}$ and the character α is trivial (see the main theorem at the beginning of [80]); therefore, $K(\alpha) = K$, and hence, $\beta = 1$ by [80, (3.1)]. According to [80, 7.3, 7.5, 7.5.3], we have to show that our hypotheses imply $C_i(\mathfrak{p}) = 0$ for $i = 1, \ldots, 6, 0$ (with $C_i(\mathfrak{p})$ as defined in [80]):

(1) If $\mathfrak{p} \nmid \mathrm{Tam}(J/\mathbf{Q})$, then $C_1(\mathfrak{p}) = 0$ because of the definition of $C_1(\mathfrak{p})$ in [80, Proposition 5.12] and by the argument in the proof of theorem 5.6.
(2) If $\ker\big(\mathrm{H}^1(K, J[\mathfrak{p}]) \overset{\mathrm{res}}{\to} \mathrm{H}^1(K(J[\mathfrak{p}]), J[\mathfrak{p}])\big) = 0$, then $C_2(\mathfrak{p}) = 0$ [80, Proposition 6.1.2]. By proposition 5.4 with $F = K$ and the inflation-restriction sequence, this holds since $\rho_{\mathfrak{p}}|_{G_K}$ is irreducible by corollary 2.36 (here, we use $D_K \neq -4, -8, -3$; compare Assumption 5.5).
(3) Since α is trivial, $H = K(\alpha) = K$ in [80, §6]. Hence, there we only need to consider the Dirichlet character $\eta = \varepsilon_K \colon \mathrm{Gal}(K|\mathbf{Q}) \longrightarrow \{\pm 1\}$ of $\mathrm{Gal}(K|\mathbf{Q})$ in [80, Proposition 6.2.2]; thus, $C_3(\mathfrak{p}) = 0$ if $K \in \mathscr{K}_{\mathfrak{p}}(f)$.
(4) We have $C_4(\mathfrak{p}) = 0$ because $\beta^2 = 1$.
(5) By definition [80, (7.4)], $C_5(\mathfrak{p}) = 0$ since $H = K(\alpha) = K$.
(6) One has $C_6(\mathfrak{p}) := \mathrm{ord}_{\mathfrak{p}} \deg \varphi$ with $\varphi \colon J \longrightarrow J^\vee$ a polarization (for the Weil pairing) [80, (7.4)]. Hence, $C_6(\mathfrak{p}) = 0$ because J is principally polarized.
(0) Let $x \in J(K)$ be a Heegner point. One has

$$C_0(\mathfrak{p}) := \max\{c \in \mathbf{Z}_{\geq 0} : x \in J(K)_{\mathrm{tors}} + \mathfrak{p}^c J(K)\}\,;$$

see [80, (7.4)]. Hence, $C_0(\mathfrak{p}) = 0$ if $\mathfrak{p} \nmid \mathcal{I}_{K,\pi}$.

Note that these results imply $Ш(J/K)[\mathfrak{p}] = 0$. Since $\mathfrak{p} \nmid 2$, $Ш(J/\mathbf{Q})[\mathfrak{p}] = 0$ follows. □

We use the refined information that is provided by considering $\mathrm{Tam}(J/\mathbf{Q})$ as an $\mathcal{O}$-ideal in the following way.

Proposition 5.8. *We assume that J is the Jacobian of a curve of genus 2. Fix an odd prime q. Let $\mathscr{J}/\mathbf{Z}$ be the Néron model of $J/\mathbf{Q}$. If*

(i) *there is exactly one rational prime p with $v_q(c_p(J/\mathbf{Q})) \geq 1$ and we have $v_q(c_p(J/\mathbf{Q})) = 1$ (then $a_p(f) \in \{\pm 1, 0\}$),*
(ii) *$q\mathcal{O} = \mathfrak{q}\mathfrak{q}'$ is split in $\mathcal{O}$ with $\rho_{\mathfrak{q}'}$ irreducible,*
(iii) *$v_q(\exp(J(\mathbf{Q})_{\mathrm{tors}})) > v_q(p - a_p(f))$, where $\exp(J(\mathbf{Q})_{\mathrm{tors}})$ denotes the exponent of the rational torsion subgroup of J,*

then $v_{\mathfrak{q}'}(\mathrm{Tam}(J/\mathbf{Q})) = 0$ and $v_{\mathfrak{q}}(\mathrm{Tam}(J/\mathbf{Q})) = 1$.

Proof. Since q is odd, the q-primary part of $J(\mathbf{Q})_{\mathrm{tors}}$ injects into $\mathscr{J}(\mathbf{F}_p)$. The group of $\mathbf{F}_p$-points on the connected component of the identity of $\mathscr{J}_{\mathbf{F}_p}$ has exponent $p - a_p(f)$ since it is a product of two copies of $\mathbf{F}_p^\times$ (when $a_p(f) = 1$) or of the norm 1 subgroup of $\mathbf{F}_{p^2}^\times$ (when $a_p(f) = -1$) or of $\mathbf{F}_p$ (when $a_p(f) = 0$). So (iii) implies that the q-primary part of $J(\mathbf{Q})_{\mathrm{tors}}$ maps nontrivially into the q-primary part of the group of $\mathbf{F}_p$-points of the component group, $\pi_0(\mathscr{J}_{\mathbf{F}_p})(\mathbf{F}_p)$. By (i), the latter is the same as the q-primary part of the ideal $\mathrm{Tam}(J/\mathbf{Q})$, and it has order q, so by (ii), this q-primary part of $\mathrm{Tam}(J/\mathbf{Q})$ is either $\mathfrak{q}$ or $\mathfrak{q}'$. The map from the q-primary part of $J(\mathbf{Q})_{\mathrm{tors}}$ to $\pi_0(\mathscr{J}_{\mathbf{F}_p})(\mathbf{F}_p)$ respects the action of the endomorphism ring. Since $\rho_{\mathfrak{q}'}$ is irreducible, only $\mathfrak{q}$ can occur in the characteristic ideal of $J(\mathbf{Q})_{\mathrm{tors}}$, so only $\mathfrak{q}$ can occur in $\mathrm{Tam}(J/\mathbf{Q})$. □

Examples 5.9. There are three Jacobians of curves from the LMFDB for which we need to apply proposition 5.8 to show that the $\mathfrak{p}$-primary part of $Ш(J/\mathbf{Q})$ is trivial for a degree 1 prime ideal $\mathfrak{p}$ such that $\rho_{\mathfrak{p}}$ is irreducible. For one curve each at levels $N = 39$ and 123, the Tamagawa product is 7 and 7 is split in the endomorphism ring. In both cases, there is rational 7-torsion and $c_3 = 7$, so the proposition applies. In the last case, $N = 133$ and the Tamagawa product is 3, with $c_7 = 3$. We have $a_7 = 1$, so $v_3(7 - a_7(f)) = 1$, but luckily, $J(\mathbf{Q}) \cong \mathbf{Z}/9$, so condition (iii) above is still satisfied.

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

Under stronger assumptions on $\mathfrak{p}$, we can even get an upper bound for $\#\text{Ш}(J/K)[\mathfrak{p}^\infty]$.

Theorem 5.10. *Assume that* $L'(f/K,1) \neq 0$. *Let* $\mathfrak{p} \mid p > 2$ *be a regular prime ideal of* $\operatorname{End}_{\mathbf{Q}}(J)$ *with* $p \nmid h_K \cdot u_K \cdot N$. *Suppose* $\operatorname{im}\rho_{\mathfrak{p}^\infty} = G^{\max}_{\mathfrak{p}^\infty}$. *Then*

$$\operatorname{Sel}_{\mathfrak{p}^\infty}(J/K) \cong (E_{\mathfrak{p}}/\mathcal{O}_{\mathfrak{p}}) \oplus M \oplus M$$

with M *finite of order bounded by* $\#\mathcal{O}_{\mathfrak{p}}/I_{K,\pi}$. *Here,* $E_{\mathfrak{p}}$ *is the completion of* $E = \operatorname{End}^0_{\mathbf{Q}}(J)$.

Proof. This is [55, Theorem A]. □

Note that this implies $\text{Ш}(J/K)[\mathfrak{p}^\infty] \cong M \oplus M$, so in particular,

$$\#\text{Ш}(J/K)[\mathfrak{p}^\infty] \leq \#(\mathcal{O}_{\mathfrak{p}}/I_{K,\pi})^2.$$

theorem 5.10 requires p to be a prime of good reduction and $\rho_{\mathfrak{p}^\infty}$ to be surjective, which theorems 5.6 and 5.7 do not.

6. Computing $\text{Ш}(J/\mathbf{Q})[\mathfrak{p}^\infty]$ using descent

In this section, let J be the Jacobian of a curve of genus 2 whose endomorphism ring $\mathcal{O} = \operatorname{End}_{\mathbf{Q}}(J)$ is an order in a real quadratic field. Let $\mathfrak{p}$ be a prime ideal of degree 1 of $\mathcal{O}$ of residue characteristic p. Then J is modular; let N be the level.

The results of the preceding section reduce the problem of showing that $\#\text{Ш}(J/\mathbf{Q}) = \#\text{Ш}_{\text{an}}(J/\mathbf{Q})$ to the verification that

$$v_p(\#\text{Ш}(J/\mathbf{Q})) = v_p(\#\text{Ш}_{\text{an}}(J/\mathbf{Q}))$$

for finitely many primes p. The left-hand side can be computed by studying $\text{Ш}(J/\mathbf{Q})[\mathfrak{p}^\infty]$ for the prime ideals $\mathfrak{p}$ of $\mathcal{O}$ dividing p. In most cases, we need to show that $\text{Ш}(J/\mathbf{Q})[\mathfrak{p}^\infty] = 0$, for which it is sufficient to show that $\text{Ш}(J/\mathbf{Q})[\mathfrak{p}] = 0$. We can compute (the size of) $\text{Ш}(J/\mathbf{Q})[\mathfrak{p}]$ in principle by doing a *descent* (i.e., by computing the $\mathfrak{p}$-Selmer group $\operatorname{Sel}_{\mathfrak{p}}(J/\mathbf{Q})$ of $J/\mathbf{Q}$). Recall that

$$\operatorname{Sel}_{\mathfrak{p}}(J/\mathbf{Q}) := \ker\Big(\mathrm{H}^1(\mathbf{Q}, J[\mathfrak{p}]) \to \prod_v \mathrm{H}^1(\mathbf{Q}_v, J(\bar{\mathbf{Q}}_v))\Big)$$

and that the Selmer group sits in the following exact sequence:

$$0 \longrightarrow \frac{J(\mathbf{Q})}{\mathfrak{p}J(\mathbf{Q})} \longrightarrow \operatorname{Sel}_{\mathfrak{p}}(J/\mathbf{Q}) \longrightarrow \text{Ш}(J/\mathbf{Q})[\mathfrak{p}] \longrightarrow 0.$$

(There are analogous definitions with p in place of $\mathfrak{p}$.) This implies that

$$v_p\big(\#\text{Ш}(J/\mathbf{Q})[\mathfrak{p}]\big) = v_p(\#\operatorname{Sel}_{\mathfrak{p}}(J/\mathbf{Q})) - (\deg\mathfrak{p})\operatorname{rk}_{\mathcal{O}}(J/\mathbf{Q}) - v_p(\#J(\mathbf{Q})[\mathfrak{p}]).$$

So to verify that $\#\text{Ш}(J/\mathbf{Q})[\mathfrak{p}] = 0$, it is sufficient to show that

$$\dim_{\mathbf{F}_p}\operatorname{Sel}_{\mathfrak{p}}(J/\mathbf{Q}) \leq (\deg\mathfrak{p})\operatorname{rk}_{\mathcal{O}}(J/\mathbf{Q}) + \dim_{\mathbf{F}_p} J(\mathbf{Q})[\mathfrak{p}].$$

6.1. Dealing with $p = 2$

We always need to determine $\#\text{Ш}(J/\mathbf{Q})[2^\infty]$ since primes dividing 2 are always excluded in theorems 5.6 and 5.7. Luckily, for Jacobians of hyperelliptic curves, the size of the 2-Selmer group can be computed fairly easily. This is described in [112] and is implemented in Magma. If this computation shows that $\text{Ш}(J/\mathbf{Q})[2] = 0$, then we know that $\#\text{Ш}(J/\mathbf{Q})$ is odd.

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

The 2-primary part of $Ш(J/\mathbf{Q})$ is somewhat special, as its cardinality can be twice a square (the odd part, if finite, is always the square of some group). Using results of [86], we can determine whether this is the case; in particular, the computation of $J(\mathbf{Q})$ and the 2-Selmer group is sufficient to detect that $\#Ш(J/\mathbf{Q})[2^\infty] = 2$. In all cases from our database where the 2-part of $\#Ш_{\mathrm{an}}(J/\mathbf{Q})$ is 1 or 2, this computation shows that $\#Ш(J/\mathbf{Q})[2^\infty]$ has the expected value.

When $\#Ш(J/\mathbf{Q})[2] > 2$, but $Ш(J/\mathbf{Q})[4] = Ш(J/\mathbf{Q})[2]$, then this can be verified by computing the Cassels–Tate pairing on $\mathrm{Sel}_2(J/\mathbf{Q})$ (this is a symmetric bilinear form on the $\mathbf{F}_2$-vector space $\mathrm{Sel}_2(J/\mathbf{Q})$ whose kernel is the preimage of $2Ш(J/\mathbf{Q})[4]$). A method for doing this is described in the recent preprint [44] by Fisher and Yan, and an alternative approach will be detailed in forthcoming work by Shukla.

There are ten cases in our database where $\#Ш_{\mathrm{an}} = 4$ (in all cases, $\#Ш_{\mathrm{an}} \in \{1, 2, 4\}$), corresponding to the levels and isogeny classes

$$67c,\ 73a,\ 133e,\ 211a,\ 275a,\ 313a,\ 358a,\ 640a,\ 640b,\ 887a,$$

each of which occurs only once in the list. In each case, the 2-descent computation shows that $\#Ш(J/\mathbf{Q})[2] = 4$ as expected. For the two curves at level 640 (that are quadratic twists by -1 of each other), there exists a Richelot isogenous Jacobian J', for which a 2-descent shows that $Ш(J'/\mathbf{Q})[2] = 0$. This shows that in both cases, $\#Ш(J/\mathbf{Q})[2^\infty] = 4$ since elements of order 4 would have to survive the isogeny.

To deal with the remaining eight cases, we need to compute the kernel of the Cassels–Tate pairing on $Ш(J/\mathbf{Q})[2]$ and verify that this kernel is trivial. Fortunately, Fisher and Yan [44] have computed the pairing on the 2-Selmer groups of all Jacobians of genus 2 curves in the LMFDB with even analytic order of Ш. In particular, they have verified that $\#Ш(J/\mathbf{Q})[2^\infty] = 4$ in all cases where $\#Ш_{\mathrm{an}}(J/\mathbf{Q}) = 4$. This finishes the verification for the 2-primary part of Ш in our LMFDB examples. There is one of the 'Wang only' curves that also has $\#Ш(J/\mathbf{Q})[2] = \#Ш(J/\mathbf{Q})_{\mathrm{an}} = 4$ (the curve with label 125B); Tom Fisher has kindly checked for us using the code from [44] that $\#Ш(J/\mathbf{Q})[2^\infty] = 4$ for this curve as well.

6.2. Odd primes

We will now assume that $\mathfrak{p}$ is a prime ideal of $\mathcal{O}$ dividing an odd prime. We will also assume that $\deg \mathfrak{p} = 1$, as for primes of degree 2, the computation tends to get fairly involved. The situation is then analogous to that of a full p-descent (where $p = p(\mathfrak{p})$) on an elliptic curve: the kernel of the isogeny is isomorphic to $\mathbf{Z}/p \times \mathbf{Z}/p$ as a group, and it carries a Weil pairing. How to do a p-descent on an elliptic curve is analyzed in detail in [93]; most of what is done below builds on this analysis. For the general theory of how to perform descent computations, see [16]. We assume that the prime ideal $\mathfrak{p}$ is principal, generated by a prime element ϖ. This ensures that $J/J[\mathfrak{p}] \cong J$ via the multiplication-by-ϖ map. This assumption is satisfied in all the examples that we have considered.

We now assume in addition that $\rho_{\mathfrak{p}}$ is reducible; this is the most common situation when the general results do not allow us to conclude that $Ш(J/\mathbf{Q})[\mathfrak{p}] = 0$. We then have an exact sequence of Galois modules

$$0 \longrightarrow M_1 \longrightarrow J[\mathfrak{p}] \longrightarrow M_2 \longrightarrow 0,$$

where M_1 and M_2 are one-dimensional Galois modules corresponding to characters with values in $\mathbf{F}_p^\times$. A frequently occurring case is that $J[\mathfrak{p}]$ contains a rational point of order p; then $M_1 \cong \mathbf{Z}/p$, and the action on M_2 is via the cyclotomic character χ_p. Let $A = J/M_1$ be the isogenous abelian surface; write $\varphi\colon J \to A$ for the corresponding isogeny and $\psi\colon A \to J$ for the isogeny such that $\psi \circ \varphi = \varpi$; its kernel is $\varphi(J[\mathfrak{p}]) \simeq M_2$. Then we have the associated Selmer groups $\mathrm{Sel}(\varphi) \subseteq \mathrm{H}^1(\mathbf{Q}, M_1)$ and

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

$\mathrm{Sel}(\psi) \subseteq \mathrm{H}^1(\mathbf{Q}, M_2)$ and an exact sequence (see [93, Lemma 6.1])

$$0 \longrightarrow \frac{M_2(\mathbf{Q})}{\varphi(J[\mathfrak{p}](\mathbf{Q}))} \longrightarrow \mathrm{Sel}(\varphi) \longrightarrow \mathrm{Sel}_{\mathfrak{p}}(J/\mathbf{Q}) \longrightarrow \mathrm{Sel}(\psi).$$

This allows us to bound $\dim_{\mathbf{F}_p} \mathrm{Sel}_{\mathfrak{p}}(J/\mathbf{Q})$ via

$$\dim_{\mathbf{F}_p} \mathrm{Sel}_{\mathfrak{p}}(J/\mathbf{Q}) \leq \dim_{\mathbf{F}_p} \mathrm{Sel}(\varphi) + \dim_{\mathbf{F}_p} \mathrm{Sel}(\psi) - \dim_{\mathbf{F}_p} \frac{M_2(\mathbf{Q})}{\varphi(J[\mathfrak{p}](\mathbf{Q}))}.$$

Let S be a finite set of primes. For a finite Galois module M such that $pM = 0$, we denote by $\mathrm{H}^1(\mathbf{Q}, M; S)$ the subgroup of cohomology classes unramified outside S (i.e., mapping to zero in $\mathrm{H}^1(I_q, M)$ for all primes $q \notin S$, where I_q is the inertia group at q). (Since p is odd, we can ignore the infinite place.)

By Lemma 3.1 and the following text in [93] (the arguments carry over from elliptic curves to abelian varieties), the Selmer group $\mathrm{Sel}(\theta)$ of an isogeny $\theta\colon A_1 \to A_2$ is contained in $\mathrm{H}^1(\mathbf{Q}, \ker\theta; S)$, where S is the set of primes q such that the Tamagawa number $c_q(A_2)$ is divisible by p, together with p. We set

$$S_J := \{p\} \cup \{q \text{ prime} : p \mid c_q(J)\}$$

and define S_A in a similar way. Then

$$S_A \subseteq S'_J := \{p\} \cup \{q \text{ prime} : q \mid N\}.$$

By considering the reduction type of J at q, we may be able to obtain a smaller upper bound for S_A.

Now let M be a one-dimensional (over $\mathbf{F}_p$) Galois representation given by the character $\chi\colon \mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}) \to \mathbf{F}_p^\times$. Let $M^\vee := \mathrm{Hom}(M, \mu_p)$ be the Cartier dual, with character $\chi_p\chi^{-1}$. Let L be the fixed field of the kernel of $\chi_p\chi^{-1}$. The degree of $L/\mathbf{Q}$ divides $p-1$, so is prime to p, so by inflation-restriction, we see that

$$\mathrm{H}^1(\mathbf{Q}, M) \simeq \mathrm{H}^1(L, M)^{\mathrm{Gal}(L/\mathbf{Q})} \simeq \mathrm{H}^1(L, \mu_p)^{(1)} \simeq (L^\times/L^{\times p})^{(1)},$$

where the superscript (1) denotes the subspace on which the action of $\sigma \in \mathrm{Gal}(L/\mathbf{Q})$ is given by multiplying by a_σ / raising to the a_σth power, where $a_\sigma = \chi_p\chi^{-1}(\sigma) \in \mathbf{F}_p^\times$. We can restrict this isomorphism to the elements that are unramified outside S. Here, $\alpha L^{\times p} \in L^\times/L^{\times p}$ is considered to be unramified outside S when the extension $L(\sqrt[p]{\alpha})/L$ is unramified outside places above primes in S; equivalently (when $p \in S$), p divides all valuations $v_{\mathfrak{q}}(\alpha)$ for $\mathfrak{q} \mid q \notin S$. Denoting the subgroup of elements unramified outside S by $L(S,p)$, this shows that $\mathrm{Sel}(\varphi) \subseteq L_1(S_A, p)^{(1)}$ and $\mathrm{Sel}(\psi) \subseteq L_2(S_J, p)^{(1)}$, where L_1 and L_2 are the fields associated to M_1 and M_2, respectively.

Since it occurs frequently, we give an explicit statement in the case that $J[\mathfrak{p}]$ contains a rational point of order p (then $M_1 = \mathbf{Z}/p$ and $M_2 = \mu_p$). We will use the notation

$$[\mathcal{A}] := \begin{cases} 1, & \text{if } \mathcal{A} \text{ is true} \\ 0, & \text{otherwise.} \end{cases}$$

Proposition 6.1. *Let J be the Jacobian of a curve of genus 2 that has real multiplication; as before, let N be its level. Let $\mathfrak{p}$ be a prime ideal of degree 1 of $\mathcal{O} = \mathrm{End}_{\mathbf{Q}}(J)$ of residue characteristic $p > 2$. Assume that $J[\mathfrak{p}](\mathbf{Q}) \cong \mathbf{Z}/p$ and that the class number of $\mathbf{Q}(\mu_p)$ is not divisible by p. Then*

$$\begin{aligned}\dim_{\mathbf{F}_p} Ш(J/\mathbf{Q})[\mathfrak{p}] \leq \#\{&q \textit{ prime} : q \mid N \textit{ and } q \equiv 1 \bmod p\} \\ &+ \#\{q \textit{ prime} : p \mid c_q(J)\} + [p \mid N] - \mathrm{rk}_{\mathcal{O}} J(\mathbf{Q}).\end{aligned}$$

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

If, in addition, there is a prime $\ell \equiv 1 \bmod p$ such that the natural map

$$r_\ell \colon \mathbf{Q}(\{q : p \mid c_q(J) \text{ or } q = p \mid N\}, p) \to \mathbf{Q}_\ell^\times/\mathbf{Q}_\ell^{\times p}$$

is nontrivial and the map

$$r'_\ell \colon \mathbf{Q}(\mu_p)(\{p\} \cup \{q : q \mid N \text{ and } q \equiv 1 \bmod p\}, p)^{(1)} \to \mathbf{Q}_\ell^\times/\mathbf{Q}_\ell^{\times p}$$

induced by any embedding $\mathbf{Q}(\mu_p) \to \mathbf{Q}_\ell$ is surjective, then the above inequality is strict.

Proof. Since $M_1 = \langle P \rangle \cong \mathbf{Z}/p$, we have $L_1 = \mathbf{Q}(\mu_p)$. Similarly, since $M_2 \cong \mu_p$, we have $L_2 = \mathbf{Q}$. Let $F \in \mathbf{Q}(X)^\times$ be a function whose divisor is pD, where the linear equivalence class of D is P; then the 'descent map' $\delta \colon J(\mathbf{Q}) \to \mathrm{H}^1(\mathbf{Q}, M_2) \simeq \mathbf{Q}^\times/\mathbf{Q}^{\times p}$ is given by evaluating F on a representative divisor whose support is disjoint from that of D. We have the analogous map $\delta_q \colon J(\mathbf{Q}_q) \to \mathbf{Q}_q^\times/\mathbf{Q}_q^{\times p}$ for each prime q. By the above, $\mathrm{Sel}(\psi \colon A \to J)$ is contained in the unramified outside S_J part of $\mathbf{Q}^\times/\mathbf{Q}^{\times p}$, which is the subgroup generated by the classes of the primes in S_J. When $p \nmid N$, so that J has good reduction at p, then we can choose F in such a way that its reduction mod p is well-defined. When evaluating δ_p on a point $Q \in J(\mathbf{Q}_p)$, we can pick a representative divisor whose support is disjoint mod p from the support of D; this shows that $F(Q)$ is in the image of $\mathbf{Z}_p^\times$ and hence that $\mathrm{Sel}(\psi) \subseteq \langle q : p \mid c_q(J) \rangle$ in this case. So in any case, we have

$$\dim_{\mathbf{F}_p} \mathrm{Sel}(\psi) \le \#\{q \text{ prime} : p \mid c_q(J)\} + [p \mid N]. \tag{6.1}$$

We obtain a bound on $\mathrm{Sel}(\varphi)$ from the inclusion $\mathrm{Sel}(\varphi) \subseteq L_1(S'_J, p)^{(1)} = \mathbf{Q}(\mu_p)(S'_J, p)^{(1)}$. Since we assume that the class number of $\mathbf{Q}(\mu_p)$ is not divisible by p, the group $\mathbf{Q}(\mu_p)(S'_J, p)$ is generated by the images of a primitive pth root of unity ζ_p, a choice of fundamental units, $1 - \zeta_p$, and one element generating a suitable power of each prime ideal above a prime in S'_J. Of these, only ζ_p and the totally split primes contribute to the relevant eigenspace (the fundamental units come, up to index prime to p, from the maximal real subfield, and the ideal $\langle 1 - \zeta_p \rangle$ and the nonsplit prime ideals have nontrivial stabilizer), and the contribution of each totally split prime q is exactly 1. Since q is totally split in $\mathbf{Q}(\mu_p)$ if and only if $q \equiv 1 \bmod p$, we obtain the bound

$$\begin{aligned} \dim_{\mathbf{F}_p} \mathrm{Sel}(\varphi) &\le \dim_{\mathbf{F}_p} \mathbf{Q}(\mu_p)(S'_J, p)^{(1)} \\ &= 1 + \#\{q \text{ prime} : q \mid N \text{ and } q \equiv 1 \bmod p\}. \end{aligned} \tag{6.2}$$

Finally, we have

$$\begin{aligned} \dim_{\mathbf{F}_p} Ш(J/\mathbf{Q})[\mathfrak{p}] &= \dim_{\mathbf{F}_p} \mathrm{Sel}(J/\mathbf{Q})[\mathfrak{p}] - \dim_{\mathbf{F}_p} \frac{J(\mathbf{Q})}{\mathfrak{p}J(\mathbf{Q})} \\ &\le \dim_{\mathbf{F}_p} \mathrm{Sel}(\varphi) + \dim_{\mathbf{F}_p} \mathrm{Sel}(\psi) - 1 - \mathrm{rk}_{\mathcal{O}} J(\mathbf{Q}) \\ &\le \#\{q \text{ prime} : q \mid N \text{ and } q \equiv 1 \bmod p\} \\ &\qquad + \#\{q \text{ prime} : p \mid c_q(J)\} + [p \mid N] - \mathrm{rk}_{\mathcal{O}} J(\mathbf{Q}), \end{aligned}$$

where we have used $\dim J(\mathbf{Q})/\mathfrak{p}J(\mathbf{Q}) = \mathrm{rk}_{\mathcal{O}} J(\mathbf{Q}) + \dim J(\mathbf{Q})[\mathfrak{p}]$ and Equations (6.1) and (6.2).

To show the refinement, consider the kernel-cokernel exact sequence associated to $J(\mathbf{Q}_\ell) \xrightarrow{\varphi} A(\mathbf{Q}_\ell) \xrightarrow{\psi} J(\mathbf{Q}_\ell)$,

$$\begin{aligned} &0 \longrightarrow \mathbf{Z}/p \longrightarrow J(\mathbf{Q}_\ell)[\mathfrak{p}] \xrightarrow{\varphi} \mu_p(\mathbf{Q}_\ell) \longrightarrow \\ &\longrightarrow \frac{A(\mathbf{Q}_\ell)}{\varphi(J(\mathbf{Q}_\ell))} \xrightarrow{\psi} \frac{J(\mathbf{Q}_\ell)}{\mathfrak{p}J(\mathbf{Q}_\ell)} \longrightarrow \frac{J(\mathbf{Q}_\ell)}{\psi(A(\mathbf{Q}_\ell))} \longrightarrow 0. \end{aligned}$$

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

Since $\ell \equiv 1 \bmod p$, $\dim \mu_p(\mathbf{Q}_\ell) = 1$. Since $p \nmid \ell$, $\dim J(\mathbf{Q}_\ell)/\mathfrak{p}J(\mathbf{Q}_\ell) = \dim J(\mathbf{Q}_\ell)[\mathfrak{p}]$. These facts imply that

$$\dim \frac{A(\mathbf{Q}_\ell)}{\varphi(J(\mathbf{Q}_\ell))} + \dim \frac{J(\mathbf{Q}_\ell)}{\psi(A(\mathbf{Q}_\ell))} = 2.$$

We note that the elements of $\mathrm{Sel}(\varphi)$ (respectively, $\mathrm{Sel}(\psi)$) map into the image of $A(\mathbf{Q}_\ell)/\varphi(J(\mathbf{Q}_\ell))$ in $\mathrm{H}^1(\mathbf{Q}_\ell, \mathbf{Z}/p) \cong \mathbf{Q}_\ell^\times/\mathbf{Q}_\ell^{\times p}$ (respectively, into the image of $J(\mathbf{Q}_\ell)/\psi(A(\mathbf{Q}_\ell))$ in $\mathrm{H}^1(\mathbf{Q}_\ell, \mu_p) \simeq \mathbf{Q}_\ell^\times/\mathbf{Q}_\ell^{\times p}$) under r'_ℓ (respectively, r_ℓ). If $\dim J(\mathbf{Q}_\ell)/\psi(A(\mathbf{Q}_\ell)) = 0$, then $\mathrm{Sel}(\psi)$ is contained in the kernel of r_ℓ; since r_ℓ is assumed to be nontrivial, this implies that the bound on $\dim \mathrm{Sel}(\psi)$ can be reduced by 1. Otherwise, $\dim A(\mathbf{Q}_\ell)/\varphi(J(\mathbf{Q}_\ell)) \leq 1 < 2 = \dim \mathbf{Q}_\ell^\times/\mathbf{Q}_\ell^{\times p}$. Since r'_ℓ is assumed to be surjective, this implies that the bound on $\dim \mathrm{Sel}(\varphi)$ can be reduced by 1. So in all cases, the bound on $\dim \mathrm{Sel}(\varphi) + \dim \mathrm{Sel}(\psi)$ is reduced by 1, which gives a corresponding improvement for the bound on $\dim Ш(J/\mathbf{Q})[\mathfrak{p}]$. □

Remark 6.2. In some cases (for example in Examples 6.10 (iii)), we can improve the bound in proposition 6.1 by 1 when $p \mid N$. Assume that we can find enough ‘descent functions, $F \in \mathbf{Q}(X)^\times$ (i.e., whose divisor is p times a divisor D such that $[D] \in J(\mathbf{Q})$ generates $J[\mathfrak{p}]$) that reduce to well-defined functions $\bar{F}$ on $X_{\mathbf{F}_p}$ and such that the support of $\bar{F}$ consists of smooth points on $X_{\mathbf{F}_p}$ and that the following holds: if D is a divisor of degree zero on X defined over $\mathbf{Q}$ with reduction $\bar{D}$ modulo p, then we can find some F such that the divisor of $\bar{F}$ has support disjoint from $\bar{D}$. Then the argument near the beginning of the proof of proposition 6.1 shows that $F(D) \in \mathbf{Z}_p^\times$; hence,

$$\mathrm{Sel}(\psi) \subseteq \mathbf{Q}(\{q \text{ prime} : p \mid c_q(J)\}, p),$$

and so we can remove the term ‘$[p \mid N]$’ in the final bound.

We also note the following.

Lemma 6.3. *If we assume additionally that* $\mathrm{rk}_{\mathcal{O}} J(\mathbf{Q}) \leq 1$ *in the situation above, then* $\dim_{\mathbf{F}_p} Ш(J/\mathbf{Q})[\mathfrak{p}]$ *is even. In particular,* $\dim_{\mathbf{F}_p} Ш(J/\mathbf{Q})[\mathfrak{p}] \leq 1$ *implies that* $Ш(J/\mathbf{Q})[\mathfrak{p}] = 0$.

Proof. By the general results on abelian surfaces with RM, J is modular. The additional assumption then implies by [64] that $Ш(J/\mathbf{Q})$ is finite. Therefore, the Cassels–Tate pairing on $Ш(J/\mathbf{Q})$ is perfect. It is also anti-symmetric, which implies (since p is odd) that its restriction to $Ш(J/\mathbf{Q})[\mathfrak{p}^\infty]$ is perfect and alternating. This in turn implies that $Ш(J/\mathbf{Q})[\mathfrak{p}^\infty] \cong M \times M$ for some finite $\mathcal{O}_\mathfrak{p}$-module M. In particular, $Ш(J/\mathbf{Q})[\mathfrak{p}] \cong M[\mathfrak{p}] \times M[\mathfrak{p}]$, and so $\dim_{\mathbf{F}_p} Ш(J/\mathbf{Q})[\mathfrak{p}] = 2\dim_{\mathbf{F}_p} M[\mathfrak{p}]$. □

Examples 6.4. For most pairs (X, p) consisting of a curve X in our database of LMFDB curves and an odd prime p such that the table in Section 2.14 says that the semisimplification of $\rho_\mathfrak{p}$ splits as $\mathbf{1} \oplus \chi_p$, where $\mathfrak{p}$ is a prime ideal of the endomorphism ring of degree 1, the non-strict bound in proposition 6.1 together with lemma 6.3 show that $Ш(J/\mathbf{Q})[\mathfrak{p}] = 0$. The exceptions are as follows. (We frequently indicate the isogeny class with a letter appended to the level N.)

(i) Two of the four curves at level $N = 31$, where $p = 5$ (one has no rational point of order 5, the other gives a bound $\dim Ш(J/\mathbf{Q})[\mathfrak{p}] \leq 2$). This is unproblematic, since these Jacobians are isogenous to the Jacobians of the two other curves at that level, for which the simple bound proves that $Ш(J/\mathbf{Q})[\mathfrak{p}] = 0$. By invariance of BSD in isogeny classes, it suffices to verify strong BSD for one of these Jacobians.

(ii) The pairs $(N, p) = (73a, 3)$ and $(85b, 3)$, where there is no rational point of order 3.

(iii) The curves at level $133d$ with $p = 3$ and at level $275a$ with $p = 5$, where the non-strict bound only gives $\dim Ш(J/\mathbf{Q})[\mathfrak{p}] \leq 2$.

Examples 6.5. We consider the curves listed under (ii) above. In these cases, the $\mathfrak{p}$-torsion (where $\mathfrak{p}$ is an ideal of norm 3) sits in an exact sequence

$$0 \longrightarrow \mu_3 \longrightarrow J[\mathfrak{p}] \longrightarrow \mathbf{Z}/3\mathbf{Z} \longrightarrow 0.$$

Using the fact that $M_2(\mathbf{Q})/\varphi(J[\mathfrak{p}]) \cong \mathbf{Z}/3\mathbf{Z}$ in these cases and that the Tamagawa numbers at all bad primes are not divisible by 3 (and 3 is not a bad prime, which implies that $\mathrm{Sel}(\psi) \subseteq \mathbf{Q}(\{q\text{prime} : q \mid N\}, 3)$), this leads to a general bound of the form

$$\begin{aligned}\dim_{\mathbf{F}_3} Ш(J/\mathbf{Q})[\mathfrak{p}] &\le \dim_{\mathbf{F}_3} \mathrm{Sel}(\psi) - 1 + \dim_{\mathbf{F}_3} \mathrm{Sel}(\varphi) - \mathrm{rk}_{\mathcal{O}} J(\mathbf{Q}) \\ &\le \dim_{\mathbf{F}_3} \mathbf{Q}(\{q \text{ prime} : q \mid N\}, 3) - 1 \\ &\qquad + \dim_{\mathbf{F}_3} \mathbf{Q}(\mu_3)(\{3\}, 3)^{(1)} - \mathrm{rk}_{\mathcal{O}} J(\mathbf{Q}) \\ &\le \#\{q \text{ prime} : q \mid N\} - \mathrm{rk}_{\mathcal{O}} J(\mathbf{Q}),\end{aligned}$$

which evaluates to 1 and 2, respectively, for $N = 73$ and 85. Using lemma 6.3, this already shows that $Ш(J/\mathbf{Q})[\mathfrak{p}] = 0$ for $N = 73$.

To improve the bound for $N = 85$, we note that in this case,

$$\mathrm{Sel}_{\mathfrak{p}}(J/\mathbf{Q}) \subseteq \mathrm{H}^1(\mathbf{Q}, J[\mathfrak{p}]; S) \subseteq \mathbf{Q}(\sqrt[3]{5})(\{3\}, 3) \times \mathbf{Q}(\mu_3)(\{3\}, 3)$$

and that $\mathrm{Sel}(\psi) \subseteq \mathbf{Q}(\{5, 17\}, 3)$ maps into the first factor by the obvious map. (Compare Section 6 of [93]; one can check that the algebra that is called D there is a product of two copies of $\mathbf{Q}(\sqrt[3]{5})$.) Since any element involving 17 will have image ramified at 17, this shows that actually, $\mathrm{Sel}(\psi) \subseteq \mathbf{Q}(\{5\}, 3)$ (we even have equality here, since we know the map to $\mathrm{Sel}_{\mathfrak{p}}(J/\mathbf{Q})$ has one-dimensional kernel), thus improving the bound by 1, which is sufficient to conclude.

Examples 6.6. We now consider the cases listed under (iii) above. For both pairs (N, p), we can use the strict bound in proposition 6.1. The non-strict bound for $\dim Ш(J/\mathbf{Q})[\mathfrak{p}]$ is 2 in both cases.

In the first case, $(7 \cdot 19, 3)$ for the curve in isogeny class 133d, we use $\ell = 7$. Here, $c_7 = 3$ and $c_{19} = 1$, so the first condition is that $\mathbf{Q}(\{7\}, 3) \to \mathbf{Q}_7^\times/\mathbf{Q}_7^{\times 3}$ is nontrivial, which is clearly the case. The second condition is that $\mathbf{Q}(\mu_3)(\{3, 7, 19\}, 3)^{(1)} \to \mathbf{Q}_7^\times/\mathbf{Q}_7^{\times 3}$ is surjective, which follows from the fact that $\mathbf{Q}_7$ does not contain a primitive ninth root of unity. So both conditions are satisfied, and the bound can be improved to $\dim Ш(J/\mathbf{Q})[\mathfrak{p}] \le 1$, which is sufficient to conclude that $Ш(J/\mathbf{Q})[\mathfrak{p}] = 0$ by lemma 6.3.

We now consider $(5^2 \cdot 11, 5)$ for the curve in isogeny class 275a. Here, we use $\ell = 11$. Both Tamagawa numbers are 1, so the first condition is that $\mathbf{Q}(\{5\}, 5) \to \mathbf{Q}_{11}^\times/\mathbf{Q}_{11}^{\times 5}$ is nontrivial. This follows from the fact that 5 is not a fifth power in $\mathbf{F}_{11}$. The second condition is that $\mathbf{Q}(\mu_5)(\{5, 11\}, 5)^{(1)} \to \mathbf{Q}_{11}^\times/\mathbf{Q}_{11}^{\times 5}$ is surjective. This follows in the same way as for the previous example. So we can again reduce the bound by 1 and obtain that $Ш(J/\mathbf{Q})[\mathfrak{p}] = 0$.

We note that with some more work, one can show that in both these cases, we have $\mathrm{Sel}(\psi) = 0$.

The remaining cases (where $\rho_{\mathfrak{p}}^{\mathrm{ss}}$ splits into two nontrivial characters) come from the following pairs of level (+ isogeny class) and prime.

$$\begin{aligned}&(125a, 5),\ (147a, 7),\ (245a, 7),\ (250a, 5),\ (275b, 3) \\ &\qquad (289a, 3),\ (289a, 17),\ (375a, 5),\ (841a, 29).\end{aligned}$$

Examples 6.7. We consider the curve at level $N = 125 = 5^3$ and $\mathfrak{p} = \langle\sqrt{5}\rangle$. According to example 2.20, (1), we have $\rho_{\mathfrak{p}} \cong \chi_5^2 \oplus \chi_5^3$. This implies that

$$\mathrm{Sel}_{\mathfrak{p}}(J/\mathbf{Q}) \subseteq \mathbf{Q}(\mu_5)(\{5\}, 5)^{(-1)} \oplus \mathbf{Q}(\sqrt{5})(\{5\}, 5)^{(2)},$$

where the superscript (m) indicates that the action is via χ_5^m. One finds easily that the first summand is trivial and the second has dimension 1. Since the $\mathcal{O}$-rank of $J(\mathbf{Q})$ is 1, we obtain the bound

$$\dim_{\mathbf{F}_5} Ш(J/\mathbf{Q})[\sqrt{5}] \le 0 + 1 - 1 = 0,$$

so $Ш(J/\mathbf{Q})[\sqrt{5}] = 0$.

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

Similarly, for the curves at levels $2 \cdot 5^3$ and $3 \cdot 5^3$, we have (for $\mathfrak{p} = \langle\sqrt{5}\rangle$) that $\rho_{\mathfrak{p}}^{\mathrm{ss}} \cong \chi_5^2 \oplus \chi_5^3$. Since 2 and 3 are primitive roots mod 5, we still have that $\mathbf{Q}(\mu_5)(\{q,5\},5)^{(-1)}$ is trivial and $\mathbf{Q}(\sqrt{5})(\{q,5\},5)^{(1)}$ is one-dimensional, where $q = 2$ or 3. This gives the bound

$$\dim_{\mathbf{F}_5} Ш(J/\mathbf{Q})[\sqrt{5}] \leq 0 + 1 - \mathrm{rk}_{\mathcal{O}} J(\mathbf{Q}) \leq 1$$

(the rank is zero for the curve at level $2 \cdot 5^3$ and one for the curve at level $3 \cdot 5^3$), which again suffices to conclude that $Ш(J/\mathbf{Q})[\sqrt{5}] = 0$.

The two pairs $(N, p) = (17^2, 17)$ and $(29^2, 29)$ can be dealt with in a similar way as $(N, p) = (5^3, 5)$.

Examples 6.8. We now consider $(N, p) = (3 \cdot 7^2, 7)$ and $(5 \cdot 7^2, 7)$. In both cases, $\mathcal{O} = \mathbf{Z}[\sqrt{2}]$, and $\rho_{\mathfrak{p}}$ is reducible for exactly one of the two prime ideals above 7, with $\rho_{\mathfrak{p}}^{\mathrm{ss}} \cong \chi_7^3 \oplus \chi_7^4$. The two relevant groups are $\mathbf{Q}(\mu_7)^+(\{q,7\},7)^{(4)}$ and $\mathbf{Q}(\sqrt{-7})(\{q,7\},7)^{(3)}$, with $q = 3$ or $q = 5$. Since both are primitive roots mod 7, q does not contribute to the relevant eigenspaces, and it is easy to see that the first group has dimension 1, whereas the second one is trivial. The $\mathcal{O}$-rank is 1 in both cases, which directly shows that $Ш(J/\mathbf{Q})[\mathfrak{p}] = 0$.

Examples 6.9. For $(N, p) = (17^2, 3)$, we have $\rho_{\mathfrak{p}}^{\mathrm{ss}} \cong \varepsilon_{17} \oplus \varepsilon_{-3\cdot 17}$, where ε_m denotes the quadratic character mod m. This is one of two cases in our examples where the two characters are not powers of χ_p. The two relevant groups are $\mathbf{Q}(\sqrt{-3 \cdot 17})(\{3,17\},3)^-$, which is trivial, and $\mathbf{Q}(\sqrt{17})(\{3,17\},3)^-$, which has dimension 1. The $\mathcal{O}$-rank is 1, which directly gives that $Ш(J/\mathbf{Q})[\mathfrak{p}] = 0$.

The other similar case is $(N, p) = (5^2 \cdot 11, 3)$, where $\rho_{\mathfrak{p}}^{\mathrm{ss}} \cong \varepsilon_5 \oplus \varepsilon_{-3\cdot 5}$, and we obtain the same bound with a similar argument. (Note that 5 and 11, like 17, are primitive roots mod 3.)

Examples 6.10. There are three ‘Wang only’ curves for which a $\mathfrak{p}$-descent is necessary – namely,

(i) Curve 117B with $\mathfrak{p} \mid 7$,
(ii) Curve 125B with $\mathfrak{p} \mid 5$, and
(iii) Curve 175 with $\mathfrak{p} \mid 5$.

In all cases, we have to show that $Ш(J/\mathbf{Q})[\mathfrak{p}] = 0$.

In case (i), we have an exact sequence

$$0 \longrightarrow \varepsilon_{-3} \longrightarrow J[\mathfrak{p}] \longrightarrow \varepsilon_{-3} \cdot \chi_7 \longrightarrow 0.$$

This case can be dealt with in a similar way as in Examples 6.8; we obtain $\dim Ш(J/\mathbf{Q})[\mathfrak{p}] \leq 1$.

In case (ii), $J[\mathfrak{p}] \cong \mathbf{1} \oplus \chi_5$ is split. It can be dealt with similarly to Examples 6.7, leading again to $\dim Ш(J/\mathbf{Q})[\mathfrak{p}] \leq 1$.

Finally, in case (iii), we have a non-split exact sequence

$$0 \longrightarrow \mathbf{1} \longrightarrow J[\mathfrak{p}] \longrightarrow \chi_5 \longrightarrow 0,$$

and $\mathfrak{p} = \langle\sqrt{5}\rangle$. The non-strict bound from proposition 6.1 gives us only $\dim Ш(J/\mathbf{Q})[\mathfrak{p}] \leq 2$: we have $\mathrm{Sel}(\varphi) \subseteq \mathbf{Q}(\mu_5)(\{5,7\},5)^{(1)} = \mathbf{Q}(\mu_5)(\emptyset,5)^{(1)}$, which has dimension 1, and $\mathrm{Sel}(\psi) \subseteq \mathbf{Q}(\{5,7\},5)$ of dimension 2. We can improve the bound using remark 6.2. The functions

$$\frac{(8x^5 + 5x^4 + 15x^3 + 30x^2 + 15x + 4) \pm (6x^2 + x - 2)y}{(x-a)^5}$$

for $a \in \{0, \pm 1, \pm 2, \infty\}$ (where we set $1/(x-\infty)^5 := 1$) form a suitable set of descent functions on the model

$$X\colon\, y^2 = x^6 - 2x^5 - 3x^4 - 6x^3 - 14x^2 - 8x - 3$$

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

of the curve, so in fact, $\mathrm{Sel}(\psi) \subseteq \mathbf{Q}(\{7\}, 5)$ has dimension at most 1, which is enough to conclude that $Ш(J/\mathbf{Q})[\mathfrak{p}] = 0$. (In fact, $\dim \mathrm{Sel}(\psi) = 1$, since evaluating a suitable descent function on a point of order 5 gives 7^2, which is a fifth power in $\mathbf{Q}_5$, but nontrivial in $\mathbf{Q}_7^\times/\mathbf{Q}_7^{\times 5}$.)

7. Bounding $Ш(J/\mathbf{Q})[\mathfrak{p}^\infty]$ using Iwasawa Theory

The Main Conjectures for modular forms in Iwasawa Theory imply the p-part of strong BSD under certain conditions when the L-rank is 0 or 1; see theorem 7.3 below and [21]. For fixed p of good ordinary reduction, we can also compute an approximation to the p-adic L-function and use the known results on the p-adic BSD conjecture (see theorem 7.6 below) to determine or at least bound the p-valuation of the order of Ш; this works even for higher rank, assuming Schneider's conjecture on the nonvanishing of the p-adic Schneider regulator (see [109]).

As we will only need these results in the case that p is a prime of good ordinary reduction that is inert in $\mathbf{Z}[f]$, we restrict to this situation in the following, although more general results are available, which apply more generally in the case when there is exactly one prime ideal of $\mathbf{Z}[f]$ lying above p.

This section generalizes [109] from elliptic curves to modular abelian varieties of arbitrary dimension. The results in Sections 7.1 and 7.2 are not fully used in this paper but can be used to extend the verification of strong BSD to examples not contained in our database.

Let f be a newform of level N with coefficient ring $\mathbf{Z}[f]$. We assume that $a_p(f)$ is a p-adic unit (i.e., that p is *ordinary* for f). This implies that the Euler factor at p of f (equivalently, the characteristic polynomial of the Frobenius at p on the associated compatible system of ℓ-adic Galois representations) has exactly one root that is a p-adic unit; we denote this root by α. We use the following notation. Let f be a newform and $\mathfrak{p} \mid p$ a prime of $\mathbf{Z}[f]$. Let $\mathscr{L}_\mathfrak{p}(f,T) \in \mathbf{Q}(f)_\mathfrak{p}[\![T]\!]$ be the $\mathfrak{p}$-*adic L-function* of f constructed in [5, §2.2]. If A is the abelian variety associated to f, $\mathscr{L}_\mathfrak{p}(A,T) = \prod_{\sigma\colon \mathbf{Z}[f]\hookrightarrow \mathbf{R}} \mathscr{L}_\mathfrak{p}(f^\sigma,T)$; see [5, §2.3].

7.1. The Iwasawa–Greenberg Main Conjecture

We use the following known cases of the GL_2 Iwasawa–Greenberg Main Conjecture.

Theorem 7.1 (Skinner–Urban, Skinner). *Let $f \in S_2(\Gamma_0(N))$ be a newform and $p > 2$ be a prime with*

(ord) $v_p(N) \le 1$ *and* $|a_p(f)|_p = 1$.

Let $\mathfrak{p} \mid p$ be a finite place of $\mathbf{Q}(f)$ and $\mathbf{Q}_\infty$ be the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}$ with Galois group $\Gamma := \mathrm{Gal}(\mathbf{Q}_\infty|\mathbf{Q})$. *Let $\Lambda := \mathbf{Z}[f]_\mathfrak{p}[\![\Gamma]\!]$ be the Iwasawa algebra.*

Assume that

(irr) *$\rho_{f,\mathfrak{p}}$ is irreducible and*
(♠) *that there exists a prime $q \ne p$ with $v_q(N) = 1$ such that $\rho_{f,\mathfrak{p}}$ is ramified at q.*

Then one has an equality

$$\mathrm{Char}_{\mathbf{Q}_\infty,\mathbf{Z}[f]_\mathfrak{p}}(f) = (\mathscr{L}_\mathfrak{p}(f,T))$$

of ideals in Λ. Here, $\mathrm{Char}_{\mathbf{Q}_\infty,\mathbf{Z}[f]_\mathfrak{p}}(f)$ is the characteristic ideal of the $\mathfrak{p}$-adic Selmer group of f over $\mathbf{Q}_\infty$ and $\mathscr{L}_\mathfrak{p}(f,T)$ is the $\mathfrak{p}$-adic L-function of f; both are defined in [107, §1.1].

Proof. See [107, Theorem 1] in the case $v_p(N) = 0$ and [106, Theorem A] in the case $v_p(N) = 1$ (by reduction to [107] using Hida theory). (Note the footnote 1 in [106, p. 172], which says one can weaken the condition that there exists an $\mathbf{Z}[f]_\mathfrak{p}$-basis of T_f with respect to which the image of $\rho_{f,\mathfrak{p}^\infty}$ contains $\mathrm{SL}_2(\mathbf{Z}_p)$ to condition (♠) for the Iwasawa Main Conjecture to hold integrally in [107, Theorem 1].) □

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

Example 7.2. We expect that theorem 7.1 combined with the computation of $\mathscr{L}_{\mathfrak{p}}(f,T)$ can be used to verify strong BSD for the Jacobian J of level 145 of the curve

$$C\colon y^2 = 20x^5 - 19x^4 + 118x^3 - 169x^2 + 50x + 25$$

with $\mathrm{End}_{\mathbf{Q}}(J) \cong \mathbf{Z}[\sqrt{2}]$. Our algorithm gives us that $\#\text{Ш}(J/\mathbf{Q})_{\mathrm{an}} = 1$ and $\text{Ш}(J/\mathbf{Q})[\mathfrak{p}] = 0$ except maybe for the two primes $\mathfrak{p}$ lying above 7. For them, one can compute the $\mathfrak{p}$-adic L-function using Sage. (This curve is not contained in our dataset and is only an illustration of how the results in this section can be used in the verification of the p-part of BSD when descent methods are impractical. It came up in forthcoming work of Kaya–Masdeu–Müller–van der Put that computes Schneider regulators of Mumford curves. A verification the p-adic BSD conjecture for this example up to high precision is likely to be included in their article.)

7.2. Results on the p-part of BSD from Main Conjectures in Iwasawa Theory

We state a result that follows from Iwasawa Theory and shows that the p-part of BSD holds in the L-rank 0 case under fairly mild assumptions when p is inert in $\mathbf{Z}[f]$. Note that an explicit descent computation is hard when p is inert and $\rho_{f,p}$ is irreducible, so this is useful to deal with such primes when our other methods do not show that $\text{Ш}(A/\mathbf{Q})[p^\infty]$ is trivial.

Theorem 7.3 (p-part of BSD in the L-rank 0 case). *Let $A/\mathbf{Q}$ be a simple modular abelian variety associated to a newform f of level N. Let $p > 2$ be a prime inert in $\mathbf{Z}[f]$ with*

(ord) $v_p(N) \le 1$ *and* $|a_p(f)|_p = 1$.

Assume that

(irr) $\rho_{f,p}$ *is irreducible and*

(♠) *that there exists a prime $q \neq p$ with $v_q(N) = 1$ such that $\rho_{f,p}$ is ramified at q.*

If $L(A/\mathbf{Q},1) \neq 0$, then the p-part of BSD holds for $A/\mathbf{Q}$; that is,

$$\left|\frac{L(A/\mathbf{Q},1)}{\Omega_A}\right|_p = \left|\frac{\mathrm{Tam}(A/\mathbf{Q}) \cdot \#\text{Ш}(A/\mathbf{Q})[p^\infty]}{\#A(\mathbf{Q})_{\mathrm{tors}} \cdot \#A^\vee(\mathbf{Q})_{\mathrm{tors}}}\right|_p$$
$$= \left|\mathrm{Tam}(A/\mathbf{Q})\right|_p \cdot \left|\#\text{Ш}(A/\mathbf{Q})\right|_p.$$

Proof. This is [106, Theorem C] (the proof generalizes from elliptic curves to modular abelian varieties because [106, Theorem B] is for general newforms, and p is inert in $\mathbf{Z}[f]$). Note that $|\#A(\mathbf{Q})_{\mathrm{tors}} \cdot \#A^\vee(\mathbf{Q})_{\mathrm{tors}}|_p = 1$ since $\rho_{f,p}$ is irreducible. □

Remark 7.4.

(i) We have restricted ourselves to inert primes for simplicity. (The results hold more generally if there is exactly one prime above p.) The proofs for other primes $\mathfrak{p}$ would need to be adapted from the case of elliptic curves, and one would need to define the algebraic factors in the strong BSD formula as elements of $\mathbf{Z}[f]_{\mathfrak{p}}$ up to units. (It is likely that one can even define them up to squares of units over the Heegner field as most terms are in fact squares.)

(ii) In the L-rank 1 case, there is [118, Theorem 10.3] for elliptic curves, which builds upon [118, Theorem 9.3], which is for general newforms. These theorems have stronger assumptions than theorem 7.3.

(iii) [19] proves the p-part in the L-rank 1 case for odd good ordinary primes p completely split in the Heegner field K with ρ_p *reducible* if $\rho_p|_{G_K}^{\mathrm{ss}} \cong \varphi \oplus \psi$ such that $\varphi|_{G_{K_v}}, \psi|_{G_{K_v}} \neq \mathbf{1}, \chi_p$ for the places $v \mid p$ of K. For example, this excludes the case $A(K)[p] \neq 0$. The work of the first author and Mulun Yin [60] removes the restriction on φ and ψ. Depending on [20] and [17], it also treats the L-rank 0 case and the case of bad multiplicative reduction. The introduction of [60] contains an example of a

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

modular abelian surface over $\mathbf{Q}$ that illustrates the use of the results proved there to make a descent computation for a torsion prime unnecessary.

(iv) The preprint [21] proves the p-part of strong BSD in the L-rank 0 and 1 cases also for p good *non-ordinary*, but it assumes that the level N is squarefree.

(v) theorems 5.6 and 5.7 give $\text{Ш}(J/\mathbf{Q})[\mathfrak{p}] = 0$ under the assumptions there, but they do not prove the p-part of BSD. theorem 7.3 does this, but not for non-inert primes or supersingular or bad additive primes. Note that by the Sato–Tate conjecture, there are infinitely many p with $a_p = 0$, and they can be treated with [21] only when N is squarefree.

7.3. The p-adic BSD conjecture

We continue to assume that p is inert in $\mathbf{Z}[f]$. The coefficient of the leading term of $\mathscr{L}_p(A,T)$ at $T=0$ is denoted by $\mathscr{L}_p^*(A,0)$. Recall from the introduction to this section that $\alpha \in \mathbf{Z}[f]_{\mathfrak{p}}^{\times}$ is the p-adic unit root of the Euler factor of f at p. As in [5], the *p-adic multiplier* is

$$\varepsilon_p(A/\mathbf{Q}) := \mathbf{N}_{\mathbf{Z}[f]_{\mathfrak{p}}|\mathbf{Z}_p}(1-\alpha^{-1})^2.$$

(Note that if $a_p = 1$ and $p \mid N$, then $\alpha = 1$ and $\varepsilon_p(A/\mathbf{Q}) = 0$, so conjecturally there will be an *extra zero*.) The *p-adic regulator* $\mathrm{Reg}_p(A/\mathbf{Q})$ is the determinant of the p-adic height pairing on $A(\mathbf{Q})$ defined in [5, Definition 3.3]. According to a Conjecture of Schneider, $\mathrm{Reg}_p(A/\mathbf{Q})$ should be nonzero, but this is not known in general. Assume $p > 2$. Let $\gamma \in 1 + p\mathbf{Z}_p$ be a topological generator, the same as used in the construction of $\mathscr{L}_p(A,T)$. We take $\gamma = 1 + p$ in our computations. Let $\mathrm{Reg}_\gamma(A/\mathbf{Q}) := \mathrm{Reg}_p(A/\mathbf{Q})/\log_p(\gamma)^r$, where $r = \mathrm{rk}\, A(\mathbf{Q})$. We then have the following p-adic version of the BSD conjecture; see [5, Conjecture 1.4], generalizing [71].

Conjecture 7.5 (p-adic BSD conjecture). *Let $A/\mathbf{Q}$ be a principally polarized modular abelian variety and p a prime of good ordinary reduction for $A/\mathbf{Q}$. Then*

$$\mathrm{rk}\, A(\mathbf{Q}) = \mathrm{ord}_{T=0}\, \mathscr{L}_p(A,T)$$

and

$$\mathscr{L}_p^*(A,0) = \varepsilon_p(A/\mathbf{Q}) \cdot \frac{\#\text{Ш}(A/\mathbf{Q}) \cdot \mathrm{Tam}(A/\mathbf{Q}) \cdot \mathrm{Reg}_\gamma(A/\mathbf{Q})}{(\#A(\mathbf{Q})_{\mathrm{tors}})^2}.$$

We are interested in the size of the p-part of $\text{Ш}(A/\mathbf{Q})$, so it is sufficient to compare the p-adic valuations of both sides.

The following result due to Schneider shows that the conjecture holds in some cases at least up to a p-adic unit, but with $\mathscr{L}_p(A/\mathbf{Q},T)$ replaced by the *Iwasawa L-function* $\mathscr{L}_p^{(1)}(A/\mathbf{Q},T)$ defined in [95, §2]. Note that the latter is defined without using modularity, but in a more algebraic way.

Theorem 7.6. *Let $A/\mathbf{Q}$ be a simple principally polarized modular abelian variety with associated newform f. If*

(i) *p is a prime of good ordinary reduction,*

(ii) *such that the p-adic regulator $\mathrm{Reg}_\gamma(A/\mathbf{Q})$ is nonzero, and*

(iii) *$\text{Ш}(A/\mathbf{Q})[p^\infty]$ is finite,*

then the p-adic BSD conjecture holds (up to a p-adic unit) for $A/\mathbf{Q}$ and $\mathscr{L}_p^{(1)}(A/\mathbf{Q},T)$:

The Iwasawa L-function $\mathscr{L}_p^{(1)}(A/\mathbf{Q},T)$ vanishes to order $\mathrm{rk}\, A(\mathbf{Q})$ at $T=0$, and its leading term has p-valuation equal to that of

$$\varepsilon_p(A/\mathbf{Q}) \cdot \frac{\#\text{Ш}(A/\mathbf{Q})[p^\infty] \cdot \mathrm{Tam}(A/\mathbf{Q}) \cdot \mathrm{Reg}_\gamma(A/\mathbf{Q})}{(\#A(\mathbf{Q})_{\mathrm{tors}})^2}.$$

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

Proof. See [95, Theorem 2′]. □

We need to compare the two L-functions $\mathscr{L}_p(A/\mathbf{Q}, T)$ and $\mathscr{L}_p^{(1)}(A/\mathbf{Q}, T)$.

Theorem 7.7. *Let $p > 2$ be a prime of good ordinary reduction for $A/\mathbf{Q}$. Let $\mathfrak{p}$ be a prime ideal of $\mathbf{Z}[f]$ lying above p. Assume that the image of $\mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}(\mu_{p^\infty})) \to \mathrm{Aut}_{\mathbf{Z}[f]_\mathfrak{p}}(T_\mathfrak{p} A)$ contains $\mathrm{SL}_2(\mathbf{Z}_p)$ (see Section 2.13). Then*

$$\mathscr{L}_p^{(1)}(A/\mathbf{Q}, T) \mid \mathscr{L}_p(A/\mathbf{Q}, T) \in \mathbf{Z}[f]_p[\![T]\!].$$

Proof. See [58, Theorem 17.4 (3)]. □

Theorem 7.8. *Let $p > 2$ such that $a_p(f) \in \mathbf{Z}[f]_p^\times$. Then*

$$\mathrm{ord}_{T=0}\, \mathscr{L}_p(f, T) \geq \mathrm{cork}_{\mathbf{Z}[f]_p} \mathrm{Sel}_{p^\infty}(A_f/\mathbf{Q}) \geq \mathrm{rk}_{\mathbf{Z}[f]} A_f(\mathbf{Q}).$$

Here, the corank $\mathrm{cork}_{\mathbf{Z}[f]_p} M$ of a discrete torsion $\mathbf{Z}[f]_p$-module is the $\mathbf{Z}[f]_p$-rank of its $\mathbf{Z}[f]_p$-Pontrjagin dual.

Proof. See [58, Theorem 18.4]. □

Corollary 7.9. *Let $A/\mathbf{Q}$ be a simple principally polarized modular abelian variety with associated newform f. If*

(i) *$p > 2$ is a prime of good ordinary reduction*
(i) *such that the p-adic regulator $\mathrm{Reg}_\gamma(A/\mathbf{Q})$ is nonzero,*
(iii) *$\text{Ш}(A/\mathbf{Q})[p^\infty]$ is finite,*
(iv) *the image of $\mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q}(\mu_{p^\infty})) \to \mathrm{Aut}_{\mathbf{Z}[f]_p}(T_p A)$ contains $\mathrm{SL}_2(\mathbf{Z}_p)$, and*
(v) *$\mathrm{ord}_{T=0}\mathscr{L}_p(f^\sigma, T) \leq \mathrm{rk}_\mathcal{O} A(\mathbf{Q})$ for all σ,*

then equality holds in (7.9) and

$$v_p(\#\text{Ш}(A/\mathbf{Q})[p^\infty]) \leq v_p\left(\frac{\prod_\sigma \mathscr{L}_p^*(f^\sigma, 0) \cdot (\#A(\mathbf{Q})_{\mathrm{tors}})^2}{\varepsilon_p(A/\mathbf{Q}) \cdot \mathrm{Reg}_\gamma(A/\mathbf{Q}) \cdot \mathrm{Tam}(A/\mathbf{Q})}\right).$$

Proof. Combine theorems 7.6 to 7.8 . □

Note that [106, Theorems A and B] (with the case of good ordinary reduction coming from [107]) establishes equality up to units in $\mathbf{Z}[f]_p[\![T]\!]$ in the ordinary case under some conditions like ρ_p being surjective.

So if we can compute the p-adic valuations of $\mathscr{L}_p^*(A, 0)$ and of $\mathrm{Reg}_\gamma(A/\mathbf{Q})$, this result allows us to bound the order of the p-part of $\text{Ш}(A/\mathbf{Q})$ from above. Note that we know by the results of Kolyvagin–Logachëv and their extensions that $\text{Ш}(A/\mathbf{Q})[p^\infty]$ is finite in the cases of interest, so the main assumption is that p is a prime of good ordinary reduction. When the L-rank is zero, then the p-adic regulator is 1, so it remains to compute $\mathscr{L}_p(A, T)$. We explain in the next subsection how to do this. When the L-rank is 1, we also need to compute the p-adic height pairing. In the case that p is a prime of good ordinary reduction for the Jacobian of a genus 2 curve, this is accomplished in [5, §3.4]; see also [48].

7.4. Computing approximations to p-adic L-functions

We use Greenberg's improvement [49] of the Pollack–Stevens algorithm [84] to compute the p-adic L-function of a newform f with $a_p(f)$ a p-adic unit. Our Magma implementation is based on that of Darmon–Pollack [36] with their Magma code available at [35]. We modified the code so that it also works with newforms with arbitrary coefficient rings, accepts newforms as input and outputs the p-adic L-function as a p-adic power series to any specified precision for the uniformizer π of $\mathcal{O}_\mathfrak{p}$ and T. For performance reasons, we specialized to weight $k = 2$.

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

7.4.1. Computing the p-stabilization of φ_f if $p \nmid N$.
The construction of the p-adic L-function via the overconvergent modular symbol algorithm of [49, 84] needs $v_p(N) = 1$. In the case that $p \nmid N$ is a good ordinary prime, one has to *p-stabilize* f to a form of level Np with the same T_ℓ-eigenvalues as f and U_p-eigenvalue the unit root of $T^2 - a_p(f)T + p$. Note that the p-adic L-function is defined with respect to that (p-stabilized if $p \nmid N$) lift; see [6, §§4.1, 4.2, 4.4].

Recall that $a_p(f) \in \mathbf{Z}[f]_\mathfrak{p}^\times$. If $p \nmid N$, let $\alpha \in \mathbf{Z}[f]_\mathfrak{p}^\times$ be the unit root of $T^2 - a_p(f)T + p$. Let β be the other root. We then p-stabilize in the sense that we replace f by its *p-stabilization* $f_\alpha(z) = f(z) - \beta f(pz)$ of level Np with the same Hecke eigenvalues away from p. Otherwise (i.e., if $v_p(N) = 1$), we can directly use the algorithm of [49, 84] to compute a lift. (The reason for the p-stabilization is that the distribution property for the modular symbol follows if it is an eigenvector under the U_p-operator, but not under the T_p-operator.)

7.4.2. Modular symbols.
Let Δ_0 be the left $\mathbf{Z}[\mathrm{GL}_2(\mathbf{Q})]$-module $\mathrm{Div}^0(\mathbf{P}^1(\mathbf{Q}))$, where $\mathrm{GL}_2(\mathbf{Q})$ acts via fractional linear transformations on $\mathbf{P}^1(\mathbf{Q})$. We write an element $[s] - [r]$ of Δ_0 with $r, s \in \mathbf{P}^1(\mathbf{Q})$ as $\{r \to s\}$.

Consider the monoid

$$\Sigma_0(p) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Mat}_2(\mathbf{Z}) : (a, p) = 1,\ p \mid c,\ ad - bc \neq 0 \right\}.$$

Note that because $p \mid N$, $\Gamma_0(N) \subseteq \Sigma_0(p)$. Let V be a right $\Sigma_0(p)$-module with the action of $S \in \Sigma_0(p)$ on $v \in V$ denoted by $v|S$. Then the Hecke operators

$$T_\ell := \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix} + \sum_{a=0}^{\ell-1} \begin{pmatrix} 1 & a \\ 0 & \ell \end{pmatrix} \in \mathbf{Z}[\Sigma_0(p)], \quad \ell \neq p \text{ prime},$$

and

$$U_p := \sum_{a=0}^{p-1} \begin{pmatrix} 1 & a \\ 0 & p \end{pmatrix} \in \mathbf{Z}[\Sigma_0(p)]$$

act on V on the right, making it into a Hecke module. (The matrices constituting T_ℓ, U_ℓ are in $\Sigma_0(p)$, but not in $\Gamma_0(N)$.) In Magma, the elements of Δ_0 are called the *modular symbols* of $\Gamma_0(N)$, but we refer to the elements of the module

$$\mathrm{Symb}_{\Gamma_0(N)}(V) := \mathrm{Hom}_{\mathbf{Z}[\Gamma_0(N)]}(\Delta_0, V)$$

as the *V-valued modular symbols*. The abelian group $\mathrm{Hom}_\mathbf{Z}(\Delta_0, V)$ is a *right* $\mathbf{Z}[\Gamma_0(N)]$-module, and we write the action similarly as $\varphi|S$. Spelled out explicitly, the $\Gamma_0(N)$-equivariance means that for $\varphi \in \mathrm{Symb}_{\Gamma_0(N)}(V)$ one has $\varphi|S = \varphi$ (i.e., $\varphi(S\{r \to s\})|S = \varphi\{r \to s\}$ for $\{r \to s\} \in \Delta_0$ and $S \in \Gamma_0(N)$). Then $\mathrm{Symb}_{\Gamma_0(N)}(V)$ is a right Hecke module via the left action on Δ_0 and the right action on V.

7.4.3. Computing the canonical periods $(\Omega^\pm_{f^\sigma})_\sigma$ attached to f.
We have to find canonical periods of $\{f^\sigma\}$ as defined in [5, §2], unique up to $\mathbf{Z}[f]^\times$. We compute an approximation of the periods $(\Omega^\pm_{f^\sigma})_\sigma$ with $\sigma\colon \mathbf{Q}(f) \hookrightarrow \mathbf{R}$ as follows: We compute the period integrals

$$p^\pm_{f^\sigma}(r) := \pi i \Big(\int_r^{i\infty} f^\sigma(z)\, dz \pm \int_{-r}^{i\infty} f^\sigma(z)\, dz \Big)$$

(i.e., over the path $\{r \to \infty\} \in \mathrm{H}_1(X_0(N)(\mathbf{C}), \{\text{cusps}\}; \mathbf{Z})$) for a finite set of $r \in \mathbf{Q}$ such that the $\{r \to \infty\}$ generate Δ_0 as a $\Gamma_0(N)$-module to a high enough precision. By [5, §2.1, Theorem 2.2

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

and 2.4], there are *canonical periods* $(\Omega^{\pm}_{f^\sigma})_\sigma$ attached to f such that $p^{\pm}_{f^\sigma}/\Omega^{\pm}_{f^\sigma} \in \mathbf{Q}(f)$ and 'being compatible with twists', (for a precise formulation see [5, Theorem 2.2]).

By [5, text after Remark 2.6], there is a $b \in \mathbf{Q}(f)^\times$ such that $(\Omega^{\pm}_{f^\sigma})_\sigma = (\sigma(b)p^{\pm}_{f^\sigma}(r))_\sigma$. We approximate a representative vector of an equivalence class $(\Omega^{\pm}_{f^\sigma})_\sigma$. To compute the period integrals $p^{\pm}_{f^\sigma}(r)$, we combine (4.2) (and the equation before it) and lemma 4.9 and get

$$\Omega_{J/\mathbf{Q}} = \frac{c_f c_\pi}{\sqrt{\operatorname{disc}\mathbf{Z}[f]}} \cdot \frac{\#\operatorname{coker}\pi_{\mathbf{R}}}{\#\ker\pi_{\mathbf{R}}} \cdot \left|\prod_\sigma \Omega^{+}_{f^\sigma}\right|. \tag{7.1}$$

We compute $\Omega_{J/\mathbf{Q}}$ as in lemma 3.7, $c_f c_\pi$ as in lemma 3.6, and $\#\operatorname{coker}\pi_{\mathbf{R}}$, $\#\ker\pi_{\mathbf{R}}$ as described in Section 3.1. In fact, since the latter two constants are powers of 2, we do not need to compute them if $p \neq 2$. Since we work with a $\mathbf{Z}$-basis (g_i) of $S_2(f,\mathbf{Z})$, there is no factor $\sqrt{\operatorname{disc}\mathbf{Z}[f]}$ when we replace $\prod_\sigma \Omega^{+}_{f^\sigma}$ by the corresponding product for the (g_i).

Assuming that Equation (7.1) holds, the canonical periods are unique up to $\sigma(b)$ for some $b \in \mathbf{Z}[f]^\times_{\mathfrak{p}}$. So the $\mathfrak{p}$-adic valuation of the leading term of the p-adic L-function is uniquely determined.

7.4.4. The modular symbol φ_f.

The *modular symbol associated with* f is $\varphi_f \in \operatorname{Hom}_{\mathbf{Z}[\Gamma_0(N)]}(\Delta_0, \mathbf{Q}(f))$, where $\mathbf{Q}(f)$ is a trivial $\Gamma_0(N)$-module. It is defined as $\varphi_f\{r \to \infty\} = p^+_f(r)/\Omega^+_f + p^-_f(r)/\Omega^-_f \in \mathbf{Q}(f)$ and by extension $\varphi_f\{r \to s\} = \varphi_f\{r \to \infty\} - \varphi_f\{s \to \infty\}$ to all paths between cusps $r, s \in \mathbf{P}^1(\mathbf{Q})$. It is enough to know φ_f on a finite set of generators of Δ_0 as a $\mathbf{Z}[\Gamma_0(N)]$-module, which can be obtained via *Manin symbols* [31, §§2.2, 2.3].

7.4.5. Overconvergent modular symbols and p-adic L-functions.

Let $\mathfrak{p} \mid p$ be a prime ideal of $\mathbf{Z}[f]$ inducing an embedding of $\mathbf{Q}(f)$ into the completion $\mathbf{Q}(f)_{\mathfrak{p}}$. To approximate the distribution $L_{\mathfrak{p}}(f)$ (see [84, §6.2]) and its associated power series $\mathscr{L}_{\mathfrak{p}}(f,T)$, we implemented Greenberg's improvement [49] of Pollack–Stevens's computation of an overconvergent modular eigenlift of the modular symbol $\varphi_f \in \operatorname{Symb}_{\Gamma_0(N)}(\mathbf{Q}(f))$ (see [84, §6.3]).

For the following, see [84, §3.1] and [49, §1]. For $r \in |\mathbf{C}_p^\times|_p$, define $\mathscr{A}[r](\mathbf{Q}(f)_{\mathfrak{p}})$ to be the $\mathbf{Q}(f)_{\mathfrak{p}}$-Banach space of $\mathbf{Q}(f)_{\mathfrak{p}}$-affinoid functions on

$$B[\mathbf{Z}_p, r] := \{z \in \mathbf{C}_p : \exists a \in \mathbf{Z}_p \text{ with } |a-z|_p \leq r\}$$

endowed with the supremum norm. Let

$$\mathscr{A}^\dagger(\mathbf{Z}_p) := \varinjlim_{s>1} \mathscr{A}[s](\mathbf{Q}(f)_{\mathfrak{p}}),$$

endowed with the colimit topology, denote the algebra of $\mathbf{Q}(f)_{\mathfrak{p}}$-overconvergent functions on $B[\mathbf{Z}_p, 1]$. The overconvergent distributions $\mathscr{D}^\dagger(\mathbf{Q}(f)_{\mathfrak{p}})$ are defined as its continuous $\mathbf{Q}(f)_{\mathfrak{p}}$-linear dual endowed with the strong topology.

7.4.6. The strategy to compute the distribution $L_{\mathfrak{p}}(f)$.

We abbreviate $\Gamma_0(N)$ by Γ in the following. The method of constructing the $\mathfrak{p}$-adic L-function $L_{\mathfrak{p}}(f)$ of f as a distribution is summarized in the following diagram. Here, $\operatorname{Symb}_\Gamma(\mathbf{Q}(f))[f]$ denotes the subspace of $\operatorname{Symb}_\Gamma(\mathbf{Q}(f))$ on which the Hecke operators T_n with $p \nmid n$ act as multiplication by $a_n(f)$, and the superscript '$U_p = \alpha$' means the subspace where the Hecke operator U_p acts as multiplication

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

by the unit root eigenvalue α of the characteristic polynomial at p.

$$\begin{tikzcd}
\mathrm{Symb}_\Gamma(\mathscr{D}^\dagger(\mathbf{Q}(f)_\mathfrak{p}))[f]^{U_p=\alpha} \arrow[r, "\Phi_f \mapsto \Phi_f\{0\to\infty\}=L_\mathfrak{p}(f)"] \arrow[d, dashed, "\simeq"', "\rho^*"] & \mathscr{D}^\dagger(\mathbf{Q}(f)_\mathfrak{p}) \arrow[d, "L_\mathfrak{p}(f)\mapsto\int_{\mathbf{Z}_p^\times}\mathbf{1}L_\mathfrak{p}(f)"] \\
\mathrm{Symb}_\Gamma(\mathbf{Q}(f))[f]^{U_p=\alpha} \arrow[r, "\varphi_f \mapsto \varphi_f\{0\to\infty\}"] & \mathbf{Q}(f)_\mathfrak{p}
\end{tikzcd}$$

To compute the distribution $L_\mathfrak{p}(f)$, we start with φ_f in the lower left corner and lift it via the algorithm described below to a distribution valued modular symbol Φ_f; this is the left vertical isomorphism. Then $L_\mathfrak{p}(f)$ is the evaluation $\Phi_f\{0 \to \infty\}$ (i.e., the image under the top horizontal morphism).

7.4.7. Computing the modular symbol $\varphi_f^\pm$ attached to *f*.

Knowing the canonical periods, we can compute $\varphi_f^\pm\{r \to s\}$ with $r, s \in \mathbf{P}^1(\mathbf{Q})$ as described in [117] by computing the corresponding period integrals for all f^σ and dividing by $\Omega_{f^\sigma}^\pm$ and recognizing the elements in $\mathbf{Q}(f)$ using that

$$\prod_\sigma (X - \varphi_{f^\sigma}^\pm\{r \to s\}) \in \mathbf{Q}[X]$$

has rational coefficients with the denominator of the coefficient of $X^{[\mathbf{Q}(f):\mathbf{Q}]-n}$ bounded by $(4^g \cdot c_f c_\pi \cdot \#J(\mathbf{Q})_{\mathrm{tors}})^n$; see Section 4.2 and [117, Prop. 1].

One can compute the modular symbol associated to f up to a factor in $\mathbf{Q}(f)$ with Magma. (Note that one has to take a suitable $\mathbf{Q}(f)$-linear combination because Magma takes a basis of $S_2(f, \mathbf{Z})$.) Hence, alternatively, one can compute this factor by comparing with our above computation for some $\varphi_f\{r \to s\} \neq 0$ and scale.

7.4.8. Determining the required *p*-adic precision for the desired *T*-adic precision of $\mathscr{L}_p(f, T)$.

Note that a distribution $\mu \in \mathscr{D}^\dagger(\mathbf{Q}(f)_\mathfrak{p})$ is uniquely determined by its moments $\mu(x^j)$, $j \geq 0$. We represent a distribution in an approximation module $\mathbf{A}^M\mathscr{D}^\dagger(\mathbf{Z}[f]_\mathfrak{p})$ by storing its j-th moment up to precision $M + 1 - j$ (i.e., as an element of $\mathbf{Z}[f]_\mathfrak{p}/\mathfrak{p}^{M+1-j}$). To be able to compute lifts, we store the 0-th moment up to the final precision.

To ensure the moments we consider are integral, we do the following: According to [84, Corollary 7.6, §8.3 3], to obtain a precision of np-adic digits, one needs to compute with a precision M satisfying

$$M - \lceil \log(M + 2)/\log p \rceil - 1 \geq n.$$

We take m minimal with $p^m > M+1$ and scale φ_f by p^{m+1}. Then we perform M steps of the algorithm to obtain the approximation to $p^{m+1}\Phi_f$ in $\mathbf{A}^M\mathscr{D}(\mathbf{Z}[f]_\mathfrak{p})$. Finally, we divide by p^{m+1}.

7.4.9. Computing the lift Φ of φ.

This is the key step in the computation of the p-adic L-function and a simplification of [84] due to Greenberg [49], with the additional non-critical slope assumption, which is satisfied if there is a unit root of the characteristic polynomial of p-Frobenius.

Let $\varphi \in \mathrm{Symb}_\Gamma(\mathbf{Q}(f))[f]^{U_p=\alpha}$ be a Hecke eigensymbol. The action of $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $p \mid c$ and $p \nmid a$ on a distribution μ is given by $(\mu|\gamma)(f) = \mu(\gamma \cdot f)$, where γ acts on the function f as $(\gamma \cdot f)(z) = (a + cz)^2 \cdot f(\frac{b+dz}{a+cz})$.

We start with $(\Phi)_0 := \varphi$. To lift $(\Phi)_M$ from $\mathrm{Symb}_{\Gamma_0(N)}(\mathbf{A}^M\mathscr{D}^\dagger(\mathbf{Z}[f]_\mathfrak{p}))$ to precision $M + 1$, we first lift all values on the finitely many generators of Δ_0 (computed using Manin symbols) arbitrarily to precision $M + 1$. The resulting function will usually not be additive, $\Gamma_0(N)$-equivariant or an U_p-eigensymbol anymore, but it will be after we apply the operator U_p.

We stop after we have reached the precision from 7.4.8.

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

7.4.10. Computing an approximation to the p-adic L-function from the distribution $L_{\mathfrak{p}}(f)$.

To go from an approximation of $L_{\mathfrak{p}}(f)$ to the power series $\mathscr{L}_{\mathfrak{p}}(f,T)$, we use the formulas in [84, §9]. The computation depends on the choice of a topological generator $\gamma \in 1 + p\mathbf{Z}_p$. We take $\gamma = 1 + p$ in our computations.

7.5. Examples

The example below represents the only case where our other methods are not sufficient to compute $\#Ш(A/\mathbf{Q})[p^\infty]$, so that we need to use p-adic L-functions. (Note that a $\mathfrak{p}$-descent would amount to a full 3-descent in this case, which is not really feasible with current methods.)

Example 7.10. For the Jacobian J of the curve X of level $188 = 2^2 \cdot 47$ in our data set, the Tamagawa product is 9 (we have $c_2 = 9$ and $c_{47} = 1$); the prime 3 is inert in the endomorphism ring $\mathbf{Z}[(1+\sqrt{5})/2]$. To show that $Ш(J/\mathbf{Q})[3^\infty] = 0$ in this case, we therefore compute the 3-adic L-function. Since $3 \nmid N$, we have to 3-stabilize; see 7.4.1. Note that $a_3(f) = -\frac{3+\sqrt{5}}{2}$ is a 3-adic unit; hence, the reduction at 3 is good ordinary. Then $\varepsilon_3(J/\mathbf{Q})$ is a unit as well (since $\alpha \equiv a_3(f) \not\equiv 1 \bmod 3$).

We verify using propositions 2.58 and 2.59 that $\mathrm{SL}_2(\mathbf{Z}_3)$ is contained in the image of $\rho_{f,3^\infty}$.

The L-rank is 1 and $J(\mathbf{Q}) \cong \mathbf{Z}^2$. A computation of 3-adic heights shows that $v_3(\mathrm{Reg}_3(J/\mathbf{Q})) = 0$. Therefore, one has

$$v_3(\mathrm{Reg}_\gamma(J/\mathbf{Q})) = 0 - r \cdot v_3(\log_3(1+3)) = -2.$$

We thank Steffen Müller for computing the 3-adic regulator for us using the code described in [48]. Using the algorithm sketched above, we find that

$$\begin{aligned}\mathscr{L}_3(J,T) &= \mathscr{L}_3(f,T) \cdot \mathscr{L}_3(f^\tau,T)\\ &= (O(3^3) + uT + O(T^2)) \cdot (O(3^3) + u'T + O(T^2))\end{aligned}$$

with 3-adic units u, u', where τ is the nontrivial automorphism of $\mathbf{Z}[f]$. (The computation took 30 minutes and 214 MiB RAM on a AMD Ryzen 7 PRO 6850U.) Since $\mathrm{rk}\, J(\mathbf{Q}) = 2$ and $Ш(J/\mathbf{Q})[3^\infty]$ is finite, $\mathrm{cork}_{\mathbf{Z}[f]_3} \mathrm{Sel}_{3^\infty}(J/\mathbf{Q}) = 1$, so corollary 7.9 shows that the vanishing order of $\mathscr{L}_3(J,T)$ at $T = 0$ must be exactly 2 and that

$$v_3\big(\#Ш(J/\mathbf{Q})[3^\infty]\big) \leq v_3\left(\frac{\prod_\sigma 1 \cdot 1 \cdot 1}{1 \cdot 3^{-2} \cdot 9}\right) = 0\,;$$

hence, $Ш(J/\mathbf{Q})[3^\infty] = 0$.

8. Examples

8.1. Jacobians of genus 2 Atkin–Lehner quotients

Tables displaying the results for the Hasegawa curves can be found in [59].

8.2. All genus 2 curves with absolutely simple modular Jacobian from the LMFDB

We compute the analytic order of Ш using the results from Sections 3 and 4. It turns out that all of them are 1, 2 or 4. We also discover some twists J^K which have analytic order of Ш divisible by 3^2, 5^2 or 7^2.

It turns out that combining the information about the images of the residual Galois representations from Section 2 with the Heegner indices from Section 3 (for a few examples, we have to use two Heegner fields) and the Euler system from Section 5 prove that $Ш(J/\mathbf{Q})[\mathfrak{p}] = 0$ except in the following cases:

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

- ○ $p(\mathfrak{p}) = 2$: these are dealt with in Section 6.1.
- ○ Odd primes $\mathfrak{p}$ with $\rho_{\mathfrak{p}}$ reducible: these are dealt with in Section 6.2.
- ○ One example with $N = 188$ for which $3 \mid \mathrm{Tam}(J/\mathbf{Q})$ and ρ_3 is irreducible: see example 7.10.

This completes the verification of strong BSD for all the 97 absolutely simple modular Jacobians in the LMFDB.

The Heegner discriminants used in the computation were typically ≤ 51 in absolute value. The largest Heegner discriminant used was -131 for the example of level 165. We needed two Heegner discriminants in the examples of level 523 and 621. The Heegner point used in one of the examples of level 275 has unusually large height (≈ 83.863). Computing the Heegner point and the Mordell–Weil group of the Jacobian over the Heegner field are the most time-consuming computations in our verification.

8.3. Jacobians of the four remaining Wang curves

The Jacobians J of the four Wang curves of levels 65A, 117B, 125B and 175 (in the notation of [45]) also have analytic order of Sha in $\{1, 2, 4\}$. The remaining descent computations that are necessary to finish the proof that $\#\text{Ш}(J/\mathbf{Q}) = \#\text{Ш}(J/\mathbf{Q})_{\mathrm{an}}$ in these cases are sketched in Examples 6.10.

A. An example with 7-torsion in Ш

In this appendix, which heavily relies on contributions by Sam Frengley, we verify strong BSD for a genus 2 Jacobian J such that $\#\text{Ш}(J/\mathbf{Q}) = 7^2$. This contrasts with the examples in our database, where we always have $\#\text{Ш}(J/\mathbf{Q}) \mid 4$.

A.1. Visibility

We first briefly recall some generalities about visibility of elements of Tate–Shafarevich groups of abelian varieties, following, for example, [2, 3, 30, 43].

Let A_1/K and A_2/K be abelian varieties defined over a number field K. Suppose that there exist finite $\mathrm{Gal}(\overline{K}|K)$-submodules $\Delta_1 \subset A_1(\overline{K})$ and $\Delta_2 \subset A_1(\overline{K})$ equipped with an isomorphism $\varphi\colon \Delta_1 \xrightarrow{\sim} \Delta_2$ of $\mathrm{Gal}(\overline{K}|K)$-modules. Write $A_1' = A_1/\Delta_1$ and $A_2' = A_2/\Delta_2$ and let $\psi_1\colon A_1 \to A_1'$ and $\psi_2\colon A_2 \to A_2'$ be the quotient morphisms. The isomorphism φ induces an isomorphism on Galois cohomology $\mathrm{H}^1(K, \Delta_1) \xrightarrow{\sim} \mathrm{H}^1(K, \Delta_2)$. We might hope that if enough 'local coincidences' occur at the bad primes, then the ψ_1 and ψ_2-Selmer groups $\mathrm{Sel}(\psi_1)$ and $\mathrm{Sel}(\psi_2)$ may be isomorphic. In this case, if the order of the group $A_1(K)/\psi_1 A_1'(K)$ is smaller than the order of $A_2(K)/\psi_2 A_2'(K)$, the latter will contribute to a discrepancy between the order of $A_1(K)/\psi_1 A_1'(K)$ and $\mathrm{Sel}(\psi_1)$, thereby 'explaining' some nontrivial elements of $\text{Ш}(A_1/K)[\psi_1]$.

To make this idea precise, let $\Delta \subset (A_1 \times A_2)(\overline{K})$ be the graph of the isomorphism φ and consider the abelian variety $B = (A_1 \times A_2)/\Delta$. We have a pair of morphisms

$$\iota\colon A_1 \longrightarrow A_1 \times A_2 \longrightarrow B.$$

Definition A.1. We say that an element or subgroup of $\mathrm{H}^1(K, A_1)$ is *visible in B* if it is contained in the kernel of the homomorphism $\iota_*\colon \mathrm{H}^1(K, A_1) \to \mathrm{H}^1(K, B)$. We write $\mathrm{Vis}_B\, \mathrm{H}^1(K, A_1)$ (respectively $\mathrm{Vis}_B\, \text{Ш}(A_1/K)$) for the subgroup of $\mathrm{H}^1(K, A_1)$ (respectively $\text{Ш}(A_1/K)$) consisting of elements visible in B.

We will use the following theorem (which is proved in [43, Theorem 2.2] (see also [2] and [3, Appendix])), which we state in the case when $K = \mathbf{Q}$.

Theorem A.2. *If* $A_1(\mathbf{Q})/\varphi_1 A_1'(\mathbf{Q}) = 0$, *then the subgroup* $\mathrm{Vis}_B\, \mathrm{H}^1(\mathbf{Q}, A)$ *is isomorphic to* $A_2(\mathbf{Q})/\varphi_2 A_2'(\mathbf{Q})$. *Moreover if* $\#\Delta$ *is odd, and*

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

(i) *all Tamagawa numbers of $A_1/\mathbf{Q}$ and $A_2/\mathbf{Q}$ are coprime to $\#\Delta$, and*
(ii) *the abelian variety B has good reduction at all primes dividing $\#\Delta$,*

then $\mathrm{Vis}_B\,\text{Ш}(A_1/\mathbf{Q}) \cong A_2(\mathbf{Q})/\varphi_2 A_2'(\mathbf{Q})$.

A.2. The example

Let $C/\mathbf{Q}$ be the genus 2 curve given by the Weierstrass equation

$$C\colon\, y^2 = -10(x^6 - 10x^5 + 32x^4 - 40x^3 + 38x^2 - 20x + 4).$$

Its Jacobian J is of GL_2-type; the level is $N = 3200$. This genus 2 curve is obtained, up to quadratic twist, by specializing the family of genus 2 curves with $\sqrt{2}$-multiplication given by Bending [7, Theorem 4.1] at $(A, P, Q) = (-10, 1, -5)$. This example was found by computing (for many such specializations) twists $X^{\pm}_{J[\mathfrak{p}]}(7)$ of the modular curve $X(7)$ whose K-points parameterize elliptic curves E equipped with an isomorphism of $\mathrm{Gal}(\overline{K}|K)$-modules $J[\mathfrak{p}] \cong E[7]$ (see, for example, [85, Section 4.4] for the construction of these twists). The details of these calculations and further examples appear in the PhD thesis of Sam Frengley [46] and in [47].

We begin by showing that the support of $\text{Ш}(J/\mathbf{Q})$ is contained in $\{7\}$.

Proposition A.3. *The Jacobian J has $\mathcal{O} := \mathrm{End}_{\mathbf{Q}}(J) \cong \mathbf{Z}[\sqrt{2}]$ and $r_{\mathrm{an}} = 0 = r$, $J(\mathbf{Q}) = 0$, $\mathrm{Sel}_2(J/\mathbf{Q}) = 0$, $c_2 = c_5 = 1$, and $I_{\mathbf{Q}(\sqrt{-31}),\pi} = 7$.*

In particular, $\#\text{Ш}(J/\mathbf{Q})_{\mathrm{an}} = 7^2$, and $\#\text{Ш}(J/\mathbf{Q})$ is a power of 7.

Proof. The endomorphism ring contains $\mathbf{Z}[\sqrt{2}]$ by construction of the curve. Since $\mathbf{Z}[\sqrt{2}]$ is the maximal order of $\mathbf{Q}(\sqrt{2})$, it follows that $\mathcal{O} \cong \mathbf{Z}[\sqrt{2}]$. A computation of the 2-Selmer group shows that $\mathrm{rk}\, J(\mathbf{Q}) = 0$ and $\text{Ш}(J/\mathbf{Q})[2^\infty] = 0$. We check that $L(J/\mathbf{Q}, 1) \neq 0$ by computing $L(J/\mathbf{Q}, 1)/\Omega_J$ as described in Section 4.2. The torsion subgroup of $J(\mathbf{Q})$ turns out to be trivial. The Tamagawa number at 5 can be determined using van Bommel's Magma code [11, §4.4]. However, Magma is unable to compute a regular model at 2. So we computed a regular model by hand (see `Sha7-curve.m` for the computation of c_2) and found that the reduction type is $[\mathrm{III}_2^*]$ in [79]. Note that this is also needed to determine the power of 2 in the 'compensation factor' C in lemma 3.7, which we need for the computation of $\#\text{Ш}(J/\mathbf{Q})_{\mathrm{an}} = 7^2$. Using the approach in Section 3, we find that $I_{K,\pi} = 7$ for $K = \mathbf{Q}(\sqrt{-31})$. As all residual Galois representations are irreducible, the claim now follows from theorem 5.6. □

Lemma A.4. *We have that $\#\text{Ш}(J/\mathbf{Q})[7^\infty] \mid 7^2$.*

Proof. Note that 7 is split in the endomorphism ring $\mathcal{O} \cong \mathbf{Z}[\sqrt{2}]$, so the Heegner index as an ideal of $\mathcal{O}$ equals $\mathfrak{p}$ with $\mathfrak{p}$ one of the two prime ideals above 7. Using proposition 2.58, we find that the $\mathfrak{p}$-adic Galois representations for these two primes have image $\mathrm{GL}_2(\mathbf{Z}_7)$. Furthermore, $7 \nmid h_{\mathbf{Q}(\sqrt{-31})} N$. Hence, theorem 5.10 shows $\text{Ш}(J/K) \hookrightarrow (\mathbf{Z}/7)^2$. Since $[K : \mathbf{Q}] = 2$ is coprime to 7, we get $\text{Ш}(J/\mathbf{Q}) \hookrightarrow (\mathbf{Z}/7)^2$. □

Applying theorem A.2, we can show the following.

Proposition A.5 (Sam Frengley). *Let E be the elliptic curve with LMFDB label* `3200.a1` *and Weierstrass equation*

$$E\colon\, y^2 = x^3 - 100x + 400.$$

There exists a prime $\mathfrak{p} \mid 7$ in $\mathcal{O}$ such that $J[\mathfrak{p}] \cong E[7]$ as $\mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q})$-modules. Moreover, if $\Delta \subset J \times E$ is the graph of this isomorphism, then $\text{Ш}(J/\mathbf{Q})$ contains a subgroup isomorphic to $(\mathbf{Z}/7)^2$ which is visible in the abelian threefold $(J \times E)/\Delta$.

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

Proof. We first show that $J[\mathfrak{p}]$ is isomorphic to $E[7]$ as a $\mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q})$-module, following [43, Theorem 6.3]. Let $\mathcal{K} := J/\{\pm 1\}$ be the Kummer surface of J given by the model in [18, Chapter 3] and let $x_J\colon J \to \mathcal{K}$ be the quotient morphism. Similarly, let $x_E\colon E \to E/\{\pm 1\} \cong \mathbf{P}^1$ be the x-coordinate morphism. Since the mod-7 Galois representation attached to $E/\mathbf{Q}$ is surjective, by [43, Proposition 6.1] to show that there exists a quadratic twist $E^d/\mathbf{Q}$ of $E/\mathbf{Q}$ such that $J[\mathfrak{p}]$ is isomorphic to $E^d[7]$ as a $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-module, it suffices to show that there exist points $P \in J[\mathfrak{p}]$ and $Q \in E[7]$ such that $\mathbf{Q}(x_J(P))$ and $\mathbf{Q}(x_E(Q))$ are isomorphic. Using the approach detailed in [43, Theorem 6.3], we give an explicit degree 24 number field $L/\mathbf{Q}$ and equations for points $x_J(P) \in \mathcal{K}(L)$ and $x_E(Q) \in \mathbf{P}^1(L)$ which generate $L/\mathbf{Q}$. For the computations, see the file `congruence.m`.

Finally, if $d \in \mathbf{Z}$ is chosen to be squarefree, then d is divisible only by bad primes of E and C. As discussed in [43, (5.2)], by [45, Section 2.1] or [72, Lemma 3], an isomorphism of Galois modules $J[\mathfrak{p}] \cong E^d[7]$ induces a congruence

$$a_p(E^d)^2 - t_p a_p(E^d) + n_p \equiv 0 \bmod 7. \tag{A.1}$$

Here, $t_p = p + 1 - N_1$ and $n_p = (N_1^2 + N_2)/2 - (p+1)N_1 - p$, where $N_1 = \#C(\mathbf{F}_p)$ and $N_2 = \#C(\mathbf{F}_{p^2})$. Note that E and C have bad reduction at 2 and 5 and good reduction at all other primes, and for each integer $d \neq 1$ dividing 10, the congruence in (A.1) fails to hold at one of $p = 11$, 17, or 23. It follows that $J[\mathfrak{p}]$ and $E[7]$ are isomorphic as $\mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q})$-modules.

To show that $\text{Ш}(J/\mathbf{Q})$ contains a subgroup isomorphic to $(\mathbf{Z}/7)^2$, first note that the Tamagawa numbers of $E/\mathbf{Q}$ are coprime to 7 and by proposition A.3 so are the Tamagawa numbers of $J/\mathbf{Q}$. The torsion subgroups of $E/\mathbf{Q}$ and $J/\mathbf{Q}$ are trivial, the rank of $E/\mathbf{Q}$ is 2, and the rank of $J/\mathbf{Q}$ is 0, again by proposition A.3. It follows from Theorem A.2 that $\text{Ш}(J/\mathbf{Q})[7]$ contains a subgroup isomorphic to $(\mathbf{Z}/7)^2$, which is visible in $(J \times E)/\Delta$. □

Combining these results, we obtain the following.

Theorem A.6. *For J as above, we have* $\#\text{Ш}(J/\mathbf{Q})_{\mathrm{an}} = 7^2 = \#\text{Ш}(J/\mathbf{Q})$.

The computations with precision 462 took 57 hours and 3.3 GiB RAM on an MIT server running Magma V2.28-3 provided to us by Andrew Sutherland. The log of `N3200.m` can be found in `3200.log`. The bottleneck was the computation of the Heegner point, which required 783700 Fourier coefficients of the newform. (The remaining computations take less than 2 minutes.) Note that one must use $c_2 = 1$ from proposition A.3 to obtain the correct value $\#\text{Ш}(J/\mathbf{Q})_{\mathrm{an}} = 7^2$; Magma cannot compute a regular semistable model of the curve at $p = 2$.

A.3. Further examples

One expects the existence of elements of order p in Ш in quadratic twists of $A/\langle P\rangle$, where $0 \neq P \in A[p](K)$ by [105].

Our computations of the analytic orders of Sha for the Jacobians J of the LMFDB examples with L-rank 1 yield the following examples of twists of J by the first Heegner field such that there is nontrivial p-torsion in Sha for some $p \in \{3, 5, 7\}$. The number in parentheses indicates the index of the curve in the list of LMFDB examples.

(30) The twist of the second curve with $N = 133$ by $D_K = -31$ has $I_K = 3^2$ and $\#\text{Ш}(J^K/\mathbf{Q})_{\mathrm{an}} = 2^2 \cdot 3^2$.
(55) The twist of the first curve with $N = 275$ by $D_K = -19$ has $I_K = 3$ and $\#\text{Ш}(J^K/\mathbf{Q})_{\mathrm{an}} = 2^2 \cdot 3^2$.
(57) The twist of the curve with $N = 289$ by $D_K = -15$ has $I_K = 3$ and $\#\text{Ш}(J^K/\mathbf{Q})_{\mathrm{an}} = 2^2 \cdot 3^2$.
(74) The twist of the curve with $N = 523$ by $D_K = -35$ has $I_K = 3^2$ and $\#\text{Ш}(J^K/\mathbf{Q})_{\mathrm{an}} = 2^2 \cdot 3^4$.
(77) The twist of the first curve with $N = 621$ by $D_K = -11$ has $I_K = 7$ and $\#\text{Ш}(J^K/\mathbf{Q})_{\mathrm{an}} = 7^2$.
(82) The twist of the curve with $N = 647$ by $D_K = -11$ has $I_K = 5$ and $\#\text{Ш}(J^K/\mathbf{Q})_{\mathrm{an}} = 2^2 \cdot 5^2$.

To obtain these values, we computed $\#\text{Ш}(J/K)_{\mathrm{an}}$ for a Heegner field $K = \mathbf{Q}(\sqrt{D})$ and use that $\#\text{Ш}(J/\mathbf{Q})_{\mathrm{an}}$ is a power of 2 for the LMFDB examples; hence, $\#\text{Ш}(J^K/\mathbf{Q})_{\mathrm{an}}$ and $\#\text{Ш}(J/K)_{\mathrm{an}}$ differ by

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

a power of 2. By corollary 2.36, the set of $\mathfrak{p} \nmid 2$ with $\rho_{J/\mathbf{Q},\mathfrak{p}}$ irreducible remains the same when ρ is restricted to G_K. By lemma 4.21 and (4.6), the odd prime factors of $\mathrm{Tam}(J^K/\mathbf{Q})$ are those of $\mathrm{Tam}(J/\mathbf{Q})$.

To also show that $\#\text{Ш}(J^K/\mathbf{Q})$ agrees with the analytic order of Sha, one has to compute $\text{Ш}(J^K/\mathbf{Q})[2^\infty]$, which our computation predicts to be $(\mathbf{Z}/2)^2$ in all of the above cases except the curve with $N = 621$. We verified this using the code from [44]. Thus, using theorems 5.7 and 5.10, the remaining tasks for verifying strong BSD are as follows.

(30) Show that $\dim_{\mathbf{F}_\mathfrak{p}} \text{Ш}(J^K/\mathbf{Q})[\mathfrak{p}] = 0$ and $= 2$ for the two prime ideals $\mathfrak{p} \mid 3$, respectively.

(55) Show that $\dim_{\mathbf{F}_\mathfrak{p}} \text{Ш}(J^K/\mathbf{Q})[\mathfrak{p}] = 2$ for one of the two prime ideals $\mathfrak{p} \mid 3$. Since the Heegner index as an $\mathcal{O}$-ideal has norm 3, this shows $\text{Ш}(J^K/\mathbf{Q})[\mathfrak{p}] = 0$ for the other $\mathfrak{p} \mid 3$.

(57) Show that $\dim_{\mathbf{F}_\mathfrak{p}} \text{Ш}(J^K/\mathbf{Q})[\mathfrak{p}] = 2$ for one of the two prime ideals $\mathfrak{p} \mid 3$. Since the Heegner index as an $\mathcal{O}$-ideal has norm 3, this shows $\text{Ш}(J^K/\mathbf{Q})[\mathfrak{p}] = 0$ for the other $\mathfrak{p} \mid 3$. For one of them, one can perform an isogeny descent.

(74) Show that $\text{Ш}(J^K/\mathbf{Q})$ has a subgroup isomorphic to $(\mathbf{Z}/3)^4$; note that the prime 3 is inert in $\mathbf{Z}[f]$.

(77) Show that $\dim_{\mathbf{F}_\mathfrak{p}} \text{Ш}(J^K/\mathbf{Q})[\mathfrak{p}] = 2$ for one of the two prime ideals $\mathfrak{p} \mid 7$. Since the Heegner index as an $\mathcal{O}$-ideal has norm 7, this shows $\text{Ш}(J^K/\mathbf{Q})[\mathfrak{p}] = 0$ for the other $\mathfrak{p} \mid 7$.

(82) Show that $\dim_{\mathbf{F}_\mathfrak{p}} \text{Ш}(J^K/\mathbf{Q})[\mathfrak{p}] = 2$ for one of the two prime ideals $\mathfrak{p} \mid 5$.

Acknowledgements. We thank Francesc Castella, Kęstutis Česnavicius, Maarten Derickx, Michael Dettweiler, Tom Fisher, Sam Frengley, Pip Goodman, Walter Gubler, Peter Humphries, David Loeffler, Steffen Müller, Yusuf Mustopa, Jakob Stix, Chris Williams and Chris Wuthrich for hints and helpful discussions. We thank the referee for their careful reading and suggestions to improve the article.

Competing interest. The authors have no competing interest to declare.

Financial Support. The authors were supported by the Deutsche Forschungsgemeinschaft (DFG), STO 299/18-1 (AOBJ: 667349) (MS and TK) and STO 299/18-2 (AOBJ: 686837) (MS) while working on this article. TK was partially supported by the 2021 MSCA Postdoctoral Fellowship 01064790 – ExplicitRatPoints. MS was supported by the National Science Foundation under Grant No. DMS-1928930 while he was in residence at the Simons Laufer Mathematical Sciences Institute in Berkeley, California, during the spring 2023 semester. This stay was also supported through DFG grants STO 299/13-1 (AOBJ: 635353) and STO 299/17-1 (AOBJ: 662415).

References

[1] A. Agashe, K. Ribet and W. A. Stein, ‘The Manin constant’, *Pure Appl. Math. Q.* **2**(2) (2006), 617–636.

[2] A. Agashe and W. Stein, ‘Visibility of Shafarevich-Tate groups of abelian varieties’, *J. Number Theory* **97**(1) (2002), 171–185.

[3] A. Agashe and W. Stein, ‘Visible evidence for the Birch and Swinnerton-Dyer conjecture for modular abelian varieties of analytic rank zero’, *Math. Comp.* **74**(249) (2005), 455–484, With an appendix by J. Cremona and B. Mazur.

[4] E. Arbarello, M. Cornalba, P. A. Griffiths and J. Harris, *Geometry of Algebraic Curves. Vol. I*(Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]) vol. 267 (Springer-Verlag, New York, 1985).

[5] J. S. Balakrishnan, J. S. Müller and W. A. Stein, ‘A p-adic analogue of the conjecture of Birch and Swinnerton-Dyer for modular abelian varieties’, *Math. Comp.* **85**(298) (2016), 983–1016.

[6] K. Belabas and B. Perrin-Riou, ‘Overconvergent modular symboles and p-adic L-functions’, Preprint, 2021, arXiv:2101.06960.

[7] P. R. Bending, ‘Curves of genus 2 with $\sqrt{2}$ multiplication’, Preprint, 1999, arXiv:math/9911273.

[8] B. J. Birch and H. P. F. Swinnerton-Dyer, ‘Notes on elliptic curves. II’, *J. Reine Angew. Math.* **218** (1965), 79–108.

[9] C. Birkenhake and H. Lange, *Complex Abelian Varieties*, second edn. (Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]) vol. 302 (Springer-Verlag, Berlin, 2004).

[10] E. Bombieri and W. Gubler, *Heights in Diophantine Geometry* (New Mathematical Monographs) vol. 4 (Cambridge University Press, Cambridge, 2006).

[11] R. van Bommel, ‘Numerical verification of the Birch and Swinnerton-Dyer conjecture for hyperelliptic curves of higher genus over **Q** up to squares’, *Exp. Math.* (2019), 1–8.

[12] S. Bosch, W. Lütkebohmert and M. Raynaud, *Néron Models* (Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]) vol. 21 (Springer-Verlag, Berlin, 1990).

[13] W. Bosma, J. Cannon and C. Playoust, ‘The Magma algebra system. I. The user language’, *J. Symbolic Comput.* **24**(3–4) (1997), 235–265, Computational algebra and number theory (London, 1993).

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

[14] G. Boxer, F. Calegari, T. Gee and V. Pilloni, ‘Abelian surfaces over totally real fields are potentially modular’, *Publ. Math. Inst. Hautes Études Sci.* **134** (2021), 153–501.

[15] C. Breuil, B. Conrad, F. Diamond and R. Taylor, ‘On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises’, *J. Amer. Math. Soc.* **14**(4) (2001), 843–939.

[16] N. Bruin, B. Poonen and M. Stoll, ‘Generalized explicit descent and its application to curves of genus 3’, *Forum Math. Sigma* **4** (2016), Paper No. e6, 80.

[17] A. Burungale, C. Skinner, Y. Tian and X. Wan, ‘Zeta elements for elliptic curves and applications’, Preprint, 2024, arXiv:2409.01350.

[18] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus* 2, (London Mathematical Society Lecture Note Series) vol. 230 (Cambridge University Press, Cambridge, 1996).

[19] F. Castella, G. Grossi, J. Lee and C. Skinner, ‘On the anticyclotomic Iwasawa theory of rational elliptic curves at Eisenstein primes’, *Invent. Math.* **227** (2022), 517–580.

[20] F. Castella, G. Grossi and C. Skinner, ‘Mazur’s main conjecture at Eisenstein primes’, Preprint, 2023, arXiv:2303.04373.

[21] F. Castella, M. Çiperiani, C. Skinner and F. Sprung, ‘On the Iwasawa main conjectures for modular forms at non-ordinary primes’, Preprint, 2018, arXiv:1804.10993.

[22] K. Česnavičius, ‘The Manin constant in the semistable case’, *Compos. Math.* **154**(9) (2018), 1889–1920.

[23] B. Cha, ‘Vanishing of some cohomology groups and bounds for the Shafarevich-Tate groups of elliptic curves’, *J. Number Theory* **111**(1) (2005), 154–178.

[24] J. Coates and C.-G. Schmidt, ‘Iwasawa theory for the symmetric square of an elliptic curve’, *J. Reine Angew. Math.* **375/376** (1987), 104–156.

[25] H. Cohen, ‘Haberland’s formula and numerical computation of Petersson scalar products’, in *ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium* (Open Book Ser.) vol. 1 (Math. Sci. Publ., Berkeley, CA, 2013), 249–270.

[26] A. C. Cojocaru, ‘On the surjectivity of the Galois representations associated to non-CM elliptic curves’, *Canad. Math. Bull.* **48**(1) (2005), 16–31, With an appendix by Ernst Kani.

[27] J. E. Cremona, T. A. Fisher, C. O’Neil, D. Simon and M. Stoll, ‘Explicit n-descent on elliptic curves. I. Algebra’, *J. Reine Angew. Math.* **615** (2008), 121–155.

[28] J. E. Cremona, T. A. Fisher, C. O’Neil, D. Simon and M. Stoll, ‘Explicit n-descent on elliptic curves. II. Geometry’, *J. Reine Angew. Math.* **632** (2009), 63–84.

[29] J. E. Cremona, T. A. Fisher, C. O’Neil, D. Simon and M. Stoll, ‘Explicit n-descent on elliptic curves III. Algorithms’, *Math. Comp.* **84**(292) (2015), 895–922.

[30] J. E. Cremona and B. Mazur, ‘Visualizing elements in the Shafarevich-Tate group’, *Experiment. Math.* **9**(1) (2000), 13–28.

[31] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, second edn. (Cambridge University Press, Cambridge, 1997).

[32] J. E. Cremona, ‘The BSD formula over number fields’, Preprint, 2023, https://github.com/JohnCremona/BSD/blob/master/BSD.pdf (Version 2023-01-18).

[33] B. Creutz, ‘Second p-descents on elliptic curves’, *Math. Comp.* **83**(285) (2014), 365–409.

[34] B. Creutz and R. L. Miller, ‘Second isogeny descents and the Birch and Swinnerton-Dyer conjectural formula’, *J. Algebra* **372** (2012), 673–701.

[35] H. Darmon and R. Pollack, ‘Magma code for p-adic L-functions’, https://www.math.mcgill.ca/darmon/programs/programs.html.

[36] H. Darmon and R. Pollack, ‘Efficient calculation of Stark-Heegner points via overconvergent modular symbols’, *Israel J. Math.* **153** (2006), 319–354.

[37] P. Deligne, ‘Formes modulaires et représentations l-adiques’, in *Séminaire Bourbaki. Vol. 1968/69: Exposés 347–363* (Lecture Notes in Math.) vol. 175 (Springer, Berlin, 1971), Exp. No. 355, 139–172.

[38] L. V. Dieulefait, ‘Explicit determination of the images of the Galois representations attached to abelian surfaces with $End(A) = \mathbf{Z}$’, *Experiment. Math.* **11**(4) (2002), 503–512 (2003).

[39] N. Dogra and S. Le Fourn, ‘Quadratic Chabauty for modular curves and modular forms of rank one’, *Math. Ann.* **380**(1–2) (2021), 393–448.

[40] T. Dokchitser, ‘Computing special values of motivic L-functions’, *Experiment. Math.* **13**(2) (2004), 137–149.

[41] T. Dokchitser and J. Silverman, ‘Answers to question ‘BSD conjecture for $X_0(17)$’, https://mathoverflow.net/questions/139575 (version: 2013-08-17).

[42] B. Edixhoven, ‘Néron models and tame ramification’, *Compos. Math.* **81**(3) (1992), 291–306.

[43] T. Fisher, ‘Visualizing elements of order 7 in the Tate-Shafarevich group of an elliptic curve’, *LMS J. Comput. Math.* **19** (2016), no. suppl. A, 100–114.

[44] T. Fisher and J. Yan, ‘Computing the Cassels-Tate pairing on the 2-Selmer group of a genus 2 Jacobian’, Preprint, 2023, arXiv:2306.06011.

[45] E. V. Flynn, F. Leprévost, E. F. Schaefer, W. A. Stein, M. Stoll and J. L. Wetherell, ‘Empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves’, *Math. Comp.* **70**(236) (2001), 1675–1697.

[46] S. Frengley, ‘*Explicit moduli spaces for curves of genus 1 and 2*’, 2023, PhD Thesis, University of Cambridge. https://www.repository.cam.ac.uk/handle/1810/369243Permalink

[47] S. Frengley, ‘Explicit 7-torsion in the Tate-Shafarevich groups of genus 2 Jacobians’, Preprint, 2024, arXiv:2405.11693.

[48] S. Gajović and J. S. Müller, ‘Computing p-adic heights on hyperelliptic curves’, Preprint, 2023, arXiv:2307.15787.

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press

[49] M. Greenberg, ‘Lifting modular symbols of non-critical slope’, *Israel J. Math.* **161** (2007), 141–155.

[50] G. Grigorov, A. Jorza, S. Patrikis, W. A. Stein and C. Tarniţă, ‘Computational verification of the Birch and Swinnerton-Dyer conjecture for individual elliptic curves’, *Math. Comp.* **78**(268) (2009), 2397–2425.

[51] B. H. Gross, ‘Heegner points on $X_0(N)$’, in *Modular Forms (Durham, 1983)* (Ellis Horwood Ser. Math. Appl.) (Statist. Oper. Res., Horwood, Chichester, 1984), 87–105.

[52] B. H. Gross and D. B. Zagier, ‘Heegner points and derivatives of L-series’, *Invent. Math.* **84**(2) (1986), 225–320.

[53] L. H. Halle and J. Nicaise, *Néron Models and Base Change* (Lecture Notes in Mathematics) vol. 2156 (Springer, Cham, 2016).

[54] Y. Hasegawa, ‘Table of quotient curves of modular curves $X_0(N)$ with genus 2’, *Proc. Japan Acad. Ser. A Math. Sci.* **71**(10) (1995), 235–239 (1996).

[55] B. Howard, ‘Iwasawa theory of Heegner points on abelian varieties of GL_2 type’, *Duke Math. J.* **124**(1) (2004), 1–45.

[56] D. Jetchev, ‘Global divisibility of Heegner points and Tamagawa numbers’, *Compos. Math.* **144**(4) (2008), 811–826.

[57] A. Jorza, ‘The Birch and Swinnerton-Dyer Conjecture for abelian varieties over number fields’, 2005, https://www3.nd.edu/ajorza/notes/bsd.pdf.

[58] K. Kato, ‘p-adic Hodge theory and values of zeta functions of modular forms’, in Astérisque no. 295 (2004), ix, 117–290. Cohomologies p -adiques et applications arithmétiques. III.

[59] T. Keller and M. Stoll, ‘Exact verification of the strong BSD conjecture for some absolutely simple abelian surfaces’, *C. R. Math. Acad. Sci. Paris* **360** (2022), 483–489.

[60] T. Keller and M. Yin, ‘On the anticyclotomic Iwasawa theory of newforms at Eisenstein primes of semistable reduction’, Preprint, 2024, arXiv:2402.12781.

[61] C. Khare and J.-P. Wintenberger, ‘Serre’s modularity conjecture’, in *Proceedings of the International Congress of Mathematicians. Volume II* (Hindustan Book Agency , New Delhi, 2010), 280–293.

[62] O. H. King, ‘The subgroup structure of finite classical groups in terms of geometric configurations’, in *Surveys in Combinatorics* (London Math. Soc. Lecture Note Ser.) vol. 327 (Cambridge Univ. Press, Cambridge, 2005), 29–56.

[63] V. A. Kolyvagin, ‘Finiteness of $E(\mathbf{Q})$ and for a subclass of Weil curves’, *Izv. Akad. Nauk SSSR Ser. Mat.* **52**(3) (1988), 522–540, 670–671 (Russian).

[64] V. A. Kolyvagin and D. Yu. Logachëv, ‘Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties’, *Algebra i Analiz* **1**(5) (1989), 171–196 (Russian).

[65] S. Lang, *Algebra* (Graduate Texts in Mathematics) vol. 211, third edn. (Springer-Verlag, New York, 2002).

[66] E. Larson and D. Vaintrob, ‘On the surjectivity of Galois representations associated to elliptic curves over number fields’, *Bull. Lond. Math. Soc.* **46**(1) (2014), 197–209.

[67] T. Lawson and C. Wuthrich, ‘Vanishing of some Galois cohomology groups for elliptic curves’, in *Elliptic Curves, Modular Forms and Iwasawa Theory* (Springer Proc. Math. Stat.) vol. 188 (Springer, Cham, 2016), 373–399.

[68] The LMFDB collaboration , ‘L-functions and modular forms database’, https://www.lmfdb.org/Genus2Curve/Q/.

[69] D. Lombardo, ‘Explicit surjectivity of Galois representations for abelian surfaces and GL_2-varieties’, *J. Algebra* **460** (2016), 26–59.

[70] D. Lombardo, ‘Computing the geometric endomorphism ring of a genus-2 Jacobian’, *Math. Comp.* **88**(316) (2019), 889–929.

[71] B. Mazur, J. Tate and J. Teitelbaum, ‘On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer’, *Invent. Math.* **84**(1) (1986), 1–48.

[72] J. R. Merriman and N. P. Smart, ‘Curves of genus 2with good reduction away from 2 with a rational Weierstrass point’, *Math. Proc. Cambridge Philos. Soc.* **114**(2) (1993), 203–214.

[73] R. L. Miller, ‘ *Empirical evidence for the Birch and Swinnerton-Dyer conjecture*’, 2010, PhD Thesis, University of Washington, ProQuest LLC, Ann Arbor, MI.

[74] R. L. Miller, ‘Proving the Birch and Swinnerton-Dyer conjecture for specific elliptic curves of analytic rank zero and one’, *LMS J. Comput. Math.* **14** (2011), 327–350.

[75] R. L. Miller and M. Stoll, ‘Explicit isogeny descent on elliptic curves’, *Math. Comp.* **82**(281) (2013), 513–529.

[76] J. S. Milne, ‘Abelian varieties’, in *Arithmetic Geometry (Storrs, Conn. 1984)* (Springer, New York, 1986), 103–150.

[77] J. S. Milne, ‘On the arithmetic of abelian varieties’, *Invent. Math.* **17** (1972), 177–190.

[78] J. S. Milne, *Arithmetic Duality Theorems*, second edn. (BookSurge, LLC, Charleston, SC, 2006).

[79] Y. Namikawa and K. Ueno, ‘The complete classification of fibres in pencils of curves of genus two’, *Manuscripta Math.* **9** (1973), 143–186.

[80] J. Nekovář, ‘The Euler system method for CM points on Shimura curves’, in *L-functions and Galois Representations* (London Math. Soc. Lecture Note Ser.) vol. 320 (Cambridge Univ. Press, Cambridge, 2007), 471–547.

[81] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of Number Fields* (Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]) vol. 323, second edn. (Springer-Verlag, Berlin, 2008). https://www.mathi.uni-heidelberg.de/ schmidt/NSW2e/NSW2.3.pdf

[82] V. Pal, ‘Periods of quadratic twists of elliptic curves’, *Proc. Amer. Math. Soc.* **140**(5) (2012), 1513–1525. With an appendix by Amod Agashe.

[83] H. Petersson, ‘Über die Berechnung der Skalarprodukte ganzer Modulformen’, *Comment. Math. Helv.* **22** (1949), 168–199.

[84] R. Pollack and G. Stevens, 'Overconvergent modular symbols and p-adic L-functions', *Ann. Sci. Éc. Norm. Supér. (4)* **44**(1) (2011), 1–42.

[85] B. Poonen, E. F. Schaefer and M. Stoll, 'Twists of $X(7)$ and primitive solutions to $x^2 + y^3 = z^7$', *Duke Math. J.* **137**(1) (2007), 103–158.

[86] B. Poonen and M. Stoll, 'The Cassels-Tate pairing on polarized abelian varieties', *Ann. of Math. (2)* **150**(3) (1999), 1109–1149.

[87] M. Raynaud, 'Schémas en groupes de type $(p, \ldots, p)$', *Bull. Soc. Math. France* **102** (1974), 241–280 (French).

[88] K. A. Ribet, 'Galois representations attached to eigenforms with Nebentypus', in *Modular Functions of One Variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)* (Lecture Notes in Math.) vol. 601 (Springer, Berlin, 1977), 17–51.

[89] K. A. Ribet, 'Galois action on division points of Abelian varieties with real multiplications', *Amer. J. Math.* **98**(3) (1976), 751–804.

[90] K. A. Ribet, 'Images of semistable Galois representations', *Pacific J. Math.* **Special Issue** (1997), 277–297. Olga Taussky-Todd: in memoriam.

[91] K. A. Ribet, 'Abelian varieties over **Q** and modular forms', in *Modular Curves and Abelian Varieties* (Progr. Math.) vol. 224 (Birkhäuser, Basel, 2004), 241–261.

[92] E. F. Schaefer, 'Class groups and Selmer groups', *J. Number Theory* **56**(1) (1996), 79–114.

[93] E. F. Schaefer and M. Stoll, 'How to do a p-descent on an elliptic curve', *Trans. Amer. Math. Soc.* **356**(3) (2004), 1209–1231.

[94] C.-G. Schmidt, ' p-adic measures attached to automorphic representations of GL(3)', *Invent. Math.* **92**(3) (1988), 597–631.

[95] P. Schneider, 'p-adic height pairings. II', *Invent. Math.* **79**(2) (1985), 329–374.

[96] M. Schütt, 'CM newforms with rational coefficients', *Ramanujan J.* **19**(2) (2009), 187–205.

[97] J.-P. Serre, 'Sur les représentations modulaires de degré 2de Gal$\left(\overline{\mathbf{Q}}/\mathbf{Q}\right)$', *Duke Math. J.* **54**(1) (1987), 179–230.

[98] J.-P. Serre, 'Propriétés galoisiennes des points d'ordre fini des courbes elliptiques', *Invent. Math.* **15**(4) (1972), 259–331 (French).

[99] J.-P. Serre, 'Quelques applications du théorème de densité de Chebotarev', *Inst. Hautes Études Sci. Publ. Math.* **54** (1981), 323–401 (French).

[100] J.-P. Serre, *Abelian l-adic Representations and Elliptic Curves* (Research Notes in Mathematics) vol. 7 (A K Peters, Ltd., Wellesley, MA, 1998) With the collaboration of Willem Kuyk and John Labute; Revised reprint of the 1968 original.

[101] G. Shimura, *Abelian Varieties with Complex Multiplication and Modular Functions* (Princeton Mathematical Series) vol. 46 (Princeton University Press, Princeton, NJ, 1998).

[102] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions* (Publications of the Mathematical Society of Japan) No. 11 (Iwanami Shoten, Publishers, Tokyo; Princeton University Press, Princeton, NJ, 1971). Kanô Memorial Lectures, No. 1.

[103] G. Shimura, 'On the holomorphy of certain Dirichlet series', *Proc. London Math. Soc. (3)* **31**(1) (1975), 79–98.

[104] G. Shimura, 'The special values of the zeta functions associated with cusp forms', *Comm. Pure Appl. Math.* **29**(6) (1976), 783–804.

[105] A. Shnidman and A. Weiss, 'Elements of prime order in Tate-Shafarevich groups of abelian varieties over $\mathbb{Q}$', *Forum Math. Sigma* **10** (2022), Paper No. e98, 10.

[106] C. Skinner, 'Multiplicative reduction and the cyclotomic main conjecture for GL_2', *Pacific J. Math.* **283**(1) (2016), 171–200.

[107] C. Skinner and E. Urban, 'The Iwasawa main conjectures for GL_2', *Invent. Math.* **195**(1) (2014), 1–277.

[108] W. Stein, '*Gross-Zagier: Heegner points and derivatives of L-series*', 2008, https://389a.blogspot.com/2008/11/gross-zagier-heegner-points-and.html.

[109] W. Stein and C. Wuthrich, 'Algorithms for the arithmetic of elliptic curves using Iwasawa theory', *Math. Comp.* **82**(283) (2013), 1757–1792.

[110] M. Stoll, 'Descent on elliptic curves', in *Explicit Methods in Number Theory* (Panor. Synthèses) vol. 36 (Soc. Math. France, Paris, 2012), 51–80.

[111] M. Stoll, 'On the height constant for curves of genus two', *Acta Arith.* **90**(2) (1999), 183–201.

[112] M. Stoll, 'Implementing 2-descent for Jacobians of hyperelliptic curves', *Acta Arith.* **98**(3) (2001), 245–277.

[113] J. Tate, 'On the conjectures of Birch and Swinnerton-Dyer and a geometric analog', in *Séminaire Bourbaki*, Vol. 9 (Soc. Math. France, Paris, 1995), Exp. No. 306, 415–440.

[114] R. Taylor and A. Wiles, 'Ring-theoretic properties of certain Hecke algebras', *Ann. of Math. (2)* **141**(3) (1995), 553–572.

[115] user334725 (https://mathoverflow.net/users/334725/user334725), 'Computing the Petersson norm of newforms of weight 2 from the symmetric square L-function', https://mathoverflow.net/q/410483 (version: 2021-12-11).

[116] A. Wiles, 'Modular elliptic curves and Fermat's last theorem', *Ann. of Math. (2)* **141**(3) (1995), 443–551.

[117] C. Wuthrich, 'Numerical modular symbols for elliptic curves', *Math. Comp.* **87**(313) (2018), 2393–2423.

[118] W. Zhang, 'Selmer groups and the indivisibility of Heegner points', *Camb. J. Math.* **2**(2) (2014), 191–253.

https://doi.org/10.1017/fms.2024.133 Published online by Cambridge University Press