Forum of Mathematics, Sigma (2016), Vol. 4, e4, 79 pages
doi:10.1017/fms.2015.33

COMPUTING IMAGES OF GALOIS REPRESENTATIONS ATTACHED TO ELLIPTIC CURVES

ANDREW V. SUTHERLAND

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA;
email: drew@math.mit.edu

Received 9 September 2015; accepted 16 November 2015

Abstract

Let E be an elliptic curve without complex multiplication (CM) over a number field K, and let $G_E(\ell)$ be the image of the Galois representation induced by the action of the absolute Galois group of K on the ℓ-torsion subgroup of E. We present two probabilistic algorithms to simultaneously determine $G_E(\ell)$ up to local conjugacy for all primes ℓ by sampling images of Frobenius elements; one is of Las Vegas type and the other is a Monte Carlo algorithm. They determine $G_E(\ell)$ up to one of at most two isomorphic conjugacy classes of subgroups of $\mathbf{GL}_2(\mathbf{Z}/\ell\mathbf{Z})$ that have the same semisimplification, each of which occurs for an elliptic curve isogenous to E. Under the GRH, their running times are polynomial in the bit-size n of an integral Weierstrass equation for E, and for our Monte Carlo algorithm, quasilinear in n. We have applied our algorithms to the non-CM elliptic curves in Cremona's tables and the Stein–Watkins database, some 140 million curves of conductor up to 10^{10}, thereby obtaining a conjecturally complete list of 63 exceptional Galois images $G_E(\ell)$ that arise for $E/\mathbf{Q}$ without CM. Under this conjecture, we determine a complete list of 160 exceptional Galois images $G_E(\ell)$ that arise for non-CM elliptic curves over quadratic fields with rational j-invariants. We also give examples of exceptional Galois images that arise for non-CM elliptic curves over quadratic fields only when the j-invariant is irrational.

2010 Mathematics Subject Classification: 11G05, 11Y16 (primary); 11F80, 11G20, 14H52, 20G40 (secondary)

1. Introduction

Let E be an elliptic curve over a number field K with algebraic closure $\overline{K}$. For each integer $m > 1$, let $E[m]$ denote the m-torsion subgroup of $E(\overline{K})$, which we recall is a free $\mathbf{Z}/m\mathbf{Z}$ module of rank two. The absolute Galois group $\mathrm{Gal}(\overline{K}/K)$

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

acts on $E[m]$ via its action on the coordinates of its points, and this action induces a Galois representation (a continuous homomorphism):

$$\rho_{E,m}\colon \operatorname{Gal}(\overline{K}/K) \to \operatorname{Aut}(E[m]) \simeq \mathbf{GL}_2(m) := \mathbf{GL}_2(\mathbf{Z}/m\mathbf{Z}).$$

We regard the image of $\rho_{E,m}$ as a subgroup $G_E(m)$ of $\mathbf{GL}_2(m)$ that is determined only up to conjugacy, since the isomorphism $\operatorname{Aut}(E[m]) \simeq \mathbf{GL}_2(m)$ depends on a choice of basis. For fixed E and varying m, the representations $\rho_{E,m}$ form a compatible system, and we have the adelic Galois representation

$$\rho_E\colon \operatorname{Gal}(\overline{K}/K) \to \mathbf{GL}_2(\hat{\mathbf{Z}}) = \varprojlim_m \mathbf{GL}_2(m),$$

whose image we denote as G_E.

By Serre's open image theorem (see [57, Section IV.3.2] and [58]), so long as E does not have complex multiplication (CM), the adelic image G_E has finite index in $\mathbf{GL}_2(\hat{\mathbf{Z}})$. In particular, there is a minimal positive integer m_E for which G_E is the full inverse image of $G_E(m_E)$, and a finite set S_E of exceptional primes ℓ for which $G_E(\ell)$ is properly contained in $\mathbf{GL}_2(\ell)$. Each such ℓ necessarily divides m_E, but the converse is not true in general (and almost never true for elliptic curves over $\mathbf{Q}$). Nevertheless, a first step toward computing m_E and $G_E(m_E)$ is to determine the set S_E and the groups $G_E(\ell)$ for $\ell \in S_E$.

A related motivating question is this: for a given number field K, which exceptional groups $G_E(\ell)$ can arise for a non-CM elliptic curve E/K? Serre's theorem implies that for any fixed E this is a finite list, and Serre has asked whether this is still true when only K is fixed and E/K is allowed to vary; it is expected that the answer is yes. This can be regarded as a generalization of Mazur's results [46, 47], which determine the primes ℓ for which an elliptic curve $E/\mathbf{Q}$ may admit a rational point of order ℓ, or a rational isogeny of degree ℓ. Both of these properties are determined by $G_E(\ell)$, but the converse does not hold: $G_E(\ell)$ may be exceptional when E does not admit a rational isogeny of degree ℓ, and even when E has a rational point of order ℓ, many different $G_E(\ell)$ may occur. Serre's question remains open for all number fields K, but there has been some recent progress in the case $K = \mathbf{Q}$: for $\ell > 37$ any exceptional $G_E(\ell)$ must lie in the normalizer of a nonsplit Cartan group in $\mathbf{GL}_2(\ell)$, as shown in [5], and for $\ell \leqslant 11$ the possible $G_E(\ell)$ have been completely determined [74]. Little is known for number fields other than $\mathbf{Q}$.

We are thus led to the problem at hand: given an elliptic curve E/K without CM, determine the set S_E of exceptional primes ℓ and the groups $G_E(\ell)$ for each prime $\ell \in S_E$. Serre's open image theorem can be made effective, and under the generalized Riemann hypothesis (GRH) reasonably good bounds on the exceptional primes ℓ are known; quasilinear in the norm of the conductor

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

of E, by [42]. This leaves the problem of computing $G_E(\ell)$. In principle, this is straightforward: pick a basis for $E[\ell]$ and compute the action of $\mathrm{Gal}(\overline{K}/K)$ on this basis. This approach can be made completely effective. The points in $E[\ell]$ are defined over the ℓ-torsion field $K(E[\ell])$, which is an extension of the splitting field of the ℓ-division polynomial $f_{E,\ell}(x)$ whose roots are the x-coordinates of the nontrivial ℓ-torsion points. Using well-known formulas for $f_{E,\ell}(x)$ one can explicitly construct its splitting field and take a quadratic extension if necessary to obtain the y-coordinates of the points in $E[\ell]$ (a quadratic extension always suffices, see Lemma 5.17). One then finds generators for $\mathrm{Gal}(K(E[\ell])/K)$ and applies them to a basis for $E[\ell]$. Using the algorithm in [40], this computation can be accomplished in deterministic polynomial time; a Magma [11] script that implements this procedure is available at the author's website [68].

Unfortunately, this is feasible only for very small ℓ. While $\mathrm{Gal}(K(E[\ell])/K)$ can be computed in time polynomial in ℓ, the exponents involved are quite large; indeed, the necessary first step of factoring $f_{E,\ell}(x)$ is already nontrivial, even when $K = \mathbf{Q}$. For $\ell > 2$, the polynomial $f_{E,\ell}$ has degree $(\ell^2 - 1)/2$ and coefficients with bit-size $O(\ell^2)$, which gives an $O(\ell^{12+o(1)})$ time for factoring $f_{E,\ell} \in \mathbf{Z}[x]$ using the best known bounds for polynomial factorization [54]. More generally, the time to factor $f_{E,\ell}$ in $K[x]$ given in [40] is $O(\ell^{18+o(1)}[K:\mathbf{Q}]^{9+o(1)})$, and the time to compute its splitting field may be substantially larger. By contrast, the Monte Carlo algorithm presented in this article computes $G_E(\ell)$ up to local conjugacy (as defined below) in time that is quasilinear in both ℓ and $[K:\mathbf{Q}]$; in fact, it does this simultaneously for all primes in S_E in time quasilinear in $\max(S_E)$.

Two Galois representations $\rho_1, \rho_2\colon \mathrm{Gal}(\overline{K}/K) \to \mathbf{GL}_2(m)$ are said to be *locally conjugate* if $\rho_1(\sigma)$ and $\rho_2(\sigma)$ are conjugate in $\mathbf{GL}_2(m)$ for every σ (not necessarily by the same matrix in each case). We call two subgroups G and H of $\mathbf{GL}_2(m)$ locally conjugate if there is a bijection of sets that maps each $g \in G$ to an element $h \in H$ that is conjugate to g in $\mathbf{GL}_2(m)$; equivalently, $(\mathbf{GL}_2(m), G, H)$ is a (nontrivial) Gassmann–Sunada triple [31, 69]. Local conjugacy defines an equivalence relation on the set of subgroups of $\mathbf{GL}_2(m)$.

We present two probabilistic algorithms to determine the exceptional primes ℓ for a given elliptic curve E/K and to determine the groups $G_E(\ell)$ up to local conjugacy. The algorithms work by computing the images in $G_E(\ell)$ of Frobenius elements (conjugacy classes) $\mathrm{Frob}_\mathfrak{p}$ for unramified primes $\mathfrak{p} \nmid \ell$ of K where E has good reduction, either for all $\mathfrak{p}$ of bounded norm, or for randomly chosen $\mathfrak{p}$ with norms in a bounded interval. This implies that our algorithms can only determine $G_E(\ell)$ up to local conjugacy, but we show that this imposes very strong constraints on $G_E(\ell)$. In particular, we prove that every local conjugacy class of subgroups of $\mathbf{GL}_2(\ell)$ consists of at most two conjugacy classes of subgroups of $\mathbf{GL}_2(\ell)$ that are isomorphic as abstract groups and have the same

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

semisimplification. Moreover, we prove that whenever $G_E(\ell)$ is locally conjugate to a subgroup G' of $\mathbf{GL}_2(\ell)$, there is an isogenous elliptic curve E'/K for which $G_{E'}(\ell) = G'$ (see Theorem 3.32). We also describe some global methods for efficiently distinguishing pairs of locally conjugate but nonconjugate Galois images that are applicable in most (but not all) cases, including every case that we encountered in our computations (see Section 5.5).

To compute the conjugacy class $\rho_{E,m}(\mathrm{Frob}_\mathfrak{p})$ for unramified primes $\mathfrak{p}$ of K that do not divide m we rely on three fundamental algorithms for elliptic curves over finite fields that we apply to the reduction $E_\mathfrak{p}/\mathbf{F}_\mathfrak{p}$ of E modulo $\mathfrak{p}$; here $\mathbf{F}_\mathfrak{p} := \mathcal{O}_K/\mathfrak{p}$ is the residue field, a finite field with $q := N(\mathfrak{p})$ elements. The first is Schoof's algorithm [55, 56], which computes the trace $t \in \mathbf{Z}$ of the Frobenius endomorphism in time polynomial in $\log q$. The second is a Las Vegas algorithm to compute the endomorphism ring $\mathrm{End}(E_\mathfrak{p})$ when $E_\mathfrak{p}$ is ordinary, due to Bisson and the author [8, 9]; under the GRH its expected running time is subexponential in $\log q$. It follows from a theorem of Duke and Tóth [25] that the pair $(t, \mathrm{End}(E_\mathfrak{p}))$ determines an integer matrix $A_\mathfrak{p}$ whose reduction modulo m lies in the conjugacy class $\rho_{E,m}(\mathrm{Frob}_\mathfrak{p})$ for every positive integer m. The third is Miller's algorithm to compute the Weil pairing [49], which we use to compute the rank of the ℓ-torsion subgroup of $E_\mathfrak{p}(\mathbf{F}_\mathfrak{p})$ in quasicubic time. This allows us to determine the dimension of the 1-eigenspace of $\rho_{E,\ell}(\mathrm{Frob}_\mathfrak{p})$ without computing $A_\mathfrak{p}$, providing an efficient method to distinguish unipotent elements of $G_E(\ell)$, which are not distinguished by their characteristic polynomials.

In order to bound the norms of the primes $\mathfrak{p}$ that we use, we rely on explicit Chebotarev bounds that depend on the GRH. In principle, our algorithms can be implemented so that they do not rely on this hypothesis, but the running times would increase exponentially. The GRH also gives us bounds on the largest exceptional prime ℓ that can occur for a given elliptic curve E/K; the results of Larson and Vaintrob [42] give bounds that are quasilinear in $\log N_E$, where N_E is the absolute value of the norm of the conductor of E. Together, these allow us to bound the norms of the primes $\mathfrak{p}$ that we must consider by a polynomial in $\log \|f\|$, where $\|f\|$ denotes the maximum of the absolute values of the norms of the coefficients appearing in an integral Weierstrass equation $y^2 = f(x)$ for E.

We now state our two main results. The first is a Las Vegas algorithm that, given an elliptic curve E/K specified by an integral Weierstrass equation, outputs a complete list S_E of the primes ℓ for which $G_E(\ell) \neq \mathbf{GL}_2(\ell)$ and for each $\ell \in S_E$ a subgroup of $\mathbf{GL}_2(\ell)$ specified by generators that is locally conjugate to $G_E(\ell)$ (see Algorithm 5). Under the GRH its expected running time is bounded by

$$(\log \|f\|)^{11+o(1)}$$

in Theorem 5.7. Our second main result is a Monte Carlo algorithm that has the same output as our Las Vegas algorithm and is correct with probability at

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

least $2/3$; see Algorithm 7. Its error is one-sided in the sense that each subgroup of $\mathbf{GL}_2(\ell)$ output by the algorithm is guaranteed to be locally conjugate to a subgroup of $G_E(\ell)$, but it may be a proper subgroup. By running the algorithm repeatedly the error probability can be made arbitrarily small. Under the GRH its running time is bounded by

$$(\log \|f\|)^{1+o(1)},$$

which is quasilinear in the size of the input, the equation $y^2 = f(x)$ (see Theorem 5.15).

An essential ingredient to both of our algorithms is the ability to distinguish and explicitly construct subgroups of $\mathbf{GL}_2(\ell)$ based on a compact representation of a subset of their element conjugacy classes. The classification of the possible images of subgroups of $\mathbf{GL}_2(\ell)$ in $\mathbf{PGL}_2(\ell)$ has long been known [23], but for our work we require a complete list of the subgroups of $\mathbf{GL}_2(\ell)$ up to conjugacy, and a precise understanding of the element conjugacy classes each contain. We address these questions in Section 3, in which we obtain exact formulas for the number of subgroups of $\mathbf{GL}_2(\ell)$ up to conjugacy (and for subgroups of various types) that may be of independent interest. We also give a quasilinear time algorithm to enumerate these subgroups with explicit generators for each (see Algorithm 2).

We have applied our algorithms to various databases of elliptic curves over $\mathbf{Q}$, including all non-CM curves of conductor up to 350 000 listed in Cremona's tables [19], and the non-CM curves in the Stein and Watkins database [61], which includes a large proportion of all elliptic curves over $\mathbf{Q}$ of conductor up to 10^8, and of prime conductor up to 10^{10}; some 140 million elliptic curves in all. We also analyzed parameterized families of elliptic curves that are known to have exceptional Galois images, and large families of elliptic curves of bounded height (more than 10^9 curves). In each case, we were able to compute a complete list S_E of the exceptional primes ℓ and the subgroups $G_E(\ell)$ up to conjugacy (not just local conjugacy), using the methods described in Section 5.5. This work yields a conjecturally complete list of 63 exceptional subgroup conjugacy classes that arise as $G_E(\ell)$ for some non-CM elliptic curve $E/\mathbf{Q}$ and prime ℓ; these are listed in Table 3 and of Section 6. Thanks to recent work by Zywina [74], we have been able to independently verify our results for all the non-CM elliptic curves in Cremona's tables, and in every case we found that the output of our Monte Carlo algorithm (which we executed repeatedly in order to amplify its success probability) was correct. This motivates the following conjecture:

CONJECTURE 1.1. *Let $E/\mathbf{Q}$ be an elliptic curve without complex multiplication and let ℓ be a prime. Then $G_E(\ell)$ is either equal to $\mathbf{GL}_2(\ell)$ or conjugate to one of the* 63 *groups listed in Table* 3.

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

Under this conjecture, we determine a complete list of 160 exceptional Galois images $G_E(\ell)$ not containing $\mathbf{SL}_2(\ell)$ that arise for non-CM elliptic curves with rational j-invariants over quadratic fields; these include the 63 groups that already arise over $\mathbf{Q}$ along with 68 new groups that arise for base changes of elliptic curves over $\mathbf{Q}$, and 29 that arise for quadratic twists of these curves but not for any base change from $\mathbf{Q}$; see Theorem 6.3 and Tables 4–6. A key ingredient to this result is an analysis of how $G_{E^F}(\ell)$ varies within a family of quadratic twists E^F of a fixed elliptic curve E/K as F varies over quadratic extensions of K; this appears in Section 5.6. We find that for any odd prime ℓ, up to three nonconjugate groups $G_{E^F}(\ell)$ may arise in such a family and we give an explicit method to determine quadratic extensions F/K that realize every possibility.

We have also run our algorithms on tables of elliptic curves defined over quadratic fields that have recently been made available in the L-functions and modular forms database (LMFDB) [45], including the five real quadratic fields and five imaginary quadratic fields of least absolute discriminant. Examples of exceptional Galois images $G_E(\ell)$ that occur only for non-CM elliptic curves with irrational j-invariants over these fields are listed in the tables at the end of Section 6, as well as examples over the cubic field of discriminant -23.

In principle, our algorithms can also be used to determine $G_E(m)$ up to local conjugacy for any positive integer m, but the situation is more complicated when m is composite for three reasons: (1) local conjugacy imposes fewer constraints when m is composite, for example, locally conjugate subgroups of $\mathbf{GL}_2(m)$ need not be isomorphic; (2) the integers m for which $G_E(m)$ is exceptional and not the full inverse image of $G_E(m')$ for some $m'|m$ may be exponentially larger than the largest exceptional prime ℓ; (3) our understanding of the subgroup structure of $\mathbf{GL}_2(m)$ is less refined than it is for $\mathbf{GL}_2(\ell)$. In spite of these obstacles, it is entirely feasible to apply our algorithms when m is small, and if we set the more modest goal of simply computing the index of $G_E(m)$ in $\mathbf{GL}_2(m)$, this can be done quite efficiently. This suggests a practical method for computing m_E and the index of G_E in $\mathbf{GL}_2(\hat{\mathbf{Z}})$ for a non-CM elliptic curve E/K that we plan to address in a future article.

2. Notation and terminology

Throughout this article, the symbols ℓ and p denote rational primes, and r, m, and n denote positive integers. We use $\tau(n)$ to denote the number of positive divisors of an integer n and $\phi(n) := \#(\mathbf{Z}/n\mathbf{Z})^\times$ for the Euler function. For any prime power q, we use $\mathbf{F}_q$ to denote the field with q elements. For sets S and T we write $S - T$ for the set of elements of S that do not lie in T.

For any ring R, we use $\mathbf{M}_r(R)$ to denote the ring of $r \times r$ matrixes, $\mathbf{GL}_r(R)$ for its multiplicative subgroup of invertible matrixes, $\mathbf{SL}_r(R)$ for the kernel of the determinant map $\det\colon \mathbf{GL}_r(R) \to \mathbf{GL}_1(R)$, and $\mathbf{PGL}_r(R)$ for the quotient of $\mathbf{GL}_r(R)$ by its center. For each integer $m > 1$ we define the notations

$$\begin{aligned} \mathbf{Z}(m) &:= \mathbf{Z}/m\mathbf{Z}, \\ \mathbf{M}_r(m) &:= \mathbf{M}_r(\mathbf{Z}/m\mathbf{Z}), \\ \mathbf{SL}_r(m) &:= \mathbf{SL}_r(\mathbf{Z}/m\mathbf{Z}), \\ \mathbf{GL}_r(m) &:= \mathbf{GL}_r(\mathbf{Z}/m\mathbf{Z}), \\ \mathbf{PGL}_r(m) &:= \mathbf{PGL}_r(\mathbf{Z}/m\mathbf{Z}). \end{aligned}$$

The center of $\mathbf{GL}_2(m)$ consists of the subgroup of scalar matrixes $\left(\begin{smallmatrix} z & 0 \\ 0 & z \end{smallmatrix}\right)$, which we denote $Z(m)$; when there is no risk of ambiguity we may identify $Z(m) \simeq \mathbf{Z}(m)^\times$ and use z to denote $\left(\begin{smallmatrix} z & 0 \\ 0 & z \end{smallmatrix}\right)$. The scalar matrixes form the kernel of the canonical projection

$$\pi : \mathbf{GL}_2(m) \twoheadrightarrow \mathbf{PGL}_2(m)$$

which we denote by π throughout.

In our identification of $\mathrm{Aut}(E[m])$ with $\mathbf{GL}_2(m)$, we view elements of $\mathbf{GL}_2(m)$ as 2×2 matrixes acting on column vectors by multiplication on the **left**, and distinguish subgroups of $\mathbf{GL}_2(m)$ only up to conjugacy. For an elliptic curve E over a number field K, composing the two-dimensional representation

$$\rho_E\colon\ \mathrm{Gal}(\overline{K}/K) \to \mathbf{GL}_2(\hat{\mathbf{Z}})$$

with the determinant map $\mathbf{GL}_2(\hat{\mathbf{Z}}) \to \hat{\mathbf{Z}}^\times$ induces a one-dimensional representation

$$\det \circ \rho_E\colon\ \mathrm{Gal}(\overline{K}/K) \to \mathbf{GL}_1(\hat{\mathbf{Z}}) = \hat{\mathbf{Z}}^\times.$$

Throughout this article, we use $\mathfrak{p}$ to denote a prime of K, by which we mean a nonzero prime ideal in its ring of integers $\mathcal{O}_K$, and we use $\mathbf{F}_\mathfrak{p}$ to denote the residue field $\mathcal{O}_K/\mathfrak{p}$. For each prime $\mathfrak{p} \nmid m$ that is unramified in $K(E[m])/K$ (all but finitely many $\mathfrak{p}$), the value of $\det \circ \rho_E$ on the Frobenius element $\mathrm{Frob}_\mathfrak{p}$ (which we recall is defined only up to conjugacy) is $N(\mathfrak{p}) := [\mathcal{O}_K : \mathfrak{p}]$. The image of $\det \circ \rho_E$ thus depends only on K, not on E; in fact, it depends only on the intersection of K with the maximal cyclotomic extension $\mathbf{Q}^{\mathrm{cyc}}$ of $\mathbf{Q}$ in $\overline{K}$, and $\det \circ \rho_{E,\ell}$ is surjective for all but finitely many ℓ.

Our complexity bounds always count bit operations. We use $\mathsf{M}(n)$ to denote the time to multiply two n-bit integers, which we may bound by

$$\mathsf{M}(n) = n(\log n)^{1+o(1)}$$

via [53]; see [34] for a more precise bound. This bound implies that arithmetic operations in finite fields $\mathbf{F}_q$ can be performed in $(\log q)^{1+o(1)}$ time, which we assume throughout (we refer the reader to [32] for details).

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

Many of the algorithms we present are probabilistic algorithms, which we recall are typically classified as one of two types. *Las Vegas algorithms* produce output that is guaranteed to be correct but have potentially unbounded running times that may depend on probabilistic choices; for such algorithms, we bound their expected running times, which are required to be finite. *Monte Carlo algorithms*, by contrast, have bounded running times but may produce outputs that are incorrect with probability bounded by some $c < 1/2$; we use $c = 1/3$. Assuming the correct output is unique, by running a Monte Carlo algorithm repeatedly and choosing the output produced most frequently, the probability of error can be made arbitrarily close to zero at a rate exponential in the number of repetitions.

For integers $n \geqslant 3$, we use A_n and S_n to denote the alternating and symmetric groups on n elements, respectively. For the purpose of this article we consider the noncyclic group of order 4 (the Klein group) to be a dihedral group.

3. Subgroups of $\mathbf{GL}_2(\mathbf{F}_\ell)$

The classification of subgroups of $\mathbf{PGL}_2(\ell)$ is well-known (see Proposition 3.1 below). Our algorithms require a more refined classification of the subgroups of $\mathbf{GL}_2(\ell)$, up to conjugacy in $\mathbf{GL}_2(\ell)$, that allows us to distinguish subgroups by sampling element conjugacy classes corresponding to Frobenius elements. In this section, we obtain such a classification, as well as explicit formulas to count subgroups of $\mathbf{GL}_2(\ell)$ up to conjugacy and an efficient algorithm to enumerate them. Many of the proofs in this section are elementary, but as our algorithms depend crucially on these results, we give at least a sketch of each proof. Except when the case $\ell = 2$ is specifically noted, we assume throughout this section that ℓ is an odd prime.

For any $g \in \mathbf{GL}_2(\ell)$ we define the discriminant

$$\Delta(g) := \operatorname{tr}(g)^2 - 4\det(g) \in \mathbf{Z}(\ell),$$

and its quadratic character

$$\chi(g) := \left(\frac{\Delta(g)}{\ell}\right) \in \{-1, 0, 1\}.$$

For ease of reference we list the element conjugacy classes of $\mathbf{GL}_2(\ell)$ in Table 1. Here and throughout, ε denotes a fixed nonsquare element of $\mathbf{Z}(\ell)^\times$; for the sake of concreteness, let ε be the least positive integer that generates $\mathbf{Z}(\ell)^\times$. We note that $\left(\begin{smallmatrix} x & 0 \\ 0 & y \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} y & 0 \\ 0 & x \end{smallmatrix}\right)$ are conjugate via $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, and $\left(\begin{smallmatrix} x & \varepsilon y \\ y & x \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} x & -\varepsilon y \\ -y & x \end{smallmatrix}\right)$ are conjugate via $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, which explains the restrictions on y in Table 1 below.

Table 1. Element conjugacy classes in $\mathbf{GL}_2(\ell)$ for primes $\ell > 2$.

Representative		Size	Number	det	tr	χ	Order
$\left(\begin{smallmatrix}x&0\\0&x\end{smallmatrix}\right)$	$0 < x < \ell$	1	$\ell - 1$	x^2	$2x$	0	divides $\ell - 1$
$\left(\begin{smallmatrix}x&1\\0&x\end{smallmatrix}\right)$	$0 < x < \ell$	$\ell^2 - 1$	$\ell - 1$	x^2	$2x$	0	divisible by ℓ
$\left(\begin{smallmatrix}x&0\\0&y\end{smallmatrix}\right)$	$0 < x < y < \ell$	$\ell^2 + \ell$	$\binom{\ell-1}{2}$	xy	$x + y$	$+1$	divides $\ell - 1$
$\left(\begin{smallmatrix}x&\varepsilon y\\y&x\end{smallmatrix}\right)$	$0 < y \leqslant \ell - 1/2$	$\ell^2 - \ell$	$\binom{\ell}{2}$	$x^2 - \varepsilon y^2$	$2x$	-1	divides $\ell^2 - 1$

For any $g \in \mathbf{GL}_2(\ell)$ and positive integer n, the trace of g^n can be computed as $\operatorname{tr} g^n = a_n$, where a_n is defined by the recurrence:

$$a_0 := 2, \quad a_1 := \operatorname{tr}(g), \quad a_{n+2} := a_1 a_{n+1} - a_n \det g. \tag{3.1}$$

This implies that for elements g whose order $|g|$ is not divisible by ℓ, we can derive $|g|$ from $(\det g, \operatorname{tr} g)$. We are also interested in the order of the image of g in $\mathbf{PGL}_2(\ell)$. For this purpose we define

$$u(g) := \frac{\operatorname{tr}(g)^2}{\det(g)} \in \mathbf{Z}(\ell).$$

If $|g|$ is divisible by ℓ then g is conjugate to some $\left(\begin{smallmatrix}x&1\\0&x\end{smallmatrix}\right)$ and $u(g) = 4$. Otherwise, the order r of $\pi(g)$ in $\mathbf{PGL}_2(\ell)$ is prime to ℓ and we have

$$u(g) = \zeta_r + \zeta_r^{-1} + 2, \tag{3.2}$$

for some primitive rth root of unity for which $\zeta_r + \zeta_r^{-1} \in \mathbf{F}_\ell^\times$, as explained in [41, page 190]. Note that ζ_r may lie in a quadratic extension $\mathbf{F}_\ell$, but in any case r divides either $\ell - 1$ or $\ell + 1$ and is uniquely determined by $u(g)$; this allows $|\pi(g)| = r$ to be unambiguously determined from $u(g)$, and hence from the pair $(\det g, \operatorname{tr} g)$ whenever $|g|$ is prime to ℓ. This implies, in particular, that the elements of $\mathbf{GL}_2(\ell)$ that have order 2 in $\mathbf{PGL}_2(\ell)$ are precisely the elements of trace zero.

For each odd prime ℓ we define the *split Cartan group* $C_s(\ell)$ and *nonsplit Cartan group* $C_{ns}(\ell)$ by

$$C_s(\ell) := \left\{ \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} : xy \neq 0 \right\} \subseteq \mathbf{GL}_2(\ell),$$

$$C_{ns}(\ell) := \left\{ \begin{pmatrix} x & \varepsilon y \\ y & x \end{pmatrix} : (x, y) \neq (0, 0) \right\} \subseteq \mathbf{GL}_2(\ell),$$

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

and note that $C_s(\ell) \simeq \mathbf{F}_\ell^\times \times \mathbf{F}_\ell^\times$ and $C_{ns}(\ell) \simeq \mathbf{F}_{\ell^2}^\times$. Both $C_s(\ell)$ and $C_{ns}(\ell)$ have index 2 in their normalizers

$$C_s^+(\ell) := C_s(\ell) \cup \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} C_s, \quad C_{ns}^+(\ell) := C_{ns} \cup \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} C_{ns}(\ell).$$

Elements of $C_s^+(\ell)$ that are conjugate in $\mathbf{GL}_2(\ell)$ are conjugate in $C_s^+(\ell)$, and similarly for $C_{ns}^+(\ell)$. We define $C_s(2)$ as the trivial group, and $C_{ns}(2)$ as the kernel of the sign homomorphism $\mathbf{GL}_2(2) \simeq \mathrm{S}_3 \twoheadrightarrow \{\pm 1\}$; both are normal in $\mathbf{GL}_2(2)$.

We refer to the conjugates of $C_s(\ell)$ and $C_{ns}(\ell)$ in $\mathbf{GL}_2(\ell)$ as *split* and *nonsplit Cartan groups*, respectively. For $\ell > 2$, all elements in the nontrivial coset of a Cartan group in its normalizer have trace zero, and the square of such an element g is the scalar matrix $\left(\begin{smallmatrix} z & 0 \\ 0 & z \end{smallmatrix}\right)$, where $z = -\det g$.

The *Borel group* $B(\ell) \subseteq \mathbf{GL}_2(\ell)$ is the subgroup of upper triangular matrixes; we refer to its conjugates in $\mathbf{GL}_2(\mathbf{F}_\ell)$ as *Borel groups*. For $\ell > 2$, the group $B(\ell)$ is nonabelian, and its commutator subgroup $B(\ell)'$ is the cyclic group of order ℓ generated by $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. The split Cartan subgroup $C_s(\ell)$ is contained in $B(\ell)$, and for $\ell > 2$ it is isomorphic to the abelian quotient $B(\ell)/[B(\ell), B(\ell)]$. We also note that

$$Z(\ell) = C_s(\ell) \cap C_{ns}(\ell) \subseteq B(\ell).$$

We now recall the classification of subgroups of $\mathbf{GL}_2(\ell)$ in terms of their images in $\mathbf{PGL}_2(\ell)$, originally due to Dickson [23].

PROPOSITION 3.1. *Let ℓ be an odd prime and let G be a subgroup of $\mathbf{GL}_2(\ell)$ with image H in $\mathbf{PGL}_2(\ell)$. If G contains an element of order ℓ then $G \subseteq B(\ell)$ or $\mathbf{SL}_2(\ell) \subseteq G$. Otherwise, one of the following holds:*

(1) *H is cyclic and G lies in a Cartan group;*

(2) *H is dihedral and G lies in the normalizer of a Cartan group, but not in any Cartan group;*

(3) *H is isomorphic to A_4, S_4, or A_5 and G is not contained in the normalizer of any Cartan group.*

Proof. See [70, Lemma 2] or [58, Section 2]. □

REMARK 3.2. In the exceptional case (3), if G contains an element whose determinant is not a square, then H contains a subgroup of index 2, which rules out $H \simeq \mathrm{A}_4$ and $H \simeq \mathrm{A}_5$. This applies when $G = G_E(\ell)$ arises from an elliptic curve E over a number field K that does not contain the quadratic subfield of the cyclotomic field $\mathbf{Q}(\zeta_\ell)$, which includes $K = \mathbf{Q}$.

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

3.1. Borel cases. In this section, we address subgroups of the Borel group $B(\ell)$ that contain an element of order ℓ (hence do not lie in $C_s(\ell)$), where ℓ is an odd prime.

LEMMA 3.3. *Let ℓ be an odd prime and let G be a subgroup of $B(\ell)$ that contains an element of order ℓ. Then G contains $t = \left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ and is equal to the internal semidirect product*

$$G = \langle t\rangle \rtimes (G \cap C_s(\ell)),$$

which is a direct product if and only if $G \cap C_s(\ell) \subseteq Z(\ell)$.

Proof. If G contains an element $g = \left(\begin{smallmatrix}a & b\\ 0 & d\end{smallmatrix}\right)$ of order divisible ℓ then $g^{\ell-1} = \left(\begin{smallmatrix}1 & x\\ 0 & 1\end{smallmatrix}\right)$ for some nonzero x, and for $ex \equiv 1 \pmod{\ell}$ we have $g^{e\ell-e} = t \in G$. For any $g = \left(\begin{smallmatrix}a & b\\ 0 & d\end{smallmatrix}\right)$, the product $gt^e = \left(\begin{smallmatrix}a & ae+d\\ 0 & d\end{smallmatrix}\right)$ is diagonal if and only if $e \equiv -d/a \pmod{\ell}$. Thus every coset of $\langle t\rangle$ in G contains a unique element of $H = G \cap C_s(\ell)$. Thus $G = \langle t\rangle \rtimes H$, since $\langle t\rangle$ is normal in G, and the action of H on $\langle t\rangle$ is trivial if and only if $H \subseteq Z(\ell)$. □

Formulas to count subgroups of a given finite abelian group are well-known; see [6], for example. In the case of interest here, the answer is particularly simple. The lemma below is a special case of [71, Theorem 4.1].

LEMMA 3.4. *Let n be a positive integer. There is a one-to-one correspondence between triples (a, b, i) with $a, b|n$ and $0 \leqslant i < \gcd(a, b)$ given by*

$$(a, b, i) \mapsto \langle (a, -a), (ic, d - ic)\rangle,$$

where $c = a/\gcd(a, b)$ and $d = n/b$. The total number of distinct subgroups of $\mathbf{Z}(n) \times \mathbf{Z}(n)$ is thus

$$\alpha(n) := \sum_{a,b|n} \gcd(a, b).$$

Proof. For each subgroup of $H \subseteq \mathbf{Z}(n) \times \mathbf{Z}(n)$ there is a triple (a, b, i) with $a, b|n$ and $0 \leqslant i < \gcd(a, b)$ determined by the generator $x = (a, -a)$ of the trace-zero subgroup $H_0 \subseteq H$, the order b of H/H_0, and the least $i \geqslant 0$ for which $y := (ia/\gcd(a, b),\ n/b - ia/\gcd(a, b)) \in H$. Conversely, each such triple (a, b, i) determines a subgroup $H = \langle x, y\rangle$; we thus have a bijection, and $\alpha(n)$ counts the triples (a, b, i). □

COROLLARY 3.5. *Let ℓ be an odd prime. The number of nonconjugate subgroups of $\mathbf{GL}_2(\ell)$ that lie in a Borel group and contain an element of order ℓ is $\alpha(\ell - 1)$, the number of subgroups of $C_s(\ell)$.*

Proof. It suffices to consider subgroups $G \subseteq B(\ell)$ containing $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ up to conjugation in $B(\ell)$, since $B(\ell)$ is selfnormalizing in $\mathbf{GL}_2(\ell)$. Every such G is normal in $B(\ell)$: the subgroup generated by $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ is normal and the $B(\ell)$-conjugates of $G \cap C_s(\ell)$ all lie in G. This gives a one-to-one correspondence between subgroups of $B(\ell)$ containing $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$, all of which are nonconjugate, and subgroups of $C_s(\ell) \simeq \mathbf{F}_\ell^\times \times \mathbf{F}_\ell^\times \simeq \mathbf{Z}(\ell-1) \times \mathbf{Z}(\ell-1)$. □

LEMMA 3.6. *Let ℓ be an odd prime. Let G and H be conjugate subgroups of $\mathbf{GL}_2(\ell)$ that lie in $C_s(\ell)$ and let $t = \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$. The groups $G' := \langle G, t\rangle$ and $H' := \langle H, t\rangle$ of $B(\ell)$ are locally conjugate in $\mathbf{GL}_2(\ell)$ and isomorphic.*

Proof. When $G = H$ the lemma clearly holds, so we assume $G \neq H$, in which case G and H are conjugate via $s = \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$. We have $G' = \langle t\rangle \rtimes G$ and $H' = \langle t\rangle \rtimes H$, by Lemma 3.3, and the bijection from G' to H' given by swapping diagonal entries preserves conjugacy classes (but is typically not a homomorphism); hence G' and H' are locally conjugate. Let $g \in G$ be an element with maximal projective order e, and let $z \in G$ be a generator for $G \cap Z(\ell)$ with order f; then $g^e = z^d$ for some integer $d \in [1, \ell-1]$. We have $gtg^{-1} = t^n$, where $n \in (\mathbf{Z}/\ell\mathbf{Z})^\times$ is the ratio of the diagonal entries of g, while z commutes with t and g. Thus G' is isomorphic to the abstract group

$$\mathcal{G} := \langle t, g, z : t^\ell = g^e z^{-d} = z^f = ztz^{-1}t^{-1} = zgz^{-1}g^{-1} = gtg^{-1}t^{-n} = 1\rangle.$$

We now note that t lies in H', and z generates $H' \cap Z(\ell)$. The element $h = sgs$ of H has maximal projective order e, with $h^e = z^d$, and $hth^{-1} = t^{1/n}$, where $1/n$ is the inverse of n and has order e in $(\mathbf{Z}/\ell\mathbf{Z})^\times$. The action of $h' = h^{e-1}$ on t is thus identical to that of g, and there exists a $z' \in H' \cap Z(\ell)$ of the same order f as z for which $(h')^e = (z')^d$. It follows that H' is also isomorphic to $\mathcal{G}$. □

REMARK 3.7. The situation in Lemma 3.6 is the only case where nonconjugate but locally conjugate subgroups can arise; see Corollary 3.30.

3.2. Cyclic cases.

We now consider the subgroups of $\mathbf{GL}_2(\ell)$ with cyclic image in $\mathbf{PGL}_2(\ell)$.

LEMMA 3.8. *Let $n = \prod_p p^{e_p}$ be a positive integer. The number of subgroups of $\mathbf{Z}(n) \times \mathbf{Z}(n)$ that are fixed by the automorphism $\sigma : (x, y) \mapsto (y, x)$ is*

$$\beta(n) := \beta_2(n) \prod_{p\neq 2} (e_p + 1)^2,$$

where $\beta_2(n) = 2(e_2^2 - e_2) + 3$ if n is even and $\beta_2(n) = 1$ if n is odd.

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

Proof. Let G be a subgroup of $\mathbf{Z}(n) \times \mathbf{Z}(n)$ fixed by σ. The automorphism σ fixes each p-Sylow subgroup of G, so it suffices to consider the case $\#G = p^e$. The map φ defined by $g \mapsto \sigma(g) - g$ is an endomorphism of G with kernel $D := \{(x, y) \in G : x = y\}$ and image contained in $T := \{(x, y) \in G : x + y = 0\}$.

If p is odd then $\varphi(G) = T$ and $D \cap T$ is trivial, so $G = D \times T$. Conversely, every product of a diagonal and trace-zero subgroup of $\mathbf{Z}(n) \times \mathbf{Z}(n)$ is fixed by σ, and there are $(e_p + 1)^2$ such subgroups.

For $p = 2$ we have $\beta(2) = 3$, and $\beta(2^{n+1}) = \beta(2^n) + 4n$, where the $4n$ new groups all have exponent 2^{n+1}: one is the full group, one is the even trace subgroup of index 2, two are index 4 subgroups $\langle(1, 1), (0, 4)\rangle$ and $\langle(1, -1), (0, 4)\rangle$, and four are subgroups of index 2^i, for i from 3 to $n + 1$, of the form $\langle(1, \pm 1), (0, 2^i)\rangle$, $\langle(1, 2^{i-1} \pm 1), (0, 2^i)\rangle$. The formula for $\beta_2(n)$ then follows by induction. □

REMARK 3.9. In terms of the bijection given by Lemma 3.4, the triples (a, b, i) that correspond to subgroups of $\mathbf{Z}(n) \times \mathbf{Z}(n)$ fixed by $\sigma\colon (x, y) \mapsto (y, x)$ are those for which the congruence $2ic \equiv d \pmod{a}$ has a solution, where $d = n/b$ and $c = a/\gcd(a, b)$. More generally, two triples (a, b, i) and (a, b, j) correspond to subgroups in the same σ-orbit if and only if $c(i + j) \equiv d \pmod{a}$ has a solution.

COROLLARY 3.10. *Let ℓ be an odd prime. The number of subgroups H of $C_s(\ell)$ that are normal in $C_s^+(\ell)$ is $\beta(\ell - 1)$.*

Proof. The split Cartan group $C_s(\ell) \simeq \mathbf{Z}(\ell - 1) \times \mathbf{Z}(\ell - 1)$ is abelian of index 2 in its normalizer $C_s^+(\ell) = \langle C_s(\ell), s\rangle$, where $s = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. It follows that a subgroup H of $C_s(\ell)$ is normal in $C_s^+(\ell)$ if and only if it is fixed under conjugation by s, which acts on H by swapping the diagonal entries of each element. □

COROLLARY 3.11. *Let ℓ be an odd prime. The number of nonconjugate subgroups of $\mathbf{GL}_2(\ell)$ that lie in a split Cartan group is*

$$\frac{\alpha(\ell - 1) + \beta(\ell - 1)}{2}.$$

Proof. It suffices to count $\mathbf{GL}_2(\ell)$-conjugacy classes of subgroups of $C_s(\ell)$, and it is enough to consider $C_s^+(\ell)$ conjugacy classes, since $C_s^+(\ell)$ is the normalizer of $C_s(\ell)$. The orbit of each subgroup $G \subseteq C_s(\ell)$ under conjugation by $C_s^+(\ell)$ has order 1 or 2, depending on whether G is fixed by the action of $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, which swaps the diagonal entries. The counting formula then follows from Corollary 3.4 and Lemma 3.8. □

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

LEMMA 3.12. *Let ℓ be an odd prime. The number of nonconjugate subgroups of* $\mathbf{GL}_2(\ell)$ *that lie in a nonsplit Cartan group is* $\tau(\ell^2-1)$, *where* $\tau(n)$ *counts the positive divisors of* n.

Proof. This is clear: $C_{ns}(\ell) \simeq \mathbf{F}_{\ell^2}^\times$ is cyclic of order ℓ^2-1 and therefore contains a subgroup of order n for each divisor n of ℓ^2-1, none of which are conjugate. □

3.3. Dihedral cases. We now address the subgroups of $\mathbf{GL}_2(\ell)$ with dihedral image in $\mathbf{PGL}_2(\ell)$; as above we assume that ℓ is an odd prime and recall that we consider the Klein group to be dihedral.

If G is a subgroup of $\mathbf{GL}_2(\ell)$ with dihedral image in $\mathbf{PGL}_2(\ell)$, then G lies in the normalizer C^+ of a Cartan group C and it contains the abelian subgroup $H = G\cap C$ with index 2. Let $Z = G \cap Z(\ell) \subseteq H$ denote the scalar subgroup of G. The subgroup H is normal in G and in C, hence in $C^+ = GC$, and it follows that each nonscalar element h of H has a distinct conjugate $\bar{h} \in H$; indeed, $\bar{h} = \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)h\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$ if $C = C_s(\ell)$ and $\bar{h} = \left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right)h\left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right)$ if $C = C_{ns}(\ell)$). To better understand the relationship between G and H we consider the following maps:

$$\begin{aligned} H &\to Z & \qquad (G-H) &\to Z \\ h &\mapsto h\bar{h} = \begin{pmatrix}\det h & 0\\ 0 & \det h\end{pmatrix} & g &\mapsto g^2 = \begin{pmatrix}-\det g & 0\\ 0 & -\det g\end{pmatrix}. \end{aligned}$$

There are two possibilities, depending on whether the set $\det(H)$ and the set

$$-\det(G-H) := \{-\det g : g \in G-H\} \subseteq \mathbf{GL}_1(\ell)$$

coincide or not.

LEMMA 3.13. *Let ℓ be an odd prime. Let G be a subgroup of* $\mathbf{GL}_2(\ell)$ *with dihedral image in* $\mathbf{PGL}_2(\ell)$ *that lies in the normalizer C^+ of a Cartan group C, let $H = G \cap C$, and let $Z = G \cap Z(\ell)$. Then H is normal in C^+ and one of the following holds:*

(2a) $\det(H)$ *and* $-\det(G-H)$ *coincide, in which case* $G = \langle H, \gamma\rangle$ *for some* $\gamma \in G - H$ *with* $\det\gamma = -1$.

(2b) $\det(H)$ *and* $-\det(G-H)$ *are disjoint, in which case* $\det(H) = \det(Z)$ *and* H *contains* -1.

If G' is another subgroup of C^+ with dihedral image in $\mathbf{PGL}_2(\ell)$ *with $H = G'\cap C$ and* $-\det(G'-H) = -\det(G-H)$, *then G and G' are conjugate in C^+.*

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

Proof. We have $[G : H] = 2$, so H is normal in G, and its normalizer in C^+ contains the abelian group C and is therefore equal to C^+; so H is normal in C^+.

If $\det(H)$ and $-\det(G - H)$ intersect then we may pick $g \in G - H$ and $h \in H$ so $\gamma = g/h \in G - H$ has $\det \gamma = -1$. Then $G - H = \gamma H$ and $\det(H) = -\det(G - H)$.

Otherwise, $\det(H)$ and $-\det(G-H)$ are disjoint. The image of $H \to Z$ is then an even index subgroup of Z, and its index is at most 2, since the image of the subgroup $Z \subseteq H$ has index 2. It follows that $\det(H) = \det(Z)$ corresponds to an index 2 subgroup of Z, and since Z has even order, it contains -1.

Now suppose G' is another subgroup of C^+ with dihedral image in $\mathbf{PGL}_2(\ell)$ for which $H = G' \cap C$ and $-\det(G' - H) = -\det(G - H)$. In case (2a) we have $G' = \langle H, \gamma' \rangle$ for some $\gamma' \in G - H$ with $\det \gamma' = -1$, and then γ' is conjugate to γ in C^+, and therefore $G' = \langle H, \gamma' \rangle$ is conjugate to $G = \langle H, \gamma \rangle$. In case (2b) the image of $(G - H) \to Z$ is the nontrivial coset of $\mathrm{im}(h \mapsto h\bar{h})$ in Z, thus we may pick $\left(\begin{smallmatrix} z & 0 \\ 0 & z \end{smallmatrix}\right) \in Z$ that is the square of some $\gamma \in G - H$ with $\det \gamma = -z$. There must then be a $\gamma' \in G' - H$ with $\det \gamma' = -z$ that is conjugate to γ in C^+, and therefore $G' = \langle H, \gamma' \rangle$ is conjugate to $G = \langle H, \gamma \rangle$. □

REMARK 3.14. For an elliptic curve E over a number field with a real embedding, the group $G_E(\ell)$ necessarily contains an element γ with $\operatorname{tr} \gamma = 0$ and $\det \gamma = -1$ corresponding to complex conjugation. This implies $G_E(\ell) \not\subseteq C_{ns}(\ell)$ for $\ell > 2$ (although $G_E(\ell) \subseteq C_s(\ell)$ is possible). Indeed, $C_{ns}(3)$ is the unique subgroup $G \subseteq \mathbf{GL}_2(3)$ with $\det(G) = \mathbf{F}_3^\times$ that does not arise for any elliptic curve $E/\mathbf{Q}$; the corresponding modular curve $X_{ns}(3)$ has genus zero but no noncuspidal rational points.

REMARK 3.15. For composite m and elliptic curves E over a number field with a real embedding, the criterion that $G_E(m)$ contains an element γ with $\operatorname{tr} \gamma = 0$ and $\det \gamma = -1$ is necessary but not sufficient. A stronger criterion is that γ must also fix an order-m element of $\mathbf{Z}(m) \times \mathbf{Z}(m)$. When m is prime this is already implied by $\operatorname{tr} \gamma = 0$ and $\det \gamma = -1$, but not in general. This explains why, for example, $G_E(4) \neq \left\langle \left(\begin{smallmatrix} 1 & 2 \\ 2 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 3 & 0 \\ 0 & 3 \end{smallmatrix}\right) \right\rangle$ for any elliptic curve $E/\mathbf{Q}$, even though this group contains an element γ with $\operatorname{tr} \gamma = 0$ and $\det \gamma = -1$. As in the previous remark, the corresponding modular curve has genus 0 but no noncuspidal rational points. More generally, the ten pointless conics noted in [52] that are models of modular curves associated to subgroups of $\mathbf{GL}_2(2^n)$ lack rational points for this reason.

The following lemma determines the cases in which $\mathbf{GL}_2(\ell)$-conjugate subgroups of the normalizer C^+ of a Cartan group C have intersections with C that are not $\mathbf{GL}_2(\ell)$-conjugate. This can occur only when C is a split Cartan group with $\ell \equiv 1 \pmod 4$ and the projective images of the subgroups are isomorphic to the Klein group of order 4.

LEMMA 3.16. *Let ℓ be an odd prime. Let G_1 and G_2 be $\mathbf{GL}_2(\ell)$-conjugate subgroups of the normalizer C^+ of a Cartan group C with dihedral images in $\mathbf{PGL}_2(\ell)$ such that $H_1 := G_1 \cap C$ and $H_2 := G_2 \cap C$ are not conjugate in $\mathbf{GL}_2(\ell)$. Then C is a split Cartan group, $\ell \equiv 1 \pmod 4$, $|\pi(G_1)| = |\pi(G_2)| = 4$, $Z := \langle\left(\begin{smallmatrix} z & 0 \\ 0 & z\end{smallmatrix}\right)\rangle := G_1 \cap Z(\ell)$ contains -1 with $z = x^2$ square, and*

$$\{H_1, H_2\} = \left\{\left\langle\begin{pmatrix} x & 0 \\ 0 & -x\end{pmatrix}\right\rangle, \left\langle\begin{pmatrix} z & 0 \\ 0 & z\end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1\end{pmatrix}\right\rangle\right\}.$$

Conversely, whenever $\ell \equiv 1 \pmod 4$ there is a pair of conjugate G_1 and G_2 as above for each scalar subgroup $\langle\left(\begin{smallmatrix} z & 0 \\ 0 & z\end{smallmatrix}\right)\rangle$ that contains -1 with z square.

Proof. Let $G_2 = gG_1g^{-1}$, let $Z := \langle\left(\begin{smallmatrix} z & 0 \\ 0 & z\end{smallmatrix}\right)\rangle = G_1 \cap Z(\ell) = G_2 \cap Z(\ell)$, and choose $h_1 \in H_1$ so that $H_1 = \langle h_1, Z\rangle$. The group H_1 is normal in C, and thus contains all the $\mathbf{GL}_2(\ell)$-conjugates of h_1 that lie in C, none of which lie in H_2 (otherwise H_1 and H_2 would coincide). Thus $\gamma_2 := gh_1g^{-1}$ lies in $G_2 - H_2$, and therefore both h_1 and γ_2 have trace zero, and we can similarly choose $h_2 \in H_2$ so that $\gamma_1 := g^{-1}h_2g$ lies in $G_1 - H_1$. We then have $G_1 = \langle h_1, \gamma_1, Z\rangle$ and $G_2 = \langle h_2, \gamma_2, Z\rangle$ with $h_1, h_2, \gamma_1, \gamma_2$ all elements of trace zero and order 2 in $\mathbf{PGL}_2(\ell)$, thus $\pi(G_1)$ and $\pi(G_2)$ are both isomorphic to the Klein group. And Z must contain $-1 = h_1\bar{h}_1^{-1} = h_2\bar{h}_2^{-1}$.

Since H_1 and H_2 are nonconjugate we must have $\det h_1 \neq \det h_2$ (no matter which h_1 and h_2 we pick); thus, one of them is cyclic, say H_1, and the other, H_2, is not. This rules out the nonsplit Cartan case, so we now assume $C = C_s(\ell)$. We can assume h_1^2 generates Z, so z must be square, and we can assume $h_1 = \left(\begin{smallmatrix} x & 0 \\ 0 & -x\end{smallmatrix}\right)$; and we must have $h_2^2 = h^2$ for some scalar $h \in Z$, so we can assume $h_2 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1\end{smallmatrix}\right)$.

Since γ_1 is conjugate to h_2 and γ_2 is conjugate to h_1, we may assume that $G_1 = \langle\left(\begin{smallmatrix} x & 0 \\ 0 & -x\end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0\end{smallmatrix}\right)\rangle$ and $G_2 = \langle\left(\begin{smallmatrix} z & 0 \\ 0 & z\end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1\end{smallmatrix}\right), \left(\begin{smallmatrix} 0 & x \\ x & 0\end{smallmatrix}\right)\rangle$; this shows whenever $\ell \equiv 1 \pmod 4$, for each square $z \in \mathbf{Z}(\ell)^\times$ of even order we can construct conjugate G_1 and G_2 with H_1 and H_2 nonconjugate as above. □

COROLLARY 3.17. *Let ℓ be an odd prime, let $\gamma = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1\end{smallmatrix}\right)$, and let δ generate $C_{ns}(\ell)$. For each subgroup $H \subseteq C_{ns}(\ell)$ not in $Z(\ell)$ the group $G_1 := \langle H, \gamma\rangle \subseteq C_{ns}^+(\ell)$ has dihedral image in $\mathbf{PGL}_2(\ell)$ and satisfies $H = G_1 \cap C_{ns}(\ell)$ with* $\det(H) = -\det(G_1 - H)$. *If H satisfies* $\det(H) = \det(H \cap Z(\ell))$ *and $-1 \in H$, then for $e := [Z(\ell)\colon H \cap Z(\ell)]$, the group $G_2 := \langle H, \gamma\delta^e\rangle \subseteq C_{ns}^+(\ell)$ has dihedral image in $\mathbf{PGL}_2(\ell)$ and satisfies $H = G_2 \cap C_{ns}(\ell)$ with* $\det(H)$ *and* $-\det(G_2 - H)$ *disjoint. Up to conjugacy in $\mathbf{GL}_2(\ell)$, this accounts for all subgroups that lie in the normalizer of a nonsplit Cartan group and have dihedral image in $\mathbf{PGL}_2(\ell)$,*

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

of which there are

$$\tau(\ell^2-1)-\tau(\ell-1)+\tau\left(\frac{\ell^2-1}{4}\right)-\tau\left(\frac{\ell-1}{2}\right).$$

Proof. It is clear that G_1 and G_2 both have dihedral image in $\mathbf{PGL}_2(\ell)$ and intersect $C_{ns}(\ell)$ in H, since γ and γr^e both lie in $C_{ns}^+(\ell)$ but not $C_{ns}(\ell)$ and their squares lie in $H\cap Z(\ell)$. For G_1 it is clear that $\det(H)=-\det(G_1-H)$, and for G_2 we note that $(\gamma\delta^e)^2$ generates $H\cap Z(\ell)$, by construction, and if $\det(H)=\det(H\cap Z(\ell))$ then $-\det(\gamma r^e)\not\in\det(H)$, and by Lemma 3.13, the sets $\det(H)$ and $-\det(G_2-H)$ must then be disjoint.

Every subgroup $H\subseteq C_{ns}(\ell)$ is normal in $C_{ns}^+(\ell)$ and has no nontrivial $\mathbf{GL}_2(\ell)$-conjugates in $C_{ns}^+(\ell)$. It follows from Lemmas 3.13 and 3.16 that up to conjugacy in $\mathbf{GL}_2(\ell)$, each G_1, G_2 arises for exactly one H.

The first two terms in the formula count subgroups $H\subseteq C_{ns}(\ell)$ not in $Z(\ell)$. Among these, those that satisfy $\det(H)=\det(H\cap Z(\ell))$ and $-1\in H$ are precisely those that lie in the index 2 subgroup of $C_{ns}(\ell)$ (squares) and contain a subgroup of order 2, which accounts for the last two terms in the formula. □

The split dihedral case is slightly more complicated due to the fact that $C_s(\ell)$ contains subgroups H that are not normal in $C_s^+(\ell)$, and Lemma 3.16 implies that even when H is normal in $C_s^+(\ell)$ it may have distinct $\mathbf{GL}_2(\ell)$-conjugates that also lie in $C_s^+(\ell)$.

COROLLARY 3.18. *Let ℓ be an odd prime, let $\gamma=\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$, and let $\delta\in C_s(\ell)$ be a coset representative of a generator for $C_s(\ell)/(C_s(\ell)\cap\mathbf{SL}_2(\ell))$. For each subgroup $H\subseteq C_s(\ell)$ not in $Z(\ell)$ that is normal in $C_s^+(\ell)$, the group $G_1=\langle H,\gamma\rangle\subseteq C_s^+(\ell)$ satisfies $H=G_1\cap C_s(\ell)$ with $\det(H)=-\det(G_1-H)$. If H satisfies $\det(H)=\det(H\cap Z(\ell))$ and $-1\in H$, then for $e:=[Z(\ell):H\cap Z(\ell)]$, the group $G_2:=\langle H,\gamma\delta^e\rangle\subseteq C_s^+(\ell)$ satisfies $H=G_2\cap C_s(\ell)$ with $\det(H)$ and $-\det(G_2-H)$ disjoint. Up to conjugacy in $\mathbf{GL}_2(\ell)$, this accounts for all subgroups that lie in the normalizer of a split Cartan group and have dihedral image in $\mathbf{PGL}_2(\ell)$, of which there are*

$$\beta(\ell-1)-\tau(\ell-1)+\tau\left(\frac{\ell-1}{2}\right)^2-\tau\left(\frac{\ell-1}{2}\right)-\frac{1}{2}\left(1+\left(\frac{-1}{\ell}\right)\right)\tau\left(\frac{\ell-1}{4}\right).$$

Proof. The argument that G_1 and G_2 have the claimed properties is identical to that in the proof of Corollary 3.17, as is the argument that they are uniquely determined by H.

The first two terms in the formula count the normal subgroups H of $C_s(\ell)$ not in $Z(\ell)$, via Corollary 3.10, each of which gives rise to a G_1; these G_1 are all nonconjugate so long as we are not in the exceptional case of Lemma 3.16.

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

The last term in the formula is a correction factor for double counting the exceptional cases.

The third and fourth terms in the formula account for subgroups H that satisfy $\det(H) = \det(H \cap Z(\ell))$ and $-1 \in H$. To see this, note that in the proof of Lemma 3.8, adding the restriction $\det(H) = \det(H \cap Z(\ell))$ replaces the factor $\beta_2(n)$ with $(e_2+1)^2$ and the modified formula for $\beta(n)$ is then $\tau(n)^2$; using $n = (\ell-1)/2$ accounts for the constraint $-1 \in H$. Each such H gives rise to a G_2, and these are all nonconjugate. □

LEMMA 3.19. *Let ℓ be an odd prime and let G be a subgroup of $\mathbf{GL}_2(\ell)$ with dihedral image in $\mathbf{PGL}_2(\ell)$. Then G is contained in both the normalizer of a split Cartan group and the normalizer of a nonsplit Cartan group if and only if G is conjugate to a subgroup of the form*

$$H_z := \left\langle \begin{pmatrix} 0 & 1 \\ z & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\rangle,$$

where $z \in \mathbf{Z}(\ell)^\times$ is not a square, in which case the image of G in $\mathbf{PGL}_2(\ell)$ is the Klein group of order 4. There is exactly one such H_z for each odd divisor of $\ell - 1$.

Proof. Every nonscalar element of G lies in the nontrivial coset of a subgroup of a Cartan group in its normalizer, hence has trace zero and order 2 in $\mathbf{PGL}_2(\ell)$. It follows that the image of G in $\mathbf{PGL}_2(\ell)$ has order 4, and we have $G = \langle g_1, g_2 \rangle$ with $\operatorname{tr} g_1 = \operatorname{tr} g_2 = 0$, and $\det g_1$ square, while $\det g_2$ is not square.

If $\ell \equiv 1 \pmod 4$, then after multiplication by a scalar, we can assume $\det g_1 = -1$, and G is then conjugate to $H_z \subseteq C_s^+(\ell)$ via an action that sends g_1 to $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ and g_2 to $\left(\begin{smallmatrix} 0 & 1 \\ z & 0 \end{smallmatrix}\right)$, with $z = -\det g_2$ not a square.

If $\ell \equiv 3 \pmod 4$, then after multiplication by a scalar we can assume $\det g_2 = -1$ and G is then conjugate to $H_z \subseteq C_{ns}^+(\ell)$ via an action that sends g_2 to $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ and g_1 to $\left(\begin{smallmatrix} 0 & 1 \\ z & 0 \end{smallmatrix}\right)$, with $z = -\det g_1$ not a square.

Conversely, for each nonsquare $z \in \mathbf{Z}(\ell)^\times$ the subgroup H_z lies in $C_s^+(\ell) \cap C_{ns}^+(\ell)$ and has dihedral image in $\mathbf{PGL}_2(\ell)$. If we fix a generator r for $\mathbf{Z}(\ell)^\times$, the distinct groups H_z that can arise are precisely those with $z = r^e$, where e is an odd divisor of $\ell - 1$. □

REMARK 3.20. Not every $G \subseteq \mathbf{GL}_2(\ell)$ with projective image isomorphic to the Klein group is contained in both the normalizer of a split Cartan group and the normalizer of a nonsplit Cartan group; this occurs if and only if G contains elements g, h with $\chi(g) = 1$ and $\chi(h) = -1$.

3.4. Exceptional cases.

We now consider the exceptional case (3) of Proposition 3.1. In all of these cases the group $G \subseteq \mathbf{GL}_2(\ell)$ is determined up to conjugacy by three criteria: the isomorphism class of its image in $\mathbf{PGL}_2(\ell)$, the cardinality of its scalar subgroup $Z := G \cap Z(\ell)$, and the index $[\det(G) : \det(Z)]$.

LEMMA 3.21. *Let $\ell \geqslant 5$ be prime, and suppose that G is a subgroup of $\mathbf{GL}_2(\ell)$ with projective image isomorphic to $H \in \{\mathrm{A}_4, \mathrm{S}_4, \mathrm{A}_5\}$ and scalar subgroup $Z := G \cap Z(\ell)$ containing -1.*

(3a) *If $H = \mathrm{A}_4$ then one of the following holds:*

- (i) $[\det(G) : \det(Z)] = 1$.
- (ii) $[\det(G) : \det(Z)] = 3$ *and* $\ell \equiv 1 \pmod 3$ *with* $[Z(\ell) : Z]$ *divisible by* 3.

(3b) *If $H = \mathrm{S}_4$ then one of the following holds:*

- (i) $[\det(G) : \det(Z)] = 1$ *and* $\ell \equiv \pm 1 \pmod 8$.
- (ii) $[\det(G) : \det(Z)] = 2$ *and* $\ell \equiv 1 \pmod 8$ *with* $[Z(\ell) : Z)]$ *divisible by* 2.
- (iii) $[\det(G) : \det(Z)] = 2$ *and* $\ell \equiv 3 \pmod 8$.
- (iv) $[\det(G) : \det(Z)] = 2$ *and* $\ell \equiv 5 \pmod 8$ *with* $\#Z$ *divisible by* 4.

(3c) *If $H = \mathrm{A}_5$ then* $[\deg(G) : \det(Z)] = 1$ *and* $\ell \equiv \pm 1 \pmod 5$.

Moreover, every case listed above arises for exactly one conjugacy class of subgroups G in $\mathbf{GL}_2(\ell)$.

Proof. The lemma follows from the classification in [28]; see Theorems 5.5, 5.8, and 5.11. It can also be derived from the analysis in [1, Section 5.2]. □

The explicit classification of primitive subgroups of $\mathbf{GL}_2(\ell)$ in [28] also provides a method for constructing a subgroup $G \subseteq \mathbf{GL}_2(\ell)$ that satisfies Lemma 3.21 for given values of H, Z, and $[\det(G) : \det(Z)]$, whenever such a G exists (if it exists, it is unique up to conjugacy, by the previous lemma). The complexity of this algorithm is important to what follows, so we give it in detail and then bound its complexity. The construction given in [28] gives generators for a subgroup $\tilde{G}$ of $\mathbf{GL}_2(\mathbf{F}_{\ell^2})$ that is conjugate to our desired $G \subseteq \mathbf{GL}_2(\ell)$; we then use the algorithm of [33] to efficiently conjugate $\tilde{G}$ to G.

ALGORITHM 1. Given a prime $\ell \geqslant 5$, a group $H \in \{\mathrm{A}_4, \mathrm{S}_4, \mathrm{A}_5\}$, a subgroup $Z \subseteq \mathbf{Z}(\ell)$ containing -1 generated by λ, and $i \in \{1, 2, 3\}$, output generators for a group $G \subseteq \mathbf{GL}_2(\ell)$ with projective image isomorphic to H, and scalar subgroup $Z \subseteq Z(\ell)$ such that $[\det(G) : \det(Z)] = i$, or report that no such G exists.

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

1. Let $\omega \in \mathbf{F}_{\ell^2}$ be a primitive fourth root of unity, let $s := \frac{1}{2}\begin{pmatrix} \omega-1 & \omega-1 \\ \omega+1 & -(\omega+1) \end{pmatrix}$, and let $t := \begin{pmatrix} \omega & 0 \\ 0 & -\omega \end{pmatrix}$.

2. If $H = \mathrm{A}_4$ then

- **a.** If $i = 1$ let $\tilde{G} := \langle s, t, \lambda \rangle$.
- **b.** If $i = 3$ and $\ell \equiv 1 \pmod 3$ with $3 | [Z(\ell) : Z]$ let $\tilde{G} := \langle \mu s, t, \lambda \rangle$ where $\mu \in Z(\ell) - Z$ satisfies $\mu^3 = \lambda$.
- **c.** Otherwise, report that no such G exists and terminate.

3. If $H = \mathrm{S}_4$ then

- **a.** Let $\alpha \in \mathbf{F}_{\ell^2}$ be a square root of 2 and let $u := \begin{pmatrix} 1+\omega & 0 \\ 0 & 1-\omega \end{pmatrix}$.
- **b.** If $i = 1$ and $\ell \equiv \pm 1 \pmod 8$ let $\tilde{G} := \langle s, \frac{u}{\alpha}, \lambda \rangle$.
- **c.** If $i = 2$ and $\ell \equiv 1 \pmod 8$ with $[Z(\ell) : Z]$ even, let $\tilde{G} := \langle s, \frac{\mu}{\alpha} u, \lambda \rangle$ where $\mu \in Z(\ell)$ satisfies $\mu^2 = \lambda$.
- **d.** If $i = 2$ and $\ell \equiv 3 \pmod 8$ let $\tilde{G} := \langle s, \frac{\mu}{\alpha} u, \lambda \rangle$ where $\mu \in Z(\ell)$ satisfies $\mu^2 = \lambda$.
- **e.** If $i = 2$ and $\ell \equiv 5 \pmod 8$ with $4 | \#Z$, let $\tilde{G} := \langle s, \frac{\mu}{\alpha} u, \lambda \rangle$ where $\frac{\mu}{\alpha} \in Z(\ell)$ satisfies $(\frac{\mu}{\alpha})^2 = \frac{\lambda}{2}$
- **f.** Otherwise, report that no such G exists and terminate.

4. If $H = \mathrm{A}_5$ then

- **a.** If $i = 1$ and $\ell \equiv \pm 1 \pmod 5$ then let $v := \frac{1}{4}\begin{pmatrix} 2\omega & 1-\beta-\omega-\beta\omega \\ \beta-1-\omega-\beta\omega & -2\omega \end{pmatrix}$ and let $\tilde{G} := \langle s, t, v, \lambda \rangle$.
- **b.** Otherwise, report that no such G exists and terminate.

5. By solving a linear system in 4 variables and at most 16 equations, construct a matrix $C \in \mathbf{GL}_2(\mathbf{F}_{\ell^2})$ for which $gC = Cg^{\sigma}$ holds for all $g \in \tilde{G}$, where $\langle \sigma \rangle = \mathrm{Gal}(\mathbf{F}_{\ell^2}/\mathbf{F}_{\ell})$.

6. Generate random matrixes $X \in \mathbf{M}_2(\mathbf{F}_{\ell^2})$ until $A := X + CX$ is invertible.

7. Output $G := A^{-1}\tilde{G}A \subseteq \mathbf{GL}_2(\ell)$ and terminate.

The last 3 steps of Algorithm 1 implement a special case of the probabilistic (Las Vegas) algorithm in [33] which, given a subgroup $\tilde{G}$ of $\mathbf{GL}_r(\mathbf{F}_{p^n})$, finds a conjugate subgroup G in $\mathbf{GL}_r(\mathbf{F}_{p^m})$ with $m|n$ minimal. The correctness of Algorithm 1, including the fact that a subgroup $G \subseteq \mathbf{GL}_2(\ell)$ conjugate to $\tilde{G} \subseteq \mathbf{GL}_2(\mathbf{F}_{\ell^2})$ necessarily exists, is guaranteed by [28, Theorems 5.5, 5.8, and 5.11]. We now analyze its complexity.

PROPOSITION 3.22. *The expected running time of Algorithm 1 is* $O(\mathsf{M}(\log \ell)\log \ell)$.

Proof. Using standard probabilistic root-finding algorithms we can find the roots of any polynomial of bounded degree over $\mathbf{F}_\ell$ or $\mathbf{F}_{\ell^2}$ in $O(\mathsf{M}(\log \ell)\log \ell)$ expected time [32]. Every other operation in Algorithm 1 takes $O(\mathsf{M}(\log \ell))$ time, including the linear algebra in step 5, since the dimensions of the system are bounded. The expected number of random matrixes needed in step 6 is at most 4; see [33, page 1707]. □

3.5. Counting and enumerating subgroups. As a result of our classification we can now count the number of subgroups of $\mathbf{GL}_2(\ell)$ up to conjugacy. For $\ell = 2$ there are four nonconjugate subgroups of $\mathbf{GL}_2(2)$, namely, $C_s(2)$, $C_{ns}(2)$, $B(2)$, and $\mathbf{GL}_2(2) = \mathbf{SL}_2(2)$. For primes $\ell > 2$, every subgroup of $\mathbf{GL}_2(\ell)$ is conjugate to at least one of the groups enumerated below. The 11 cases that appear are disjoint except for C_s and C_{ns}, which intersect in Z, and C_s^+ and C_{ns}^+, which intersect in $C_{s\cap ns}^+$. Other than these intersections all of the groups listed are nonconjugate in $\mathbf{GL}_2(\ell)$.

We thus obtain an explicit formula for the number of nonconjugate subgroups of $\mathbf{GL}_2(\ell)$ by summing the formulas for the 11 listed cases with the counts for Z and $C_s \cap C_{ns}^+$ negated. Table 2 lists this data for odd primes $\ell < 200$ along with several larger primes. These formulas can easily be adapted to count subgroups of $\mathbf{SL}_2(\ell)$ instead.

$\mathbf{SL}_2$: $\tau(\ell-1)$ subgroups that contain $\mathbf{SL}_2(\ell)$;

B: $\alpha(\ell-1)$ subgroups of $B(\ell)$ that contain an element of order ℓ;

C_s: $\frac{1}{2}\big(\alpha(\ell-1)+\beta(\ell-1)\big)$ subgroups of $C_s(\ell)$;

C_{ns}: $\tau(\ell^2-1)$ subgroups of $C_{ns}(\ell)$;

Z: $\tau(\ell-1)$ subgroups of $C_s(\ell)\cap C_{ns}(\ell) = Z(\ell)$;

C_s^+: $\beta(\ell-1)-\tau(\ell-1)+\tau\big(\frac{\ell-1}{2}\big)^2-\tau\big(\frac{\ell-1}{2}\big)-\frac{1}{2}\big(1+\big(\frac{-1}{\ell}\big)\big)\tau\big(\frac{\ell-1}{4}\big)$ subgroups of $C_s^+(\ell)$ not in $C_s(\ell)$;

C_{ns}^+: $\tau(\ell^2-1)-\tau(\ell-1)+\tau\big(\frac{\ell^2-1}{4}\big)-\tau\big(\frac{\ell-2}{2}\big)$ subgroups of $C_{ns}^+(\ell)$ not in $C_{ns}(\ell)$;

$C_{s\cap ns}^+$: $\tau\big((\ell-1)/2^{v_2(\ell-1)}\big)$ subgroups of $C_s^+(\ell)\cap C_{ns}^+(\ell)$ not in $C_s(\ell)$ or $C_{ns}(\ell)$;

A_4: $\tau\big(\frac{\ell-1}{2}\big)+\frac{1}{2}(1+(\frac{-3}{\ell})\tau\big(\frac{\ell-1}{6}\big)$ subgroups $G \not\supseteq \mathbf{SL}_2(\ell)$ with $\pi(G)\simeq \mathrm{A}_4$;

S_4: $\big(1-\frac{1}{4}\big(1-\big(\frac{2}{p}\big)\big)\big(1-\big(\frac{-1}{p}\big)\big)\big)\tau\big(\frac{\ell-1}{2}\big)+\frac{1}{2}\big(1+\big(\frac{-1}{p}\big)\big)\tau\big(\frac{\ell-1}{4}\big)$ subgroups $G \not\supseteq \mathbf{SL}_2(\ell)$ with $\pi(G)\simeq \mathrm{S}_4$;

A_5: $\frac{1}{2}\big(1+\big(\frac{5}{p}\big)\tau\big(\big(\frac{\ell-1}{2}\big)\big)$ subgroups $G \not\supseteq \mathbf{SL}_2(\ell)$ with $\pi(G)\simeq \mathrm{A}_5$.

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

Table 2. Subgroups of $\mathbf{GL}_2(\ell)$ up to conjugacy. See Section 3.5 for an explanation of the column headings.

ℓ	$\mathbf{SL}_2$	B	C_s	C_{ns}	Z	C_s^+	C_{ns}^+	C_{sns}^+	A_4	S_4	A_5	$\mathbf{GL}_2$
3	2	5	4	4	2	1	3	1	0	0	0	16
5	3	15	11	8	3	5	7	1	2	1	0	48
7	4	30	21	10	4	10	10	2	3	2	0	84
11	4	40	26	16	4	10	18	2	2	2	2	114
13	6	90	59	16	6	32	14	2	6	2	0	217
17	5	83	55	18	5	31	21	1	4	7	0	218
19	6	115	71	24	6	27	27	3	5	3	3	272
23	4	70	41	20	4	10	26	2	2	2	0	169
29	6	150	89	32	6	32	38	2	4	2	4	349
31	8	240	144	28	8	52	36	4	6	4	4	510
37	9	345	204	24	9	81	21	3	10	3	0	685
41	8	296	178	40	8	78	50	2	6	10	6	662
43	8	300	174	32	8	52	36	4	6	4	0	600
47	4	130	71	24	4	10	34	2	2	2	0	271
53	6	240	134	32	6	32	38	2	4	2	0	480
59	4	160	86	32	4	10	42	2	2	2	2	334
61	12	720	416	32	12	152	28	4	12	4	8	1368
67	8	420	234	32	8	52	36	4	6	4	0	780
71	8	400	224	60	8	52	84	4	4	4	4	828
73	12	851	493	30	12	189	27	3	15	15	0	1617
79	8	480	264	48	8	52	68	4	6	4	4	922
83	4	220	116	32	4	10	42	2	2	2	0	422
89	8	518	289	60	8	78	82	2	6	10	6	1047
97	12	1062	617	42	12	242	50	2	15	18	0	2044
101	9	675	369	48	9	81	57	3	6	3	6	1242
103	8	600	324	40	8	52	52	4	6	4	0	1074
107	4	280	146	32	4	10	42	2	2	2	0	512
109	12	1140	626	64	12	152	76	4	14	4	8	2080
113	10	830	469	48	10	148	62	2	8	14	0	1577
127	12	1150	629	54	12	126	78	6	10	6	0	2047
131	8	640	344	64	8	52	84	4	4	4	4	1192
137	8	740	400	40	8	78	50	2	6	10	0	1322
139	8	780	414	64	8	52	84	4	6	4	4	1404
149	6	600	314	48	6	32	62	2	4	2	4	1064
151	12	1350	729	60	12	126	78	6	9	6	6	2358
157	12	1440	776	32	12	152	28	4	12	4	0	2440
163	10	1185	630	40	10	85	45	5	9	5	0	1994
167	4	430	221	40	4	10	58	2	2	2	0	761

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

Table 2. *Continued.*

173	6	690	359	32	6	32	38	2	4	2	0	1155
179	4	460	236	48	4	10	66	2	2	2	2	824
181	18	2760	1506	96	18	360	114	6	20	6	12	4868
191	8	880	464	64	8	52	100	4	4	4	4	1568
193	14	2202	1227	32	14	360	30	2	18	22	0	3889
197	9	1125	594	72	9	81	93	3	6	3	0	1971
199	12	1610	859	90	12	126	126	6	10	6	6	2827
10^3+9	30	19090	10031	144	30	1476	186	6	40	42	24	31027
10^4+7	4	25030	12521	60	4	10	90	2	2	2	0	37713
10^5+3	16	715200	357696	128	16	232	168	8	12	8	0	1073436
10^6+3	8	5000100	2500074	96	8	52	132	4	6	4	0	7500460

REMARK 3.23. From the formulas for $\alpha(n)$ and $\beta(n) \leqslant \alpha(n)$, and the bound $\tau(n) = 2^{O(\log n/\log\log n)} = n^{o(1)}$, one may deduce that the number of subgroups of $\mathbf{GL}_2(\ell)$ is quasilinear in ℓ. Indeed, the lower bound $\alpha(n) = \Omega(n)$ is immediate, and the upper bound $\alpha(n) = O(n \log\log\log n)$ is easy to prove.

We now give an efficient Las Vegas algorithm to enumerate the subgroups of $\mathbf{GL}_2(\ell)$ up to conjugacy. It outputs a short list of $O(1)$ generators for each subgroup and has a total expected running time that is quasilinear in ℓ, hence in the size of its output.

ALGORITHM 2. Given a prime ℓ, output a list of the subgroups of $\mathbf{GL}_2(\ell)$ up to conjugacy as follows:

1. **(even $\boldsymbol{\ell}$)** If $\ell = 2$ then output $\langle\rangle$, $\langle\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)\rangle$, $\langle\left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right)\rangle$, $\langle\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right)\rangle$ and terminate.
2. Compute a generator r for $\mathbf{Z}(\ell)$, a generator g for $C_{ns}(\ell)$, lists of the divisors of $\ell - 1$ and $\ell^2 - 1$, and a lookup table
$$T := \{(u(g), |\pi(g)|) : g \in C_s(\ell) \cup C_{ns}(\ell)\}$$
indexed by $u(g) := \operatorname{tr}(g)^2/\det(g)$.
3. **(contains $\mathbf{SL}_2(\boldsymbol{\ell})$)** For each e dividing $\ell - 1$ output $\langle\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&0\\0&r^e\end{smallmatrix}\right)\rangle$.
4. **(in $\boldsymbol{B(\ell)}$)** For each triple (a, b, i) with $a, b | (\ell - 1)$ and $0 \leqslant i < \gcd(a, b)$, output
$$\left\langle \begin{pmatrix} r^a & 0 \\ 0 & 1/r^a \end{pmatrix}, \begin{pmatrix} r^{ic} & 0 \\ 0 & r^{d-ic} \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle$$
where $c = a/\gcd(a, b)$ and $d = n/b$.

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

5. **(exceptional cases)** If $\ell \geqslant 5$ then call Algorithm 1 for each $H \in \{A_4, S_4, A_5\}$, $i \in \{1, 2, 3\}$, and $Z = \langle \left(\begin{smallmatrix} r^n & 0 \\ 0 & r^n \end{smallmatrix}\right) \rangle$ with n dividing $(\ell - 1)/2$.

6. **(cyclic cases)**

   a. **(split)** For each (a, b, i) with $a, b | (\ell - 1)$ and $0 \leqslant i < \gcd(a, b)$, put $c = a/\gcd(a, b)$ and $d = (\ell - 1)/b$, and if there is no integer j in the interval $[1, i - 1]$ satisfying $jc \equiv d - ic \pmod{a}$ then output

   $$H_{a,b,i} := \left\langle \begin{pmatrix} r^a & 0 \\ 0 & 1/r^a \end{pmatrix}, \begin{pmatrix} r^{ic} & 0 \\ 0 & r^{d-ic} \end{pmatrix} \right\rangle.$$

   b. **(nonsplit)** For each $n | (\ell^2 - 1)$ not divisible by $\ell + 1$ output $H_n := \langle g^n \rangle$, where $C_{ns}(\ell) = \langle g \rangle$.

7. **(dihedral cases)**

   a. **(split)** Let $\gamma := \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\delta := \left(\begin{smallmatrix} 1 & 0 \\ 0 & r \end{smallmatrix}\right)$. For each $H_{a,b,i}$ as in step 6.a with $2ic \equiv d \pmod{a}$:

   i. Compute $Z_{a,b,i} := H_{a,b,i} \cap Z(\ell)$ using the table T as described below.

   ii. Unless $-1 \in Z_{a,b,i}$, $[H_{a,b,i} : Z_{a,b,i}] = 2$, and $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \in H_{a,b,i}$, output $\langle H_{a,b,i}, \gamma \rangle$.

   iii. If $-1 \in Z_{a,b,i}$ and $\det(H_{a,b,i}) = \det(Z_{a,b,i})$ then output $\langle H, \gamma\delta^e \rangle$, where $e := [Z(\ell) : Z_{a,b,i}]$.

   b. **(nonsplit)** Let $\gamma = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. For each $H_n = \langle g^n \rangle$ as in step 6.b:

   i. Compute $Z_n := H_n \cap Z(\ell)$ using the table T as described below.

   ii. Output $\langle H_n, \gamma \rangle$.

   iii. If $-1 \in Z_n$ and $\det(H_n) = \det(Z_n)$ then output $\langle H_n, \gamma g^e \rangle$, where $e := [Z(\ell) : Z_n]$.

The scalar subgroup $Z_{a,b,i} := H_{a,b,i} \cap Z(\ell)$ computed in step 7.a.ii is uniquely determined by its order, which we can compute as $\#H_{a,b,i}/\#\pi(H_{a,b,i})$, where $\pi : \mathbf{GL}_2(\ell) \twoheadrightarrow \mathbf{PGL}(\ell)$ is the canonical projection. Since $\pi(H_{a,b,i})$ is cyclic, we may compute its order as the least common multiple of the projective orders of the generators of $H_{a,b,i}$, which may be determined using the lookup table T computed in step 2. Similar comments apply to computing $Z_n := H_n \cap Z(\ell)$ in step 7.b.ii.

The correctness of Algorithm 2 follows from Proposition 3.1, the correctness of Algorithm 1, and the analysis in Sections 3.1 to 3.3. The constraint on i in step 6.a ensures that we pick just one of the two possible conjugacy class representatives of a subgroup of $C_s(\ell)$, and the constraint on $H_{a,b,i}$ in step 7.a.ii uses Lemma 3.16

to pick just one of the two possible conjugacy class representatives of a subgroup of $C_s(\ell)^+$ with projective image isomorphic to the Klein group.

PROPOSITION 3.24. *The expected running time of Algorithm 2 is $\ell^{1+o(1)}$.*

Proof. We first consider step 2. We can compute the generators r and g in $(\log \ell)^{2+o(1)}$ expected time using probabilistic algorithms. We can compute the divisors of $\ell - 1$ and $\ell + 1$ in $\ell^{1+o(1)}$ time using a sieve, and these lists can then be used to construct a complete list of the divisors of $\ell^2 - 1 = (\ell - 1)(\ell + 1)$ in $\ell^{o(1)}$ time (here we are using the fact that an integer n has at most $n^{o(1)}$ divisors). To compute the table T, we note that for $C_s(\ell)$ it suffices to compute each pair $(u(a^e), (\ell - 1)/e)$ using $a = \left(\begin{smallmatrix} 1 & 0 \\ 0 & r \end{smallmatrix}\right)$ for $1 \leqslant e \leqslant \ell - 1$, and for $C_{ns}(\ell)$ it suffices to compute $(u(g^e), (\ell + 1)/e)$ using the generator g for $C_{ns}(\ell)$ for $1 \leqslant e \leqslant \ell + 1$. Thus step 2 takes $\ell^{1+o(1)}$ time.

Step 3 clearly takes $\ell^{o(1)}$ time. For step 4 we note that the number of triples (a, b, i) is given by

$$\begin{aligned}\alpha(\ell - 1) &= \sum_{a,b|(\ell-1)} \gcd(a, b) = \prod_p \Bigg(\sum_{0\leqslant i\leqslant v_p(\ell-1)} (2(v_p(\ell - 1) - i) + 1)p^i \Bigg) \\ &= \ell^{1+o(1)},\end{aligned}$$

and the time to compute generators for each individual subgroup of $B(\ell)$ is $\ell^{o(1)}$. There are $\ell^{o(1)}$ calls to Algorithm 1 in step 5, each of which takes $\ell^{1+o(1)}$ expected time, by Proposition 3.22. The number of subgroups $H_{a,b,i}$ in step 6.a is bounded by $\alpha(\ell - 1) = \ell^{1+o(1)}$, and each takes $\ell^{o(1)}$ time to compute, while step 6.b takes $\ell^{o(1)}$ time. The number of groups arising in step 7 is similarly bounded by $\ell^{1+o(1)}$, and the time for each group is $(\log \ell)^{2+o(1)}$, using the table T to compute the projective orders of $H_{a,b,i}$ and H_n as described above in order to determine their scalar subgroups. □

A Magma [11] script implementing Algorithm 2 is available from the author's website [68]. In practical terms, it typically takes just a few seconds for $\ell \approx 10^3$ and less than an hour for $\ell \approx 10^6$, computations that would be infeasible using the `Subgroups` function in Magma, or similar functionality in GAP [30].

3.6. Subgroup signatures.

DEFINITION 3.25. For each $g \in \mathbf{GL}_2(\ell)$ we define

$$\mathrm{sig}(g) := (\det(g), \mathrm{tr}(g), \dim_1(g)),$$

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

where $\dim_1(g) \in \{0, 1, 2\}$ is the dimension of the 1-eigenspace of g. For each subgroup $G \subseteq \mathbf{GL}_2(\ell)$ we define the *signature* of G to be the set

$$\operatorname{sig}(G) := \{\operatorname{sig}(g) : g \in G\}.$$

LEMMA 3.26. *Let ℓ be an odd prime, and let G be a subgroup of $\subseteq \mathbf{GL}_2(\ell)$. Then $(1, 2, 1) \in \operatorname{sig}(G)$ if and only if G contains an element of order ℓ.*

Proof. If G contains an element g of order ℓ then it is conjugate to $\left(\begin{smallmatrix} x & 1 \\ 0 & x \end{smallmatrix}\right)$ and $\operatorname{sig}(g^{\ell-1}) = (1, 2, 1) \in G$. Conversely, if $(1, 2, 1) \in \operatorname{sig}(G)$ then G contains an element conjugate to $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, which has order ℓ. □

LEMMA 3.27. *Suppose G and H are nonconjugate subgroups of $\mathbf{GL}_2(\ell)$ for which $\operatorname{sig}(G) = \operatorname{sig}(H)$, with $\#G \geqslant \#H$. Up to conjugacy in $\mathbf{GL}_2(\ell)$ exactly one of the following holds:*

(a) *$G = \langle C, \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\rangle$ and $H = \langle C', \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\rangle$ where $C, C' \subseteq C_s(\ell)$ are distinct $C_s^+(\ell)$-conjugates.*

(b) *$G \subseteq C_s^+(\ell)$ with $\det(G) \subseteq \mathbf{F}_\ell^{\times 2}$ and $H = G \cap C_s(\ell) \subsetneq G$; in this case $\ell \equiv 1 \pmod 4$.*

(c) *$G \subseteq C_{ns}^+(\ell)$ with $\det(G) \subseteq \mathbf{F}_\ell^{\times 2}$ and $H = G \cap C_{ns}(\ell) \subsetneq G$; in this case $\ell \equiv 3 \pmod 4$.*

(d) *the images of G and H in $\mathbf{PGL}_2(\ell)$ are isomorphic to A_4 and S_3, respectively.*

For every subgroup $G \subseteq \mathbf{GL}_2(\ell)$ there is at most one conjugacy class of nonconjugate subgroups H that have the same signature.

Proof. The four conjugacy classes of subgroups in $\mathbf{GL}_2(2)$ all have distinct signatures, in which case the lemma is vacuously true, so we assume ℓ is odd. The group G contains $\mathbf{SL}_2(\ell)$ if and only if $\operatorname{sig}(G)$ contains $(1, 2, 1)$ and a triple $(1, t, 0)$ with $t^2 - 4$ not square, and in this case the conjugacy class of G is then determined by $\det(G)$, which is also determined by $\operatorname{sig}(G)$. The same applies to H, so this case cannot arise. Lemma 3.26 implies that either G and H both contain an element of order ℓ, or neither do, and if the former holds than we must be in case (a), by Lemma 3.6 and its proof.

We now assume neither G nor H contain an element of order ℓ. The scalar subgroup $G \cap Z(\ell)$ of G and the possible orders of all $g \in G$ and $h \in \pi(G)$ are determined by $\operatorname{sig}(G)$, and they must be the same as for H. The groups $\pi(G)$ and $\pi(H)$ cannot both be cyclic, since Corollary 3.11 and Lemma 3.12 imply that in this case the conjugacy classes of G and H are determined by their signatures.

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

Similarly, Corollaries 3.17, 3.18, and Lemma 3.19 imply that $\pi(G)$ and $\pi(H)$ cannot both be dihedral.

The group S_4 (respectively A_5) may be distinguished from any cyclic or dihedral group by the fact that it contains elements of order 3 and 4 (respectively 3 and 5), but no element of order 12 (respectively 15). For the group A_4, the only cyclic or dihedral group with the same set of element orders is S_3. By Lemma 3.21, the conjugacy class of G in $\mathbf{GL}_2(\ell)$ with $\pi(G)$ isomorphic to A_4, S_4, or A_5 is determined by $\det(G)$ and $G \cap Z(\ell)$; thus, the only case that can arise in which G or H has an exceptional projective image is case (d) of the lemma.

The only remaining possibility is that $\pi(G)$ is dihedral and $\pi(H)$ is cyclic (since we assume $\#G \geqslant \#H$), and $\pi(H)$ cannot be trivial, so H is contained in either a split Cartan group or a nonsplit Cartan group, but not both. We have $G \cap Z(\ell) = H \cap Z(\ell)$ with G distinguished up to conjugacy among subgroups with dihedral projective image by its signature and H distinguished up to conjugacy among subgroups with cyclic projective image by its signature, and this implies that G must contain an index 2 subgroup conjugate to H. So without loss of generality we assume $H = G \cap C$, where C is either $C_s(\ell)$ or $C_{ns}(\ell)$, and let γH be the nontrivial coset of H in G, for some $\gamma \in G - H$. Now $\pi(H)$ contains an element of order 2, since $\pi(G)$ does and their signatures coincide, so H contains a trace-zero element h, and every trace-zero element of H is a scalar multiple of h. It follows that either all or none of the trace-zero elements in H (and hence in G) have square determinants, depending on whether $\det h$ is square or not.

Suppose $\det h$ is not a square. The same must be true of every element of γH (since they all have trace zero), including γ, so every element of $\gamma\gamma H = H$ has square determinant; but this includes h, which is a contradiction. So h and every element of γH has a square determinant, including γ, and the same holds for $\gamma\gamma H = H$ and hence for G; thus $\det(G) \subseteq \mathbf{F}_\ell^{\times 2}$, as claimed.

If $H \subseteq C_s(\ell)$ then $h = \left(\begin{smallmatrix} x & 0 \\ 0 & -x \end{smallmatrix}\right)$ for some $x \in \mathbf{Z}(\ell)^\times$; thus $\det h = -x^2$ is square only if -1 is square in $\mathbf{Z}(\ell)^\times$, in which case $\ell \equiv 1 \pmod 4$. If $H \subseteq C_{ns}(\ell)$ then $h = \left(\begin{smallmatrix} 0 & 0 \\ 0 & \varepsilon y \end{smallmatrix}\right) y0$ for some $y \in \mathbf{Z}(\ell)^\times$ with ε not square; thus $\det h = -\varepsilon y^2$ is square only if -1 is not square in $\mathbf{Z}(\ell)^\times$, in which case $\ell \equiv 3 \pmod 4$. □

We note that when $\det(G)$ is not contained in the subgroup of squares in $\mathbf{Z}(\ell)^\times$ only case (a) of Lemma 3.27 can arise, and in this case G and H are isomorphic, by Lemma 3.6. This yields the following corollary.

COROLLARY 3.28. *Let E be an elliptic curve over a number field K and let ℓ be a prime for which $K \cap \mathbf{Q}(\zeta_\ell) = \mathbf{Q}$ (any prime if $K = \mathbf{Q}$). Then $G_E(\ell)$ is determined up to isomorphism by its signature.*

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

To address cases (b) to (d) of Lemma 3.27 that may arise when we have $\det(G) \subseteq \mathbf{F}_\ell^{\times 2}$ we need an additional datum. For any subgroup $G \subseteq \mathbf{GL}_2(\ell)$, let

$$z(G) := \frac{\#\{g : g \in G, \operatorname{tr} g = 0\}}{\#G}$$

denote the proportion of trace-zero elements in G.

Lemma 3.29. *Let G and H be as in Lemma 3.27 and suppose case* (a) *does not apply. Then*

$$|z(G) - z(H)| \geqslant \tfrac{1}{4}.$$

Proof. If we are in case (b) or (c) of Lemma 3.27, then H lies in a Cartan group C and has index 2 in G, and the nontrivial coset gH of H in G does not intersect C. In this case every element of gH has trace zero, while at most half the elements of H can have trace zero, thus

$$z(G) - z(H) = \frac{1 + z(H)}{2} - z(H) = \frac{1 - z(H)}{2} \geqslant \frac{1}{4}.$$

In case (d) we have $z(G) = 1/4$ and $z(H) = 1/2$, thus $z(H) - z(G) = 1/4$. □

Corollary 3.30. *If G and H are subgroups of $\mathbf{GL}_2(\ell)$ with $\operatorname{sig}(G) = \operatorname{sig}(H)$ and $z(G) = z(H)$ then either G and H are conjugate or case (a) of Lemma 3.27 applies. In particular, G and H are locally conjugate and isomorphic.*

Proof. This follows from the previous lemma and Lemma 3.6. □

We now give an efficient algorithm to determine a set of generators for a subgroup G of $\mathbf{GL}_2(\ell)$ that satisfies $\operatorname{sig}(G) = s$ and $z(G) = z$, given the signature $s = \operatorname{sig}(G')$ and trace-zero ratio $z = z(G')$ of some subgroup G' of $\mathbf{GL}_2(\ell)$. By Corollary 3.30, the group G must be locally conjugate to G'. In order to do this more efficiently, we note that each signature s is uniquely determined by a small subset of its triples. It suffices to retain a subset $\bar{s}$ of s of signatures $\operatorname{sig}(g)$ for $g \in G'$ that includes

- the triple $(1, 2, 1)$ if $\#G'$ is divisible by ℓ;
- a triple $\operatorname{sig}(g)$ for which $\langle \det(g) \rangle = \det(G') =: \det(s)$;
- a triple $\operatorname{sig}(g)$ for which $\langle g \rangle = Z(G') =: Z(s)$;
- a triple $\operatorname{sig}(g)$ for which $|\pi(g)| = \max\{|\pi(h)| : h \in G'\} =: m(s)$;
- triples $\operatorname{sig}(g_i)$ for which $\operatorname{lcm}|\pi(g_i)| = \operatorname{lcm}\{|\pi(h) : h \in G'\} =: \lambda(s)$;

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

- triples $\operatorname{sig}(g_i)$ for which $\{\chi(g_i)\} = \{\chi(h) : h \in G'\} =: \chi(s)$;
- if $\pi(G')$ is not cyclic, triples $\operatorname{sig}(g_1)$ and $\operatorname{sig}(g_2)$ with $|\pi(g_1)| = |\pi(g_2)| = 2$ but $\pi(g_1) \neq \pi(g_2)$.

Given any signature $s = \operatorname{sig}(G')$ we can always reduce s to a subset $\overline{s}$ of at most 11 elements that satisfy all of the criteria above. Alternatively, as we shall do in Section 5, we can construct $\overline{s}$ by randomly sampling a sufficiently large subset of s, without ever needing to store more than $O(\log \ell)$ triples, which requires just $O(\log^2 \ell)$ bits of space, as opposed to $O(\ell^2 \log \ell)$ for the entire signature. More importantly, with the algorithm below we can obtain generators for a subgroup G locally conjugated to G' in expected time polynomial in $\log \ell$ rather than ℓ, an exponential improvement. For any subgroup G of $\mathbf{GL}_2(\ell)$ let $Z(G)$ denote the subgroup of scalar elements, and similarly let $Z(s)$ denote the subset of signatures of scalar elements (d, t, n) with $n \in \{0, 2\}$ and $t^2 - 4d = 0$.

ALGORITHM 3. Given a subset $\overline{s}$ of the signature s of a subgroup G' of $\mathbf{GL}_2(\ell)$ satisfying the requirements above and a rational number $z \in [0, 1]$ with denominator at most $\#\mathbf{GL}_2(\ell)$ satisfying $|z(G') - z| < \frac{1}{8}$, output a set of generators for a subgroup G of $\mathbf{GL}_2(\ell)$ that is locally conjugate to G' as follows:

1. **(even $\boldsymbol{\ell}$)** If $\ell = 2$ then output $G = \left\langle \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)\right\rangle$, $\left\langle \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)\right\rangle$, $\left\langle \left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right)\right\rangle$, or $\left\langle \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right), \left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right)\right\rangle$ when $\overline{s}$ is equal to $\{(1, 0, 2)\}$, $\{(1, 0, 2), (1, 0, 1)\}$, $\{(1, 0, 2), (1, 1, 0)\}$, or $\{(1, 0, 2), (1, 0, 1), (1, 1, 0)\}$, respectively, then terminate.
2. **(cases with order divisible by $\boldsymbol{\ell}$)** If $\overline{s}$ contains the triple $(1, 2, 1)$ then:
    - **a.** **(contains $\mathbf{SL_2(\boldsymbol{\ell})}$)** If $-1 \in \chi(s)$ output $G = \left\langle \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right), \left(\begin{smallmatrix}1&0\\0&d\end{smallmatrix}\right)\right\rangle$ with $\langle d\rangle = \det(s)$ and terminate.
    - **b.** **(in $\boldsymbol{B(\ell)}$)** Output $G = \left\langle \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right), g, c\right\rangle \subseteq B(\ell)$, with $g \in C_s(\ell)$ satisfying $|\pi(g)| = m(s)$ and $\langle c\rangle = Z(s)$, and terminate.
3. **(exceptional cases)** Check for projective image A_4, S_4, A_5 as follows:
    - **a.** **($\mathbf{A_4}$)** If $z < 3/8$, $m(s) = 3$ and $\lambda(s) = 6$, use Algorithm 1 to construct G with $\pi(G) \simeq A_4$, $Z(G) = Z(s)$, and $[\det(G) : \det(Z(G))] = [\det(s) = \det(Z(s))]$. Output G and terminate.
    - **b.** **($\mathbf{S_4}$)** If $m(s) = 4$ and $\lambda(s) = 12$ use Algorithm 1 to construct G with $\pi(G) \simeq S_4$, $Z(G) = Z(s)$, and $[\det(G) : \det(Z(G))] = [\det(s) = \det(Z(s))]$. Output G and terminate.
    - **c.** **($\mathbf{A_5}$)** If $m(s) = 5$ and $\lambda(s) = 30$ use Algorithm 1 to construct G with $\pi(G) \simeq A_5$, $Z(G) = Z(s)$, and $[\det(G) : \det(Z(G))] = [\det(s) = \det(Z(s))]$. Output G and terminate.

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

4. **(trivial cases)** If $\chi(s) = \{0\}$ output $Z(s)$ and terminate.
5. **(cyclic cases)** Construct a maximal $H \subset C_s(\ell) \cup C_{ns}(\ell)$ with $\pi(H)$ cyclic such that $\mathrm{sig}(H) \subseteq s$:
   - **a.** Let $\langle c\rangle = Z(s)$ let $g \in C_s(\ell) \cup C_{ns}(\ell)$ satisfy $|\pi(g)| = m(s)$ and $\mathrm{sig}(g) \in \overline{s}$, and set $H = \langle g, c\rangle$.
   - **b.** If $s \subseteq \mathrm{sig}(H)$ and $|z(H) - z| < 1/8$ then output $G = H$ and terminate.
6. **(dihedral cases)** Determine the unique $G \supseteq H$ with $\pi(G)$ dihedral such that $\mathrm{sig}(G) = s$:
   - **a.** Let $e = [Z(\ell) : H \cap Z(\ell)]$, where H is as in step 5.
   - **b.** If $\chi(g) = 1$ let $\gamma = \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$ and $r = \left(\begin{smallmatrix}1&0\\0&\varepsilon\end{smallmatrix}\right)$, otherwise let $\gamma = \left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right)$ and let r be a generator for $C_{ns}(\ell)$.
   - **c.** Output whichever of $G = \langle H, \gamma\rangle$ or $G = \langle H, \gamma r^e\rangle$ satisfies $\overline{s} \subseteq \mathrm{sig}(G)$.

The correctness of Algorithm 3 follows from Proposition 3.1, Lemma 3.26, and Corollaries 3.17, 3.18, and 3.30. Note that in the dihedral case $\overline{s}$ is guaranteed to contain the signature of some $h \in G - H$, since we retain two projectively distinct elements of order 2 in this case, and $\det h$ will determine whether $\det(G) = -\det(G - H)$ or not, which determines which of the two possible subgroups G to output in step 6c, by Corollaries 3.17 and 3.18.

PROPOSITION 3.31. *The expected running time of Algorithm 3 is* $O(\mathsf{M}(\log \ell)\log \ell)$.

Proof. All the individual arithmetic operations in the algorithm involve $O(\log \ell)$-bit integers, including the numerator and denominator of z, and can be accomplished using $O(\mathsf{M}(\log \ell)\log\log \ell)$ bit operations (including any field inversions). The subset $\overline{s}$ contains just $O(1)$ elements, there are $O(1)$ steps in the algorithm, and each can be completed in $O(\mathsf{M}(\log \ell)\log \ell)$ expected time, including the calls to Algorithm 1, by Proposition 3.22, and the time to obtain a generator ε for $\mathbf{Z}(\ell)^\times$ and r for $C_{ns}(\ell)$ using a Las Vegas algorithm. □

3.7. Locally conjugate subgroups.

We conclude this section with a theorem that precisely characterizes the circumstances in which we may have an elliptic curve E/K for which $G_E(\ell)$ is locally conjugate but not conjugate to another subgroup of $\mathbf{GL}_2(\ell)$.

THEOREM 3.32. *Let ℓ be a prime and let E be an elliptic curve over a number field K for which there exists a subgroup G' of $\mathbf{GL}_2(\ell)$ that is locally conjugate* *to $G_E(\ell)$ but not conjugate to $G_E(\ell)$. Then G' arises as $G_{E'}(\ell)$ for an elliptic curve E'/K that is related to E by a cyclic isogeny whose degree is a power of ℓ; the curve E' is unique up to isomorphism.*

Proof. It follows from the classification of Section 3 that up to conjugacy, $G = G_E(\ell)$ and G' are of the form $G = H \rtimes \langle t\rangle$ and $G' = H' \rtimes \langle t\rangle$, where $t = \left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ and H and H' are distinct subgroups of $C_s(\ell)$ that are conjugate in $\mathbf{GL}_2(\ell)$ via $\left(\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right)$. This implies that neither H nor H' lie in $Z(\ell)$.

The group G lies in $B(\ell)$ but not $C_s(\ell)$, so E admits a rational isogeny φ_1 of degree ℓ that is unique up to isomorphism. Let $E_1 = \varphi_1(E)$ and let $G_1 = G_{E_1}(\ell)$. The isogeny φ_1 induces a homomorphism $G \to G_1$ with kernel $\langle t\rangle$. The existence of the dual isogeny implies that the order of G_1 is either equal to that of G or smaller by a factor of ℓ (it cannot be larger because ℓ^2 does not divide $\#\mathbf{GL}_2(\ell)$). In the latter case, G_1 lies in a split Cartan group but is not contained in $Z(\ell)$ (since H is not), and E_1 admits exactly two distinct rational ℓ-isogenies, one of which is the dual of φ_1.

If we let $\varphi_2 : E_1 \to E_2$ be the rational ℓ-isogeny that is not dual to φ_1 and put $G_2 = G_{E_2}(\ell)$, then either G_2 also lies in a split Cartan group but not $Z(\ell)$ and we can repeat the same argument, or G_2 has the same order as G. The isogeny class of E is finite, so by following a chain of ℓ-isogenies whose composition φ has a cyclic kernel of ℓ-power order, we must eventually reach an elliptic curve $E_n = \varphi_n(E)$ for which $G_n := G_{E_n}(\ell)$ has the same order as G. We may thus assume that G_n lies in $B(\ell)$ but not $C_s(\ell)$, and therefore has the form $H_n \rtimes \langle t\rangle$, where H_n is a subgroup of $C_s(\ell)$. The isogeny φ_n induces a group homomorphism $\phi_n : G \to G_n$ with kernel $\langle t\rangle$. We can pick bases (P, Q) and (P', Q') for $E[\ell]$ and $E_n[\ell]$ (respectively) so that $\varphi_n(P) = 0$ and $\varphi_n(Q) = Q'$, while for the dual isogeny $\hat{\varphi}_n$ we have $\hat{\varphi}_n(Q') = 0$ and $\hat{\varphi}_n(P') = P$. It follows that ϕ_n restricts to an isomorphism from H to H_n that corresponds to conjugation by $\left(\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right)$ (swapping the diagonal elements). We therefore have $H_n = H'$ and $G_n = G'$. The curve $E' := E_n$ is determined up to isomorphism by the kernel of the separable isogeny φ_n, which is in turn determined up to isomorphism by E. □

REMARK 3.33. The theorem allows for the possibility that E/K has CM, but rarely applies in this case. When E/K has CM the hypothesis of the theorem is satisfied only when ℓ is ramified in the CM field and the ideal above ℓ in the CM field is nonprincipal (and thus has order 2 in the class group). This corresponds to an ℓ-volcano that consists of a single edge; see [66].

EXAMPLE 3.34. Consider the chain of 5 isogenies $E \longleftrightarrow E_1 \longleftrightarrow E'$, where E, E_1, and E' are the elliptic curves over $\mathbf{Q}$ with Cremona labels 11a3, 11a1, and 11a2, respectively. In this example, the groups $G = \langle \left(\begin{smallmatrix} 1 & 0 \\ 0 & 2 \end{smallmatrix}\right) \rangle$ and $H = \langle \left(\begin{smallmatrix} 2 & 0 \\ 0 & 1 \end{smallmatrix}\right) \rangle$ are both conjugate to $G_{E_1}(5)$, while the groups $G_E(5) = \langle G, t \rangle$ and $G_{E'}(5) = \langle H, t \rangle$ are nonconjugate but locally conjugate and isomorphic (as required by Lemma 3.6). As can be seen from the groups $G_E(5)$ and $G_{E'}(5)$, the elliptic curve E has a rational 5-torsion point, but E' does not.

4. GRH bounds

By the generalized Riemann hypothesis (GRH) we refer to the assumption that the nontrivial zeros of the Dedekind zeta function of a number field all lie on the critical line $\{s \in \mathbf{C} : \operatorname{Re}(s) = 1/2\}$. We also recall the logarithmic integral $\operatorname{Li}(x) := \int_2^x dt/\log t$.

PROPOSITION 4.1 (Lagarias–Odlyzko, Serre). *Assume the GRH. Let L be a finite Galois extension of a number field K with Galois group $G = \operatorname{Gal}(L/K)$, let $n_L := [L : \mathbf{Q}]$, and $d_L := |\operatorname{disc}(L)|$. For each nonempty subset C of G stable under conjugation define*

$$\pi_C(x) := \#\left\{\mathfrak{p} : \left(\frac{L/K}{\mathfrak{p}}\right) \subseteq C,\ N(\mathfrak{p}) \leqslant x\right\},$$

where $\mathfrak{p}$ ranges over the primes of K that are unramified in L, $N(\mathfrak{p})$ is its absolute norm, and $(\frac{L/K}{\cdot})$ is the Artin symbol. There are absolute effective constants c_1 and c_2 such that

$$\left|\pi_C(x) - \frac{\#C}{\#G}\operatorname{Li}(x)\right| \leqslant c_1 \frac{\#C}{\#G}\sqrt{x}(\log d_L + n_L \log x)$$

holds for all $x \geqslant 2$, and $\pi_C(x) \geqslant 1$ for all $x \geqslant c_2 \log^2 d_L$.

Proof. The first bound is [59, Theorem 4], which sharpens [38]. The second is [59, Theorem 5], which is also sketched in [38]. For the third bound, see the remark regarding an improvement to Corollary 1.2 in [38]. □

REMARK 4.2. As noted in [59], Oesterlé announced the explicit values $c_1 = 2$ and $c_2 = 70$ in [51]. Proofs of these values have not been published, but in [72] one can find proofs that use somewhat larger constants (one can take $c_1 = 185$ via [72, Theorem 1.2]; if one assumes d_L is sufficiently large one can take $c_1 \approx 32$).

PROPOSITION 4.3 (Larson–Vaintrob). *Assume the GRH. Let E be an elliptic curve without CM defined over a number field K, and let N_E be the absolute* *value of the norm of its conductor. There is an effective constant c_K depending only on K such that $G_E(\ell) \neq \mathbf{GL}_2(\ell)$ only occurs for primes*

$$\ell \leqslant c_K \log N_E (\log\log N_E)^3.$$

Proof. See [42, Theorem 2]. □

REMARK 4.4. Without the GRH the best known bounds on ℓ are exponentially worse. Even in the case $K = \mathbf{Q}$ the best unconditional bound known is quasilinear in N_E [18]. For elliptic curves over $\mathbf{Q}$ with no primes of multiplicative reduction, an $O(\sqrt{N_E})$ bound is given in [73], which also gives much stronger bounds (logarithmic in the discriminant) for elliptic curves with nonintegral j-invariants.

PROPOSITION 4.5. *Let E be an elliptic curve defined over a number field K, and let N_E be the absolute value of the norm of the conductor of E. Let $m > 1$ be an integer, let $L := K(E[m])$ be the m-torsion field of E, and let $d_L := |\mathrm{disc}(L)|$, $d_K := |\mathrm{disc}(K)|$, and $n_K := [K : \mathbf{Q}]$, Then*

$$\log d_L \leqslant m^4 d_K (4n_K \log_2 m + d_K + 1) \log(mN_E).$$

Proof. We have

$$d_L = d_K^{[L:K]} |N_{K/\mathbf{Q}}(d_{L/K})|,$$

where $d_{L/K}$ denotes the relative discriminant of L/K. The extension L/K has degree at most $\#\mathbf{GL}_2(m)$ which is less than m^4, and is unramified at all primes $\mathfrak{p}$ of K that do not divide m and for which E has good reduction; see [25, Theorem 1]. The ramification index e of any prime $\mathfrak{q}|\mathfrak{p}$ cannot exceed $[L : K] < m^4$; therefore, the multiplicity of any prime $\mathfrak{q}$ in the relative different $\mathcal{D}_{L/K}$ cannot exceed

$$e - 1 + v_{\mathfrak{p}}(e)e < e(n_K \log_2 e + 1) < m^4(4n_K \log_2 m + 1) =: B.$$

The multiplicity of any prime $\mathfrak{p}$ in the relative discriminant $d_{L/K} = N_{L/K}(\mathcal{D}_{L/K})$ is also bounded by B, and since every ramified prime divides mN_E, we have

$$|N_{K/\mathbf{Q}}(d_{L/K})| \leqslant mN_E.$$

Thus

$$\log d_L \leqslant m^4 d_K + B \log(mN_E) = m^4(4n_K \log_2 m + d_K + 1) \log(mN_E). \qquad \square$$

REMARK 4.6. The conductor norm N_E can be replaced by its square-free part in the proposition above.

COROLLARY 4.7. *Assume the GRH. Let E be an elliptic curve defined over a number field K and let N_E be the absolute value of the norm of its conductor. Let ℓ*

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

be a prime and let $L = K(E[\ell])$. There is an effective constant c'_K depending only on K such that every conjugacy class in $G_E(\ell)$ arises as the image of a Frobenius element of $\mathrm{Gal}(L/K)$ *for a prime $\mathfrak{p} \nmid \ell$ of good reduction for E with absolute norm $N(\mathfrak{p}) \leqslant x$, provided that*

$$x \geqslant c'_K \ell^8 (\log \ell \log(\ell N_E))^2.$$

For $\ell \leqslant c_K \log N_E (\log \log N_E)^3$ as in Proposition 4.3, it suffices to have

$$x \geqslant c'_K (\log N_E)^{10} (\log \log N_E)^4 (\log \log \log N_E)^{24}.$$

Moreover, if a good prime $\mathfrak{p} \nmid \ell$ is chosen uniformly at random from the set

$$\{\mathfrak{p} : N(\mathfrak{p}) \in [P, 2P]\}$$

with $P \geqslant x \log \log x$ and x as above, then for any nonempty subset C of $G_E(\ell)$ stable under conjugation the probability that $\mathrm{Frob}_{\mathfrak{p}}$ *lies in C is*

$$(1 + o(1)) \frac{\#C}{\#G},$$

where the implied constant in $o(1)$ is effective.

Proof. Applying Proposition 4.5 with $n = \ell$ yields $\log d_L = O(\ell^4 \log \ell \log(\ell N_E))$, where the implied constant is effective and depends only on K. We then apply the last part of Proposition 4.1 to get the first lower bound on x. The second bound on x follows immediately, and the last statement follows from the upper and lower bounds on $\pi_C(x)$ given by Proposition 4.5 (we just need P to grow strictly faster than x). □

REMARK 4.8. Analogous results that do not depend on the GRH are known (see, e.g., [38, 39]), but the bounds are typically polynomial in the absolute discriminant d_L, rather than its logarithm.

5. Algorithms and applications

All the fields k that we shall consider are either number fields K or finite fields $\mathbf{F}_q$ of odd characteristic p; in both cases k is a finite extension of its prime field k_0 and can be explicitly represented as $k_0[\alpha]/(F(\alpha))$ for some fixed monic polynomial $F \in \mathbf{Z}[\alpha]$ of degree $[k : k_0]$ whose image in $k_0[\alpha]$ is irreducible. For the purpose of explicit computation, we assume that elements of k are uniquely represented as integer polynomials of degree less than $[k : k_0]$, with coefficients in the interval $[0, p - 1]$ in the case that k_0 is the finite field $\mathbf{F}_p$.

For number fields $K = \mathbf{Q}[\alpha]/(F(\alpha))$, we assume that the polynomial F is fixed in advance, and that elliptic curves E/K are specified by an integral Weierstrass

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

equation $y^2 = f(x)$, where $f \in \mathbf{Z}[\alpha][x]$ is a cubic polynomial whose coefficients in $\mathbf{Z}[\alpha]$ represent elements of K as described above. For each prime $\mathfrak{p}$ of $K/\mathbf{Q}$ that does not divide $\operatorname{disc}(F)$, we may represent the residue field $\mathbf{F}_\mathfrak{p}$ of $\mathfrak{p}$ as $\mathbf{F}_p[\alpha]/(G(\alpha))$, where $p = \mathfrak{p} \cap \mathbf{Z}$ and G divides the image of F in $\mathbf{F}_p[\alpha]$; such a G can be efficiently obtained by factoring F over $\mathbf{F}_p$ (indeed, this is how the $\mathfrak{p} \mid p$ are typically determined; see [17, Section 4.8.2], for example). If $\mathfrak{p}$ is a prime of good reduction for E, we may compute $E_\mathfrak{p} := E \pmod{\mathfrak{p}}$ by reducing the $\mathbf{Z}[\alpha]$-coefficients of $f(x)$ modulo $(p, G(\alpha))$ to obtain elements of $\mathbf{F}_\mathfrak{p}$.

REMARK 5.1. We do not assume $O_K = \mathbf{Z}[\alpha]$ (which is possible only when $\mathcal{O}_K$ is monogenic), so $\operatorname{disc}(F)$ may be divisible by primes that do not divide $\operatorname{disc}(K)$. Such primes $\mathfrak{p}$ are finite in number and there is no harm in ignoring them for the purpose of computing $G_E(\ell)$. More generally, as we are only interested in primes $\mathfrak{p}$ of bounded norm, there is no loss of generality in assuming that $N(\mathfrak{p}) = p$ is prime, so that we have $\deg G = 1$ and $\mathbf{F}_\mathfrak{p} \simeq \mathbf{F}_p$; this accounts for all but a negligible proportion of the primes $\mathfrak{p}$ with $N(\mathfrak{p}) \leqslant B$ for any sufficiently large bound B. Doing so simplifies the practical implementation of our algorithms.

5.1. Computing Frobenius triples.

Our strategy is to determine the signature of $G_E(\ell)$ by computing the images of Frobenius elements $\operatorname{Frob}_\mathfrak{p}$ under $\rho_{E,\ell}$ for primes $\mathfrak{p}$ of good reduction for E that do not divide ℓ or $\operatorname{disc}(F)$ (such primes are unramified in both $K(E[\ell])/K$ and $K/\mathbf{Q}$). This requires us to compute the determinant, trace, and 1-eigenspace dimension of $\rho_{E,\ell}(\operatorname{Frob}_\mathfrak{p})$. If we put $q := N(\mathfrak{p})$, then for any prime ℓ not divisible by $\mathfrak{p}$, the Frobenius triple

$$(\det \rho_{E,\ell}(\operatorname{Frob}_\mathfrak{p}), \operatorname{tr} \rho_{E,\ell}(\operatorname{Frob}_\mathfrak{p}), \dim_1(\rho_{E,\ell}(\operatorname{Frob}_\mathfrak{p})) \tag{5.1}$$

of E/K at $\mathfrak{p}$ is given by

$$(q \bmod \ell, \operatorname{tr} \pi_{E_\mathfrak{p}} \bmod \ell, \log_\ell \#E_\mathfrak{p}[\ell](\mathbf{F}_\mathfrak{p})),$$

where $\operatorname{tr} \pi_{E_\mathfrak{p}} := q + 1 - \#E_\mathfrak{p}(\mathbf{F}_\mathfrak{p})$ is the trace of the Frobenius endomorphism $\pi_{E_\mathfrak{p}}$ of $E_\mathfrak{p}$. We can efficiently compute $\operatorname{tr} \pi_{E_\mathfrak{p}}$ using Schoof's algorithm [55, 56], which runs in time $(\log q)^{5+o(1)}$ (see [60, Corollary 11] for a sharp bound when q is prime; up to factors of $\log \log q$, the nonprime case is the same). To compute $\#E_\mathfrak{p}[\ell](\mathbf{F}_\mathfrak{p})$ we rely on Miller's algorithm [49] for computing the Weil pairing. Recall that for an elliptic curve E over any field k any prime $\ell \neq \operatorname{char}(k)$, the Weil pairing

$$\omega_\ell : E[\ell] \times E[\ell] \to \mu_\ell$$

is a nondegenerate alternating bilinear pairing. For $P, Q \in E[\ell] \simeq \mathbf{Z}(\ell) \times \mathbf{Z}(\ell)$ we have $E[\ell] = \langle P, Q \rangle$ if and only if $\omega_\ell(P, Q) \neq 1$. In [49], Miller gives an efficient algorithm to compute ω_ℓ; when $k = \mathbf{F}_q$ is a finite field and P, Q lie in $E(\mathbf{F}_q)$ it runs in time $(\log q)^{3+o(1)}$.

We now give a Las Vegas algorithm to compute Frobenius triples for a set S of primes ℓ for a given reduction $E_\mathfrak{p}$ of E/K at an unramified prime $\mathfrak{p}$ of norm q. The algorithm can be applied to any elliptic curve over a finite field, but in order to keep the context clear we denote the curve $E_\mathfrak{p}/\mathbf{F}_\mathfrak{p}$, since we have in mind a reduction of our fixed elliptic curve E/K.

ALGORITHM 4. Given an elliptic curve $E_\mathfrak{p}$ over a finite field $\mathbf{F}_\mathfrak{p}$ of characteristic p and cardinality q, and a finite set S of primes $\ell \neq p$, compute the set of triples $T = \{(\ell, q \bmod \ell, \operatorname{tr}\pi_E \bmod \ell, \log_\ell \#E_\mathfrak{p}[\ell](\mathbf{F}_\mathfrak{p})) : \ell \in S\}$ as follows:

```
1. Use Schoof's algorithm to compute $t = q + 1 - \#E_\mathfrak{p}(\mathbf{F}_\mathfrak{p})$ and put $N := q + 1 - t$.
2. Initialize $T$ to $\{\,\}$ and for each prime $\ell \in S$:
    a. Put $e := v_\ell(N)$.
    b. If $e = 0$ then add $(\ell, q \bmod \ell, t \bmod \ell, 0)$ to $T$ and proceed to the next prime $\ell \in S$.
    c. If $e = 1$ or $q \not\equiv 1 \pmod{\ell}$ then add $(\ell, q \bmod \ell, t \bmod \ell, 1)$ to $T$ and proceed to the next prime $\ell \in S$.
    d. Repeat the following:
        i. Generate random points $P_1, P_2 \in E_\mathfrak{p}(\mathbf{F}_\mathfrak{p})$ and compute $Q_1 := (N/\ell^e)P_1$ and $Q_2 := (N/\ell^e)P_2$.
        ii. For $i = 1, 2$, determine the least $e_i \in [0, e]$ such that $\ell^{e_i} Q_i = 0$.
        iii. If $\max(e_1, e_2) = e$ then add $(\ell, q \bmod \ell, t \bmod \ell, 1)$ to $T$ and proceed to the next prime $\ell \in S$.
        iv. Use Miller's algorithm to compute $\zeta := \omega_\ell(\ell^{e_1-1}Q_1, \ell^{e_2-1}Q_2)$.
        v. If $\zeta \neq 1$ then add $(\ell, q \bmod \ell, t \bmod \ell, 2)$ to $T$ and proceed to the next prime $\ell \in S$.
3. Output $T$ and terminate.
```

Steps 2.b and 2.c of the algorithm allow us to quickly treat cases where we can immediately determine the ℓ-rank $r := \log_\ell \#E_\mathfrak{p}[\ell](\mathbf{F}_\mathfrak{p})$: if ℓ does not divide $N = \#E_\mathfrak{p}(\mathbf{F}_\mathfrak{p})$ (so $e = 0$), then clearly $r = 0$; if ℓ divides N then $r \geqslant 1$, and we can have $r > 1$ only if ℓ^2 divides $\#E_\mathfrak{p}(\mathbf{F}_\mathfrak{p})$ (so $e > 1$) and $q \equiv 1 \pmod{\ell}$.

PROPOSITION 5.2. *The expected running time of Algorithm 4 is*

$$O\big((\log q)^{5+o(1)} + \#S \cdot (\log q)^{3+o(1)}\big).$$

Proof. As noted above, the complexity of step 1 is bounded by $(\log q)^{5+o(1)}$. Generating uniformly random nontrivial points $P \in E_{\mathfrak{p}}(\mathbf{F}_{\mathfrak{p}})$ in step 2.d.i can be accomplished by repeatedly choosing uniformly random $x_0 \in \mathbf{F}_{\mathfrak{p}}$ and attempting to find a root y_0 of $y^2 - f(x_0) \in \mathbf{F}_{\mathfrak{p}}[y]$; to obtain a uniform distribution over $E_{\mathfrak{p}}(\mathbf{F}_{\mathfrak{p}}) - \{0\}$ one picks the sign of y_0 at random and discards points with $y_0 = 0$ with probability $1/2$. The expected time per random point (x_0, y_0) is $(\log q)^{1+o(1)}$, which matches the cost of step 2.d.ii. The time for step 2.d.iv is $(\log q)^{3+o(1)}$, and this dominates the total cost of step 2.d, which we expect to execute less than twice, on average, for each $\ell \in S$. If $E_{\mathfrak{p}}(\mathbf{F}_{\mathfrak{p}})[\ell]$ has order ℓ, then with probability at least $1 - 1/\ell^2$ one of Q_1 or Q_2 will be a generator and the algorithm will then proceed to the next $\ell \in S$ in step 2.d.iii; otherwise we have $E_{\mathfrak{p}}[\ell] \subseteq E_{\mathfrak{p}}(\mathbf{F}_{\mathfrak{p}})$, and with probability at least $1 - 1/\ell$ the points Q_1 and Q_2 generate $E_{\mathfrak{p}}[\ell]$ and the algorithm proceeds to the next $\ell \in S$ in step 2.d.v. The expected time for step 2.d is thus $(\log q)^{3+o(1)}$ for each prime ℓ, and the total time for step 2 is $\#S \cdot (\log q)^{3+o(1)}$. □

REMARK 5.3. By using the Schoof–Elkies–Atkin (SEA) algorithm in step 2 of Algorithm 4, under the GRH one obtains a tighter bound on its average running time for reductions of a fixed elliptic curve E/K modulo primes $\mathfrak{p}$ of K with norm contained in any dyadic interval $[x, 2x]$. An extension of [60, Corollary 3] yields an average expected time of

$$O\big((\log x)^{4+o(1)} + \#S \cdot (\log x)^{3+o(1)}\big)$$

per prime. This also applies if we restrict to degree-1 primes, or to primes in an arithmetic progression with a sufficiently small modulus.

5.2. Computing Frobenius conjugacy classes. We now give an asymptotically slower algorithm that instead of computing Frobenius triples for a given set of primes computes a single integer matrix

$$A_{\mathfrak{p}} := \begin{pmatrix} (a_{\mathfrak{p}} + b_{\mathfrak{p}}\delta_{\mathfrak{p}})/2 & b_{\mathfrak{p}} \\ b_{\mathfrak{p}}(\Delta_{\mathfrak{p}} - \delta_{\mathfrak{p}})/4 & (a_{\mathfrak{p}} - b_{\mathfrak{p}}\delta_{\mathfrak{p}})/2 \end{pmatrix} \in \mathbf{M}_2(\mathbf{Z})$$

whose reduction modulo m lies in the conjugacy class $\rho_{E,m}(\mathrm{Frob}_{\mathfrak{p}})$ for all integers $m > 1$ prime to $\mathfrak{p}$ (including all primes ℓ not divisible by $\mathfrak{p}$). The quantities $a_{\mathfrak{p}}$, $b_{\mathfrak{p}}$, $\Delta_{\mathfrak{p}}$, $\delta_{\mathfrak{p}}$ appearing in $A_{\mathfrak{p}}$ are defined as follows. Let $R_{\mathfrak{p}}$ be the subring of $\mathrm{End}(E_{\mathfrak{p}})$ generated by $\pi_{E_{\mathfrak{p}}}$; if $\pi_{E_{\mathfrak{p}}} \in \mathbf{Z}$ then $R_{\mathfrak{p}} = \mathbf{Z}$ and otherwise $R_{\mathfrak{p}}$ is an order in an imaginary quadratic field. We then define the quantities

$$\Delta_{\mathfrak{p}} := \mathrm{disc}(R_{\mathfrak{p}}), \qquad \delta_{\mathfrak{p}} := 0, 1 \text{ as } \Delta_{\mathfrak{p}} \equiv 0, 1 \pmod 4,$$

$$a_{\mathfrak{p}} := \mathrm{tr}\,\pi_{E_{\mathfrak{p}}}, \qquad b_{\mathfrak{p}} := \sqrt{(a_{\mathfrak{p}}^2 - 4N(\mathfrak{p}))/\Delta_{\mathfrak{p}}}.$$

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

Note that $b_{\mathfrak{p}} = 0$ if $R_{\mathfrak{p}} = \mathbf{Z}$ (and in this case $A_{\mathfrak{p}}$ is a scalar matrix), otherwise $b_{\mathfrak{p}}$ is the index of $\mathbf{Z}[\pi_{E_{\mathfrak{p}}}]$ in $R_{\mathfrak{p}}$. In either case, we always have

$$4N(\mathfrak{p}) = a_{\mathfrak{p}}^2 - b_{\mathfrak{p}}^2 \Delta_{\mathfrak{p}},$$

with $\operatorname{tr} A_{\mathfrak{p}} = a_{\mathfrak{p}}$ and $\det A_{\mathfrak{p}} = N(\mathfrak{p}) \neq 0$.

THEOREM 5.4 (Duke–Tóth). *Let E be an elliptic curve over a number field K and let $\mathfrak{p}$ be a prime of good reduction for E. For any integer m for which $\mathfrak{p} \nmid m$ is unramified in $K(E[m])$ the reduction of $A_{\mathfrak{p}}$ modulo m lies in the conjugacy class of $\rho_{E,m}(\mathrm{Frob}_{\mathfrak{p}})$ in $\mathbf{GL}_2(m)$.*

Proof. See [25, Theorem 2.1]. □

When $E_{\mathfrak{p}}$ is supersingular, the matrix $A_{\mathfrak{p}}$ is determined by $N(\mathfrak{p})$ and $a_{\mathfrak{p}}$. This follows from the fact that in this case $\mathrm{End}(E_{\mathfrak{p}})$ is a maximal order in the quaternion algebra $\mathrm{End}(E) \otimes \mathbf{Q}$, by [22], hence either $R_{\mathfrak{p}} = \mathbf{Z}$ or $R_{\mathfrak{p}}$ is the maximal order of $\mathbf{Q}(\sqrt{-p})$, where $\mathfrak{p} \mid p$. In the former case $b_{\mathfrak{p}} = 0$ and in the latter case $\Delta_{\mathfrak{p}} = \mathrm{disc}(\mathbf{Q}(\sqrt{-p}))$ and $b_{\mathfrak{p}} = (a_{\mathfrak{p}}^2 - 4N(\mathfrak{p}))/\Delta_{\mathfrak{p}}$.

To treat the ordinary case, we rely on the algorithm in [8], which gives a GRH-based Las Vegas algorithm to compute the index $u_{\mathfrak{p}}$ of $\mathrm{End}(E_{\mathfrak{p}})$ in the maximal order of the imaginary quadratic field $\mathrm{End}(E_{\mathfrak{p}}) \otimes \mathbf{Q}$ with expected running time

$$\mathsf{L}(N(\mathfrak{p}))^{1+o(1)},$$

where

$$\mathsf{L}(x) := \exp\sqrt{\log x \log\log x}.$$

The first step of this algorithm is to compute $a_{\mathfrak{p}}$ via Schoof's algorithm and factor $a_{\mathfrak{p}}^2 - 4N(\mathfrak{p})$ in order to determine the discriminant $D := \mathrm{disc}(\mathbf{Q}((a_{\mathfrak{p}}^2 - 4N(\mathfrak{p}))^{1/2})$. Once the index $u_{\mathfrak{p}}$ has been determined we compute $b_{\mathfrak{p}} = (a_{\mathfrak{p}}^2 - 4N(\mathfrak{p}))/(u_{\mathfrak{p}}^2 D)$. This yields the following theorem.

THEOREM 5.5. *Let E be an elliptic curve over a number field K and let $\mathfrak{p}$ be a prime of good reduction for E. Under the GRH there is a Las Vegas algorithm to compute $A_{\mathfrak{p}}$ in $\mathsf{L}(N(\mathfrak{p}))^{1+o(1)}$ expected time.*

REMARK 5.6. An exponential-time algorithm for computing $A_{\mathfrak{p}}$ using Hilbert class polynomials H_D whose discriminants D divide $a_{\mathfrak{p}}^2 - 4N(\mathfrak{p})$ is given in [15]; the running time is not explicitly analyzed in [15], but we note that there are several algorithms to compute Hilbert class polynomials whose running times are quasilinear in $|D|$, which is close to the bit-size of H_D [7]. The fastest of

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

these relies on the GRH [64], but the algorithm in [27] does not, and as noted in [62, Remark 1.1], the heuristics used in [27] can be removed. This gives an unconditional deterministic algorithm to compute $A_\mathfrak{p}$ in time $N(\mathfrak{p})^{1+o(1)}$, but this is too slow to be useful to us here (and we require the GRH in any case).

In terms of its complexity in $q = N(\mathfrak{p})$, the subexponential-time algorithm to compute $A_\mathfrak{p}$ is much slower than Algorithm 4, which computes the Frobenius triples $(\det A_\mathfrak{p} \bmod \ell, \operatorname{tr} A_\mathfrak{p} \bmod \ell, \dim_1(A_\mathfrak{p} \bmod \ell))$ for primes $\ell \in S$ in time polynomial in $\log q$. However, when S is large (say on the order of $(\log N_E)^{1+o(1)}$) and q is relatively small (say $\log q$ is polynomial in $\log N_E$), the running times are essentially the same, and computing $A_\mathfrak{p}$ gives us more information; in particular, it allows us to distinguish the conjugacy classes of $\left(\begin{smallmatrix} x & 0 \\ 0 & x \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} x & 1 \\ 0 & x \end{smallmatrix}\right)$ in $\mathbf{GL}_2(\ell)$ even when $x \neq 1$, which is not possible with just the Frobenius triple. We shall make use of this in Section 5.4.

5.3. A Las Vegas algorithm. We now give a Las Vegas algorithm to compute $G_E(\ell)$ up to local conjugacy for all primes ℓ up to a given bound L by computing images of Frobenius elements $\mathrm{Frob}_\mathfrak{p}$ with $N(\mathfrak{p})$ up to a given bound P. Using the GRH-based bounds of Section 4 to determine L and P yields an algorithm whose expected running time is polynomial in $\log \|f\|$, where $y^2 = f(x)$ is an integral defining equation for E/K with $f \in \mathbf{Z}[\alpha][x]$ and $\|f\|$ is the maximum of the absolute values of the norms of the $\mathbf{Z}[\alpha]$-coefficients of f (which may also be defined in terms of the integer coefficients of f and $\operatorname{disc}(F)$, where $K = \mathbf{Q}[\alpha]/(F(\alpha))$).

ALGORITHM 5. Given an elliptic curve $E : y^2 = f(x)$ over $K = \mathbf{Q}[\alpha]/(F(\alpha))$ with integral coefficients and bounds L and P, compute for each prime $\ell \leqslant L$ a group $G_\ell \subseteq \mathbf{GL}_2(\ell)$ that is locally conjugate to a subgroup of $G_E(\ell)$ and contains a representative of $\rho_{E,\ell}(\mathrm{Frob}_\mathfrak{p})$ for all primes $\mathfrak{p}$ of K prime to $\ell \operatorname{disc}(F)$ and of good reduction for E with $N(\mathfrak{p}) \leqslant P$ as follows:

```
1. Let $S$ be the set of primes $\ell \leqslant L$, and for each $\ell \in S$ initialize the quantities
   $s_\ell \leftarrow \{\}$, $c_\ell \leftarrow 0$, $z_\ell \leftarrow 0$.
2. Compute the norm $\Delta_E \in \mathbf{Z}$ of the discriminant of $E$ and the discriminant
   $d_F \in \mathbf{Z}$ of the polynomial $F$.
3. For each rational prime $p \leqslant P$ that does not divide $\Delta_E$ or $d_F$:
     a. Factor $F(\alpha) \bmod p$ into irreducible $G_1(\alpha), \ldots, G_r(\alpha) \in \mathbf{F}_p[\alpha]$.
     b. For each $G_i$ with $\deg G_i \leqslant \log P / \log p$:
```

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

i. Use Algorithm 4 to compute the Frobenius triples

$$\tau_{\ell,\mathfrak{p}} := \big(\det \rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{p}}),\ \operatorname{tr} \rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{p}}),\ \dim_1 \rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{p}})\big)$$

for the prime $\mathfrak{p}$ of K with residue field $\mathbf{F}_p[\alpha]/G_i(\alpha)$ and each prime $\ell \in S - \{p\}$.

ii. For each prime $\ell \in S - \{p\}$ update $s_\ell \leftarrow s_\ell \cup \{\tau_{\ell,\mathfrak{p}}\}$ and $c_\ell \leftarrow c_\ell + 1$.

iii. If $\operatorname{tr} \rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{p}}) = 0$ then update $z_\ell \leftarrow z_\ell + 1$.

4. For each prime $\ell \in S$, use Algorithm 3 to construct generators for a subgroup G_ℓ of $\mathbf{GL}_2(\ell)$ with $\operatorname{sig}(G_\ell) = s_\ell$ and $|z(G_\ell) - z_\ell/c_\ell| < 1/8$ (if Algorithm 3 fails, report that P is too small and terminate).

5. Output the groups G_ℓ (specified by generators) and terminate.

Failure in step 4 can conceivably occur if s_ℓ and z_ℓ/c_ℓ do not actually correspond to a subgroup of $\mathbf{GL}_2(\ell)$, in which case the input to Algorithm 3 is invalid and this may cause it to fail (an event that can be easily detected), even though it is guaranteed to operate correctly on all valid inputs. This could happen if P is too small for every conjugacy class in $G_E(\ell)$ to be realized as the image of $\mathrm{Frob}_{\mathfrak{p}}$ with $N(\mathfrak{p}) \leqslant P$. The bounds in Section 4 allow us to choose P so that such a failure would disprove the GRH.

THEOREM 5.7. *Assume the GRH and let $K = \mathbf{Q}[\alpha]/(F(\alpha))$ be a fixed number field. There is a Las Vegas algorithm that, given an elliptic curve E/K in integral form $y^2 = f(x)$ with $f \in \mathbf{Z}[\alpha][x]$ that does not have complex multiplication, determines for every prime ℓ a subgroup $G_\ell \subseteq \mathbf{GL}_2(\ell)$ locally conjugate to $G_E(\ell)$. The algorithm outputs a bound L for which $G_E(\ell) = \mathbf{GL}_2(\ell)$ for all primes $\ell > L$, and a list of generators for G_ℓ for each prime $\ell \leqslant L$. The expected running time of the algorithm is bounded by*

$$(\log \|f\|)^{11+o(1)}.$$

Proof. Under the GRH, Proposition 4.3 guarantees that we have $G_E(\ell) = \mathbf{GL}_2(\ell)$ for all primes ℓ larger than $c_K(\log N_E)(\log\log N_E)^3$, where the constant c_K is effective and N_E is the absolute value of the norm of the conductor of E. By Ogg's formula [50], N_E is bounded by the norm of the discriminant of E, which can be expressed as a polynomial of bounded degree in terms of the coefficients of f. It follows that $\log N_E = O(\log \|f\|)$, where the implied constant is effective and depends only on K. We may thus take $L = (\log \|f\|)^{1+o(1)}$ as a bound on the primes ℓ that we need to consider.

Since K is fixed, we have $\deg F = O(1)$ and $\log q = O(\log p)$, and all the integers and finite field elements that arise in the algorithm have $O(\log p)$ bits.

Using fast arithmetic, we can assume the cost of each arithmetic operation in $\mathbf{Z}$, $\mathbf{F}_{\mathfrak{p}}$, $\mathbf{F}_p$ is $(\log p)^{1+o(1)}$; see [32], for example. Using the Cantor–Zassenhaus algorithm [14], step 3a takes $O((\log p)^{2+o(1)})$ expected time, by [32, Theorem 14.14], and the time to reduce E to $E_{\mathfrak{p}}$ is $(\log \|f\|)^{1+o(1)}$. The time for step 3b is $O((\log p)^{5+o(1)})$; this follows from [60, Corollary 11], which also applies to the constant degree extension $\mathbf{F}_{\mathfrak{p}}/\mathbf{F}_p$.

For the bound P, Corollary 4.7 implies that we can take $P = (\log \|f\|)^{10+o(1)}$, where the implied constants are again effective. Note that by Lemma 3.29, we only need to determine $z(G(E))$ to within $\epsilon < 1/8$. The running time of step 3 of Algorithm 5 is then bounded by

$$(\log \|f\|)^{10+o(1)}\big((\log \|f\|)^{1+o(1)} + (\log P)^{5+o(1)}\big) = (\log \|f\|)^{11+o(1)},$$

which dominates the cost of the other steps, including the time to determine the primes $\ell \leqslant L$ and $p \leqslant P$. □

5.4. A Monte Carlo algorithm. We now give a more efficient Monte Carlo algorithm to solve the same problem. Although it has a negligible impact on the worst-case asymptotic complexity that we can prove under the GRH, for practical purposes it is better to split the problem into two stages: (1) determine the primes ℓ for which $G_E(\ell) \neq \mathbf{GL}_2(\ell)$, and (2) compute $G_E(\ell)$ up to local conjugacy for each of these primes. If one assumes that Serre's question has an affirmative answer, meaning that the largest ℓ for which $G_E(\ell) \neq \mathbf{GL}_2(\ell)$ is bounded by a constant depending only on K, then the exceptional primes ℓ are bounded by $O(1)$ for any fixed K, but we do not want the correctness of the algorithm to depend on this, so we will typically consider many more primes ℓ in stage (1) (up to the GRH bound given by Corollary 4.3) than in stage (2). The key difference is that if $G_E(\ell) = \mathbf{GL}_2(\ell)$, we can unequivocally determine this after computing the image of just $O(1)$ random Frobenius elements, whereas computing $G_E(\ell) \subsetneq \mathbf{GL}_2(\ell)$ up to local conjugacy requires us to compute the image of $O(\ell)$ random Frobenius elements in the worst case.

PROPOSITION 5.8. *Let $\ell > 7$ be prime. A subgroup G of $\mathbf{GL}_2(\mathbf{F}_\ell)$ contains $\mathbf{SL}_2(\mathbf{F}_\ell)$ if and only if it contains elements g_1, g_2, g_3 with nonzero trace such that*

(1) *$\chi(g_1) = +1$;*

(2) *$\chi(g_2) = -1$;*

(3) *$u(g_3) \notin \{1, 2, 4\}$ and $u(g_3)^2 - 3u(g_3) + 1 \neq 0$ (equiv., $g_3^e \notin Z(\ell)$ for $e \leqslant 5$);*

where $\chi(g) = \left(\frac{\operatorname{tr}(g)^2 - 4\det(g)}{\ell}\right) \in \{0, \pm 1\}$ and $u(g) = \operatorname{tr}(g)^2/\det(g) \in \mathbf{F}_\ell$.

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

Proof. The reverse implication appears in [58, Proposition 19] and follows from Proposition 3.1; (1) and (2) together imply that no conjugate of G lies in $C_s^+(\ell)$, $C_{ns}^+(\ell)$, or $B(\ell)$, and (3) rules out the exceptional cases. Conversely, for $\ell > 7$ there exist $g_1, g_2, g_3 \in \mathbf{SL}_2(\mathbf{F}_\ell)$ satisfying conditions (1), (2), (3), respectively. □

Up to constant factors the following proposition is implied by [37, Theorem 5.1] (and its proof), but here we give a slightly more precise statement.

PROPOSITION 5.9. *Let $\ell > 7$ be prime and let G be subgroup of $\mathbf{GL}_2(\mathbf{F}_\ell)$ containing $\mathbf{SL}_2(\mathbf{F}_\ell)$. Let $X_1, X_2, \ldots$ be a sequence of independent random variables uniformly distributed over G. Let X be the integer random variable for which the event $X = r$ occurs if r is the least integer for which $\{X_1, \ldots, X_r\}$ include g_1, g_2, g_3 of nonzero trace that satisfy the three criteria of Proposition 5.8. The expected value $\mathbf{E}[X]$ of X satisfies $\mathbf{E}[X] < 8$, and $\mathbf{E}[X] \to 3$ as $\ell \to \infty$.*

Proof. We consider the waiting times for each of the conditions (1) to (3) in Proposition 5.8 to be satisfied. From Table 1, we see that $\mathbf{SL}_2(\mathbf{F}_\ell)$ contains $(\ell-1)(\ell^2+\ell)/2$ elements g_1 for which $\chi(g_1) = +1$, of which at most $\ell^2+\ell$ have trace zero. The same is true of every coset of $\mathbf{SL}_2(\mathbf{F}_\ell)$ in G; applying $\#\mathbf{SL}_2(\mathbf{F}_\ell) = \ell^3 - \ell$ yields

$$\frac{\#\{g \in G : \chi(g) = 1, \mathrm{tr}(g) \neq 0\}}{\#G} \geqslant \frac{\ell-3}{2\ell-2} \longrightarrow \frac{1}{2} \quad \text{as } \ell \to \infty,$$

and we note that the LHS is never less than $2/5$ for $\ell \geqslant 11$. A similar argument shows that

$$\frac{\#\{g \in G : \chi(g) = -1, \mathrm{tr}(g) \neq 0\}}{\#G} \geqslant \frac{\ell-3}{2\ell+2} \longrightarrow \frac{1}{2} \quad \text{as } \ell \to \infty,$$

and the LHS is at least $1/3$ for $\ell \geqslant 11$. The events represented by these ratios are disjoint, so with probability approaching 1 as $\ell \to \infty$, one of them occurs for X_1, and the expected waiting time for both to occur approaches 3 as $\ell \to \infty$.

The images of $C_s(\ell) \cap \mathbf{SL}_2(\mathbf{F}_\ell)$ and $C_{ns}(\ell) \cap \mathbf{SL}_2(\mathbf{F}_\ell)$ in $\mathbf{PSL}_2(\mathbf{F}_\ell)$ are cyclic groups of order $(\ell-1)/2$ and $(\ell+1)/2$, respectively, and the same applies to their conjugates. In each of these groups there are only 10 elements of order at most 5, hence these occur with probability approaching 0 as $\ell \to \infty$. Switching to a coset of $\mathbf{SL}_2(\mathbf{F}_\ell)$ and considering images in $\mathbf{PGL}_2(\mathbf{F}_\ell)$ can only decrease the probability of getting an element of order at most 5. On the other hand, every $g \in G$ with $\chi(g) = \pm 1$ lies in a conjugate of $C_s(\ell)$ or $C_{ns}(\ell)$, and we have already noted that the probability that X_1 is such an element approaches 1 as $\ell \to \infty$.

Thus with probability approaching 1 as $\ell \to \infty$, condition (3) is satisfied by X_1 and this implies $\mathbf{E}[X] \to 3$.

A direct calculation shows that for $\ell > 7$ the probability that X_1 satisfies both conditions (2) and (3) is never less than $1/6$, and since (1) and (2) are disjoint, the expected waiting time for either (1) or both (2) and (3) to be satisfied is bounded by $30/17 < 2$, and this implies $\mathbf{E}[X] < 2 + 6 = 8$. □

For $\ell \leqslant 7$ we rely on the following proposition.

PROPOSITION 5.10. *Let G be a subgroup of $\mathbf{GL}_2(\ell)$. For $\ell = 2$ the group G contains $\mathbf{SL}_2(2)$ if and only if it contains g_1, g_2 with* $\operatorname{tr}(g_1) = 1$ *and* $\dim_1(g_2) = 1$. *For $\ell > 2$ the group G contains $\mathbf{SL}_2(\ell)$ if and only if it contains g_1, g_2 with* $\chi(g_1) = -1$, $\chi(g_2) = 0$ *and* $\dim_1(g_2) = 1$.

Proof. The case $\ell = 2$ is easily checked, so we assume $\ell > 2$. For the ‘if’ direction, we note that the criteria for g_1 ensure that G is not contained in a Borel group or in the normalizer of a split Cartan. For $\ell > 5$ the fact that g_2 has projective order divisible by ℓ rules out exceptional subgroups, and for $\ell = 3, 5$ every exceptional subgroup containing an element of order ℓ also contains $\mathbf{SL}_2(\ell)$. For the ‘only if’ direction, we note that $\mathbf{SL}_2(\ell) \cap C_{ns}(\ell)$ has order $\ell + 1$ and thus contains a nonscalar element g_1 with $\chi(g_1) = -1$, and $\mathbf{SL}_2(\ell) \cap B(\ell)$ has order divisible by ℓ and contains a nonscalar element g_2 with $\chi(g_2) = 0$ and $\dim_1(g_2) = 1$. □

If one defines the integer random variable X as in Proposition 5.9 using the criterion that $\{X_1, \ldots, X_r\}$ contains g_1, g_2 as in Proposition 5.10, it is easy to show that $\mathbf{E}[X] < \ell + 2$. In particular, $\mathbf{E}[X] < 9$ for $\ell \leqslant 7$.

With these results in hand we now give a Monte Carlo algorithm for determining the set of primes ℓ for which $G_E(\ell)$ does not contain $\mathbf{SL}_2(\ell)$. Note that when $G_E(\ell)$ contains $\mathbf{SL}_2(\ell)$ we can determine $G_E(\ell)$ exactly by computing the intersection of K with the cyclotomic field $\mathbf{Q}(\zeta_\ell)$, a computation that does not depend on E and takes negligible time for any fixed number field K.

ALGORITHM 6. Given an elliptic curve $E\colon y^2 = f(x)$ over $K = \mathbf{Q}[\alpha]/(F(\alpha))$ with integral coefficients and bounds $P > L \geqslant 5$, attempt to determine the set of primes $\ell \leqslant L$ for which $\mathbf{SL}_2(\ell) \not\subseteq G_E(\ell)$ as follows:

1. Initialize $S \leftarrow \{\ell \leqslant L \text{ prime}\}$ and create a table T with Boolean entries $T_{\ell,1}$, $T_{\ell,2}$, $T_{\ell,3}$ set to 0 for each $\ell \in S$, then set $T_{\ell,3} \leftarrow 1$ for $\ell \leqslant 7$.
2. Compute the norm $\Delta_E \in \mathbf{Z}$ of the discriminant of E and the discriminant $d_F \in \mathbf{Z}$ of the polynomial F.

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

3. Repeat the following $27\lceil 1+\log_3 M\rceil$ times, where $M = \#\{\ell \leqslant L \text{ prime}\}$:

- **a.** Pick a random prime $p \in [P, 2P]$ that does not divide Δ_E or d_F and a random prime $\mathfrak{p}$ of K lying above p and use Algorithm 4 to compute Frobenius triples

  $$\tau_{\ell,\mathfrak{p}} := (\det \rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{p}}),\ \operatorname{tr} \rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{p}}),\ \dim_1 \rho_{E,\ell}(\mathrm{Frob}_{\mathfrak{p}}))$$

  for each prime $\ell \in S$.
- **b.** For each prime $\ell \in S$, set $T_{\ell,i} \leftarrow 1$ if $\tau_{\ell,\mathfrak{p}}$ matches the conjugacy class of some $g_i \in \mathbf{GL}_2(\ell)$ satisfying (i) of Proposition 5.8 (for $\ell > 7$) or Proposition 5.10 (for $\ell \leqslant 7$); if $T_{\ell,1}, T_{\ell,2}, T_{\ell,3} = 1$, remove ℓ from S.

4. Output the set S and terminate.

REMARK 5.11. As written, this is not (strictly speaking) a Monte Carlo algorithm, since it uses Algorithm 4, which is a Las Vegas algorithm (meaning that is running time is potentially unbounded, even though its expected running is bounded by Proposition 5.2). This distinction has no practical relevance, but for the sake of staying consistent with our terminology, let us assume that Algorithm 6 automatically terminates Algorithm 4 if its actual running time exceeds its expected running time by an unreasonable factor, and terminates with failure in this case. Doing so decreases the probability of success only negligibly and we can easily keep it above $2/3$.

THEOREM 5.12. *Assume the GRH and let $K = \mathbf{Q}[\alpha]/(F(\alpha))$ be a fixed number field. There is a Monte Carlo algorithm with one-sided error that, given a non-CM elliptic curve E/K in integral form $y^2 = f(x)$ with $f \in \mathbf{Z}[\alpha][x]$, determines the set S_E of primes ℓ for which $G_E(\ell)$ does not contain $\mathbf{SL}_2(\ell)$ with probability greater than $2/3$. The running time of the algorithm is bounded by*

$$(\log \|f\|)^{1+o(1)},$$

and the set S it outputs always contains S_E.

Proof. We use Algorithm 6 with the modification indicated in Remark 5.11. Under the GRH we may take $L = (\log \|f\|)^{1+o(1)}$, by Proposition 4.3, and we may choose P so that $\log P = O(\log L)$. It is clear from Propositions 5.8 and 5.10 that the set S output by Algorithm 6 always contains S_E. Each call to Algorithm 4 in step 3a then takes $O((\log \|f\|)^{1+o(1)})$ time, and these calls dominate the total running time. After 27 iterations in step 3, for each prime $\ell \leqslant L$ not in S_E, the probability that ℓ remains in S is less than $1/3$ (this follows from Proposition 5.9

and the remark following Proposition 5.10, since we always have $\mathbf{E}[X] < 9$). After all $27\lceil 1 + \log_3 M\rceil$ iterations, this probability is less than $1/(3M)$, and a union bound shows that the probability that any prime $\ell \leqslant L$ not in S_E (of which there at most M) remains in S is less than $1/3$. □

REMARK 5.13. To amplify the success probability of Algorithm 6 we run it repeatedly and take the intersection of all the sets S output by the algorithm as our final result.

We now give a Monte Carlo algorithm to compute $G_E(\ell)$ up to local conjugacy for a given set of primes ℓ. Rather than attempting to compute the full signature s of each $G_E(\ell)$, we rely on the fact that s can be compactly represented by a subset $\overline{s}$ containing at most 11 triples, as explained in Section 3.6. Since we are sampling elements of s randomly, we have no way of knowing *a priori* whether a given triple necessarily belongs to $\overline{s}$. Instead, we dynamically construct an approximation to $\overline{s}$ that we update whenever we find a triple that does belong to the minimal signature compatible with our current approximation; for example, whenever we find a triple whose projective order exceeds $m(s) = \max\{|\pi(g)| : g \in G_E(\ell)\}$ or does not divide $\lambda(s) = \operatorname{lcm}\{|\pi(g)| : g \in G_E(\ell)\}$. When doing so we simultaneously remove any triples that are no longer necessary. Depending on the order in which we find elements, it may happen that the cardinality of our approximation to $\overline{s}$ temporarily exceeds 11, but its cardinality is always bounded by $O(\log \ell)$ and will eventually be no greater than 11.

ALGORITHM 7. Given an elliptic curve $E\colon y^2 = f(x)$ over $K = \mathbf{Q}[\alpha]/(F(\alpha))$ with integral coefficients, a bound P, and a nonempty set S of primes less than P, attempt to compute $G_E(\ell)$ up to local conjugacy for each prime $\ell \in S$ as follows:

1. Initialize variables $\overline{s}_\ell \leftarrow \{\}$, $c_\ell = 0$, $z_\ell \leftarrow 0$ for each $\ell \in S$.

2. Compute the norm $\Delta_E \in \mathbf{Z}$ of the discriminant of E and the discriminant $d_F \in \mathbf{Z}$ of the polynomial F.

3. Repeat the following $9\max(S)\lceil 1 + \log \#S\rceil$ times:

  a. Pick a random prime $p \in [P, 2P]$ that does not divide Δ_E or d_F, a random prime $\mathfrak{p}$ of K above p, and compute the matrix $A_\mathfrak{p}$ as in Theorem 5.5.

  b. For each prime $\ell \in S$ dividing $(\operatorname{tr} A_\mathfrak{p})^2 - 4N(\mathfrak{p})$, determine whether the order of $A_\mathfrak{p} \pmod{\ell}$ is divisible by ℓ and if so, add the triple $(1, 2, 1)$ to $\overline{s}_\ell$.

4. Repeat the following $9\lceil 60 + 2\lceil 1 + \log\log(1 + \max(S))\rceil\lceil 1 + \log \#S\rceil$ times:

a. Pick a random prime $p \in [P, 2P]$ not in S, a random prime $\mathfrak{p}$ of K above p, and compute the integer matrix $A_{\mathfrak{p}}$ as in Theorem 5.5.

b. For each prime $\ell \in S$:

i. Compute $A = A_{\mathfrak{p}} \pmod{\ell} \in \mathbf{GL}_2(\ell)$, set $A \leftarrow A^{\ell}$, and update $\overline{s}_\ell$ to reflect the triple $(\det A, \operatorname{tr} A, \dim_1 A)$.

ii. Increment c_ℓ, and if $\operatorname{tr} A = 0$ then increment z_ℓ.

iii. Set $A \leftarrow A^{|\pi(A)|}$ and update $\overline{s}_\ell$ to reflect the triple $(\det A, \operatorname{tr} A, \dim_1 A)$.

5. If the cardinality of any of the sets $\overline{s}_\ell$ exceeds 11, return to step 3.

6. For each prime $\ell \in S$, use Algorithm 3 to construct generators for a subgroup G_ℓ of $\mathbf{GL}_2(\ell)$ for which $s := \operatorname{sig}(G_\ell)$ satisfies $\overline{s} = \overline{s}_\ell$ and $|z(G_\ell) - z_\ell/c_\ell| < 1/8$ (if this fails for any reason, return to step 2).

7. Output the groups G_ℓ (specified by generators) and terminate.

REMARK 5.14. The constants in steps 3 and 4 are larger than necessary, and for practical implementation we note that steps 3 and 4 can be combined; we have written the algorithm this way in order to simplify the complexity analysis below. We also assume that Algorithm 7 is modified as in Remark 5.11 to terminate the Las Vegas algorithm used to compute $A_{\mathfrak{p}}$ if its running time exceeds its expected running time by an unreasonable factor; this ensures that the running time of Algorithm 7 is bounded.

THEOREM 5.15. *Assume the GRH. Let $K = \mathbf{Q}[\alpha]/(F(\alpha))$ be a fixed number field, let E/K be an elliptic curve in integral form $y^2 = f(x)$ with $f \in \mathbf{Z}[\alpha][x]$, let S be a set of primes $\ell \leqslant L$ that contains S_E, with $L = (\log N_E)^{1+o(1)}$ as in Proposition 4.3, and let $P = (\log N_E)^{10+o(1)}$ be as in Corollary 4.7. Given inputs E, P, and S, Algorithm 7 correctly determines $G_E(\ell)$ up to local conjugacy for all $\ell \in S_E$ with probability greater than $2/3$, and its running time is bounded by*

$$(\log \|f\|)^{1+o(1)}.$$

Proof. As argued in the proof of Theorem 5.7, we have $\log N_E = O(\log \|f\|)$, and this implies $\log P = O(\log\log \|f\|)$. It follows from Theorem 5.5 that the time to compute $A_{\mathfrak{p}}$ for any prime $\mathfrak{p}$ with $N(\mathfrak{p}) \in [P, 2P]$ is bounded by $(\log \|f\|)^{o(1)}$. The number of primes dividing $(\operatorname{tr} A_{\mathfrak{p}})^2 - 4N(\mathfrak{p})$ is bounded by $\log P = O(\log\log \|f\|)$, and it follows that the total time for step 3 is bounded by $O((\log \|f\|)^{1+o(1)})$, and this also applies to step 4. The cost of updating $\overline{s}_\ell$ is negligible because the cardinality of $\overline{s}_\ell$ is bounded by a constant factor of

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

$\log \ell \leqslant \log P = (\log\log \|f\|)$, and computing A^ℓ can be accomplished in time $O(\mathsf{M}(\log \ell)\log \ell)$, which is also polynomial in $\log\log \|f\|$. The time for the check in step 5 is quasilinear in $\#S = O((\log \|f\|)^{1+o(1)})$, the time for step 6 is bounded by $O(\#S(\log P)^{1+o(1)}) = O((\log \|f\|)^{1+o(1)})$, by Proposition 3.22, and this also bounds the time for step 7. This addresses the bound on the running time of Algorithm 7, it remains only to show that its output is correct with probability greater than 2/3.

Let $\ell \in S$ be a prime greater than 5 for which $G_E(\ell)$ has order divisible by ℓ. The proportion of elements of $G_E(\ell)$ of order divisible by ℓ is at least $1/\ell$, since $G_E(\ell)$ does not contain $\mathbf{SL}_2(\ell)$ and must therefore either lie in a Borel group or be an exceptional group whose image in $\mathbf{PGL}_2(\ell)$ has order divisible by $\ell = 3, 5$ (the claim holds in either case). After $3 \max S$ iterations of step 3 the probability that $(1, 2, 1) \notin s_\ell$ is less than $1/10$, and after $9 \max S\lceil 1 + \log \#S\rceil$ iterations the probability that $(1, 2, 1) \notin s_\ell$ for any $\ell \in S$ for which $G_E(\ell)$ has order divisible by ℓ is less than $1/10$.

The fact that step 4.b.iii is executed at least $18\lceil 1 + \log \#S\rceil$ times ensures that the probability that for some $\ell \in S$ the set $\overline{s}_\ell$ does not contain the triple of a generator for the scalar subgroup of $G_E(\ell)$ is very small, say less than $1/1000$. The same comment applies to the probability that $\overline{s}_\ell$ does not contain a triple whose determinant generates $\det(G_E(\ell))$ for some $\ell \in S$.

For each $\ell \in S$, after $3 \cdot 60 \cdot \lceil 1 + \log \#S\rceil$ iterations of step 4 the probability that we have not encountered representative A in step 4.b.i for the projective image of every element of $G_E(\ell)$ in the case that $G_(\ell)$ is an exceptional subgroup is less than $1/10$, and after the completion of step 4 the probability that this is true for any $\ell \in S$ is less than $1/10$. Similarly, for each $\ell \in S$, after $6\lceil 1 + \log\log(1 + \max(S))\rceil$ iterations of step 4 the probability that we have not encountered an A in step 4.b.i that has maximal projective order in the image of $G_E(\ell)$ under the ℓ-power map is less than $1/10$, and after the completion of step 4 the probability that this is true for any $\ell \in S$ is less than $1/10$.

In addition, after the completion of step 4 the probability that for some $\ell \in S$ for which $G_E(\ell)$ has dihedral projective image the set s_ℓ does not contain the signature of some $h \in G_E(\ell)$ whose projective image is not contained in the subgroup generated by some $g \in G_E(\ell)$ of maximal projective order whose signature lies in s_ℓ is negligible, say less than $1/1000$. Finally, we note that the probability that $|z(G_E(\ell)) - z_\ell/c_\ell| \geqslant 1/8$ for any $\ell \in S$ after the completion of step 3 is also negligible, say less than $1/1000$.

Taking a union bound, it follows that the probability that at the end of step 3 any of the sets $\overline{s}_\ell$ does not satisfy all the criteria listed in Section 3.6 for a suitable representative subset of $s = \mathrm{sig}(G_E(\ell))$ is less than $0.304 < 1/3$, and this also bounds the probability that any $\overline{s}_\ell$ has cardinality greater than 11. Thus we expect to return to step 4 in step 5 just $O(1)$ times, and when we reach step 6 we will compute subgroups G_ℓ that are locally conjugate to $G_E(\ell)$ for all $\ell \in S$ with probability greater than $2/3$. □

Unlike the Las Vegas algorithm given in Section 5.3, our Monte Carlo algorithm explicitly relies on the use of a compact representation $\bar{s}_\ell$ of the signature of $G_E(\ell)$ that contains only a bounded number of triples (at most 11, as noted in Section 3.6), and on the fact that we can compute $A_\mathfrak{p}$ in subexponential time; both are crucial to obtaining a quasilinear running time.

5.5. Distinguishing locally conjugate subgroups. As written, our algorithms cannot distinguish nonconjugate subgroups G and G' of $\mathbf{GL}_2(\ell)$ that are locally conjugate. However, as noted in Remark 3.7, up to conjugacy the only case in which this can occur is when G and G' are of the form $G = \langle H, t\rangle$ and $G' = \langle H', t\rangle$, where $t = \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ and H and H' are subgroups of the split Cartan group $C_s(\ell)$ that are conjugate via $s = \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$ (so H' is H with the diagonal entries swapped). As proved in Theorem 3.32, if $G = G_E(\ell)$ for some elliptic curve E/K, then $G' = G_{E'}(\ell)$ for an elliptic curve E'/K isogenous to E that we can obtain by following a uniquely determined path of ℓ-isogenies with E and E' as endpoints. In most cases the curves E and E' are distinguished by the degrees of the minimal extensions of K over which they acquire a rational point of order ℓ. In terms of the groups $G := G_E(\ell)$ and $G' := G_{E'}(\ell)$, these are precisely the indices $d_1(G)$ and $d_1(G')$ of the largest subgroups of G and G' that stabilize a nonzero vector; these indices necessarily divide $\ell - 1$, and in most cases they are distinct. In this section, we give a Monte Carlo algorithm to compute $d_1(G)$ that runs in quasicubic time, using the fact that E admits a unique rational isogeny of degree ℓ.

REMARK 5.16. Even when $d_1(G) = d_1(G')$, after twisting E and E' appropriately (as described in Section 5.6), we may obtain a pair of elliptic curves $\tilde{E}$ and $\tilde{E}'$ for which $\tilde{G} := G_{\tilde{E}}(\ell)$ and $\tilde{G}' := G_{\tilde{E}'}(\ell)$ are again locally conjugate, but with $d_1(\tilde{G}) \neq d_1(\tilde{G}')$. We are then able to distinguish G and G' by computing $d_1(\tilde{G})$ and $d_1(\tilde{G}')$. This technique allowed us to distinguish every pair of locally conjugate groups that we encountered in our computations (see Section 6), but we note that there are subgroups G and G' of $\mathbf{GL}_2(\ell)$ to which it cannot be applied (the smallest example with surjective determinants occurs when $\ell = 29$).

We begin with a general result that was mentioned in the introduction. Recall that for each elliptic curve $E\colon y^2 = x^3 + Ax + B$ and integer m there is a square-free polynomial $f_{E,m}(x)$ with coefficients in $\mathbf{Z}[A, B]$ whose roots are the x-coordinates $x(P)$ of the nonzero points $P \in E[m]$, called the *m-division*

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

polynomial of E. For even integers m the factor $x^3 + Ax + B$ is typically removed from $f_{E,m}(x)$, in which case its roots are the x-coordinates of the points $P \in E[m] - E[2]$. More generally, one can remove the factor $f_{E,m'}(x)$ for each maximal proper divisor m' of m. We refer to the resulting polynomial $g_{E,m}(x)$ as the *primitive m-division polynomial* of E, which we note has the same splitting field as $f_{E,m}(x)$; the roots of $g_{E,m}(x)$ are the x-coordinates of the points in $E[m]$ of order m. The polynomials $f_{E,m}$ and $g_{E,m}$ can be efficiently computed using well-known recursive formulas [48].

LEMMA 5.17. *Let E be an elliptic curve over a number field K, let $m > 2$ be an integer, and let L be the splitting field of the m-division polynomial $f_{E,m}(x)$ over K. If $G_E(m)$ contains -1 then $K(E[m])$ is a quadratic extension of L, and otherwise $K(E[m]) = L$.*

Proof. Note that $\rho_{E,m}$ induces an isomorphism $\mathrm{Gal}(K(E[m])/K) \simeq G_E(m)$ by restricting each $\sigma \in \mathrm{Gal}(\overline{K}/K)$ to $K(E[m]) \subseteq \overline{K}$. Let $\{P, Q\}$ be a basis for $E[m]$ as a $\mathbf{Z}/m\mathbf{Z}$-module and consider the subgroup $H \subseteq G_E(m)$ corresponding to the inclusion of Galois groups

$$\mathrm{Gal}(K(E[m])/L) \subseteq \mathrm{Gal}(K(E[m])/K).$$

For each $\sigma \in H$ we have $\sigma(P) \in E[m]$ and $x(\sigma(P)) = x(P)$, and similarly for Q and $P + Q$. This implies $\sigma(P) = \pm P$, $\sigma(Q) = \pm Q$, and $\sigma(P) + \sigma(Q) = \sigma(P + Q) = \pm(P + Q)$, and therefore $\rho_{E,m}(\sigma) = \pm 1$; so $H \subseteq \{\pm 1\}$. If $-1 \in G_E(m)$ then $H = \{\pm 1\}$, since $\rho_{E,m}^{-1}(-1)$ fixes L, and otherwise H is trivial. □

COROLLARY 5.18. *Let E be an elliptic curve over a number field K, let $m > 2$ be an integer, let $g_{E,m}(x)$ be the primitive m-division polynomial of E, and let d be the minimal degree of a factor of $g_{E,m}(x)$ in $K[x]$. If $G_E(m)$ contains -1 then $d_1(G_E(m)) = 2d$.*

Proof. We assume $E\colon y^2 = x^3 + Ax + B$ is in short Weierstrass form. Let $P \in E[m]$ be a point of order m whose x-coordinate $x(P)$ is a root of a minimal degree factor of $g_{E,m}(x)$. Then $[K(x(P)) : K] = d$, and $[K(P) : K(x(P))] \leqslant 2$ since $y(P)^2 \in K(x(P))$. If $-1 \in G_E(m)$ then $[K(P) : K(x(P))] = 2$, since $\sigma\rho_{E,m}^{-1}$ fixes $K(x(P))$ but acts nontrivially on $K(P)$ (indeed, $\sigma(y(P)) = y(-P) = -y(P) \neq y(P)$ for $m > 2$). □

EXAMPLE 5.19. The converse of Corollary 5.18 is false; the curve 14a3 gives a counterexample with $m = 3$.

Locally conjugate subgroups of $\mathbf{GL}_2(\ell)$ necessarily have the same scalar subgroups, so having determined $G_E(\ell)$ up to local conjugacy, we know whether

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

or not it contains -1. As noted above, we are specifically interested in the case where $G_E(\ell)$ is a Borel subgroup (so E admits a rational isogeny of degree ℓ).

In what follows, the *degree* of a point $P \in E[m]$ is the degree of the extension $K(P)/K$ obtained by adjoining the coordinates of P to K; equivalently, it is the degree of the minimal extension L/K for which $P \in E[m](L)$. In terms of $G_E(m) \subseteq \mathrm{Aut}(E[m])$, the degree of P is the index of its stabilizer in $G_E(m)$. The quantity $d_1(G_E(m))$ is simply the minimal degree of a point of order m.

LEMMA 5.20. *Let E be an elliptic curve over a number field K that admits a unique rational isogeny φ of prime degree ℓ. The points in $E[\ell]$ of degree $d_1(G_E(\ell))$ all lie in the kernel of φ.*

Proof. We may assume that $G_E(\ell)$ lies in the Borel group $B(\ell)$ and contains $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$; it cannot lie in the split Cartan $C_s(\ell)$ because E admits only one rational isogeny of degree ℓ (up to composition with an isomorphism). The kernel of φ consists of the points $P \in E[\ell]$ whose stabilizer in $G_E(\ell)$ contains $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$. The orbit of any $P \in \ker\varphi$ under the action of $G_E(\ell)$ has cardinality at most $\ell - 1$, since $\ker\varphi$ is Galois stable and contains only $\ell - 1$ nonzero points; the stabilizer of P therefore has index at most $\ell - 1$, and it follows that $d_1(G) \leqslant \ell - 1$, since $\ker\varphi$ contains points of order ℓ. The stabilizer of any $P \in E[\ell]$ of degree less than ℓ must contain $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$, otherwise its index would be at least ℓ, so every point of degree $d_1(G)$ is in $\ker\varphi$. □

For a rational isogeny φ of prime degree $\ell > 2$, let $h_\varphi \in K[x]$ denote the *kernel polynomial* whose roots are the distinct x-coordinates $x(P)$ of the points $P \in \ker\varphi \subseteq E[\ell]$; it is a divisor of the ℓ-division polynomial $f_{E,\ell}(x)$. The kernel polynomials h_φ play a key role in Elkies' improvement to Schoof's algorithm [26, 56]; the degree of $h_\varphi(x)$ is just $(\ell - 1)/2$, compared to $(\ell^2 - 1)/2$ for $f_{E,\ell}(x)$.

COROLLARY 5.21. *Let E be an elliptic curve over a number field K that admits a unique rational isogeny φ of prime degree $\ell > 2$, and let d be the minimal degree appearing of a factor of $h_\varphi(x)$ in $K[x]$. Then $d_1(G_E(\ell)) \in \{d, 2d\}$, and if $G_E(\ell)$ contains -1 then $d_1(G_E(\ell)) = 2d$.*

Proof. The kernel of φ has prime order ℓ, hence it is generated by any nonzero $P \in \ker\varphi$. By the previous lemma, these P all have degree $d_1(G_E(\ell))$; let us pick one. The cyclic group $\langle P\rangle$ is invariant under the action of $\mathrm{Gal}(K(E[\ell])/K)$, so $K(P)/K$ is a cyclic Galois extension, and it contains the splitting field of $h_\varphi(x)$ over K, which must be equal to $K(x(P))$, an extension of degree d. Thus

$$d_1(G_E(\ell)) = [K(P) : K] = [K(P) : K(x(P))] \cdot [K(x(P)) : K]$$

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

is either d or $2d$, depending on whether $y(P)$ lies in $K(x(P))$, or a quadratic extension of $K(x(P))$. If $G_E(\ell)$ contains -1 then the latter must hold, by Corollary 5.18. □

The kernel polynomial $h_\varphi(x)$ can be computed using Elkies' algorithm (see [29, Alg. 27]), which uses the classical modular polynomial $\Phi_\ell \in \mathbf{Z}[X, Y]$ that is a canonical model for the modular curve $X_0(\ell)$. Under the GRH the polynomial $\Phi_\ell(X, Y)$ can be computed in $\ell^{3+o(1)}$ expected time [12]. By Proposition 4.3, for elliptic curves E without complex multiplication, we may assume that ℓ is bounded by $(\log \|f\|)^{1+o(1)}$, where $y^2 = f(x)$ is an integral equation for E/K. This yields a reasonably efficient algorithm to compute $h_\varphi(x)$, but factoring $h_\varphi(x)$ in $K[x]$ may be much more time consuming; the complexity bounds in [40] for factoring polynomial in $\mathcal{O}_K[x]$ give a running time of $(\log \|f\|)^{11+o(1)}$.

We can do much better than this by instead working modulo random primes $\mathfrak{p}$ of K. As noted in the proof of Corollary 5.21, the Galois group $\mathrm{Gal}(L/K)$ of the splitting field L of $h_\varphi(x)$ over K is cyclic, and this implies that we can compute the degree L/K by computing $h_\varphi(x)$ modulo several random primes $\mathfrak{p}$ and factoring the result over $\mathbf{F}_\mathfrak{p}$ (and we can restrict to degree-1 primes $\mathfrak{p}$); taking the least common multiple of the degrees of the factors will yield the degree of L/K with high probability (by the Chebotarev density theorem). Under the GRH it suffices to use $\mathfrak{p}$ with $\log N(\mathfrak{p})$ on the order of $\log \|f\|^{1+o(1)}$; with probability greater than $1/2$ just two primes $\mathfrak{p}$ are already enough to determine $[L : K]$.

The algorithm in [67] gives an efficient method to directly compute instantiated modular polynomials $\Phi_\ell(j(E), Y)$ modulo $\mathfrak{p}$, as well as instantiated derivatives of $\Phi_\ell(X, Y)$ that are required by Elkies' algorithm, allowing us to perform all our computations in finite fields $\mathbf{F}_\mathfrak{p}$. The expected time to compute the reduction of h_φ in $\mathbf{F}_\mathfrak{p}[x]$ is then bounded by $(\log \|f\|)^{3+o(1)}$, which also bounds the expected time to factor it in $\mathbf{F}_\mathfrak{p}[x]$ using probabilistic algorithms (see [32, Theorem 14.14]).

Having computed $d = [L : K]$, it remains only to determine whether $d_1(G_E(\ell))$ is equal to d or $2d$. If $-1 \in G_E(\ell)$ then Corollary 5.21 immediately implies the latter, and otherwise it suffices to determine whether the algebraic integer $f(\alpha)$ is a square in $\mathcal{O}_L$, where α is a root of the monic polynomial $h_\varphi(x)$; this computation can be efficiently accomplished via Hensel lifting and is dominated by the time to compute $h_\varphi(x)$. The following proposition summarizes our discussion.

PROPOSITION 5.22. *Let $E : y^2 = f(x)$ be a non-CM elliptic curve over a number field, and suppose that E admits a unique rational isogeny of degree ℓ. Under the GRH there is a Monte Carlo algorithm to compute $d_1(G_E(\ell))$ whose running time is bounded by* $(\log \|f\|)^{3+o(1)}$.

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

REMARK 5.23. We can easily determine ahead of time whether or not computing $d_1(G_E(\ell))$ will distinguish two locally conjugate possibilities G and G' for $G_E(\ell)$. As noted above, we may assume that G and G' lie in the Borel group $B(\ell)$ and are thus upper triangular, in which case $d_1(G)$ can be computed as the least common multiple of the orders in $\mathbf{Z}(\ell)^\times$ of the upper left entries of a set of generators for G, which takes just $(\log \ell)^{1+o(1)}$ time (and similarly for G').

5.6. Quadratic twists. Recall that if E/K is an elliptic curve and F is a quadratic extension of K, an elliptic curve E'/K whose base change to F is isomorphic to that of E is a *quadratic twist* of E. Up to K-isomorphism, for each quadratic extension F/K there is a unique elliptic curve E^F that is not K-isomorphic to E. Concretely, if E is defined by the equation $y^2 = f(x)$ and $F = K(\sqrt{d})$, then $dy^2 = f(x)$ is an equation for E^F; we assume throughout this section that E and E^F are defined by equations of this form.

We wish to consider the relationship between the Galois images $G_E(\ell)$ and $G_{E^F}(\ell)$. For $\ell = 2$ we always have $G_E(\ell) = G_{E^F}(\ell)$, since $E[2] = E^F[2]$, so we assume $\ell > 2$. Most of our results in fact apply to any integer $m > 2$, so we will work in this generality. The m-torsion points of E and E^F differ only in their y-coordinates, thus the splitting fields of the m-division polynomials $f_{E,m}(x)$ and $f_{E^F,m}(x)$ are identical; let L denote this field. It follows from Lemma 5.17 that either the m-torsion fields $K(E[m])$ and $K(E^F[m])$ are both quadratic extensions of L (the generic case), one is equal to L and the other is a quadratic extension, or both are equal to L. Which case occurs depends on whether both, one, or neither of the groups $G_E(m)$ and $G_{E^F}(m)$ contain -1.

LEMMA 5.24. *Let E be an elliptic curve over a number field K, let F be a quadratic extension of K, let $m > 2$ be an integer, and let L be the splitting field of the m-division polynomial of E. Then $-1 \notin G_{E^F}(m)$ if and only if $K(E[m])$ is the compositum of F and L.*

Proof. Let $F = K(\sqrt{d})$, $E\colon y^2 = f(x)$, and $E^F : dy^2 = f(x)$, and let φ denote the isomorphism $(x_0, y_0) \mapsto (x_0, y_0/\sqrt{d})$ between the base changes of E and E^F to F. We first suppose that $K(E[m])$ is the compositum of F and L and show that $-1 \notin G_{E^F}(m)$. If $F \subseteq L$ then $K(E[m]) = L$ and the base changes of E and E^F to L are isomorphic, hence $K(E^F[m]) = L$ and $G_{E^F}(m)$ does not contain -1, by Lemma 5.17. If $F \not\subseteq L$, then $K(E[m]) = L(\sqrt{d})$ and $K(E^F[m]) \subseteq L(\sqrt{d})$, and we claim that in fact $K(E^F[m]) = L$. Let σ be the nontrivial element of $\mathrm{Gal}(L(\sqrt{d})/L)$, corresponding to $-1 \in G_E(m)$. Then $\sigma(\sqrt{d}) = -\sqrt{d}$ and $\sigma(y_0) = -y_0$ for any nonzero $P = (x_0, y_0) \in E[m]$; it follows that σ fixes $\varphi(P)$, thus $K(E^F[m]) = L$ and $-1 \notin G_{E^F}(m)$.

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

We now suppose that $K(E[m])$ is not the compositum of F and L and show that $-1 \in G_{E^F}(m)$. If $F \subseteq L$ then $K(E[m])$ is a quadratic extension of L and the base changes of E and E^F to L are isomorphic; we cannot have $K(E^F[m]) = L$, since this would imply $K(E[m]) = L$. If $F \not\subseteq L$ then $F \not\subseteq K(E[m])$ and we cannot have $K(E^F[m]) = L$, since this would imply $\sqrt{d}$ and therefore F is contained in $K(E[m])$. Thus in either case $K(E^F[m]) \neq L$, and this implies $-1 \in G_{E^F}(m)$, by Lemma 5.17. □

COROLLARY 5.25. *Let E be an elliptic curve over a number field K, let F be a quadratic extension of K, let $m > 2$ be an integer, let L be the splitting field of the m-division polynomial of E, and let $G := \langle G_E(m), -1\rangle$.*

(a) *If $-1 \in G_E(m)$ then $G_{E^F}(m)$ is conjugate in $\mathbf{GL}_2(m)$ to either G or an index 2 subgroup of G that does not contain -1; the latter occurs precisely when F is a subfield of $K(E[m])$ not contained in L.*

(b) *If $-1 \notin G_E(m)$ then $G_{E^F}(m)$ is conjugate in $\mathbf{GL}_2(m)$ to either G or an index 2 subgroup of G that does not contain -1; the latter occurs precisely when F is a subfield of L.*

Proof. Let F, E, E^F, and φ be as in the previous lemma, and let us fix bases for $E[m]$ and $E^F[m]$ as $\mathbf{Z}/m\mathbf{Z}$-modules that are compatible with φ after base change. As an element of $\mathbf{GL}_2(m)$, the action of any $\sigma \in \mathrm{Gal}(\overline{K}/K)$ on $E[\ell]$ and $E^F[\ell]$ with respect to our chosen bases can differ only up to sign, thus we may assume $G_E(m)/(G_E(m) \cap \{\pm 1\}) = G_{E^F}(m)/(G_{E^F}(m) \cap \{\pm 1\})$.

We first consider (a), with $-1 \in G_E(m)$. In this case $K(E[m])$ is a quadratic extension of L, by Lemma 5.17. If $K(E[m])$ is not the compositum of F and L, then $G_{E^F}(m)$ contains -1 and $K(E^F[m])$ is also a quadratic extension of L (by the previous lemma), and therefore contains -1; we thus have $G_{E^F}(m)$ conjugate to $G_E(m) = G$, and either F does not lie in $K(E[m])$ or it is contained in L. If $K(E[m])$ is the compositum of F and L, then $K(E[m]) = L(\sqrt{d})$ and the previous lemma implies that $-1 \notin G_{E^F}(m)$ and therefore $K(E^F[m]) = L$. The actions of $\mathrm{Gal}(L(\sqrt{d})/K(\sqrt{d}))$ on $E[m]$ and $\mathrm{Gal}(L/K)$ on $E^F[m]$ with respect to our chosen bases commute with the isomorphism φ, and it follows that $G_{E^F}(m)$ is conjugate to the index 2 subgroup of $G_E(m) = G$ corresponding to $\mathrm{Gal}(L(\sqrt{d})/K(\sqrt{d})) = \mathrm{Gal}(K(E[m])/F)$, which does not contain -1, and this occurs only when F is a subfield of $K(E[m])$ not contained in L.

We now consider (b), with $-1 \notin G_E(m)$. in which case $K(E[m] = L$ is a subfield of $K(E^F[m])$, by Lemma 5.17. If $F \not\subseteq L$ then $K(E[m])$ is not the compositum of F and L and $-1 \in G_{E^F}(m)$, by the previous lemma; by the same argument used above, this implies that $G_E(m)$ is conjugate to an index 2

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

subgroup of $G_{E^F}(m)$, and we must have $G_{E^F}(m)$ conjugate to G. If $F \subseteq L$ then $K(E[m]) = L$ and $-1 \notin G_E(m)$, and since $K(E[m])$ is the compositum of F and L, we also have $-1 \notin G_{E^F}(m)$, by the previous lemma. So $G_{E^F}(m) = G_E(m)$ is an index 2 subgroup of G not containing -1, and this occurs only when $F \subseteq L$. □

In case (b) of Corollary 5.25, when F is a subfield of L the ℓ-torsion fields of E and its twist E^F coincide, but $E[m]$ and $E^F[m]$ are typically not isomorphic as Galois modules, and $G_E(m)$ and $G_{E^F}(m)$ need not be conjugate (or even locally conjugate) in $\mathbf{GL}_2(m)$, as shown by the following example.

EXAMPLE 5.26. Let $E/\mathbf{Q}$ be the elliptic curve $y^2 + y = x^3 - x^2 - 10x - 20$ with Cremona label 11a1, which we may also write as $y^2 = x^3 - 13392x - 1080432$. Its quadratic twist by $F = \mathbf{Q}(\sqrt{5})$ has Cremona label 275b2. The torsion field $\mathbf{Q}(E[5])$ can be written as $\mathbf{Q}[a]/(a^4 - a^3 + a^2 - a + 1)$ and is equal to the splitting field L of the 5-division polynomial of E. The field $\mathbf{Q}(E[5])$ contains F, so $\mathbf{Q}(E^F[5]) = \mathbf{Q}(E[5])$, and $G_E(\ell)$ and $G_{E^F}(\ell)$ are both index 2 subgroups of $G = \langle G_E(\ell), -1\rangle$, but they are not conjugate. Indeed, one finds that $G_E(\ell) \simeq \left\langle\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right)\right\rangle$ and $G_{E^F}(\ell) \simeq \langle\left(\begin{smallmatrix}3&0\\0&4\end{smallmatrix}\right)\rangle$ are nonconjugate cyclic groups of order 4. If we instead twist E by a quadratic field F' not contained in L, say $F' = \mathbf{Q}(\sqrt{-3})$, we obtain the elliptic curve with Cremona label 99d2 and find that $G_{E^{F'}}(\ell)$ is conjugate to both $\langle \pm\left(\begin{smallmatrix}1&0\\0&2\end{smallmatrix}\right)\rangle$ and $\langle \pm\left(\begin{smallmatrix}3&0\\0&4\end{smallmatrix}\right)\rangle$.

In the previous example, we obtained three nonconjugate subgroups of $\mathbf{GL}_2(5)$ as images of Galois representations arising in a family of quadratic twists of single elliptic curve E. The following lemma shows that for $m = \ell$ prime, up to conjugacy, three is maximal and can occur only when $G_E(\ell)$ lies in a Borel group.

LEMMA 5.27. *Let E be an elliptic curve over a number field K, let ℓ be a prime, and let n be the number of nonconjugate subgroups of $\mathbf{GL}_2(\ell)$ that arise as $G_{E^F}(\ell)$ for some quadratic twist E^F of E. Then $n \leqslant 3$; the case $n = 3$ can occur only when $G_E(\ell)$ lies in a Borel group, and the case $n = 2$ can occur only when $G_E(\ell)$ lies in either a Borel group or the normalizer of a Cartan group.*

Proof. For $\ell = 2$ we always have $n = 1$, so we assume that ℓ is odd and put $G := \langle G_E(\ell), -1\rangle$. It follows from Corollary 5.25 that n is at most one more than the number of index 2 subgroups of G that do not contain -1. Thus if $G_E(\ell) = G$ contains -1 and has no index 2 subgroups that do not contain -1, then $n = 1$; this applies whenever $G_E(\ell)$ contains $\mathbf{SL}_2(\ell)$ or has projective image isomorphic to A_4, S_4, or A_5 (by Lemma 3.21). By Proposition 3.1, we may now assume that

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

$G_E(\ell)$ (and therefore G) is contained in either a Borel group or the normalizer of Cartan group (possibly both).

Let us first suppose that the image of G in $\mathbf{PGL}_2(\ell)$ is dihedral; then G is a subgroup of the normalizer C^+ of a Cartan group C. If G_2 is an index 2 subgroup of G that does not contain -1, then G_2 also has dihedral image in $\mathbf{PGL}_2(\ell)$. If we put $H := G \cap C$ and $H_2 := G_2 \cap C$ and apply Lemma 3.13, we must be in case (2a) of the lemma, since H_2 does not contain -1, and H_2 is an index 2 subgroup of H that is normal in C^+. It follows from Corollaries 3.17 and 3.18 that H_2 determines G_2, and H has at most one index 2 subgroup that does not contain -1 and is normal in C^+, so there is at most one possible G_2; thus $n \leqslant 2$.

If G lies in a nonsplit Cartan group C_{ns} then it has at most one index 2 subgroup, since C_{ns} is cyclic, and we again have $n \leqslant 2$. Otherwise G lies in a Borel group B, which we now assume. The group G and its index 2 subgroups are uniquely determined by their intersections with the split Cartan group C_s contained in B; these are abelian groups, each of which can be written as a product of at most two cyclic groups. It follows that $G \cap C_s$ has at most three subgroups of index 2. If it has three, then at least one of them must contain -1, since if H_1 and H_2 are distinct index 2 subgroups of $G \cap C_s$ that do not contain -1 then $\langle H_1 \cap H_2, -1\rangle$ is an index 2 subgroup that contains -1. Thus G has at most two index 2 subgroups that do not contain -1, and we therefore have $n \leqslant 3$. □

REMARK 5.28. Lemma 5.27 does not apply to composite integers m. Indeed, for $m = 8$ there may be as many as 20 nonconjugate $G_{E^F}(m)$ that arise as F ranges over quadratic extensions of K; see [52] for examples.

For any subgroup G of $\mathbf{GL}_2(\ell)$ we refer to $\langle G, -1\rangle$ and its index 2 subgroups that do not contain -1 as *twists* of G (so G is always a twist of itself). If $G = G_E(\ell)$ for some elliptic curve E/K then the twists of G are precisely the subgroups that arise as $G_{E^F}(\ell)$ for some quadratic twist E^F (up to conjugacy in $\mathbf{GL}_2(\ell)$). Quadratic twists E^F that realize every possibility for $G_{E^F}(\ell)$ can be efficiently constructed using the results in this section. It suffices to determine the quadratic fields that lie in $K(E[\ell])$ (of which there are at most 3), and to determine which of these quadratic fields lies in the splitting field L of the ℓ-division polynomial of E. The discriminants of these quadratic fields must divide the discriminant of $K(E[\ell])$, whose prime divisors include only ℓ and the primes of bad reduction for E. Provided we can factor the discriminant of E, these fields can be determined by simply testing candidate fields F with suitable discriminants by computing $G_{E^F}(\ell)$; in practice this is much faster than attempting to explicitly compute the torsion field $K(G_E(\ell))$ and the quadratic extensions F/K it contains.

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

REMARK 5.29. If G is locally conjugate to G', then each of its twists H is locally conjugate to a corresponding twist H' of G'. If $G = G_E(\ell)$ for some elliptic curve E/K, then the twists of G and the twists of any locally conjugate G' all arise as images of Galois representations of elliptic curves defined over K. Thus the discovery of a subgroup G of $\mathbf{GL}_2(\ell)$ that arises as $G_E(\ell)$ may lead directly to as many as 5 other nonconjugate subgroups G' that arise as the image of Galois representations of curves that are twists of either E or the elliptic curve E' isogenous to E given by Theorem 3.32.

EXAMPLE 5.30. Consider the elliptic curve $E/\mathbf{Q}$ with Cremona label `11a3`, which has $G_E(5) = \langle \left(\begin{smallmatrix}1 & 0\\ 0 & 2\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)\rangle$. The group $G_E(5)$ has three twists, including itself. The other two are $\langle G_E(5), -1\rangle$ and its index two subgroup $\langle \left(\begin{smallmatrix}4 & 0\\ 0 & 3\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)\rangle$, which can be obtained as Galois images by twisting E by $\mathbf{Q}(\sqrt{-3})$ and $\mathbf{Q}(\sqrt{5})$, which yields curves with Cremona labels `99d1` and `275b1`, respectively. The group $G_E(5)$ is locally conjugate to $G_{E'}(\ell) = \langle \left(\begin{smallmatrix}2 & 0\\ 0 & 1\end{smallmatrix}\right)\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)\rangle$, where E' has Cremona label `11a2`. Twisting E' by $\mathbf{Q}(\sqrt{-3})$ and $\mathbf{Q}(\sqrt{5})$ yields curves with Cremona labels `99d3` and `275b3`, respectively, whose Galois images realize the corresponding twists of $G_{E'}(\ell)$. The six subgroups of $\mathbf{GL}_2(5)$ in this example are nonconjugate and listed in Table 3 under the labels `5b.1.1`, `5B.1.2`, `5B.1.3`, `5B.1.4`, `5B.4.1`, and `5B.4.2` (the curves listed in Table 3 for these groups are not all the same as those in this example, some have smaller conductor).

6. Computational results

We implemented the algorithms described in Section 5 using the C programming language (as noted earlier, Magma scripts implementing the algorithms in Section 3 are available at [68]). For the computation of Frobenius triples in Algorithm 4, at primes up to 2^{40} we relied on the `smalljac` software library [63] based on the algorithms described in [35], and for larger primes we used the implementation of the SEA algorithm described in [67]. For the computation of the matrices $A_\mathfrak{p}$ described in Section 5.2 we used a modified version of the algorithm in [9] that was optimized for smaller primes, using techniques described in [64, Section 4] and [67].

As a key practical optimization, we precomputed tables of Frobenius triples for every elliptic curve $E/\mathbf{F}_p$, for primes $p \leqslant 2^{16}$. This allows us to compute Frobenius triples for the reductions of an elliptic curve E over a number field K at degree-1 primes $\mathfrak{p}$ of K with $N(\mathfrak{p}) \leqslant 2^{16}$ by simply doing a table lookup; this is particularly useful when computing Galois images for large families of elliptic curves. While 2^{16} is typically much smaller than the $(\log N_E)^{10+o(1)}$ bound given by the GRH-based Chebotarev bounds of Corollary 4.7, in the typical

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

case where $\rho_{E,\ell}$ is surjective we can usually obtain an unconditional proof of this fact by computing Frobenius triples for just a handful of small primes of good reduction; typically just ten or twenty primes suffice. This optimization dramatically improves the practical efficiency of our algorithms because it allows us to very quickly determine a small set of primes S that we know contains the set of exceptional primes S_E (the primes ℓ for which $G_E(\ell)$ does not contain $\mathbf{SL}_2(\ell)$); this is the main motivation for treating Algorithms 6 and 7 separately.

We have applied our algorithms to several large databases of elliptic curves, including:

- Cremona's elliptic curve data [**19**], which includes all elliptic curves over $\mathbf{Q}$ of conductor less than 350 000 (about 2 million curves);
- the Stein–Watkins table of elliptic curves [**61**], which includes a large proportion of the elliptic curves over $\mathbf{Q}$ of conductor up to 10^8, and of prime conductor up to 10^{10} (about 140 million curves);
- the L-functions and modular forms database (LMFDB) [**44**, **45**], which includes Cremona's tables as well as some 150 000 elliptic curves of small conductor over quadratic and cubic fields.

We also analyzed more than 10^9 elliptic curves of bounded height over $\mathbf{Q}$ and ten quadratic fields (the five real and five imaginary quadratic fields of least absolute discriminant). In addition to these, we analyzed elliptic curves in families parameterized by various modular curves, including:

- the modular curves X_H of genus 0 described in [**74**];
- the modular curve $X_{S_4}(7)$ of genus 0 over $\mathbf{Q}(\sqrt{-7})$, using the model in [**36**];
- the modular curve $X_s^+(11)$ of genus 2, using the model in [**2**];
- the modular curve $X_{ns}^+(11)$ of genus 1, using the model in [**16**];
- the (isomorphic) modular curves $X_s^+(13)$ and $X_{ns}^+(13)$ of genus 3, using the models given in [**4**];
- the modular curves $X_0(\ell)$ for primes $11 \leqslant \ell \leqslant 61$ of genus up to 5, using the models provided by the Magma [**11**] function `SmallModularCurve`, as well as quadratic points on these curves found in [**13**].

We restricted our attention to elliptic curves without complex multiplication and used our Monte Carlo algorithm to compute $G_E(\ell)$ up to local conjugacy. In cases where we were not able to unconditionally prove $G_E(\ell) = \mathbf{GL}_2(\ell)$ we repeated the algorithm 200 times, thereby ensuring (under the GRH) that the probability of error is less than 3^{-200}.

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

Having computed $G_E(\ell)$ up to local conjugacy, in each case with two nonconjugate groups G and G' locally conjugate to $G_E(\ell)$ we computed $d_1(G_E(\ell))$ via Proposition 5.22, and in cases with $d_1(G) \neq d_1(G')$ used this information to determine $G_E(\ell)$ up to conjugacy. We encountered only one case with $d_1(G) = d_1(G')$, arising for the groups labeled `11B.10.4` and `11B.10.5` in Table 3, but in this case G and G' have twists that are not locally conjugate, and by twisting E appropriately we were able to determine $G_E(\ell)$ up to conjugacy, as described in Section 5.6.

REMARK 6.1. Thanks to recent work by Zywina [74], for the elliptic curves $E/\mathbf{Q}$ that we found to have exceptional Galois images $G_E(\ell)$, we were able to independently verify our results using his explicit models of modular curves $X_H/\mathbf{Q}$ of prime level that include every subgroup H of $\mathbf{GL}_2(\ell)$ that is known to arise for a non-CM elliptic curve over $\mathbf{Q}$; in no instance did we find an error in our computations.

6.1. Results over Q.

In total we found 63 exceptional Galois images $G_E(\ell)$ for non-CM elliptic curves $E/\mathbf{Q}$. These are listed in Table 3, along with an elliptic curve of minimal conductor that realizes $G_E(\ell)$. In collaboration with John Cremona, our results for elliptic curves of conductor up to 350 000 have now been incorporated into Cremona's tables and the LMFDB.

REMARK 6.2. Although we analyzed a total of more than 10^{10} elliptic curves $E/\mathbf{Q}$, every exceptional $G_E(\ell)$ that we found already occurs for a curve in Cremona's tables; indeed the largest conductor needed to obtain every exceptional $G_E(\ell)$ that we found is 232, 544, which is the conductor of curve listed for the group labeled `11Nn`.

6.2. Results over quadratic fields for elliptic curves with rational j-invariants.

It follows from Conjecture 1.1 that the exceptional Galois images $G_E(\ell)$ that do not contain $\mathbf{SL}_2(\ell)$ that can arise when E is the base change of a non-CM elliptic curve over $\mathbf{Q}$ to a quadratic field are, up to conjugation in $\mathbf{GL}_2(\ell)$, the 63 exceptional $G_E(\ell)$ that arise over $\mathbf{Q}$ and their subgroups of index 2. Using Algorithm 2, we can easily enumerate these groups, and we find that up to conjugacy in $\mathbf{GL}_2(\ell)$, there are 68 groups $G_E(\ell)$ that arise for base changes from $\mathbf{Q}$ to a quadratic field but not over $\mathbf{Q}$.

An elliptic curve E over a quadratic field K whose j-invariant lies in $\mathbf{Q}$ is either the base change of an elliptic curve over $\mathbf{Q}$, or a twist of such a curve. As we are only concerned with elliptic curves without complex multiplication, we can assume $j(E) \notin \{0, 1728\}$ and only need to consider quadratic twists. It

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

follows from Corollary 5.25 that the groups $G_E(\ell)$ that can arise when E is an elliptic curve over a quadratic field with $j(E) \in \mathbf{Q}$ are the groups G that arise for base changes from $\mathbf{Q}$ and their *twists*, as defined in Section 5.6: these are the groups $\langle G, -1\rangle$ and its index 2 subgroups that do not contain -1. A computation shows that, up to conjugation in $\mathbf{GL}_2(\ell)$ and assuming Conjecture 1.1, there are 23 such twists that do not arise for the base change of an elliptic curve over $\mathbf{Q}$, We thus obtain the following result.

THEOREM 6.3. *Assume Conjecture 1.1. Up to conjugation in $\mathbf{GL}_2(\ell)$ there are* 160 *Galois images $G_E(\ell)$ that do not contain $\mathbf{SL}_2(\ell)$ and arise for non-CM elliptic curves E over quadratic fields with $j(E) \in \mathbf{Q}$ and primes ℓ; these are listed in Tables 3 to 6. Of these,* 63 *arise over $\mathbf{Q}$,* 68 *arise for base changes of elliptic curves over $\mathbf{Q}$ but not over $\mathbf{Q}$, and* 29 *arise only for elliptic curves that are not base changes from $\mathbf{Q}$.*

Of the 68 exceptional groups that arise for base changes E_K of elliptic curves $E/\mathbf{Q}$ to quadratic fields K (but not over $\mathbf{Q}$), 23 have surjective determinant map (these are listed in Table 4) and 45 do not (these are listed in Table 5). Along with each group we list an elliptic curve $E/\mathbf{Q}$ and the discriminant D of a quadratic field K for which $G_{E_K}(\ell)$ is conjugate to the group listed. In each case K is a subfield of $\mathbf{Q}(E[\ell])$; taking $D = (-1/\ell)\ell$ to be the discriminant of the quadratic subfield of the cyclotomic field $\mathbf{Q}(\zeta_\ell))$ yields the subgroup of $G_E(\ell)$ with square determinants, while any other quadratic subfield K of $\mathbf{Q}(E[\ell])$ yields a group whose determinant map is surjective.

The 29 elliptic curves listed in Table 6 are quadratic twists E_K^F of base changes of elliptic curves $E/\mathbf{Q}$ to quadratic fields K by quadratic subextensions F/K of $K(E_K[\ell])/K$ that were computed using the methods described in Section 5.6.

6.3. Results over quadratic and cubic fields. As noted above, the LMFDB includes tables of elliptic curves of small conductor over various quadratic and cubic fields, including the five real and five imaginary quadratic fields of least absolute discriminant, as well as the cubic field of discriminant -23. The enumeration of modular elliptic curves over the five imaginary quadratic fields $\mathbf{Q}(\sqrt{-1})$, $\mathbf{Q}(\sqrt{-2})$,$\mathbf{Q}(\sqrt{-3})$, $\mathbf{Q}(\sqrt{-7})$, and $\mathbf{Q}(\sqrt{-11})$ was originally addressed by Cremona in [20, 21] who constructed tables for elliptic curves of conductor norm up to 500; these results have recently extended to conductor norm 10 000 by Cremona and his student Warren Moore. The tabulation of elliptic curves over the real quadratic field $\mathbf{Q}(\sqrt{5})$ described in [10] has been extended to conductor norm 5000, and the LMFDB also contains data for elliptic curves over $\mathbf{Q}(\sqrt{2})$ and $\mathbf{Q}(\sqrt{3})$ to conductor norm 5000, and over $\mathbf{Q}(\sqrt{13})$ and $\mathbf{Q}(\sqrt{17})$ to conductor norm 2000 and 1000, respectively (as of this writing). In addition, elliptic curves over the cubic field $\mathbf{Q}[a]/(a^3 - a^2 + 1)$ of discriminant -23 of conductor norm up to 10 000 are included in the LMFDB, based on the work in [24].

In total, we computed $G_E(\ell)$ for 115, 894 non-CM elliptic curves over these fields that are listed in the LMFDB, as well as families of elliptic curves of bounded height, and curves parameterized by points of bounded height on the modular curves listed above. Table 7 list the exceptional groups $G_E(\ell)$ that we found for non-CM elliptic curves over the ten quadratic fields noted above that are not already listed in Tables 3 to 6. It follows from [74] and the results of Section 5.6 that these groups cannot arise for non-CM elliptic curves over quadratic fields that have rational j-invariants (we do not require Conjecture 1.1 here because these groups all lie in the Borel group).

Table 8 lists the exceptional groups $G_E(\ell)$ that we found for non-CM elliptic curves over the cubic field of discriminant -23 that do not already appear in Tables 3–7.

REMARK 6.4. Unlike the results listed in Tables 3–6, which are complete under Conjecture 1.1, Table 7 are known to be incomplete. In particular, it follows from [43, Proposition 4.4.8.1] that there are infinitely many elliptic curves over each of the ten quadratic fields that we consider with $G_E(11)$ conjugate to a subgroup of `11S4`, but none are listed in our tables.

REMARK 6.5. The elliptic curves listed in Table 3 for the groups labeled `7Ns.2.1` and `7Ns.3.1` both have j-invariant $2268945/128$ and represent the unique $\overline{\mathbf{Q}}$-isomorphism class of elliptic curves $E/\mathbf{Q}$ that are exceptions to the local–global principle for isogenies [65]: each admits a rational 7-isogeny locally everywhere (modulo every prime of good reduction), but not globally (over $\mathbf{Q}$). The elliptic curve listed in Table 4 for the group labeled `13A4.1[2]` is the base change of the elliptic curve over $\mathbf{Q}$ listed in Table 3 for the group labeled `13S4` to $\mathbf{Q}(\sqrt{13})$; it represents one of five $\overline{\mathbf{Q}}$-isomorphism classes of elliptic curves over $\mathbf{Q}(\sqrt{13})$ that are exceptions to the local–global principle for 13-isogenies [3, Corollary 1.9] (three have rational j-invariants and two do not). The elliptic curve listed in Table 4 for the group labeled `5Ns[2]` is one of infinitely many examples of elliptic curves over $\mathbf{Q}(\sqrt{5})$ with distinct j-invariants that admit a 5-isogeny locally everywhere but not globally, as proved in [3, Theorem 1.5], as is the curve listed in Table 7 for the group labeled `5Ns.2.1[2]`. These curves all have $G_E(5)$ conjugate to `5Ns[2]` or `5Ns.2.1[2]`; the former case may arise for the base change of an elliptic curve $E/\mathbf{Q}$ with $G_E(5)$ conjugate to `5Ns`, while the latter case can only arise only for elliptic curves $E/\mathbf{Q}(\sqrt{5})$ with $j(E) \notin \mathbf{Q}$.

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

6.4. Group labels. In the tables that follow conjugacy classes of subgroups G of $\mathbf{GL}_2(\ell)$ are identified by labels of the form

$$\ell S.a.b.c[d],$$

where ℓ is a prime, S is one of `G`, `B`, `Cs`, `Cn`, `Ns`, `Nn`, `A4`, `S4`, `A5`, while a, b, c are (optional) nonnegative integers whose meaning depends on S, as described below, and d is the index of $\det(G)$ in $\mathbf{Z}(\ell)^\times$; the suffix $[d]$ is omitted when $d = 1$. Let r be the least positive integer that generates the index d subgroup of $\mathbf{Z}(\ell)^\times$.

- `G`: G contains $\mathbf{SL}_2(\ell)$; the label ℓ`G` denotes $\mathbf{GL}_2(\ell)$ and ℓ`G`$[d]$ is used when $d = [\mathbf{GL}_2(\ell) : G] > 1$.

- `B`: G is conjugate to a subgroup of $B(\ell)$ that contains an element of order ℓ, the label ℓ`B` denotes $B(\ell)$ and ℓ`B`$[d]$ denotes ℓ`B` $\cap$ ℓ`G`$[d]$. The label ℓ`B`$.a.b[d]$ denotes the subgroup generated by

$$\begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix}, \quad \begin{pmatrix} b & 0 \\ 0 & r/b \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

  where the integers $a, b > 0$ are both as small as possible.

- `Cs`: G is conjugate to a subgroup of $C_s(\ell)$ (including scalar subgroups of $Z(\ell) \subseteq C_s(\ell)$). The label ℓ`Cs` denotes $C_s(\ell)$ and ℓ`Cs`$[d]$ denotes ℓ`Cs` $\cap$ ℓ`G`$[d]$. The label ℓ`Cs`$.a.b[d]$ denotes the subgroup generated by

$$\begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix}, \quad \begin{pmatrix} b & 0 \\ 0 & r/b \end{pmatrix},$$

  with $a, b > 0$ minimal.

- `Cn`: G is conjugate to a subgroup of $C_{ns}(\ell)$ that does not lie in $C_s(\ell)$. For $\ell = 2$ this is the index 2 subgroup of $\mathbf{GL}_2(2)$, which is denoted `2Cn`. For $\ell > 2$ the label ℓ`Cn` denotes $C_{ns}(\ell)$, and ℓ`Cn`$[d]$ denotes ℓ`Cn` $\cap$ ℓ`G`$[d]$. The label ℓ`Cn`$.a.b[d]$ denotes the subgroup generated by

$$\begin{pmatrix} a & \varepsilon b \\ b & a \end{pmatrix},$$

  with the integers $b > 0$, $a \geqslant 0$ chosen to make (a, b) lexicographically minimal.

- `Ns`: G is conjugate to a subgroup of $C_s^+(\ell)$ with dihedral projective image. The label ℓ`Ns` denotes $C_s^+(\ell)$, the label ℓ`Ns`$[d]$ denotes ℓ`Ns` $\cap$ ℓ`G`$[d]$, and ℓ`Ns`$.a.b[d]$ denotes the subgroup of $C_s^+(\ell)$ generated by

$$\begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix}, \quad \begin{pmatrix} 0 & b \\ -r/b & 0 \end{pmatrix},$$

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

with a and b minimal, and $\ell\texttt{Ns}.a.b.c[d]$ denotes the subgroup generated by

$$\begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix}, \quad \begin{pmatrix} 0 & b \\ -1/b & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & c \\ -r/c & 0 \end{pmatrix},$$

with $a, b, c > 0$ minimal.

`Nn`: G is conjugate to a subgroup of $C_{ns}^{+}(\ell)$ with dihedral projective image and not conjugate to any subgroup of $C_{s}^{+}(\ell)$. The label $\ell\texttt{Nn}$ denotes $C_{ns}^{+}(\ell)$ and $\ell\texttt{Nn}[d]$ denotes $\ell\texttt{Nn} \cap \ell\texttt{G}[d]$. The label $\ell\texttt{Nn}.a.b[d]$ denotes the subgroup generated by

$$\begin{pmatrix} a & \varepsilon b \\ b & a \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

with (a, b) lexicographically minimal, and $\ell\texttt{Nn}a.b.c[d]$ denotes the subgroup generated by

$$\begin{pmatrix} a & \varepsilon b \\ b & a \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \delta^{c},$$

where $\delta = \left(\begin{smallmatrix} x & \varepsilon y \\ y & x \end{smallmatrix}\right)$ is any generator for $C_{ns}(\ell)$ and $c = [Z(\ell) : G \cap Z(\ell)]$ as in Corollary 3.17.

`A4`: G has projective image isomorphic to A_4 and does not contain $\mathbf{SL}_2(\ell)$. This requires $d > 1$. The label $\ell\texttt{A4}.a[d]$ indicates $[\det(G) : \det(Z(G)] = a$ (which must be 1 or 3, the latter only when $\ell \equiv 1 \pmod 3$). Algorithm 1 can be used to obtain an explicit set of generators.

`S4`: G has projective image isomorphic to S_4 and does not contain $\mathbf{SL}_2(\ell)$. The label $\ell\texttt{S4}$ indicates $Z(G) = Z(\ell)$ and $d = 1$, while $\ell\texttt{S4}[d]$ is used for $d > 1$ when $[\det(G) : \det(Z(G))] = 2$, and $\ell\texttt{S4}.1[d]$ is used when $[\det(G) : \det(Z(G))] = 1$ (which implies $d > 1$). See Lemma 3.21 for a list of the cases that can occur. Algorithm 1 can be used to obtain an explicit set of generators.

`A5`: G has projective image isomorphic to A_5. This requires $\ell \equiv \pm 1 \pmod 5$ and $d > 1$. The label $\ell\texttt{A5}.[d]$ indicates $[\det(G) : \det(Z(G))] = 1$ (the only possible case, by Lemma 3.21). Algorithm 1 can be used to obtain an explicit set of generators.

A magma script that will compute the label of any subgroup of $\mathbf{GL}_2(\ell)$ is available at [68]; it also includes a procedure to construct a subgroup based on its label, with generators as above.

6.5. Tables of exceptional Galois images. Each of the tables that follow lists the following data:

- the first column lists the label of a group $G \subseteq \mathbf{GL}_2(\ell)$, as defined above, the second columns lists its index in $\mathbf{GL}_2(\ell)$, and the third lists the generators for G as indicated by the label;
- the column '-1' indicates whether the group G contains the scalar matrix -1 or not;
- t is the number of twists the group has (as defined in Section 5.6), equivalently, the number of nonconjugate $G_{E'}(\ell)$ that arise among the twists E' of E (defined over the same field K).
- d_0 is the index of the largest subgroup of G that fixes a linear subspace of $\mathbf{Z}(\ell)^2$; equivalently, the degree of the minimal extension over which E admits a rational ℓ-isogeny.
- d_1 is the index of the largest subgroup of G that fixes a nonzero vector in $\mathbf{Z}(\ell)^2$; equivalently, the degree of the minimal extension over which E has a rational point of order ℓ.
- d is the order of G; equivalently, the degree of the minimal extension L/K for which $E[\ell] \subseteq E(L)$.
- the curve column lists the Weierstrass coefficients $[a_1, a_2, a_3, a_4, a_6]$ of an integral equation
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$
that defines an elliptic curve E/K. When $K \neq \mathbf{Q}$, these may be polynomials in $a \in \mathcal{O}_K$ with minimal polynomial $f(a)$, in which case the curve is listed as $[a_1, a_2, a_3, a_4, a_6]/(f(a))$. Curves are linked to their entry in the LMFDB, when available
- for elliptic curves E over quadratic fields with $j(E) \in \mathbf{Q}$ that are not base changes from $\mathbf{Q}$ we list $j(E)$.
- N is the absolute norm of the conductor of the elliptic curve E in factored form.
- D is the discriminant of the number field K (not listed when $K = \mathbf{Q}$).

Pairs of locally conjugate groups are indicated by brackets on the left, and for each such pair the listed curves are related by a chain of ℓ-isogenies, as in Theorem 3.32. Recall from Section 2 that we view elements of $\mathrm{Aut}(E[\ell])$ as 2×2 matrixes that act on column vectors on the **left** (this distinction is important because many of the groups are not conjugate to their transposes).

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

Table 3. Exceptional $G_E(\ell)$ for non-CM elliptic curves $E/\mathbf{Q}$.

Group	Index	Generators	-1	t	d_0	d_1	d	Curve	N
2Cs	6		Yes	1	1	1	1	[1, 1, 1, −10, −10]	$3^1 5^1$
2B	3	$\begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	1	1	1	2	[1, 0, 1, 4, −6]	$2^1 7^1$
2Cn	2	$\begin{pmatrix}0&1\\1&1\end{pmatrix}$	Yes	1	3	3	3	[0, −1, 0, −2, 1]	$2^2 7^2$
3Cs.1.1	24	$\begin{pmatrix}1&0\\0&2\end{pmatrix}$	No	2	1	1	2	[1, 0, 1, 4, −6]	$2^1 7^1$
3Cs	12	$\begin{pmatrix}2&0\\0&2\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}$	Yes	2	1	2	4	[1, 1, 0, 220, 2192]	$2^1 7^2$
3B.1.1	8	$\begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	1	6	[1, 0, 1, −1, 0]	$2^1 7^1$
3B.1.2	8	$\begin{pmatrix}2&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	2	6	[1, 0, 1, −171, −874]	$2^1 7^1$
3Ns	6	$\begin{pmatrix}2&0\\0&2\end{pmatrix}, \begin{pmatrix}0&2\\1&0\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}$	Yes	1	2	4	8	[1, 1, 1, 3, −5]	$2^1 13^2$
3B	4	$\begin{pmatrix}2&0\\0&2\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	2	12	[1, 1, 1, −3, 1]	$2^1 5^2$
3Nn	3	$\begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}2&1\\2&2\end{pmatrix}$	Yes	1	4	8	16	[0, 0, 1, −7, 12]	$5^1 7^2$
5Cs.1.1	120	$\begin{pmatrix}1&0\\0&2\end{pmatrix}$	No	3	1	1	4	[0, −1, 1, −10, −20]	11^1
5Cs.1.3	120	$\begin{pmatrix}3&0\\0&4\end{pmatrix}$	No	3	1	2	4	[0, 1, 1, −258, −2981]	$5^2 11^1$
5Cs.4.1	60	$\begin{pmatrix}4&0\\0&4\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}$	Yes	3	1	2	8	[0, 0, 1, −93, 625]	$3^2 11^1$
5Ns.2.1	30	$\begin{pmatrix}2&0\\0&3\end{pmatrix}, \begin{pmatrix}0&1\\3&0\end{pmatrix}$	Yes	1	2	8	16	[0, 0, 1, −2850, −58179]	$3^2 5^2 31^1$
5Cs	30	$\begin{pmatrix}2&0\\0&3\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}$	Yes	1	1	4	16	[0, 1, 0, −4319, −100435]	$2^8 71^1$
5B.1.1	24	$\begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	1	20	[0, −1, 1, 0, 0]	11^1
5B.1.2	24	$\begin{pmatrix}2&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	4	20	[0, −1, 1, −7820, −263580]	11^1
5B.1.4	24	$\begin{pmatrix}4&0\\0&3\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	2	20	[1, 0, 1, −76, 298]	$2^1 5^2$
5B.1.3	24	$\begin{pmatrix}3&0\\0&4\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	4	20	[1, 0, 1, −1, −2]	$2^1 5^2$
5Ns	15	$\begin{pmatrix}0&4\\1&0\end{pmatrix}, \begin{pmatrix}2&0\\0&3\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}$	Yes	1	2	8	32	[0, 0, 0, −56, 4848]	$2^5 19^1$
5B.4.1	12	$\begin{pmatrix}4&0\\0&4\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	2	40	[0, 0, 1, −3, −5]	$3^2 11^1$
5B.4.2	12	$\begin{pmatrix}4&0\\0&4\end{pmatrix}, \begin{pmatrix}2&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	4	40	[0, 0, 1, −70383, 7187035]	$3^2 11^1$
5Nn	10	$\begin{pmatrix}1&0\\0&4\end{pmatrix}, \begin{pmatrix}2&3\\4&2\end{pmatrix}$	Yes	1	6	24	48	[1, −1, 1, −5, 2]	$3^3 5^2$
5B	6	$\begin{pmatrix}2&0\\0&3\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	1	1	4	80	[1, 1, 0, 504, −13112]	$2^1 13^2$
5S4	5	$\begin{pmatrix}0&3\\3&4\end{pmatrix}, \begin{pmatrix}2&0\\0&2\end{pmatrix}, \begin{pmatrix}3&0\\4&4\end{pmatrix}$	Yes	1	6	24	96	[0, 0, 0, 9, −18]	$2^2 3^4$

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

Table 3. *Continued*.

7Ns.2.1	112	$\begin{pmatrix}2&0\\0&4\end{pmatrix}, \begin{pmatrix}0&1\\4&0\end{pmatrix}$	No	2	2	6	18	[1, −1, 1, −2680, −50053]	$2^1 5^2 7^2$
7Ns.3.1	56	$\begin{pmatrix}3&0\\0&5\end{pmatrix}, \begin{pmatrix}0&1\\4&0\end{pmatrix}$	Yes	2	2	12	36	[1, −1, 0, −107, −379]	$2^1 5^2 7^2$
7B.1.1	48	$\begin{pmatrix}1&0\\0&3\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	1	42	[1, −1, 1, −3, 3]	$2^1 13^1$
7B.1.3	48	$\begin{pmatrix}3&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	6	42	[1, −1, 1, −213, −1257]	$2^1 13^1$
7B.1.2	48	$\begin{pmatrix}2&0\\0&5\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	3	42	[1, −1, 0, −107, 454]	$7^2 13^1$
7B.1.5	48	$\begin{pmatrix}5&0\\0&2\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	6	42	[1, −1, 0, 628, −17823]	$7^2 13^1$
7B.1.6	48	$\begin{pmatrix}6&0\\0&4\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	2	42	[1, 1, 1, −6910, −232261]	$2^1 3^1 7^2$
7B.1.4	48	$\begin{pmatrix}4&0\\0&6\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	3	42	[1, 1, 1, −50, 293]	$2^1 3^1 7^2$
7Ns	28	$\begin{pmatrix}0&6\\1&0\end{pmatrix}, \begin{pmatrix}3&0\\0&5\end{pmatrix}, \begin{pmatrix}1&0\\0&3\end{pmatrix}$	Yes	1	2	12	72	[0, 0, 1, 2580, 549326]	$3^2 5^2 41^1$
7B.6.1	24	$\begin{pmatrix}6&0\\0&6\end{pmatrix}, \begin{pmatrix}1&0\\0&3\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	2	84	[0, 0, 0, −43, −166]	$2^4 13^1$
7B.6.3	24	$\begin{pmatrix}6&0\\0&6\end{pmatrix}, \begin{pmatrix}3&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	6	84	[0, 0, 0, −3403, 83834]	$2^4 13^1$
7B.6.2	24	$\begin{pmatrix}6&0\\0&6\end{pmatrix}, \begin{pmatrix}2&0\\0&5\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	6	84	[1, −1, 1, −965, −11294]	$3^2 7^2 13^1$
7Nn	21	$\begin{pmatrix}1&0\\0&6\end{pmatrix}, \begin{pmatrix}2&5\\4&2\end{pmatrix}$	Yes	1	8	48	96	[0, −1, 1, −10158, 804091]	$23^2 29^1$
7B.2.1	16	$\begin{pmatrix}2&0\\0&4\end{pmatrix}, \begin{pmatrix}1&0\\0&3\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	3	126	[1, −1, 1, −5, 5]	$2^1 3^4$
7B.2.3	16	$\begin{pmatrix}2&0\\0&4\end{pmatrix}, \begin{pmatrix}3&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	6	126	[1, −1, 1, −95, −697]	$2^1 3^4$
7B	8	$\begin{pmatrix}3&0\\0&5\end{pmatrix}, \begin{pmatrix}1&0\\0&3\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	6	252	[1, −1, 0, 3, −1]	$2^1 3^4$
11B.1.4	120	$\begin{pmatrix}4&0\\0&6\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	5	110	[1, 1, 1, −305, 7888]	11^2
11B.1.6	120	$\begin{pmatrix}6&0\\0&4\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	10	110	[1, 1, 1, −30, −76]	11^2
11B.1.5	120	$\begin{pmatrix}5&0\\0&7\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	5	110	[1, 1, 0, −3632, 82757]	11^2
11B.1.7	120	$\begin{pmatrix}7&0\\0&5\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	10	110	[1, 1, 0, −2, −7]	11^2
11B.10.4	60	$\begin{pmatrix}10&0\\0&10\end{pmatrix}, \begin{pmatrix}4&0\\0&6\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	10	220	[1, −1, 0, −2745, −215726]	$3^2 11^2$
11B.10.5	60	$\begin{pmatrix}10&0\\0&10\end{pmatrix}, \begin{pmatrix}5&0\\0&7\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	10	220	[1, −1, 0, −270, 1777]	$3^2 11^2$
11Nn	55	$\begin{pmatrix}1&0\\0&10\end{pmatrix}, \begin{pmatrix}3&5\\8&3\end{pmatrix}$	Yes	1	12	120	240	[0, 0, 0, −6682520, 39157150032]	$2^5 13^2 43^1$
13S4	91	$\begin{pmatrix}3&0\\12&9\end{pmatrix}, \begin{pmatrix}2&0\\0&2\end{pmatrix}, \begin{pmatrix}9&5\\0&6\end{pmatrix}$	Yes	1	6	72	288	[0, 1, 0, −4788, 109188]	$2^2 3^1 5^2 13^2$
13B.3.1	56	$\begin{pmatrix}3&0\\0&9\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	3	468	[0, 1, 1, −114, 473]	$3^1 7^2$
13B.3.2	56	$\begin{pmatrix}3&0\\0&9\end{pmatrix}, \begin{pmatrix}2&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	12	468	[0, 1, 1, −44704, −3655907]	$3^1 7^2$
13B.3.4	56	$\begin{pmatrix}3&0\\0&9\end{pmatrix}, \begin{pmatrix}4&0\\0&7\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	6	468	[0, 1, 1, −19322, 1116938]	$3^1 7^2 13^2$
13B.3.7	56	$\begin{pmatrix}3&0\\0&9\end{pmatrix}, \begin{pmatrix}7&0\\0&4\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	12	468	[0, 1, 1, −7555032, −8001807082]	$3^1 7^2 13^2$

Table 3. *Continued.*

13B.5.1	42	$\begin{pmatrix}5&0\\0&8\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	1	1	4	624	[1, −1, 0, −139, 965]	$2^1 5^1 17^2$
13B.5.2	42	$\begin{pmatrix}5&0\\0&8\end{pmatrix}, \begin{pmatrix}2&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	1	1	12	624	[1, −1, 0, −126109, −17206537]	$2^1 5^1 17^2$
13B.5.4	42	$\begin{pmatrix}5&0\\0&8\end{pmatrix}, \begin{pmatrix}4&0\\0&7\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	1	1	12	624	[0, 0, 0, −338, 2392]	$2^8 5^1 13^2$
13B.4.1	28	$\begin{pmatrix}4&0\\0&10\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	6	936	[0, −1, 1, −2, −1]	$3^1 7^2$
13B.4.2	28	$\begin{pmatrix}4&0\\0&10\end{pmatrix}, \begin{pmatrix}2&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	12	936	[0, −1, 1, −912, 10919]	$3^1 7^2$
13B	14	$\begin{pmatrix}2&0\\0&7\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	1	1	12	1872	[1, −1, 0, −2, 6]	$2^1 5^2 7^2$
17B.4.2	72	$\begin{pmatrix}4&0\\0&13\end{pmatrix}, \begin{pmatrix}2&0\\0&10\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	1	1	8	1088	[1, 1, 0, −660, −7600]	$2^1 5^2 17^2$
17B.4.6	72	$\begin{pmatrix}4&0\\0&13\end{pmatrix}, \begin{pmatrix}6&0\\0&9\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	1	1	16	1088	[1, 1, 0, −878710, 316677750]	$2^1 5^2 17^2$
37B.8.1	114	$\begin{pmatrix}8&0\\0&14\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	1	1	12	15984	[1, 1, 1, −8, 6]	$5^2 7^2$
37B.8.2	114	$\begin{pmatrix}8&0\\0&14\end{pmatrix}, \begin{pmatrix}2&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	1	1	36	15984	[1, 1, 1, −208083, −36621194]	$5^2 7^2$

Table 4. Known exceptional $G_E(\ell)$ with surjective determinant for base changes of non-CM elliptic curves $E/\mathbf{Q}$ to quadratic fields $\mathbf{Q}(\sqrt{D})$.

Group	Index	Generators	-1	t	d_0	d_1	d	Curve	D
3Cn	6	$\begin{pmatrix}1&2\\1&1\end{pmatrix}$	Yes	1	4	8	8	[0, 0, 1, −7, 12]	−7
5Cn.0.1	60	$\begin{pmatrix}0&2\\1&0\end{pmatrix}$	Yes	1	2	8	8	[0, 0, 1, −2850, −58179]	−3
5Cn	20	$\begin{pmatrix}3&2\\1&3\end{pmatrix}$	Yes	1	6	24	24	[1, −1, 1, −5, 2]	−15
5Nn.1.1.1	20	$\begin{pmatrix}1&4\\3&4\end{pmatrix}, \begin{pmatrix}1&2\\1&1\end{pmatrix}$	Yes	1	6	24	24	[1, −1, 1, −5, 2]	−3
7Cs	56	$\begin{pmatrix}3&0\\0&5\end{pmatrix}, \begin{pmatrix}1&0\\0&3\end{pmatrix}$	Yes	2	1	6	36	[0, 0, 1, 2580, 549326]	−3
7Cn	42	$\begin{pmatrix}6&4\\6&6\end{pmatrix}$	Yes	1	8	48	48	[0, −1, 1, −10158, 804091]	−23
7Nn.1.3	42	$\begin{pmatrix}1&0\\0&6\end{pmatrix}, \begin{pmatrix}1&2\\3&1\end{pmatrix}$	Yes	1	4	24	48	[0, −1, 1, −10158, 804091]	161
11Cn	110	$\begin{pmatrix}10&1\\6&10\end{pmatrix}$	Yes	1	12	120	120	[0, 0, 0, −6682520, 39157150032]	−4
11Nn.1.3	110	$\begin{pmatrix}1&0\\0&10\end{pmatrix}, \begin{pmatrix}1&6\\3&1\end{pmatrix}$	Yes	1	6	60	120	[0, 0, 0, −6682520, 39157150032]	44
13B.12.1	84	$\begin{pmatrix}12&0\\0&12\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	2	312	[1, −1, 0, −139, 965]	17
13B.12.2	84	$\begin{pmatrix}12&0\\0&12\end{pmatrix}, \begin{pmatrix}2&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	12	312	[1, −1, 0, −126109, −17206537]	17

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

Table 4. *Continued*.

`13B.12.5`	84	$\begin{pmatrix}12&0\\0&12\end{pmatrix}, \begin{pmatrix}5&0\\0&3\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	4	312	[1, −1, 0, −139, 965]	221
`13B.12.3`	84	$\begin{pmatrix}12&0\\0&12\end{pmatrix}, \begin{pmatrix}3&0\\0&5\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	6	312	[1, −1, 0, −126109, −17206537]	221
`13B.12.4`	84	$\begin{pmatrix}12&0\\0&12\end{pmatrix}, \begin{pmatrix}4&0\\0&7\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	6	312	[0, 0, 0, −338, 2392]	8
`13B.12.6`	84	$\begin{pmatrix}12&0\\0&12\end{pmatrix}, \begin{pmatrix}6&0\\0&9\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	12	312	[0, 0, 0, −12818, −745992]	8
`17B.16.2`	144	$\begin{pmatrix}16&0\\0&16\end{pmatrix}, \begin{pmatrix}2&0\\0&10\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	8	544	[1, 1, 0, −660, −7600]	5
`17B.16.7`	144	$\begin{pmatrix}16&0\\0&16\end{pmatrix}, \begin{pmatrix}7&0\\0&15\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	16	544	[1, 1, 0, −878710, 316677750]	5
`17B.16.8`	144	$\begin{pmatrix}16&0\\0&16\end{pmatrix}, \begin{pmatrix}8&0\\0&11\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	8	544	[1, 1, 0, −660, −7600]	85
`17B.16.6`	144	$\begin{pmatrix}16&0\\0&16\end{pmatrix}, \begin{pmatrix}6&0\\0&9\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	16	544	[1, 1, 0, −878710, 316677750]	85
`37B.11.1`	228	$\begin{pmatrix}11&0\\0&27\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	6	7992	[1, 1, 1, −8, 6]	5
`37B.11.2`	228	$\begin{pmatrix}11&0\\0&27\end{pmatrix}, \begin{pmatrix}2&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	36	7992	[1, 1, 1, −208083, −36621194]	5
`37B.11.6`	228	$\begin{pmatrix}11&0\\0&27\end{pmatrix}, \begin{pmatrix}6&0\\0&25\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	12	7992	[1, 1, 1, −8, 6]	185
`37B.11.9`	228	$\begin{pmatrix}11&0\\0&27\end{pmatrix}, \begin{pmatrix}9&0\\0&29\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	18	7992	[1, 1, 1, −208083, −36621194]	185

Table 5. Known exceptional $G_E(\ell)$ with nonsurjective determinant for base changes of non-CM elliptic curves $E/\mathbf{Q}$ to quadratic fields $\mathbf{Q}(\sqrt{D})$.

Group	Index	Generators	-1	t	d_0	d_1	d	Curve	D
`3Cs.1.1[2]`	48		No	2	1	1	1	[1, 0, 1, 4, −6]	−3
`3Cs[2]`	24	$\begin{pmatrix}2&0\\0&2\end{pmatrix}$	Yes	2	1	2	2	[1, 1, 0, 220, 2192]	−3
`3B.1.1[2]`	16	$\begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	2	1	1	3	[1, 0, 1, −1, 0]	−3
`3Cn[2]`	12	$\begin{pmatrix}0&2\\1&0\end{pmatrix}$	Yes	1	2	4	4	[1, 1, 1, 3, −5]	−3
`3B[2]`	8	$\begin{pmatrix}2&0\\0&2\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	2	1	2	6	[1, 1, 1, −3, 1]	−3
`3Nn[2]`	6	$\begin{pmatrix}2&2\\2&1\end{pmatrix}, \begin{pmatrix}0&1\\2&0\end{pmatrix}$	Yes	1	4	8	8	[0, 0, 1, −7, 12]	−3
`5Cs.1.1[2]`	240	$\begin{pmatrix}1&0\\0&4\end{pmatrix}$	No	2	1	1	2	[0, −1, 1, −10, −20]	5
`5Cs.4.1[2]`	120	$\begin{pmatrix}4&0\\0&4\end{pmatrix}, \begin{pmatrix}1&0\\0&4\end{pmatrix}$	Yes	2	1	2	4	[0, 0, 1, −93, 625]	5
`5Cs[2]`	60	$\begin{pmatrix}2&0\\0&3\end{pmatrix}, \begin{pmatrix}1&0\\0&4\end{pmatrix}$	Yes	1	1	4	8	[0, 0, 1, −2850, −58179]	5
`5B.1.1[2]`	48	$\begin{pmatrix}1&0\\0&4\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	1	10	[0, −1, 1, 0, 0]	5
`5B.1.4[2]`	48	$\begin{pmatrix}4&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	2	10	[0, −1, 1, −7820, −263580]	5

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

Table 5. *Continued*.

`5Ns[2]`	30	$\begin{pmatrix}0&4\\1&0\end{pmatrix}, \begin{pmatrix}2&0\\0&3\end{pmatrix}, \begin{pmatrix}1&0\\0&4\end{pmatrix}$	Yes	1	2	8	16	[0, 0, 0, −56, 4848]	5
`5B.4.1[2]`	24	$\begin{pmatrix}4&0\\0&4\end{pmatrix}, \begin{pmatrix}1&0\\0&4\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	2	20	[0, 0, 1, −3, −5]	5
`5Nn[2]`	20	$\begin{pmatrix}4&3\\1&1\end{pmatrix}, \begin{pmatrix}4&2\\1&4\end{pmatrix}$	Yes	1	3	12	24	[1, −1, 1, −5, 2]	5
`5B[2]`	12	$\begin{pmatrix}2&0\\0&3\end{pmatrix}, \begin{pmatrix}1&0\\0&4\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	1	1	4	40	[1, 1, 0, 504, −13112]	5
`5A4.1[2]`	10	$\begin{pmatrix}2&0\\0&3\end{pmatrix}, \begin{pmatrix}3&3\\4&1\end{pmatrix}, \begin{pmatrix}2&0\\0&2\end{pmatrix}$	Yes	1	6	24	48	[0, 0, 0, 9, −18]	5
`7Cs.2.1[2]`	224	$\begin{pmatrix}2&0\\0&4\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}$	No	2	1	3	9	[1, −1, 1, −2680, −50053]	−7
`7Cs[2]`	112	$\begin{pmatrix}3&0\\0&5\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}$	Yes	2	1	6	18	[1, −1, 0, −107, −379]	−7
`7B.1.1[2]`	96	$\begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	2	1	1	21	[1, −1, 1, −3, 3]	−7
`7B.1.2[2]`	96	$\begin{pmatrix}2&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	2	1	3	21	[1, −1, 1, −213, −1257]	−7
`7B.1.4[2]`	96	$\begin{pmatrix}4&0\\0&4\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	2	1	3	21	[1, −1, 0, −107, 454]	−7
`7Ns[2]`	56	$\begin{pmatrix}0&6\\1&0\end{pmatrix}, \begin{pmatrix}3&0\\0&5\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}$	Yes	1	2	12	36	[0, 0, 1, 2580, 549326]	−7
`7B.6.1[2]`	48	$\begin{pmatrix}6&0\\0&6\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	2	1	2	42	[0, 0, 0, −43, −166]	−7
`7B.6.2[2]`	48	$\begin{pmatrix}6&0\\0&6\end{pmatrix}, \begin{pmatrix}2&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	2	1	6	42	[0, 0, 0, −3403, 83834]	−7
`7B.6.3[2]`	48	$\begin{pmatrix}6&0\\0&6\end{pmatrix}, \begin{pmatrix}3&0\\0&3\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	2	1	6	42	[1, −1, 1, −965, −11294]	−7
`7Nn[2]`	42	$\begin{pmatrix}3&3\\6&4\end{pmatrix}, \begin{pmatrix}4&6\\2&4\end{pmatrix}$	Yes	1	8	48	48	[0, −1, 1, −10158, 804091]	−7
`7B.2.1[2]`	32	$\begin{pmatrix}2&0\\0&4\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	2	1	3	63	[1, −1, 1, −5, 5]	−7
`7B[2]`	16	$\begin{pmatrix}3&0\\0&5\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	2	1	6	126	[1, −1, 0, 3, −1]	−7
`11B.1.4[2]`	240	$\begin{pmatrix}4&0\\0&9\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	2	1	5	55	[1, 1, 1, −30, −76]	−11
`11B.1.9[2]`	240	$\begin{pmatrix}9&0\\0&4\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	2	1	5	55	[1, 1, 0, −2, −7]	−11
`11B.10.2[2]`	120	$\begin{pmatrix}10&0\\0&10\end{pmatrix}, \begin{pmatrix}2&0\\0&7\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	2	1	10	110	[1, −1, 0, −2745, −215726]	−11
`11B.10.4[2]`	120	$\begin{pmatrix}10&0\\0&10\end{pmatrix}, \begin{pmatrix}4&0\\0&9\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	2	1	10	110	[1, −1, 0, −270, 1777]	−11
`11Nn[2]`	110	$\begin{pmatrix}10&9\\1&1\end{pmatrix}, \begin{pmatrix}7&2\\1&7\end{pmatrix}$	Yes	1	12	120	120	[0, 0, 0, −6682520, 39157150032]	−11
`13A4.1[2]`	182	$\begin{pmatrix}8&0\\0&5\end{pmatrix}, \begin{pmatrix}10&10\\11&2\end{pmatrix}, \begin{pmatrix}2&0\\0&2\end{pmatrix}$	Yes	1	4	48	144	[0, 1, 0, −4788, 109188]	13
`13B.3.1[2]`	112	$\begin{pmatrix}3&0\\0&9\end{pmatrix}, \begin{pmatrix}1&0\\0&4\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	3	234	[0, 1, 1, −114, 473]	13
`13B.3.4[2]`	112	$\begin{pmatrix}3&0\\0&9\end{pmatrix}, \begin{pmatrix}4&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	6	234	[0, 1, 1, −44704, −3655907]	13
`13B.4.1[2]`	56	$\begin{pmatrix}4&0\\0&10\end{pmatrix}, \begin{pmatrix}1&0\\0&4\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	6	468	[0, −1, 1, −2, −1]	13
`13B.5.1[2]`	84	$\begin{pmatrix}5&0\\0&8\end{pmatrix}, \begin{pmatrix}1&0\\0&4\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	1	1	4	312	[1, −1, 0, −139, 965]	13
`13B.5.2[2]`	84	$\begin{pmatrix}5&0\\0&8\end{pmatrix}, \begin{pmatrix}2&0\\0&2\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	1	1	12	312	[0, 0, 0, −338, 2392]	13

Table 5. *Continued.*

13B.5.4[2]	84	$\begin{pmatrix}5&0\\0&8\end{pmatrix}, \begin{pmatrix}4&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	1	1	12	312	[1, −1, 0, −126109, −17206537]	13
13B[2]	28	$\begin{pmatrix}2&0\\0&7\end{pmatrix}, \begin{pmatrix}1&0\\0&4\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	1	1	12	936	[1, −1, 0, −2, 6]	13
17B.4.1[2]	144	$\begin{pmatrix}4&0\\0&13\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	1	1	4	544	[1, 1, 0, −660, −7600]	17
17B.4.2[2]	144	$\begin{pmatrix}4&0\\0&13\end{pmatrix}, \begin{pmatrix}2&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	1	1	8	544	[1, 1, 0, −878710, 316677750]	17
37B.8.1[2]	228	$\begin{pmatrix}8&0\\0&14\end{pmatrix}, \begin{pmatrix}1&0\\0&3\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	1	1	12	7992	[1, 1, 1, −8, 6]	37
37B.8.3[2]	228	$\begin{pmatrix}8&0\\0&14\end{pmatrix}, \begin{pmatrix}3&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	1	1	36	7992	[1, 1, 1, −208083, −36621194]	37

Table 6. Known exceptional $G_E(\ell)$ for non-CM elliptic curves E over quadratic fields $\mathbf{Q}(\sqrt{D})$ with $j(E) \in \mathbf{Q}$ that are not base changes from $\mathbf{Q}$.

Group curve	Index	Generators	-1	t	d_0	d_1	d	j-invariant	D	N
7Cs.2.1	112	$\begin{pmatrix}2&0\\0&4\end{pmatrix}, \begin{pmatrix}1&0\\0&3\end{pmatrix}$	No	2	1	3	18	$2^{18}3^{3}5^{1}43^{3}41^{-7}$	−3	$5^{4}7^{2}41^{2}$
[0, 0, −1, 21500(3a+5), 152590625a+129702031]/(a^2−a+1)										
13B.1.1	168	$\begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	1	156	$-3^{3}131^{3}2^{-13}5^{-1}$	17	$2^{2}5^{2}$
[1, −1, 1, −131a−205, 1758a+2745]/(a^2−a−4)										
13B.1.2	168	$\begin{pmatrix}2&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	12	156	$-3^{3}118691^{3}2^{-1}5^{-13}$	17	$2^{2}5^{2}$
[1, −1, 1, −118691a−185455, −31941270a−49878411]/(a^2−a−4)										
13B.1.3	168	$\begin{pmatrix}3&0\\0&5\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	3	156	$-3^{3}118691^{3}2^{-1}5^{-13}$	221	$2^{2}5^{2}13^{2}$
[0, 0, 0, −36119689047(11a+80), 177741267090426(2156a+15055)]/(a^2−a−55)										
13B.1.5	168	$\begin{pmatrix}5&0\\0&3\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	4	156	$-3^{3}131^{3}2^{-13}5^{-1}$	221	$2^{2}5^{2}13^{2}$
[0, 0, 0, 39865527(11a−91), 9591463206(2156a−17211)]/(a^2−a−55)										
13B.1.4	168	$\begin{pmatrix}4&0\\0&7\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	6	156	$-2^{6}3^{3}13^{4}5^{-1}$	8	$5^{2}13^{4}$
[a, 1, 1, −85a−126, 481a+684]/(a^2−2)										
13B.1.7	168	$\begin{pmatrix}7&0\\0&4\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	12	156	$-2^{6}3^{3}13^{1}17^{3}29^{3}5^{-13}$	8	$5^{2}13^{4}$
[a, 1, 1, 1602(2a−3), 164788a−235526]/(a^2−2)										
13B.1.9	168	$\begin{pmatrix}9&0\\0&6\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	3	156	$-2^{6}3^{3}13^{4}5^{-1}$	8	$5^{2}13^{4}$
[a, 1, 1, 7140(2a−3), −1142440a+1631547]/(a^2−2)										
13B.1.6	168	$\begin{pmatrix}6&0\\0&9\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	12	156	$-2^{6}3^{3}13^{1}17^{3}29^{3}5^{-13}$	8	$5^{2}13^{4}$
[a, 1, 1, 270780(2a−3), 358789873a−512576303]/(a^2−2)										
13B.1.8	168	$\begin{pmatrix}8&0\\0&10\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	4	156	$-3^{3}131^{3}2^{-13}5^{-1}$	221	$2^{2}5^{2}13^{2}$
[0, 0, 0, 39865527(5a−64), 9591463206(860a−8607)]/(a^2−a−55)										
13B.1.10	168	$\begin{pmatrix}10&0\\0&8\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	6	156	$-3^{3}118691^{3}2^{-1}5^{-13}$	221	$2^{2}5^{2}13^{2}$
[0, 0, 0, −36119689047(56a+389), 177741267090426(24052a+166763)]/(a^2−a−55)										

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

Table 6. *Continued*.

13B.1.12	168	$\begin{pmatrix}12&0\\0&11\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	2	156	$-3^{3}131^{3}2^{-13}5^{-1}$	17	$2^{2}5^{2}13^{4}$
$[1, -1, 0, 22139a-56731, -3795909a+9723481]/(a^{2}-a-4)$										
13B.1.11	168	$\begin{pmatrix}11&0\\0&12\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	12	156	$-3^{3}118691^{3}2^{-1}5^{-13}$	17	$2^{2}5^{2}13^{4}$
$[1, -1, 0, -20058779a-31341842, -70235146527a-109676893910]/(a^{2}-a-4)$										
17B.1.2	288	$\begin{pmatrix}2&0\\0&10\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	8	272	$-17^{1}373^{3}2^{-17}$	5	$2^{2}17^{4}$
$[a, -1, 0, 132(a-2), 304(-4a+7)]/(a^{2}-a-1)$										
17B.1.10	288	$\begin{pmatrix}10&0\\0&2\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	16	272	$-17^{2}101^{3}2^{-1}$	5	$2^{2}17^{4}$
$[a+1, -a-1, 0, -175742(a+1), -12667110(4a+3)]/(a^{2}-a-1)$										
17B.1.9	288	$\begin{pmatrix}9&0\\0&6\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	8	272	$-17^{1}373^{3}2^{-17}$	85	$2^{2}17^{2}$
$[0, 0, 0, -72762975(7a+30), 29048618250(532a+2199)]/(a^{2}-a-21)$										
17B.1.6	288	$\begin{pmatrix}6&0\\0&9\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	16	272	$-17^{2}101^{3}2^{-1}$	85	$2^{2}17^{2}$
$[0, 0, 0, 96798750975(7a-37), 1257319934817750(532a-2731)]/(a^{2}-a-21)$										
17B.1.15	288	$\begin{pmatrix}15&0\\0&7\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	8	272	$-17^{1}373^{3}2^{-17}$	5	$2^{2}17^{4}$
$[a+1, a, a+1, -38178(a+1), 5707018a+4289808]/(a^{2}-a-1)$										
17B.1.7	288	$\begin{pmatrix}7&0\\0&15\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	16	272	$-17^{2}101^{3}2^{-1}$	5	$2^{2}17^{4}$
$[a, a-1, a+1, 607a-1216, 9919a-17512]/(a^{2}-a-1)$										
17B.1.8	288	$\begin{pmatrix}8&0\\0&11\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	8	272	$-17^{1}373^{3}2^{-17}$	85	$2^{2}17^{2}$
$[0, 0, 0, -72762975(9a+37), 29048618250(756a+3107)]/(a^{2}-a-21)$										
17B.1.11	288	$\begin{pmatrix}11&0\\0&8\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	16	272	$-17^{2}101^{3}2^{-1}$	85	$2^{2}17^{2}$
$[0, 0, 0, -96798750975(8a+85), -1257319934817750(1036a+7727)]/(a^{2}-a-21)$										
37B.10.1	456	$\begin{pmatrix}10&0\\0&26\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	3	3996	$-7^{1}11^{3}$	5	7^{4}
$[a+1, a, a, -78a-78, 418a+333]/(a^{2}-a-1)$										
37B.10.2	456	$\begin{pmatrix}10&0\\0&26\end{pmatrix}, \begin{pmatrix}2&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	36	3996	$-7^{1}137^{3}2083^{3}$	5	7^{4}
$[a, a-1, a, 2039213a-4078427, 2003653476a-3506903387]/(a^{2}-a-1)$										
37B.10.6	456	$\begin{pmatrix}10&0\\0&26\end{pmatrix}, \begin{pmatrix}6&0\\0&25\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	12	3996	$-7^{1}11^{3}$	185	$7^{4}37^{2}$
$[0, 0, 0, 94230675(11a-82), 28183538250(1859a-13602)]/(a^{2}-a-46)$										
37B.10.21	456	$\begin{pmatrix}10&0\\0&26\end{pmatrix}, \begin{pmatrix}21&0\\0&23\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	18	3996	$-7^{1}137^{3}2083^{3}$	185	$7^{4}37^{2}$
$[0, 0, 0, 2444609268675(11a-82), 108162428702847750(-1859a+13602)]/(a^{2}-a-46)$										
37B.10.9	456	$\begin{pmatrix}10&0\\0&26\end{pmatrix}, \begin{pmatrix}9&0\\0&29\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	9	3996	$-7^{1}137^{3}2083^{3}$	185	$7^{4}37^{2}$
$[0, 0, 0, 2444609268675(13a-95), 108162428702847750(-2353a+17179)]/(a^{2}-a-46)$										
37B.10.14	456	$\begin{pmatrix}10&0\\0&26\end{pmatrix}, \begin{pmatrix}14&0\\0&16\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	12	3996	$-7^{1}11^{3}$	185	$7^{4}37^{2}$
$[0, 0, 0, 94230675(13a-95), 28183538250(2353a-17179)]/(a^{2}-a-46)$										
37B.10.11	456	$\begin{pmatrix}10&0\\0&26\end{pmatrix}, \begin{pmatrix}11&0\\0&17\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	6	3996	$-7^{1}11^{3}$	5	$7^{4}37^{4}$
$[a+1, a, a+1, -107609(a+1), 26319665a+19766651]/(a^{2}-a-1)$										
37B.10.17	456	$\begin{pmatrix}10&0\\0&26\end{pmatrix}, \begin{pmatrix}17&0\\0&11\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	36	3996	$-7^{1}137^{3}2083^{3}$	5	$7^{4}37^{4}$
$[a, a-1, a+1, 2791683423a-5583366848, 101558059929979a-177727302798321]/(a^{2}-a-1)$										

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

Table 7. Some exceptional $G_E(\ell)$ for non-CM elliptic curves E over quadratic fields.

Group Curve	Index	Generators	-1	t	d_0	d_1	d	D	N
5Nn.2.2[2]	80	$\begin{pmatrix}2&4\\2&2\end{pmatrix}, \begin{pmatrix}1&0\\0&4\end{pmatrix}$	No	2	3	3	6	5	31^2
$[0, a-1, 1, 42a-95, 192a-332]/(a^2-a-1)$									
5Ns.2.1[2]	60	$\begin{pmatrix}2&0\\0&3\end{pmatrix}, \begin{pmatrix}0&1\\1&0\end{pmatrix}$	Yes	1	2	4	8	5	$2^2 19^2$
$[1, 0, 1, 2a, 2a+2]/(a^2-a-1)$									
5Nn.3.2[2]	40	$\begin{pmatrix}3&4\\2&3\end{pmatrix}, \begin{pmatrix}1&0\\0&4\end{pmatrix}$	Yes	2	3	6	12	5	31^2
$[0, -a-1, 1, -1, 2a+1]/(a^2-a-1)$									
7Ns.6.1.2	84	$\begin{pmatrix}6&0\\0&6\end{pmatrix}, \begin{pmatrix}0&1\\6&0\end{pmatrix}, \begin{pmatrix}0&2\\2&0\end{pmatrix}$	Yes	1	2	12	24	-3	$7^4 13^1 223^2 379^1$
$[0, a+1, -1, 3351111a+661990, -762997059a+3083596118]/(a^2-a+1)$									
7Nn.0.1.1[2]	84	$\begin{pmatrix}6&1\\2&1\end{pmatrix}, \begin{pmatrix}0&3\\1&0\end{pmatrix}$	Yes	1	4	24	24	-7	$2^8 7^2 11^2 23^2 29^1$
$[0, 0, a, -686(4a+13), 104431a+347925]/(a^2-a+2)$									
7A4.3[2]	84	$\begin{pmatrix}5&4\\4&2\end{pmatrix}, \begin{pmatrix}5&4\\0&6\end{pmatrix}$	Yes	1	4	8	24	-7	$2^2 239^2$
$[1, 1, a+3, -14a-12, -33a-17]/(a^2-a+2)$									
7A4.1[2]	28	$\begin{pmatrix}4&0\\5&2\end{pmatrix}, \begin{pmatrix}5&2\\1&2\end{pmatrix}, \begin{pmatrix}3&0\\0&3\end{pmatrix}$	Yes	1	4	24	72	-7	$2^9 79^2$
$[-a+3, 5a-7, 6a-2, 1217a-851, -19779a-3823]/(a^2-a+2)$									
7S4.1[2]	14	$\begin{pmatrix}0&4\\5&3\end{pmatrix}, \begin{pmatrix}2&4\\0&4\end{pmatrix}, \begin{pmatrix}3&0\\0&3\end{pmatrix}$	Yes	1	8	48	144	-7	$2^8 11^2$
$[-2a, 0, 2a+2, 7a-5, -a+3]/(a^2-a+2)$									
11B.1.1	120	$\begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	1	110	8	$2^1 23^1$
$[a+1, -1, 1, -2a-3, 2a+3]/(a^2-2)$									
11B.1.2	120	$\begin{pmatrix}2&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	10	110	8	$2^1 23^1$
$[a+1, -1, 1, -947a-1473, -20242a-29187]/(a^2-2)$									
11B.1.3	120	$\begin{pmatrix}3&0\\0&8\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	5	110	-7	$11^4 23^2$
$[0, 0, -1, 1210a+814, 7986a-33850]/(a^2-a+2)$									
11B.1.8	120	$\begin{pmatrix}8&0\\0&3\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	10	110	-7	$11^4 23^2$
$[0, 0, 2a-1, 2662(-55a+92), 10629366a+34424653]/(a^2-a+2)$									
11B.1.10	120	$\begin{pmatrix}10&0\\0&9\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	2	110	8	$2^1 11^4 23^1$
$[a+1, -a-1, a, 171a-326, 3124a-4706]/(a^2-2)$									
11B.1.9	120	$\begin{pmatrix}9&0\\0&10\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	5	110	8	$2^1 11^4 23^1$
$[a+1, -a-1, a, 114516a-178196, -26700245a+38567674]/(a^2-2)$									
11Ns	66	$\begin{pmatrix}2&0\\0&6\end{pmatrix}, \begin{pmatrix}0&10\\1&0\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}$	Yes	1	2	20	200	13	$23^1 521^2$
$[0, -a, 1, -711a-1975, 32565a+51092]/(a^2-a-3)$									

Table 7. *Continued.*

11B.10.1	60	$\begin{pmatrix}10&0\\0&10\end{pmatrix},\begin{pmatrix}1&0\\0&2\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	2	220	8	$2^4 23^1$
$[a, a, 0, 6a-10, 16a-26]/(a^2-2)$									
11B.10.2	60	$\begin{pmatrix}10&0\\0&10\end{pmatrix},\begin{pmatrix}2&0\\0&1\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	10	220	8	$2^4 23^1$
$[a, a, 0, 3786a-5890, -161936a+233494]/(a^2-2)$									
11B.10.3	60	$\begin{pmatrix}10&0\\0&10\end{pmatrix},\begin{pmatrix}3&0\\0&8\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	10	220	-7	$2^8 11^4 23^2$
$[0, 0, 2a+2, 352(55a+37), -511107a+2166385]/(a^2-a+2)$									
11B.3.1	24	$\begin{pmatrix}3&0\\0&4\end{pmatrix},\begin{pmatrix}1&0\\0&2\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	5	550	-7	$2^1 11^2$
$[1, 1, a, 0, 0]/(a^2-a+2)$									
11B.3.2	24	$\begin{pmatrix}3&0\\0&4\end{pmatrix},\begin{pmatrix}2&0\\0&1\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	10	550	-7	$2^1 11^2$
$[1, 1, a, 35a-135, -217a+705]/(a^2-a+2)$									
11A5.1[2]	22	$\begin{pmatrix}5&7\\0&3\end{pmatrix},\begin{pmatrix}5&5\\1&4\end{pmatrix}$	Yes	1	12	120	600	-11	$2^6 3^4 103^2$
$[0, 0, 0, 3841a+8421, 76280a+1073622]/(a^2-a+3)$									
11B	12	$\begin{pmatrix}2&0\\0&6\end{pmatrix},\begin{pmatrix}1&0\\0&2\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	10	1100	-8	$3^2 11^2$
$[1, a+1, 0, a-4, -a-5]/(a^2+2)$									
13Ns	91	$\begin{pmatrix}2&0\\0&7\end{pmatrix},\begin{pmatrix}0&12\\1&0\end{pmatrix},\begin{pmatrix}1&0\\0&2\end{pmatrix}$	Yes	1	2	24	288	8	$5^2 7^2 263^2$
$[a, 1, a+1, 14455a-27951, 2058670a-3164816]/(a^2-2)$									
17B.4.3[2]	144	$\begin{pmatrix}4&0\\0&13\end{pmatrix},\begin{pmatrix}3&0\\0&12\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	1	1	16	544	17	$2^8 17^2$
$[0, a-1, a+1, 62a-174, 378a-955]/(a^2-a-4)$									
17B.4.1	72	$\begin{pmatrix}4&0\\0&13\end{pmatrix},\begin{pmatrix}1&0\\0&3\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	1	1	4	1088	5	$2^2 29^2$
$[1, 1, a, -3a-2, 2a]/(a^2-a-1)$									
17B.4.3	72	$\begin{pmatrix}4&0\\0&13\end{pmatrix},\begin{pmatrix}3&0\\0&1\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	1	1	16	1088	5	$2^2 29^2$
$[1, 1, a, 447a-4152, -85116a+59004]/(a^2-a-1)$									
17B.2.1	36	$\begin{pmatrix}2&0\\0&9\end{pmatrix},\begin{pmatrix}1&0\\0&3\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	1	1	8	2176	-4	$2^4 17^2$
$[a+1, 1, 0, 10a-54, 80a-132]/(a^2+1)$									
17B.2.3	36	$\begin{pmatrix}2&0\\0&9\end{pmatrix},\begin{pmatrix}3&0\\0&1\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	1	1	16	2176	-4	$2^4 17^2$
$[a+1, -1, a+1, -45a+46, -21a-161]/(a^2+1)$									
17B	18	$\begin{pmatrix}3&0\\0&6\end{pmatrix},\begin{pmatrix}1&0\\0&3\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	1	1	16	4352	-4	$5^3 17^2$
$[0, a-1, a, 79a+41, 14a+286]/(a^2+1)$									

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

Table 7. *Continued.*

19B.7.1	120	$\begin{pmatrix}7&0\\0&11\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	3	1026	13	13^2
$[a, -a-1, 0, -7a+6, a+20]/(a^2-a-3)$									
19B.7.2	120	$\begin{pmatrix}7&0\\0&11\end{pmatrix}, \begin{pmatrix}2&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	18	1026	13	13^2
$[a, -a-1, 0, 73118a-178094, 15174381a-35305705]/(a^2-a-3)$									
19B.7.4	120	$\begin{pmatrix}7&0\\0&11\end{pmatrix}, \begin{pmatrix}4&0\\0&10\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	9	1026	−3	$2^4 3^4 7^2 19^4$
$[0, a+1, 0, -7314a-12540, 753536a+12257]/(a^2-a+1)$									
19B.7.10	120	$\begin{pmatrix}7&0\\0&11\end{pmatrix}, \begin{pmatrix}10&0\\0&4\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	18	1026	−3	$2^4 3^4 7^2 19^4$
$[0, 4a+1, 0, 2640723a-7167660, 5225465897a-5332549369]/(a^2-a+1)$									
19B.7.8	120	$\begin{pmatrix}7&0\\0&11\end{pmatrix}, \begin{pmatrix}8&0\\0&5\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	6	1026	13	$13^2 19^4$
$[a, -a+1, 1, -2641a+1957, -1369a-100185]/(a^2-a-3)$									
19B.7.5	120	$\begin{pmatrix}7&0\\0&11\end{pmatrix}, \begin{pmatrix}5&0\\0&8\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	9	1026	13	$13^2 19^4$
$[a, -a+1, 1, 26395484a-64292143, -103917992039a+241830189815]/(a^2-a-3)$									
19B.8.1	60	$\begin{pmatrix}8&0\\0&12\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	6	2052	13	13^2
$[a+1, 1, 1, -2a-2, -6a-8]/(a^2-a-3)$									
19B.8.2	60	$\begin{pmatrix}8&0\\0&12\end{pmatrix}, \begin{pmatrix}2&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	18	2052	13	13^2
$[a+1, 1, 1, -1727a-4177, 66984a+119182]/(a^2-a-3)$									
19B.8.4	60	$\begin{pmatrix}8&0\\0&12\end{pmatrix}, \begin{pmatrix}4&0\\0&10\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	18	2052	−3	$2^8 3^4 7^2 19^4$
$[0, 5a+5, 6, -7290a-12540, -807848a-22730]/(a^2-a+1)$									
19B.4.1	40	$\begin{pmatrix}4&0\\0&5\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	9	3078	−8	$2^1 3^4 19^2$
$[-3, 2a-5, -2a+4, -7a+13, 5a-7]/(a^2+2)$									
19B.4.2	40	$\begin{pmatrix}4&0\\0&5\end{pmatrix}, \begin{pmatrix}2&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	18	3078	−8	$2^1 3^4 19^2$
$[-3, -4a-2, 2a-1, 3717a-1680, 108119a+59932]/(a^2+2)$									
19B	20	$\begin{pmatrix}2&0\\0&10\end{pmatrix}, \begin{pmatrix}1&0\\0&2\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	18	6156	−8	$3^3 5^4$
$[0, -4a+8, -9a+9, -73a+14, -87a+111]/(a^2+2)$									
23B.2.1	48	$\begin{pmatrix}2&0\\0&12\end{pmatrix}, \begin{pmatrix}1&0\\0&5\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	11	5566	−7	$2^1 23^2$
$[1, a+1, a+1, 29a-65, -120a+121]/(a^2-a+2)$									
23B.2.5	48	$\begin{pmatrix}2&0\\0&12\end{pmatrix}, \begin{pmatrix}5&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	22	5566	−7	$2^1 23^2$
$[1, -a-1, a+1, 16a, -42a-21]/(a^2-a+2)$									

Table 7. *Continued.*

23B	24	$\begin{pmatrix}5&0\\0&14\end{pmatrix},\begin{pmatrix}1&0\\0&5\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	22	11132	−11	$3^2 23^2$
$[1, -a, a, 4a-3, -a-1]/(a^2-a+3)$									
29B.7.1	120	$\begin{pmatrix}7&0\\0&25\end{pmatrix},\begin{pmatrix}1&0\\0&2\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	7	5684	−4	29^2
$[1, a, 1, -1, 0]/(a^2+1)$									
29B.7.2	120	$\begin{pmatrix}7&0\\0&25\end{pmatrix},\begin{pmatrix}2&0\\0&1\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	28	5684	−4	29^2
$[1, a, 1, 2080a-3751, 73352a-79386]/(a^2+1)$									
29B.7.4	120	$\begin{pmatrix}7&0\\0&25\end{pmatrix},\begin{pmatrix}4&0\\0&15\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	14	5684	−4	29^4
$[-a, a-1, -a, -141a-157, -2591a-5674]/(a^2+1)$									
29B.7.8	120	$\begin{pmatrix}7&0\\0&25\end{pmatrix},\begin{pmatrix}8&0\\0&22\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	28	5684	−4	29^4
$[a, 2a-1, -2, -3645a-2261, 107979a+8482]/(a^2+1)$									
29B.4.1	60	$\begin{pmatrix}4&0\\0&22\end{pmatrix},\begin{pmatrix}1&0\\0&2\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	14	11368	−4	$2^4 29^2$
$[a+1, 5a+3, -4, 12a+24, 296a+232]/(a^2+1)$									
29B.4.2	60	$\begin{pmatrix}4&0\\0&22\end{pmatrix},\begin{pmatrix}2&0\\0&1\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	28	11368	−4	$2^4 29^2$
$[a+1, -5a+1, 4, 144a+564, -5944a+2472]/(a^2+1)$									
29B	30	$\begin{pmatrix}2&0\\0&15\end{pmatrix},\begin{pmatrix}1&0\\0&2\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	1	1	28	22736	−7	$2^4 29^2$
$[2a, -1, -a-2, 4a+8, 12a-24]/(a^2-a+2)$									
31B.5.4	320	$\begin{pmatrix}5&0\\0&25\end{pmatrix},\begin{pmatrix}4&0\\0&24\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	15	2790	−11	$3^8 5^2 31^4$
$[0, 3, 3, 136740690a-686742129, 1958685589751a-6654652545690]/(a^2-a+3)$									
31B.5.11	320	$\begin{pmatrix}5&0\\0&25\end{pmatrix},\begin{pmatrix}11&0\\0&20\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	30	2790	−11	$3^8 5^2 31^4$
$[0, 3, 3, -142290a-572319, 65600681a+157039605]/(a^2-a+3)$									
31B.6.4	160	$\begin{pmatrix}6&0\\0&26\end{pmatrix},\begin{pmatrix}4&0\\0&24\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	30	5580	−11	$2^8 3^8 5^2 31^4$
$[0, -3, 2a, -2276640a-9157149, -4205273505a-10078006254]/(a^2-a+3)$									
31B.7.1	64	$\begin{pmatrix}7&0\\0&9\end{pmatrix},\begin{pmatrix}1&0\\0&3\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	15	13950	−3	$7^2 31^2$
$[3, -5, -4, 195a+198, 5134a-6388]/(a^2-a+1)$									
31B.7.3	64	$\begin{pmatrix}7&0\\0&9\end{pmatrix},\begin{pmatrix}3&0\\0&1\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix}$	No	3	1	30	13950	−3	$7^2 31^2$
$[3a-3, 5a, -3, -5546a-1044, -214581a+68920]/(a^2-a+1)$									
31B	32	$\begin{pmatrix}3&0\\0&21\end{pmatrix},\begin{pmatrix}1&0\\0&3\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix}$	Yes	3	1	30	27900	−3	$7^4 31^2$
$[3, -a-2, -a, 95a-370, 1614a-6420]/(a^2-a+1)$									

Table 7. *Continued.*

`37B`	38	$\begin{pmatrix}2 & 0\\0 & 19\end{pmatrix}, \begin{pmatrix}1 & 0\\0 & 2\end{pmatrix}, \begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}$	Yes	1	1	36	47952	-11	$2^4 3^3 7^4$
$[0, -a+4, 6, -16170a+16494, -431712a+1866132]/(a^2-a+3)$									
`41B`	42	$\begin{pmatrix}6 & 0\\0 & 7\end{pmatrix}, \begin{pmatrix}1 & 0\\0 & 6\end{pmatrix}, \begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}$	Yes	1	1	40	65600	-4	$2^1 5^2 41^2$
$[a, 3a+1, 0, 14a, 13a+5]/(a^2+1)$									

Table 8. Some exceptional $G_E(\ell)$ for non-CM elliptic curves E over $\mathbf{Q}[a]/(a^3 - a^2 + 1)$.

Group Curve	Index	Generators	-1	t	d_0	d_1	d	D	N
`7Cs.1.1`	336	$\begin{pmatrix}1 & 0\\0 & 3\end{pmatrix}$	No	3	1	1	6	-23	$2^3 7^2$
$[1, -a^2+a, a^2+a, -3a-2, -2a-2]$									
`7Cs.1.4`	336	$\begin{pmatrix}4 & 0\\0 & 6\end{pmatrix}$	No	3	1	2	6	-23	$2^3 7^6$
$[1, 4a^2+2a+4, 0, 56a^2-114a-120, -316a^2+224a+512]$									
`7Cs.6.1`	168	$\begin{pmatrix}6 & 0\\0 & 6\end{pmatrix}, \begin{pmatrix}1 & 0\\0 & 3\end{pmatrix}$	Yes	3	1	2	12	-23	$2^3 5^2 7^2$
$[a+1, a+1, a^2+a, 12a^2+20a+5, 72a^2-49a-47]$									
`31B.5.1`	320	$\begin{pmatrix}5 & 0\\0 & 25\end{pmatrix}, \begin{pmatrix}1 & 0\\0 & 3\end{pmatrix}, \begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}$	No	3	1	3	2790	-23	$5^1 97^2$
$[a+1, a, a, -40a^2+23, -179a^2+2231a+1786]$									
`31B.5.3`	320	$\begin{pmatrix}5 & 0\\0 & 25\end{pmatrix}, \begin{pmatrix}3 & 0\\0 & 1\end{pmatrix}, \begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}$	No	3	1	30	2790	-23	$5^1 97^2$
$[a+1, a, a, 474525a^2-3200a-273302, -90370559a^2-71881939a-2769254]$									
`31B.5.6`	320	$\begin{pmatrix}5 & 0\\0 & 25\end{pmatrix}, \begin{pmatrix}6 & 0\\0 & 16\end{pmatrix}, \begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}$	No	3	1	6	2790	-23	$5^1 31^6 97^2$
$[a+1, a^2+a+1, 0, -38977a^2+261a+22342, 4547700a^2-65990438a-52406399]$									
`31B.5.16`	320	$\begin{pmatrix}5 & 0\\0 & 25\end{pmatrix}, \begin{pmatrix}16 & 0\\0 & 6\end{pmatrix}, \begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}$	No	3	1	15	2790	-23	$5^1 31^6 97^2$
$[a^2, 2a^2+3a+1, -2, -62172325a^2+61226571a+68084562, 192717035605a^2+178577917357a+44210952860]$									
`31B.6.1`	160	$\begin{pmatrix}6 & 0\\0 & 26\end{pmatrix}, \begin{pmatrix}1 & 0\\0 & 3\end{pmatrix}, \begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}$	Yes	3	1	6	5580	-23	$5^2 97^2$
$[a^2+a+1, 3, 2a^2-a, a^2+2a+3, 9a^2-a-6]$									
`31B.6.3`	160	$\begin{pmatrix}6 & 0\\0 & 26\end{pmatrix}, \begin{pmatrix}3 & 0\\0 & 1\end{pmatrix}, \begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}$	Yes	3	1	30	5580	-23	$5^2 97^2$
$[a, 2a, a^2-a, -31743a^2+58113a-42806, -4057150a^2+7108029a-5326264]$									

Acknowledgments

The author is grateful to Nicholas M. Katz for his support, and for asking the questions that motivated this research, and to David Zywina for several fruitful discussions. The author also wishes to thank John Cremona and William Stein for their assistance with many of the computations. The author was supported by NSF grant DMS-1115455.

References

[1] S. Anni, 'Images of Galois representations', PhD thesis, Universiteit Leiden and L'Université Bordeaux I, 2013.

[2] B. S. Banwait, 'On some local to global phenomena for abelian varieties', PhD thesis, University of Warwick, 2013.

[3] B. S. Banwait and J. E. Cremona, Tetrahedral elliptic curves and the local-global principle for isogenies', *Algebra Number Theory* **8** (2014), 1201–1229.

[4] B. Baran, 'An exceptional isomorphism between modular curves of level 13', *J. Number Theory* **145** (2014), 273–300.

[5] Y. Bilu, P. Parent and M. Robelledo, 'Rational points on $X_0^+(p^r)$', *Ann. Inst. Fourier (Grenoble)* **64** (2013), 957–984.

[6] G. Birkhoff, 'Subgroups of abelian groups', *Proc. Lond. Math. Soc. Ser. 2* **38** (1935), 385–401.

[7] J. Belding, R. Bröker, A. Enge and K. Lauter, 'Computing Hilbert class polynomials', in *Proceedings of the 8th International Symposium on Algorithmic Number Theory (ANTS VIII)*, Lecture Notes in Computer Science, 5011 (Springer, 2008), 282–295.

[8] G. Bisson, 'Computing endomorphism rings of elliptic curves under the GRH', *J. Math. Cryptol.* **5** (2011), 101–113.

[9] G. Bisson and A. V. Sutherland, 'Computing the endomorphism ring of an ordinary elliptic curve over a finite field', *J. Number Theory* **131** (2011), 815–831.

[10] J. Bober, A. Deines, A. Klages-Mundt, B. LeVeque, R. A. Ohana, A. Rabindranath, P. Sharaba and W. Stein, 'A database of elliptic curves over $\mathbf{Q}(\sqrt{5})$: a first report', in *Proceedings of the Tenth Algorithmic Number Theory Symposium (ANTS X)*, (eds. E. W. Howe and K. S. Kedlaya) Open Book Series, 1 (Mathematical Sciences Publishers, 2013), 145–166.

[11] W. Bosma, J. Cannon and C. Playoust, 'The Magma algebra system I: The user language', *J. Symbolic Comput.* **24** (1997), 235–265.

[12] R. Bröker, K. Lauter and A. V. Sutherland, 'Modular polynomials via isogeny volcanoes', *Math. Comp.* **81** (2012), 1201–1231.

[13] P. Bruin and F. Najman, 'Hyperelliptic modular curves $X_0(n)$ and isogenies of elliptic curves over quadratic fields', *LMS J. Comput. Math.* **18** (2015), 578–602.

[14] D. G. Cantor and H. Zassenhaus, 'A new algorithm for factoring polynomials over finite fields', *Math. Comp.* **36** (1981), 587–592.

[15] T. G. Centeleghe, 'Integral Tate modules and splitting of primes in torsion fields of elliptic curves', *Int. J. Number Theory*, to appear, doi:10.1142/S1793042116500147.

[16] I. Chen and C. Cummins, 'Elliptic curves with nonsplit mod-11 representations', *Math. Comp.* **73** (2004), 869–880.

[17] H. Cohen, *A Course in Computational Algebraic Number Theory* (Springer-Verlag, Berlin, Heidelberg, 1993).

[18] A. C. Cojocaru, 'On the surjectivity of the Galois representations associated to non-CM elliptic curves (with an appendix by E. Kani)', *Canad. Math. Bull.* **48** (2005), 16–31.

[19] J. E. Cremona, 'Elliptic curve data', available at https://homepages.warwick.ac.uk/staff/J.E.Cremona/ftp/data/, 2014.

[20] J. E. Cremona, 'Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields', *Compos. Math.* **51** (1984), 275–324.

[21] J. E. Cremona, 'Addendum and errata 'Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields', *Compos. Math.* **63** (1984), 271–272.

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

[22] M. Deuring, ‘Die Typen der Multiplikatorenringe elliptischer Funktionenkörper’, *Abh. Math. Semin. Univ. Hansischen* **14** (1941), 197–272.

[23] L. E. Dickson, *Linear Groups with an Exposition of Galois Field Theory*, Cosimo Classics 2007 reprint of original publication by B. G. Teubner, Leipzig, 1901.

[24] S. Donnelly, P. E. Gunnells, A. Klages-Mundt and D. Yasaki, ‘A table of elliptic curves over the cubic field of discriminant -23’, *Exp. Math.* **24** (2015), 375–390.

[25] W. Duke and Á. Tóth, ‘The splitting of primes in division fields of elliptic curves’, *Exp. Math.* **11** (2002), 555–565.

[26] N. D. Elkies, ‘Elliptic and modular curves over finite fields and related computational issues’, in *Computational Perspectives on Number Theory (Chicago, IL, 1995)* AMS/IP Studies in Advanced Mathematics, 7 (1998), 21–76.

[27] A. Enge, ‘The complexity of class polynomial computation via floating point approximations’, *Math. Comp.* **78** (2009), 1089–1107.

[28] D. L. Flannery and E. A. O’Brien, ‘Linear groups of small degree over finite fields’, *Internat. J. Algebra Comput.* **15** (2005), 467–502.

[29] S. D. Galbraith, *Mathematics of Public Key Cryptography* (Cambridge University Press, Cambridge, 2012).

[30] The GAP group, GAP–Groups, *Algorithms, and Programming*, version 4, 2015.

[31] F. Gassmann, ‘Bemerkung zur vorstehenden Arbeit von Hurwitz’, *Math. Z.* **25** (1926), 665–675.

[32] J. von zur Gathen and J. Gerhard, *Modern Computer Algebra*, 3rd edn (Cambridge University Press, Cambridge, 2013).

[33] S. P. Glasby and R. B. Howlett, ‘Writing representations over minimal fields’, *Commun. Algebra* **25** (1997), 1703–1711.

[34] D. Harvey, J. van der Hoeven and G. Lecerf, ‘Even faster integer multiplication’, *J. Complexity*, to appear.

[35] K. S. Kedlaya and A. V. Sutherland, ‘Computing L-series of hyperelliptic curves’, in *Algorithmic Number Theory 8th International Symposium (ANTS VIII)*, (Eds. A. J. van der Poorten and A. Stein) Lecture Notes in Computer Science, 5011 (Springer, 2008), 312–326.

[36] M. A. Kenku, ‘A note on the integral points of a modular curve of level 7’, *Mathematika* **32** (1985), 45–48.

[37] E. Kowalski and D. Zywina, ‘The Chebotarev invariant of a finite group’, *Exp. Math.* **21** (2012), 38–56.

[38] J. C. Lagarias and A. M. Odlyzko, ‘Effective versions of the Chebotarev density theorem’, in *Algebraic Number Fields: L-functions and Galois Properties (Proc. Sympos., Univ. Durham, Durham, 1975)* (Academic, London, 1977), 409–464.

[39] J. C. Lagarias, H. L. Montgomery and A. M. Odlyzko, ‘A bound for the least prime ideal in the Chebotarev density theorem’, *Invent. Math.* **54** (1979), 271–296.

[40] S. Landau, ‘Factoring polynomials over algebraic number fields’, *SIAM J. Comput.* **1985** (1985), 184–195.

[41] S. Lang, *Introduction to Modular Forms* (Springer-Verlag, Berlin, Heidelberg, 1976).

[42] E. Larson and D. Vaintrob, ‘On the surjectivity of Galois representations associated to elliptic curves over number fields’, *Bull. Lond. Math. Soc.* **46** (2014), 197–209.

[43] G. Ligozat, ‘Courbe modulaires de diveau 11’, in *Modular Functions of One Variable V*, Lecture Notes in Mathematics, 601 (Springer, 1977), 149–237.

[44] The LMFDB Collaboration, *The L-functions and modular forms database*, available at http://www.lmfdb.org, 2014.

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

[45] The LMFDB Collaboration, The L-functions and modular forms database, beta version, available at http://beta.lmfdb.org, 2015.

[46] B. Mazur, ‘Modular curves and the Eisenstein ideal’, *Publ. Math. Inst. Hautes Études Sci.* **47** (1977), 33–186.

[47] B. Mazur, ‘Rational isogenies of primes degree’, *Invent. Math.* **44** (1978), 129–162.

[48] J. McKee, ‘Computing division polynomials’, *Math. Comp.* **63** (1994), 767–771.

[49] V. S. Miller, ‘The Weil pairing and its efficient calculation’, *J. Cryptol.* **17** (2004), 235–261.

[50] A. P. Ogg, ‘Elliptic curves and wild ramification’, *Amer. J. Math.* **89** (1967), 1–21.

[51] J. Oesterlé, ‘Versions effectives du théorème de Chebotarev sous l’hypothèse de Riemann généralisée’, *Astérisque* **61** (1979), 165–167.

[52] J. Rouse and D. Zureick-Brown, ‘Elliptic curves over $\mathbf{Q}$ and 2-adic images of Galois’, *Res. Number Theory* **1** (2015).

[53] A. Schönhage and V. Strassen, ‘Schnelle Multiplikation Großer Zahlen’, *Computing* **7** (1971), 281–292.

[54] A. Schönhage, ‘Factorization of univariate integer polynomials by diophantine approximation and an improved basis reduction algorithm’, in *Automata, Languages, and Programming*, LNCS, 172 (1984), 436–447.

[55] R. Schoof, ‘Elliptic curves over finite fields and the computation of square roots mod p’, *Math. Comp.* **44** (1985), 483–494.

[56] R. Schoof, ‘Counting points on elliptic curves over finite fields’, *J. Théor. Nombres Bordeaux* **7** (1995), 219–254.

[57] J.-P. Serre, *Abelian ℓ-Adic Representations and Elliptic Curves (revised reprint of 1968 original)*, (A. K. Peters, Wellesley, MA, 1998).

[58] J.-P. Serre, ‘Propriétés galoisiennes des points d’ordre fini des courbes elliptiques’, *Invent. Math.* **15** (1972), 259–331.

[59] J.-P. Serre, ‘Quelques applications du théorème de densité de Chebotarev’, *Publ. Math. Inst. Hautes Études Sci.* **54** (1981), 323–401.

[60] I. E. Shparlinski and A. V. Sutherland, ‘On the distribution of Atkin and Elkies primes for reductions of elliptic curves on average’, *LMS J. Comput. Math.* **18** (2015), 308–322.

[61] W. A. Stein and M. Watkins, ‘A database of elliptic curves–First report’, in *Algorithmic Number Theory 5th International Symposium (ANTS V)*, (eds. C. Fieker and D. R. Kohel) Lecture Notes in Computer Science, 2369 (Springer-Verlag, Berlin, Heidelberg, 2002), 267–275.

[62] M. Streng, ‘Computing Igusa class polynomials’, *Math. Comp.* **83** (2014), 275–309.

[63] A. V. Sutherland, ‘`smalljac` software library, version 4.0.28, available at http://math.mit.edu/ drew, 2014.

[64] A. V. Sutherland, ‘Computing Hilbert class polynomials with the Chinese remainder theorem’, *Math. Comp.* **80** (2011), 501–538.

[65] A. V. Sutherland, ‘A local-global principle for isogenies of prime degree’, *J. Théor. Nombres Bordeaux* **24** (2012), 475–485.

[66] A. V. Sutherland, ‘Isogeny volcanoes’, in *Proceedings of the Tenth Algorithmic Number Theory Symposium (ANTS X)*, (eds E. W. Howe and K. S. Kedlaya) Open Book Series *1* (Mathematical Sciences Publishers, 2013), 507–530.

[67] A. V. Sutherland, ‘On the evaluation of modular polynomials’, in *Proceedings of the Tenth Algorithmic Number Theory Symposium (ANTS X)*, (eds. E. W. Howe and K. S. Kedlaya) Open Book Series, 1 (Mathematical Sciences Publishers, 2013), 531–555.

[68] A. V. Sutherland, Magma scripts related to *Computing images of Galois representations attached to elliptic curves*, available at http://math.mit.edu/ drew/galrep, 2015.

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press

[69] T. Sunada, 'Riemannian coverings and isospectral manifolds', *Ann. of Math. (2)* **121** (1985), 169–186.

[70] H. P. F. Swinnerton-Dyer, 'On ℓ-adic representations and congruences for coefficients of modular forms', in *Modular Functions of one Variable III (Antwerp, Belgium 1972)*, (eds. P. Deligne and W. Kuyk) Lecture Notes in Mathematics, 350 (Springer, 1973), 1–56.

[71] L. Tóth, 'Subgroups of finite abelian groups having rank two via Goursat's lemma', *Tatra Mt. Math. Publ.* **59** (2014), 93–103.

[72] B. Winckler, 'Théorème de Chebotarev effectif', Preprint, 2013, arXiv:1311.5715.

[73] D. Zywina, 'On the surjectivity of mod-ℓ representations associated to elliptic curves', Preprint, 2015, arXiv:1508.07661.

[74] D. Zywina, 'The possible images of the mod-ℓ representations associated to elliptic curves over $\mathbf{Q}$', Preprint, 2015, arXiv:1508.07660.

https://doi.org/10.1017/fms.2015.33 Published online by Cambridge University Press