Chapter 1

Computing Galois representations attached to elliptic curves

1.1 Introduction

Let K be a number field and $\bar{K}$ an algebraic closure of K. For an elliptic curve E defined over K, denote by $E[n]$ the kernel of the multiplication by n map, that is, the set of elements $P \in E(\bar{K})$ such that $nP = 0$. This is known to be a free $\mathbb{Z}/n\mathbb{Z}$-module of rank 2. If we let $G_K := \mathrm{Gal}(\bar{K}/K)$ denote the absolute Galois group of K, then G_K acts on $E[n]$ by group automorphisms. This gives rise to a representation

$$\rho_{E,n} : G_K \longrightarrow \mathrm{Aut}(E[n]) \simeq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

where the isomorphism on the right is obtained by choosing a basis for $E[n]$ over $\mathbb{Z}/n\mathbb{Z}$. Taking the inverse limit of this action over all n gives a

continuous representation

$$\rho_E : G_K \longrightarrow \mathrm{Aut}(E_\infty) \simeq \mathrm{GL}_2(\hat{\mathbb{Z}}),$$

where E_∞ is the torsion subgroup of $E(\bar{K})$.

We will be concerned with the question of determining the image of ρ_E in $\mathrm{Aut}(E_\infty)$ in the case where E is defined over the rationals and does not have complex multiplication over $\overline{\mathbb{Q}}$. The image of ρ_E encodes a lot of information about the properties of E, both globally and locally, so it is of interest to fully understand it. As we will see in Chapter 3 for instance, many constants appearing in classical conjectures of elliptic curves over $\mathbb{Q}$ can be described efficiently using the image of ρ_E. Determining the image of this representation is highly non-trivial, but considerable progress has been made in this direction. The most important result is the following classical theorem of Serre (see [Ser72]), which says that $\rho_E(G)$ is generically almost surjective.

Theorem 1.1.1 (Serre's open image theorem)**.** *Let E be an elliptic curve over a number field K such that E does not have complex multiplication over $\bar{K}$. Then $\rho_E(G_K)$ is open in* $\mathrm{GL}_2(\hat{\mathbb{Z}})$.

Recall that $\mathrm{GL}_2(\hat{\mathbb{Z}})$ is an inverse limit of finite groups, hence it is compact, so it follows immediately from Serre's open image theorem that $\rho_E(G_K)$ has finite index in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ for non-CM elliptic curves. This implies (see Lemma 1.2.1) that there exists an integer m_E such that the image of ρ_E can be completely determined by m_E (or any multiple of it) and the reduction of $\rho_E(G_K)$ modulo m_E. This reduction is precisely the image $\rho_{E,m_E}(G_K)$. It follows from this that we can completely describe the image of ρ_E by determining an integer m which is a multiple of m_E as well as the finite image of $\rho_{E,m}$.

In this chapter we will develop and outline an algorithm which, given as input an elliptic curve E over $\mathbb{Q}$, outputs such an integer m and $\rho_{E,m}(G_{\mathbb{Q}})$

as a subgroup of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. It is not clear a priori that such an algorithm exists, given that even though the output of such an algorithm is 'finite', the intermediate steps deal with 'infinite' objects such as $\mathrm{GL}_2(\hat{\mathbb{Z}})$ and its ℓ-adic projections $\mathrm{GL}_2(\mathbb{Z}_\ell)$. Several of these intermediate steps had already been considered and dealt with successfully by various authors (see [Sut13], [Zyw11b], [Zyw11a]), and we largely build upon this previous work. The algorithm which we outline here is meant to serve, at least initially, mainly for theoretical purposes, however we also look at some practical considerations which can make this algorithm faster and we discuss some of them in the last section.

For a prime ℓ, denote by ρ_{E,ℓ^∞} the representation given by the action of G_K on $E[\ell^\infty]$. We call the image of ρ_{E,ℓ^∞} the ℓ-adic image and denote it by G_ℓ. In Section 1.3 we consider first the so-called *vertical situation*, which is the problem of determining the ℓ-adic image for a fixed prime ℓ. In order to do this we will consider the reductions of G_ℓ modulo various powers of ℓ.

In Section 1.4 we consider the *horizontal situation*, in which we vary the prime ℓ and determine G_ℓ for all ℓ. The key result from this section is a method of Zywina which allows one to quickly find a set of primes S outside of which the mod ℓ image is surjective. This together with Corollary 1.2.4 will allow us to determine G_ℓ for all primes ℓ. In Section 1.5 we consider the *entanglements* between the various G_ℓ. This amounts to determining the intersections between the various ℓ^∞-torsion fields of E. It will be Proposition 1.5.3 that will allow us to do this. Finally, in the last section we discuss some practical considerations that can make the algorithm outlined usable in practice.

1.2 Background and notation

For the remainder of the chapter we fix our base field to be $\mathbb{Q}$. For $E/\mathbb{Q}$ an elliptic curve without complex multiplication, let E_∞ denote the group of

torsion points of E over $\overline{\mathbb{Q}}$, that is, $E(\overline{\mathbb{Q}})_{\text{tors}}$. Consider the Tate module

$$T(E) := \varprojlim_n E[n],$$

where the maps $E[n] \to E[m]$ are given by multiplication by n/m, whenever m divides n. Then $G_{\mathbb{Q}}$ acts continuously on $T(E)$. It is a classical result ([Sil09]) that $T(E)$ is a free $\widehat{\mathbb{Z}}$-module of rank 2, hence we may fix a basis for $T(E)$ so as to identify $\mathrm{Aut}(E_\infty)$ with $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, and we denote by $\rho_E : G_{\mathbb{Q}} \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$ the continuous representation given by this action. Also, set $G := \rho_E(G_{\mathbb{Q}})$. By Serre's open image theorem G is a finite index subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$. For each positive integer m we let G_m denote the projection of G onto the finite product

$$\prod_{\ell | m} \mathrm{GL}_2(\mathbb{Z}_\ell).$$

We then have $G_m \simeq \mathrm{Gal}(K_m/\mathbb{Q})$, where K_m is the m-power torsion field, that is, the infinite extension of $\mathbb{Q}$ obtained by adjoining the coordinates of all m^n-torsion points of E for all n. Let $G(m)$ denote the image of G under the reduction modulo m map $\mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, so that $G(m) \simeq \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$. We denote by $\rho_{E,m}$ the representation given by the action of $G_{\mathbb{Q}}$ on $E[m]$.

We will say that m *splits* ρ_E if we have an equality

$$G = G_m \times \prod_{\ell \nmid m} \mathrm{GL}_2(\mathbb{Z}_\ell).$$

Note that m splitting ρ_E depends only on the prime factors dividing m and not on the powers to which these primes occur in the factorisation of m. We will also say that m is *stable* if it holds that

$$G_m = \pi_m^{-1}(G(m))$$

where π_m denotes the reduction map $\prod_{\ell|m} \mathrm{GL}_2(\mathbb{Z}_\ell) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. In what follows we will also use π_m to denote the reduction map $\mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$.

Lemma 1.2.1. *Keeping the notation above, there is an integer m which splits ρ_E and is stable.*

Proof. Since G is open in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, it contains an open neighbourhood of the identity. If we let U_m be the set of all matrices in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ whose reduction modulo m is I, then $\{U_m\}_m$ is a neighbourhood base of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, so it follows that $U_m \subset G$ for some m. Clearly this m satisfies

$$G = \pi_m^{-1}(G(m))$$

where here π_m denotes the reduction map $\mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. This implies m splits ρ_E and is stable. □

Given a stable integer m which also splits ρ_E we see that G is completely determined by $G(m)$, hence can be described by finitely many conditions. Note also that if m is stable and splits ρ_E, then so does any integer m' such that $m \mid m'$. For an elliptic curve E, we will use m_E to denote the *minimal* stable integer that splits ρ_E. Note that m_E divides all other stable integers which split ρ_E. As we have stated, our primary goal is to give a description of the image of Galois G, and we do this by determining an integer m which is a multiple of m_E as well as the finite group $G(m)$. In the remainder of this section we state some results which will prove useful for computing such an integer.

1.2.1 Group theory for GL_2

We quickly recall some facts about the groups $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and $\mathrm{GL}_2(\mathbb{Z}_\ell)$ for N an integer and ℓ a prime. Most of the material from this section can be found in [Ser68], §IV.

Lemma 1.2.2. $\mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})$ *is a simple group for* $\ell \geqslant 5$. *Every proper subgroup of* $\mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})$ *is solvable or isomorphic to the alternating group* A_5, *the last possibility occurring only if* $\ell \equiv \pm 1 \pmod 5$.

Lemma 1.2.3. *Let* $\ell \geqslant 5$ *be a prime and* H *be a closed subgroup of* $\mathrm{GL}_2(\mathbb{Z}_\ell)$ *whose projection mod* ℓ *contains* $\mathrm{SL}_2(\mathbb{F}_\ell)$. *Then* H *contains* $\mathrm{SL}_2(\mathbb{Z}_\ell)$.

Proof. This follows directly from Lemma 3, §IV-23 of [Ser68]. □

Corollary 1.2.4. *Suppose* $\ell \geqslant 5$ *is a prime and suppose* $G(\ell) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. *Then* $G_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$.

Proof. This follows from Lemma 1.2.3 and the fact that the determinant map $\det : G_\ell \to \mathbb{Z}_\ell^\times$ is surjective. □

For a profinite group Y we say that a finite simple group Φ *occurs* in Y if there exist closed subgroups Y_1, Y_2 of Y such that Y_1 is normal in Y_2 and $Y_2/Y_1 \simeq \Phi$. We let $\mathrm{Occ}(Y)$ denote the set of finite simple non-abelian groups occuring in Y. The following properties of Occ are easily checked.

(i) If $Y = \varprojlim_n Y_n$ and each $Y \to Y_n$ is surjective then $\mathrm{Occ}(Y) = \bigcup_n \mathrm{Occ}(Y_n)$.

(ii) If we have a short exact sequence of profinite groups

$$1 \longrightarrow Y' \longrightarrow Y \longrightarrow Y'' \longrightarrow 1$$

then $\mathrm{Occ}(Y) = \mathrm{Occ}(Y') \cup \mathrm{Occ}(Y'')$.

Using these properties and Lemma 1.2.2 we obtain that

$$\mathrm{Occ}\big(\mathrm{GL}_2(\mathbb{Z}_\ell)\big) = \begin{cases} \emptyset & \text{if } \ell = 2, 3, \\ \{\mathrm{PSL}_2(\mathbb{Z}/5\mathbb{Z})\} = \{A_5\} & \text{if } \ell = 5, \\ \{\mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})\} & \text{if } \ell \equiv \pm 2 \pmod 5 \text{ and } \ell > 5, \\ \{\mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z}),\ A_5\} & \text{if } \ell \equiv \pm 1 \pmod 5 \text{ and } \ell > 5. \end{cases}$$

Lemma 1.2.5. *Let ℓ be prime. Then $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ has no simple non-abelian quotients.*

Proof. Suppose the converse. Then there exists a simple non-abelian group Φ and a surjective group homomorphism

$$\varphi : \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \longrightarrow \Phi.$$

Since Φ is then a composition factor of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, it follows that $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is not solvable, hence $\ell \geqslant 5$. By Lemma 1.2.2 we have that $\mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})$ is simple. The exact sequence

$$1 \longrightarrow \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \longrightarrow (\mathbb{Z}/\ell\mathbb{Z})^{\times} \longrightarrow 1$$

shows that $\Phi \simeq \mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})$, since it is the only non-abelian composition factor of $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Now the centres of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ and $\mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})$ are $(\mathbb{Z}/\ell\mathbb{Z})^{\times}$ and the trivial group, respectively, hence φ induces a surjective homomorphism

$$\psi : \mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z}) \longrightarrow \mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z}),$$

where $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z}) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})/(\mathbb{Z}/\ell\mathbb{Z})^{\times}$. By $\ell > 2$ we have

$$|\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})| = 2,$$

so $|\ker\psi| = 2$. Let N be the subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ such that $\ker\psi = N/(\mathbb{Z}/\ell\mathbb{Z})^{\times}$. Then $(\mathbb{Z}/\ell\mathbb{Z})^{\times}$ has index 2 in N, hence N is abelian. Also, as $\ker\psi \lhd \mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$, we have $N \lhd \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, hence $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ acts on N by restricting inner automorphisms. We now show that this action is trivial.

Consider the homomorphism

$$\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) \longrightarrow \mathrm{Aut}(N) \tag{1.2.1}$$

$$x \longmapsto \varphi_x \tag{1.2.2}$$

given by the action mentioned above. This map satisfies that φ_x is the trivial action when restricted to $(\mathbb{Z}/\ell\mathbb{Z})^\times$ for $x \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Also, as $(\mathbb{Z}/\ell\mathbb{Z})^\times$ is the center of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, we have that (1.2.1) factors through $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Denote this map by

$$\Psi : \mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z}) \longrightarrow \mathrm{Aut}(N).$$

Note that Ψ is trivial when restricted to $\mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})$, as this group is simple and non-abelian. Also, Ψ is trivial on $\ker\psi = N/(\mathbb{Z}/\ell\mathbb{Z})^\times$ as N is abelian. Finally, $\ker\psi \not\subset \mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})$, so $(\ker\psi)\mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z}) = \mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Hence Ψ is trivial and it follows that N is contained in the center of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, which is absurd. □

Corollary 1.2.6. *Let N be a positive integer and let Φ be a simple quotient of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Then Φ is abelian.*

Proof. Suppose this is not so, and write $N = \prod_i \ell_i^{n_i}$. Then Φ is a composition factor of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. The exact sequences

$$1 \longrightarrow \mathrm{GL}_2(\mathbb{Z}/\ell_i^{n_i}\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/(N/\ell_i^{n_i})\mathbb{Z}) \longrightarrow 1,$$
$$1 \longrightarrow I + \ell_i^{n_i-1}M_2(\mathbb{Z}/\ell_i\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/\ell_i^{n_i}\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/\ell_i^{n_i-1}\mathbb{Z}) \longrightarrow 1,$$

together with the fact that $I+\ell_i^{n_i-1}M_2(\mathbb{Z}/\ell_i\mathbb{Z}) \subset \mathrm{GL}_2(\mathbb{Z}/\ell_i^{n_i}\mathbb{Z})$ is an abelian subgroup ($n_i \geqslant 2$), show that $\Phi \simeq \mathrm{PSL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for some $\ell|N$ and $\ell \geqslant 5$. It follows from this that we may assume $N = \ell$. Now apply Lemma 1.2.5.

□

1.2.2 Fibered products of groups

Let G_1, G_2 and Q be groups, $\psi_1 : G_1 \to Q$, $\psi_2 : G_2 \to Q$ be surjective homomorphisms, and let ψ denote the abbreviation for the ordered pair (ψ_1, ψ_2). We define the *fibered product* of G_1 and G_2 over ψ, denoted $G_1 \times_\psi$

G_2, to be the group

$$G_1 \times_\psi G_2 := \{(g_1, g_2) \in G_1 \times G_2 : \psi_1(g_1) = \psi_2(g_2)\} \tag{1.2.3}$$

Note that $G_1 \times_\psi G_2$ is a subdirect product of G_1 and G_2, that is, it is a subgroup of $G_1 \times G_2$ which maps surjectively onto G_1 and G_2 under the canonical projection homomorphisms. The following lemma tells us that the converse of this also holds. We present the proof here since some elements of it will be relevant later on in this and the next Chapter.

Lemma 1.2.7 (Goursat's Lemma)**.** *Let G_1 and G_2 be groups and let $G \subseteq G_1 \times G_2$ be a subgroup such that the projections $\pi_1 : G \to G_1$ and $\pi_2 : G \to G_2$ are surjective. Then there exists a group Q and surjective homomorphisms $\psi_1 : G_1 \to Q$, $\psi_2 : G_2 \to Q$ such that $G = G_1 \times_\psi G_2$. That is,*

$$G = \{(g_1, g_2) \in G_1 \times G_2 : \psi_1(g_1) = \psi_2(g_2)\}.$$

Proof. Let $N_1 = (G_1 \times \{1\}) \cap G$ and $N_2 = (\{1\} \times G_2) \cap G$, where we use 1 to denote the identity elements of both G_1 and G_2. Then $N_1 = \ker \pi_2$ and $N_2 = \ker \pi_1$. Note that $N_1 \trianglelefteq G$ as it is the kernel of π_2. Hence $\pi_1(N_1) \trianglelefteq \pi_1(G)$, so it follows that $\pi_1(N_1) \trianglelefteq G_1$. Similarly we have $\pi_2(N_2) \trianglelefteq G_2$. Note that $\pi_i(N_i) \simeq N_i$ and hence $(G_i \times \{1\})/N_i \simeq G_i/\pi_i(N_i)$. Consider the map $f : G \to G_1/N_1 \times G_2/N_2$ defined by $(g_1, g_2) \mapsto (g_1N_1, g_2N_2)$ where we have written N_i in place of $\pi_i(N_i)$. One can easily check that for $(g_1, g_2) \in G$ one has

$$g_1N_1 = N_1 \iff g_2N_2 = N_2$$

hence the image of f is the graph of a well-defined isomorphism $G_1/N_1 \xrightarrow{\sim} G_2/N_2$. The result now follows from setting $Q := G_2/N_2$. □

We will refer to the N_i in the proof as *Goursat subgroups* and to Q as the *Goursat quotient* associated to this fibered product.

Suppose now that $L_1/K, L_2/K$ are Galois extensions of fields, with $G_i = \mathrm{Gal}(L_i/K)$ and $G = \mathrm{Gal}(L_1L_2/K)$, where L_1L_2 denotes the compositum of L_1 and L_2. Then it is well known from Galois theory that

$$G = \{(g_1, g_2) \in G_1 \times G_2 : g_1 \mid_{L_1 \cap L_2} = g_2 \mid_{L_1 \cap L_2}\} \leqslant G_1 \times G_2.$$

Lemma 1.2.8. *Keeping the above notation, we have that*

$$G = G_1 \times_\psi G_2$$

with $\psi_i : G_i \to \mathrm{Gal}(L_1 \cap L_2/K)$ *the canonical restriction maps.*

Proof. From the proof of Goursat's lemma, $N_1 = (G_1 \times \{1\}) \cap G$ and $\pi_1(N_1)$ is the subgroup of G_1 which acts trivially on $L_1 \cap L_2$, and the result follows. □

1.2.3 Modular curves and maximal subgroups of $GL_2(\mathbb{Z}/\ell\mathbb{Z})$

In this section we briefly recall the modular curves associated to the maximal subgroups of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ (for more details, see [DR73]). For a positive integer n let $X(n)$ denote the compactified modular curve which parametrizes elliptic curves with full level n structure, and let H be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ such that $\det(H) = (\mathbb{Z}/n\mathbb{Z})^\times$. The corresponding modular curve $X_H := X(n)/H$ is defined over $\mathbb{Q}$ and comes with a natural morphism

$$j : X_H \longrightarrow \mathbb{P}^1.$$

Then for any $x \in \mathbb{P}^1(\mathbb{Q})$, we have that

$$x \in j(X_H(\mathbb{Q})) \iff \begin{array}{c}\exists \text{ an elliptic curve } E \text{ over } \mathbb{Q} \text{ and a basis for } E(\overline{\mathbb{Q}})[n] \\ \text{with } j(E) = x \text{ and } \rho_{E,n}(G_\mathbb{Q}) \subseteq H.\end{array} \tag{1.2.4}$$

Now fix a prime $\ell \geqslant 3$ and suppose that H is a maximal subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ with $\det(H) = (\mathbb{Z}/\ell\mathbb{Z})^\times$. Then up to conjugation in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$,

H must be one of the following:

(i) A Borel subgroup, which is formed by the upper triangular matrices in $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

(ii) The normaliser of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

(iii) The normaliser of a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

(iv) A subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ whose projective image is S_4, A_4 or A_5 (this last occurring only for certain primes ℓ).

We define more generally the split and non-split Cartan subgroups as follows. Let A be an étale free commutative $\mathbb{Z}/\ell^n\mathbb{Z}$-algebra of rank 2. The $\mathbb{F}_\ell$-algebra $A/\ell A$ is isomorphic either to $\mathbb{F}_\ell \times \mathbb{F}_\ell$ or $\mathbb{F}_{\ell^2}$, in which case we say that A is *split* or *non-split*, respectively. The unit group $A^\times$ acts on A by multiplication, so a choice of $\mathbb{Z}/\ell^n\mathbb{Z}$-basis for A gives an embedding $A^\times \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$. A *Cartan subgroup* of $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$, denoted $C(\ell^n)$, is a subgroup that arises as the image of such an embedding. We say that $C(\ell^n)$ is split or non-split and write $C_{\mathrm{s}}(\ell^n)$ or $C_{\mathrm{ns}}(\ell^n)$ if A is split or non-split, respectively. We will denote the normaliser of a Cartan subgroup by either $C^+_{\mathrm{s}}(\ell^n)$, $C^+_{\mathrm{ns}}(\ell^n)$ or simply $C^+(\ell^n)$.

If H is one of the groups from cases (i), (ii), (iii) or (iv) above, then we will denote the corresponding modular curve by $X_0(\ell)$, $X_{\mathrm{s}}(\ell)$, $X_{\mathrm{ns}}(\ell)$ and $X_D(\ell)$, respectively where D can be one of S_4, A_4 or A_5. By 1.2.4 there is a fundamental relation between rational points on the above modular curves and the mod ℓ image of ρ_E. Specifically, let $c(E)$ be the smallest positive integer such that $\rho_{E,\ell}$ is surjective for all $\ell > c(E)$. In [Ser72] Serre asked whether one can bound $c(E)$ independent of E. It is widely conjectured that for all $E/\mathbb{Q}$ one can take $c(E) = 37$, a conjecture first posed by Serre himself in [Ser81], and which has come to be known as Serre's Uniformity Conjecture. The problem of finding explicit upper bounds for $c(E)$ has seen much progress in recent years. We will call *exceptional points* those rational

points on X_H which are non-cuspidal and do not arise from CM elliptic curves. From 1.2.4 we see that an exceptional point on X_H for H one of the groups (i), (ii), (iii) or (iv) gives rise to a non-CM elliptic curve over the rationals with non-surjective mod ℓ image. It follows then that Serre's above mentioned conjecture is equivalent to saying that the modular curves $X_0(\ell)$, $X_{\mathrm{s}}(\ell)$, $X_{\mathrm{ns}}(\ell)$ and $X_D(\ell)$ have no exceptional points for $\ell > 37$.

Mazur has shown in [Maz78] that the modular curve $X_0(\ell)$ has no exceptional points if $\ell > 17$ and $\ell \neq 37$. He has also shown that $X_0(37)$ has two exceptional points, so the value 37 in Serre's Uniformity Conjecture would be best possible. Serre himself in [Ser81] showed that $X_D(\ell)$ has no exceptional points for $\ell > 13$ and D equal to S_4, A_4 or A_5. Recent work of Bilu and Parent gives that for $\ell > 7$, $\ell \neq 13$ the curve $X_{\mathrm{s}}(\ell)$ has no exceptional points (See [BP11], [BPR11]). In general, very little is known about the curve $X_{\mathrm{ns}}(\ell)$. The combination of all of these results implies that for $\ell > 37$, is the image of $\rho_{E,\ell}$ if not surjective then it must be contained in the normaliser of a non-split Cartan subgroup. This will be of crucial importance in order to show there exists an algorithm guaranteed to terminate which determines $\rho_E(G)$.

1.3 The vertical case

In this section we consider the problem of determining the ℓ-adic image G_ℓ for a fixed prime ℓ. We do this by determining an integer n such that $G_\ell = \pi_\ell^{-1}(G(\ell^n))$ as well as computing the finite group $G(\ell^n)$.

1.3.1 Associated vector spaces

By successively adjoining to $\mathbb{Q}$ the ℓ-power torsion of E we obtain a tower of field extensions $\mathbb{Q} \subset \mathbb{Q}(E[\ell]) \subset \mathbb{Q}(E[\ell^2]) \subset \cdots \subset \mathbb{Q}(E[\ell^\infty])$. Let $M := M_2(\mathbb{Z}_\ell)$ denote the set of all 2×2 matrices with coefficients in $\mathbb{Z}_\ell$, and for

$n \geqslant 1$ let

$$\begin{aligned} V_n &= I + \ell^n M \\ &= \ker \pi_{\ell^n}, \end{aligned}$$

where π_{ℓ^n} is defined as in Section 1.2. Also, let

$$U_n = G_\ell \cap V_n = \mathrm{Gal}(\mathbb{Q}(E[\ell^\infty])/\mathbb{Q}(E[\ell^n])).$$

Note that we have $G_\ell/U_n \simeq G(\ell^n) \simeq \mathrm{Gal}(\mathbb{Q}(E[\ell^n])/\mathbb{Q})$. We obtain in this manner a filtration $G_\ell \supset U_1 \supset U_2 \supset \cdots$. Consider now the map

$$\begin{aligned} M/\ell M &\longrightarrow V_n/V_{n+1} \\ X \mod \ell M &\longmapsto I + \ell^n X \mod V_{n+1} \end{aligned}$$

Since mod ℓ^{n+1} we have $(I + \ell^n X)(I + \ell^n Y) \equiv I + \ell^n(X + Y)$ with $X, Y \in M_2(\mathbb{Z}_\ell)$ and $n \geqslant 1$, this is a group isomorphism, and $M/\ell M \simeq M_2(\mathbb{F}_\ell)$ is a vector space of dimension 4. If we look at the extension $\mathbb{Q}(E[\ell^{n+1}])/\mathbb{Q}(E[\ell^n])$, its Galois group is U_n/U_{n+1} and we have an injective group homomorphism

$$U_n/U_{n+1} \hookrightarrow M_2(\mathbb{F}_\ell), \quad I + \ell^n A \mapsto A \mod \ell.$$

It follows that $[\mathbb{Q}(E[\ell^{n+1}]) : \mathbb{Q}(E_[\ell^n])]$ divides ℓ^4. We will refer to U_n/U_{n+1} as the *associated vector space* to U_n. It has dimension at most 4 over $\mathbb{F}_\ell$.

Clearly if $G_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$ then $G(\ell^n) = \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ for all n, hence the associated vector space to U_n has dimension 4 for all $n \geqslant 1$. It could happen however that $G_\ell \subsetneq \mathrm{GL}_2(\mathbb{Z}_\ell)$, for example if $G(\ell) \subsetneq \mathrm{GL}_2(\mathbb{F}_\ell)$. In such cases the following lemma allows us to reduce the problem of determining G_ℓ to a finite computation, namely, that of determining the smallest n such that U_n/U_{n+1} has dimension 4. It is separated into two cases depending on whether ℓ is even or odd.

Lemma 1.3.1. *(i) Let $\ell \geqslant 3$. With the notation introduced above, let $n \geqslant 1$ be such that the associated vector space to U_n has dimension 4. Then we have $U_n = V_n$.*

(ii) Let $\ell = 2$. Suppose that for some $n \geqslant 2$ the associated vector space to U_n has dimension 4. Then $U_n = V_n$. If the associated vector spaces to U_1 and U_2 each have dimension 4, then we have $U_1 = V_1$.

Proof. This is shown in [LT74], §6. □

Remark 1.3.2. From $U_n = V_n$ it follows that $I + \ell^n M \subset G_\ell$, hence $G_\ell = \pi_{\ell^n}^{-1}(G(\ell^n))$, in other words, ℓ^n is stable.

1.3.2 Determining G_ℓ

The problem of computing G_ℓ can be reduced to computing $G(\ell^n)$ for various powers ℓ^n. Firstly note that for any m, there is a deterministic algorithm which computes (up to conjugacy) $G(m)$. This consists in explicitly computing the action of $\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$ on a chosen basis for $E[m]$.

Algorithm 1.3.3 (Computation of $G(m)$ for a given m)**.** *Given a non-CM curve $E/\mathbb{Q}$ and an integer m we can compute $G(m)$ as follows.*

1. Let f be the mth division polynomial of E. Construct the field $\mathbb{Q}(E[m])$ as an (at most quadratic) extension of the splitting field of f.
2. Compute $\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$ as a subgroup of S_d, where $d = [\mathbb{Q}(E[m]) : \mathbb{Q}]$ (see for instance, [Coh93], §6.3).
3. Choose a basis P, Q for $E[m]$ and determine the action of each element of $\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$ on P and Q. Compute $\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}$ as a subgroup of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ with respect to the basis P, Q.

Using this it follows that we can compute the dimension of the associated vector space to U_n for all n. When this dimension is 4 (and when $n \geqslant 2$ if

$\ell = 2$), by Lemma 1.3.1 we can recover G_ℓ as the pullback of the reduction mod ℓ^n map.

Algorithm 1.3.4 (Computation of G_ℓ for a given ℓ)**.** *Given a non-CM curve $E/\mathbb{Q}$ and a prime ℓ we can compute G_ℓ as follows.*

1. For each $n \geqslant 1$, use Algorithm 1.3.3 to compute $G(\ell^n)$.
2. If $\ell \neq 2$, continue this until $|G(\ell^{n+1})|/|G(\ell^n)| = \ell^4$, in which case set $n_\ell := n$. When $\ell = 2$, if $|G(4)|/|G(2)| = 2^4$ and $|G(8)|/|G(4)| = 2^4$ then set $n_2 = 1$. Otherwise, starting with $n = 2$ compute $G(2^n)$ until $|G(2^{n+1})|/|G(2^n)| = 2^4$, in which case set $n_2 := n$.
3. Return G_ℓ as the subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ whose reduction modulo ℓ^{n_ℓ} equals $G(\ell^{n_\ell})$.

Remark 1.3.5. In order to compute G_ℓ it suffices to find any integer n such that ℓ^n is stable, however the above algorithm finds the smallest such integer. Note also that when $G(\ell) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ and $\ell \geqslant 5$ one does not have to compute $G(\ell^2)$, since by Lemma 1.2.4 we have that ℓ is stable.

In practice this brute force computation of $G(\ell^n)$ using Algorithm 1.3.3 is computationally feasible only for very small ℓ and small n, as the degree of $\mathbb{Q}(E[\ell^n])$ is typically on the order of ℓ^{4n}. For the purposes of obtaining a deterministic algorithm we content ourselves with this approach for now. In section 1.7 we consider some of the practical considerations which can help speed up computations.

When analysing Algorithm 1.3.4, a natural question which arises is how many steps it takes to compute a stable power of ℓ. Note that since G_ℓ is an open subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$, Algorithm 1.3.4 is guaranteed to terminate after a finite number of steps. It would be of interest therefore, to have a bound on the maximum number of iterations it takes to find a stable ℓ^n for a given elliptic curve E. Let $N_{\ell,E}$ denote the smallest integer such that

$\ell^{N_{\ell,E}}$ is stable for E. For $\ell > 17$ and $\ell \neq 37$ we can obtain an upper bound for $N_{\ell,E}$ as follows. If $\rho_{E,\ell}$ is surjective, then by Corollary 1.2.4 we have that $G_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$ so the integer ℓ is already stable. By the discussion in Section 1.2.3, if $\rho_{E,\ell}$ is not surjective, then up to conjugation $G(\ell)$ must lie in the normaliser of a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Also in [Zyw11a], Zywina shows that for ℓ in the above range, one has that for every positive integer n, either $G(\ell^n)$ is contained in the normaliser of a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$, or $I + \ell^{4n}M \subset G_\ell$. In the same paper he also shows (Proposition 3.3, (ii)) that there exists a positive integer

$$M_E \leqslant \left(68N(1+\log\log N)^{1/2}\right)^{\omega(N)+1}$$

such that if $G(\ell^n)$ is contained in the normaliser of a Cartan subgroup with $\ell > 17$ and $\ell \neq 37$, then $\ell^n \mid M_E$. Here N is the product of primes for which E has bad reduction and $\omega(N)$ is the number of distinct prime factors of N. It follows from both of these results that if we let $B_E := \left(68N(1+\log\log N)^{1/2}\right)^{\omega(N)+1}$ and we take n such that $n > \log B_E/\log\ell$, then ℓ^{4n} is stable. This gives an upper bound (albeit a very poor one for practical computations) on the number of iterations it takes for ℓ^n to be stable for primes $\ell > 17,\ \ell \neq 37$.

The bound given above depends on the elliptic curve E, and no such effective upper bounds are known when $\ell \leqslant 17$ or $\ell = 37$. However, using Faltings' Theorem Zywina shows (see [Zyw11a], Lemma 5.1) that there is a non-effective bound which depends only on ℓ and holds for all elliptic curves over $\mathbb{Q}$.

With this in mind, denote by N_ℓ the smallest integer such that ℓ^{N_ℓ} is stable for all elliptic curves over $\mathbb{Q}$. For $\ell = 2$, in a recent paper [RZB14], it is shown by classifying all possible 2-adic images of $G_\mathbb{Q}$ that $N_2 = 5$. In theory it should be possible to do the same for other small primes $\ell \geqslant 3$, however as of yet there are no results as strong as this one. In numerical

computations it is observed that N_ℓ is quite small, typically at most 2 for $\ell \geqslant 3$. This is believed to be the case in particular for larger primes ℓ. In fact, as previously mentioned for $\ell > 37$ it is believed that $N_\ell = 1$.

1.4 The horizontal case

We now consider the problem of determining G_ℓ for all primes ℓ. From the previous section for any given ℓ we can compute G_ℓ, however as there are infinitely many primes, we must determine a finite subset of them outside of which the ℓ-adic image is surjective. Serre's open image theorem implies that this set exists for non-CM curves, and indeed by Corollary 1.2.4 for $\ell \geqslant 5$, having $G(\ell) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ implies $G_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$.

We now describe an algorithm of Zywina that allows one to find the set of primes S for which $\rho_{E,\ell}$ is not surjective. This uses the key fact that if $\ell > 37$, then $\rho_{E,\ell}$ is either surjective or is contained in the normaliser $C^+(\ell)$ of a Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.

Let ℓ be a prime greater than 37. The first thing to note is that $G(\ell)$ is not contained in the Cartan subgroup $C(\ell)$. If $C(\ell)$ is split, then it consists of the diagonal matrices which are contained in a Borel subgroup, hence it follows from Mazur that $G(\ell)$ is not contained in $C(\ell)$. Suppose that $C(\ell)$ is non-split, and let $\omega \in \mathbb{F}_{\ell^2}$ be such that $\omega^2 = \epsilon$, where ϵ is a non-square in $\mathbb{F}_\ell^\times$. Then by the description given in subsection 1.2.3 it follows that if we choose $\{1, \omega\}$ to be an $\mathbb{F}_\ell$-basis for $\mathbb{F}_{\ell^2}$, then we have that

$$\left\{ \begin{pmatrix} a & \epsilon b \\ b & a \end{pmatrix} : \ a, b \in \mathbb{Z}/\ell\mathbb{Z}, \ (a,b) \not\equiv (0,0) \pmod{\ell} \right\}.$$

is a non-split Cartan subgroup of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$. If we let $A \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ be the image of complex conjugation under ρ_ℓ, then it follows that A has order 2 and $\det(A) = -1$ and hence is not contained in $C(\ell)$. It follows then that in both cases $G(\ell)$ does not lie in $C(\ell)$.

Define the quadratic character

$$\psi_\ell : G_{\mathbb{Q}} \longrightarrow C^+(\ell)/C(\ell) \simeq \{\pm 1\}$$

which by the above discussion is non-trivial. Let N_E denote the conductor of E, and define M to be the product of the following prime powers:

- 8, if $4 \mid N_E$ and $\mathrm{ord}_2(j - 1728) > 0$,
- 3, if $9 \mid N_E$ and $\mathrm{ord}_3(j - 1728) > 0$,
- p, if $p^2 \mid N_E$, $p \geqslant 5$ and $\mathrm{ord}_p(j - 1728)$ is odd.

In [Zyw11b], Zywina proves the following lemma.

Lemma 1.4.1. *Keeping the above notation, we have that the following holds:*

(i) The character ψ_ℓ is unramified at all primes p such that $p \nmid M$ or $p = \ell$.

(ii) If $p \nmid N_E$ and $\psi_\ell(\mathrm{Frob}_p) = -1$, then $a_p \equiv 0 \pmod{\ell}$, where a_p denotes the trace of Frobenius.

The above lemma is useful because if $p \nmid N_E$ is a prime such that $a_p \neq 0$ and $\psi_\ell(\mathrm{Frob}_p) = -1$, then Lemma 1.4.1 implies that $\ell \mid a_p$ (note that $p \nmid M$) and the Hasse bound then gives

$$\ell \leqslant |a_p| \leqslant 2\sqrt{p}.$$

It follows that such a choice of p would give an upper bound for ℓ. We now describe how to use this to construct the set of primes S for which $\rho_{E,\ell}$ is not surjective.

Consider the group V of characters $(\mathbb{Z}/M\mathbb{Z})^\times \to \mathbb{F}_2$, which is a vector space over $\mathbb{F}_2$. Let $\chi_1, \ldots \chi_d$ be a basis of V over $\mathbb{F}_2$, which we can take to be the characters $\left(\frac{\cdot}{q}\right)$ for each odd prime $q \mid M$, the character $\chi(a) =$

$(-1)^{(a-1)/2}$ if M is even and the character $\chi(a) = (-1)^{(a^2-1)/8}$ if $8|M$. Consider the sequence of primes $p_1 < p_2 < p_3 < \dots$ such that $p_i \nmid N_E$ and $a_{p_i} \neq 0$. Note then that p_i does not divide M. For each $r \geqslant 1$, define the matrix over $\mathbb{F}_2$ given by $A_r := \left(\chi_j(p_i)\right)_{i,j}$ with $1 \leqslant i \leqslant r$, $1 \leqslant j \leqslant d$. By Dirichlet's theorem and the fact that the set of primes of supersingular reduction of a non-CM curve has density 0 ([Ser64]) we have that any vector in $\mathbb{F}_2^d$ is of the form $(\chi_1(p), \dots, \chi_d(p))$ for some prime $p \nmid N_E$ with $a_p \neq 0$. It follows then that A_r will have rank d for all sufficiently large r.

Lemma 1.4.2. *Suppose the matrix A_r has rank d, and let $\ell \geqslant 11$ be a prime that does not divide $\prod_{i=1}^{r} a_{p_i}$. Then $G(\ell)$ is not contained in the normaliser of a Cartan subgroup. In particular, $G(\ell) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for all $\ell > 37$ that do not divide $\prod_{i=1}^{r} a_{p_i}$.*

Proof. See Lemma 3.1 of [Zyw11b]. □

Algorithm 1.4.3 (Finding the set of primes S for which the mod ℓ image is not surjective)**.** *Keeping the notation above, we can compute S as follows.*

1. *Compute M, and for each $i = 1, 2, \dots$ compute the vector $(\chi_1(p_i), \dots, \chi_d(p_i))$ as well as the matrix A_r.*
2. *Continue this until A_r has rank d, in which case set S' to be the set of primes $\ell > 37$ that divide $\prod_{i=1}^{r} a_{p_i}$.*
3. *For each prime $\ell \in S'$, use Algorithm 1.3.3 to determine whether or not $\rho_{E,\ell}$ is surjective. Set S to be the subset of primes of S' for which the mod ℓ image is not surjective.*

Algorithm 1.4.3 works quite well even in practice, and as we have seen in Section 1.2.3, it is conjectured that any ℓ for which the mod ℓ image is non-surjective will satisfy $\ell \leqslant 37$. It should also be noted that in Algorithm 1.4.3 if A_r has rank d with $p_r \leqslant 419$, then $\rho_{E,\ell}$ is surjective for all primes $\ell > 37$. This follows since the Hasse bound implies that if A_r has rank d, then $\rho_{E,\ell}$ is surjective for all primes $\ell > \max(37, 2\sqrt{p_r})$.

1.5 Dealing with entanglements

From the previous two sections we have an algorithm to determine the set S of primes ℓ for which $\rho_{E,\ell}$ is not surjective. In addition, by Corollary 1.2.4 we have that $G_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$ for ℓ outside of $S \cup \{2,3\}$, hence for every prime ℓ we are able to determine the ℓ-adic image G_ℓ. What remains is to compute the possible entanglements between the torsion fields of E. Set

$$\begin{aligned} \mathcal{T} &:= \{2,3\} \cup S \cup \{\ell \ : \ \ell \mid N_E\}, \\ m &:= \prod_{\ell \in \mathcal{T}} \ell. \end{aligned}$$

Lemma 1.5.1. *The integer m splits ρ_E, that is,*

$$G = G_m \times \prod_{\ell \nmid m} \mathrm{GL}_2(\mathbb{Z}_\ell).$$

Proof. The proof follows similar lines as that of Theorem 6.1 in [LT74], as well as §IV, 3.4 of [Ser68]. Let $\mathcal{L} := \{\ell \ : \ \ell \notin \mathcal{T}\}$, and let $G_\mathcal{L}$ be the projection of G onto $\prod_{\ell \in \mathcal{L}} \mathrm{GL}_2(\mathbb{Z}_\ell)$. We first show that

$$G_\mathcal{L} = \prod_{\ell \in \mathcal{L}} \mathrm{GL}_2(\mathbb{Z}_\ell). \tag{1.5.1}$$

For B a subset of $\mathcal{L}$, denote by $\pi_{\mathcal{L},B}$ the projection

$$\pi_{\mathcal{L},B} : \prod_{\ell \in \mathcal{L}} \mathrm{GL}_2(\mathbb{Z}_\ell) \longrightarrow \prod_{\ell \in B} \mathrm{GL}_2(\mathbb{Z}_\ell) \tag{1.5.2}$$

and let $G_{\mathcal{L},B}$ denote the image of $G_\mathcal{L}$ under the map (1.5.2). We show that if $G_{\mathcal{L},B} = \prod_{\ell \in B} \mathrm{GL}_2(\mathbb{Z}_\ell)$ then for any prime $\ell_0 \in \mathcal{L} - B$ we have $G_{\mathcal{L},B\cup\{\ell_0\}} = \prod_{\ell \in B \cup \{\ell_0\}} \mathrm{GL}_2(\mathbb{Z}_\ell)$. Since $G_{\{\ell\}} = \mathrm{GL}_2(\mathbb{Z}_\ell)$, this implies $G_\mathcal{L}$ is dense in $\prod_{\ell \in \mathcal{L}} \mathrm{GL}_2(\mathbb{Z}_\ell)$ and since it is closed by Serre's open image theorem, (1.5.1) will then follow. Let then $B_0 := B \cup \{\ell_0\}$, and recall that

we may view $G_{\mathcal{L},B_0}$ as a subgroup of $G_{\mathcal{L},B} \times G_{\mathcal{L},\{\ell_0\}}$. Let Q_0 denote the Goursat quotient associated to the fibered product given by the inclusion $G_{\mathcal{L},B_0} \hookrightarrow G_{\mathcal{L},B} \times G_{\mathcal{L},\{\ell_0\}}$. By Lemma 1.2.8 we have Q_0 may be identified with $\mathrm{Gal}(K_B \cap K_{\{\ell_0\}}/\mathbb{Q})$, where K_B is the compositum of the ℓ-power torsion fields $\mathbb{Q}(E[\ell^\infty])$ for $\ell \in B$. Note that Q_0 is a common finite quotient of $G_{\mathcal{L},B} = \prod_{\ell \in B} \mathrm{GL}_2(\mathbb{Z}_\ell)$ and $G_{\mathcal{L},\{\ell_0\}} = \mathrm{GL}_2(\mathbb{Z}_{\ell_0})$. Suppose that Q_0 is non-trivial. Replacing Q_0 by a quotient and $K_B \cap K_{\{\ell_0\}}$ by a subfield if necessary, we may assume that Q_0 is a simple quotient. But then there is an integer N divisible by primes only in B and an integer n such that Q_0 is a common simple quotient of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ and $\mathrm{GL}_2(\mathbb{Z}/\ell_0^n\mathbb{Z})$, hence it must be abelian by Corollary 1.2.6. It follows that $K_B \cap K_{\{\ell_0\}}$ non-trivially intersects the maximal abelian extensions of $\mathbb{Q}$ inside $\mathbb{Q}(E[N])$ and $\mathbb{Q}(E[\ell_0^n])$. Since both N and ℓ_0 are odd, these extensions are, respectively, $\mathbb{Q}(\zeta_N)$ and $\mathbb{Q}(\zeta_{\ell_0^n})$. We conclude that $K_B \cap K_{\{\ell_0\}} = \mathbb{Q}$, hence Q_0 is trivial and (1.5.1) holds.

Consider now the inclusion $G \hookrightarrow G_m \times G_{\mathcal{L}}$ and denote by Q_m the corresponding Goursat quotient. By the same reasoning as above, it suffices to show that $K_m \cap K_{\mathcal{L}} = \mathbb{Q}$, where K_m is the compositum of the ℓ^∞-torsion fields for $\ell \mid m$. Suppose then that Q_m is non-trivial. By replacing Q_m by a quotient we may again assume Q_m is simple. Then there is an integer M divisible only by primes dividing m and an integer n coprime to m such that Q_m is a common simple quotient of $G(M)$ and $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, hence is again abelian by Corollary 1.2.6. It follows that $K_m \cap K_{\mathcal{L}}$ non-trivially intersects $\mathbb{Q}(E[M]) \cap \mathbb{Q}(\zeta_n)$. However since m is divisible by all primes of bad reduction, $\mathbb{Q}(E[M])$ is unramified outside of primes dividing m, and $\mathbb{Q}(\zeta_n)$ is unramified outside of primes dividing n, we conclude $K_m \cap K_{\mathcal{L}} = \mathbb{Q}$ and Q_m is trivial. This completes the proof. □

From the above lemma it follows that $\mathcal{T}$ contains all the prime divisors of m_E and that

$$G = G_m \times \prod_{\ell \nmid m} \mathrm{GL}_2(\mathbb{Z}_\ell)$$

so in order to determine G it remains to compute G_m. We will give a method to determine an integer $\tilde{m}$ such that

$$G_m = \pi_{\tilde{m}}^{-1}(G(\tilde{m})). \tag{1.5.3}$$

There is a natural embedding $G_m \hookrightarrow \prod_{\ell \in \mathcal{T}} G_\ell$, however this is in general not surjective due to the fact that distinct ℓ-power torsion fields can have non-trivial intersection. From an algorithmic point of view, the problem is that we need to determine intersections between fields of infinite degree over $\mathbb{Q}$. For this we will require the following lemma.

Lemma 1.5.2. *Let $N > 1$ be a positive integer, $\ell > 2$ a prime and $A \in I + \ell^N M$, where $M = M_2(\mathbb{Z}_\ell)$. Then there exists $Y \in I + \ell^{N-1}M$ such that $Y^\ell = A$. If $\ell = 2$ then we must take $N > 2$.*

Proof. Suppose $\ell > 2$. We inductively construct the sequence $\{A_n\}$ by $A_1 = I$ and

$$A_{n+1} = A_n - \frac{1}{\ell}(A_n^\ell - A)(A_n^{-1})^{\ell-1}$$

for $n \geqslant 1$. Let e_n be the largest integer such that

$$A_n^\ell - A \equiv 0 \pmod{\ell^{e_n}}.$$

We show by induction that for $n \geqslant 1$ we have

(i) $e_n \geqslant 1 + 2^{n-1}(N-1)$, and further we may write

$$A_n^\ell - A = \ell^{1+2^{n-1}(N-1)} B_n,$$

where $B_n \in M$ commutes with A_n and A.

(ii) A_n commutes with A.

(iii) $A_n \equiv I \pmod{\ell^{N-1}}$.

Note that at each step, by (i) and the fact that $1 + 2^{n-1}(N-1) > 1$ for every n we have $1/\ell(A_n^\ell - A)$ is in M. Also, by (iii) we have $A_n \in \mathrm{GL}_2(\mathbb{Z}_\ell)$ and hence A_{n+1} is a well-defined element of M. We now proceed to show (i), (ii) and (iii) for all n.

For $n = 1$, part (i) follows directly by assumption on A, and parts (ii) and (iii) are clear. Now assume (i), (ii) and (iii) are true for n. We first show (i) for $n+1$. By (i) for n we have

$$A_n^\ell - A = \ell^{1+2^{n-1}(N-1)} B_n,$$

where B_n commutes with A_n and A. Then compute

$$\begin{aligned}
A_{n+1}^\ell - A &= \left(A_n - \ell^{2^{n-1}(N-1)} B_n (A_n^{-1})^{\ell-1}\right)^\ell - A \\
&= A_n^\ell - \ell^{1+2^{n-1}(N-1)} B_n + \cdots \\
&\qquad + (-1)^\ell \ell^{2^{n-1}(N-1)\ell} B_n^\ell (A_n^{-1})^{\ell^2-\ell} - A \\
&= \binom{\ell}{2} \ell^{2^n(N-1)} B_n^2 A_n^{-1} + \cdots \\
&\qquad + (-1)^\ell \ell^{2^{n-1}(N-1)\ell} B_n^\ell (A_n^{-1})^{\ell^2-\ell} \\
&= \ell^{1+2^n(N-1)} B_{n+1},
\end{aligned}$$

where in the second equality we have used the fact that A_n and B_n commute, in the third one we have used that

$$A_n^\ell - A = \ell^{1+2^{n-1}(N-1)} B_n,$$

and in the last one we have used the fact that $\ell > 2$, which gives $2^{n-1}(N-1)\ell \geqslant 1 + 2^n(N-1)$. Now note that A commutes with A_n and B_n, and also A_n commutes with B_n, hence both A_{n+1} and A commute with B_{n+1}, establishing (i). Part (ii) follows immediately from the fact that A commutes

with A_n. Finally, observe that $2^{n-1}(N-1) \geqslant N-1$, hence

$$A_{n+1} = A_n - \ell^{2^{n-1}(N-1)} B_n (A_n^{-1})^{\ell-1}$$

satisfies $A_{n+1} \equiv I \pmod{\ell^{N-1}}$, establishing (iii), and this completes the induction.

Observe now that this sequence satisfies

$$\begin{aligned} A_{n+1} - A_n &= -\frac{1}{\ell}(A_n^\ell - A)(A_n^{-1})^{\ell-1} \\ &\equiv 0 \pmod{\ell^{2^{n-1}(N-1)}} \end{aligned}$$

hence A_n converges to some limit $Y \in I + \ell^{N-1}M$ by (iii). Finally by (i), we obtain $Y^\ell = A$, as desired. The case $\ell = 2$ is shown similarly, except here the we obtain $e_n \geqslant 2 + 2^{n-1}(N-2)$, so we must take $N > 2$. □

Let $\ell_1 > \ell_2 > \cdots > \ell_n$ be the primes in $\mathcal{T}$, where $\ell_n = 2$. For B a subset of $\{\ell_1, \ldots, \ell_n\}$ we denote by G_B the projection of G_m onto the product of primes in B. Also, for each $1 \leqslant k \leqslant n$ let $B_k := \{\ell_1, \ell_2, \ldots, \ell_k\}$.

Proposition 1.5.3. *Let $k < n$, let m_k be such that $G_{B_k} = \pi_{m_k}^{-1}(G(m_k))$. Let $\ell_{k+1}^{e_k}$ be the largest power of ℓ_{k+1} dividing the order of $G(\ell_1 \cdots \ell_k)$, and let $t_k \geqslant 1$ be such that $\ell_{k+1}^{t_k}$ is stable. Also, set*

$$\alpha := \begin{cases} t_k + e_k & \text{if } \ell_{k+1} > 3, \\ 3 \cdot \max\{t_k + e_k, 2 + e_k\} & \text{if } \ell_{k+1} = 2 \end{cases}$$

and $m_{k+1} := \ell_{k+1}^\alpha m_k$. Then $G_{B_{k+1}} = \pi_{m_{k+1}}^{-1}(G(m_{k+1}))$.

Remark 1.5.4. Note that because $G_{B_1} = G_{\ell_1}$ is known, then so is m_1. Also since $G_{B_n} = G_m$, the above proposition allows us to determine $\tilde{m} = m_n$ in a finite number of steps. In particular we have that m_E divides m_n.

Proof. Recall that G_{B_k} may be identified with $\mathrm{Gal}(K_{B_k}/\mathbb{Q})$ where as before K_{B_k} is the compositum of the ℓ-power torsion fields $\mathbb{Q}(E[\ell^\infty])$ for $\ell \in B_k$.

Note that $G_{B_{k+1}}$ may be viewed as a subgroup of $G_{B_k} \times G_{\ell_{k+1}}$ whose projections are surjective, so let N_{B_k} and $N_{\ell_{k+1}}$ be the corresponding Goursat subgroups. By Lemma 1.2.8 the isomorphic quotients

$$G_{B_k}/N_{B_k} \xrightarrow{\sim} G_{\ell_{k+1}}/N_{\ell_{k+1}}$$

may be identified with $\mathrm{Gal}(K_{B_k} \cap K_{\ell_{k+1}}/\mathbb{Q})$, which we will denote by Φ. We see that determining Φ is equivalent to determining the intersection $K_{B_k} \cap K_{\ell_{k+1}}$.

Suppose that $\ell_{k+1} > 2$. Define U_k to be

$$U_k := \{A \in G_{B_k} : A \equiv I \pmod{\ell_1 \cdots \ell_k}\}$$

and observe that the order of any finite quotient of U_k is divisible only by primes in B_k, all of which are greater than ℓ_{k+1}. Then since any finite quotient of $G_{\ell_{k+1}}$ is divisible only by primes dividing the product $(\ell_{k+1} - 1)\ell_{k+1}(\ell_{k+1} + 1)$ and $\ell_{k+1} \neq 2$ it follows that U_k maps to the identity in the composite map

$$U_k \longrightarrow G_{B_k}/N_{B_k} \xrightarrow{\sim} G_{\ell_{k+1}}/N_{\ell_{k+1}}$$

and so $U_k \subset N_{B_k}$. Also, since we have that U_k may be identified with $\mathrm{Gal}(K_{B_k}/\mathbb{Q}(E[\ell_1 \cdots \ell_k]))$ it follows

$$K_{B_k} \cap K_{\ell_{k+1}} \subset \mathbb{Q}(E[\ell_1 \cdots \ell_k]).$$

Consider the subgroup of $G_{\ell_{k+1}}$ given by

$$Q := \langle A^{\ell_{k+1}^{e_k}} : A \in G_{\ell_{k+1}} \rangle \leqslant G_{\ell_{k+1}}.$$

We claim that the map $G_{\ell_{k+1}} \to \Phi$ factors via $G_{\ell_{k+1}}/((I + \ell_{k+1}M) \cap Q)$.

This is clear since for any $A \in (I+\ell_{k+1}M)\cap Q$, the image of A in Φ will have order a power of ℓ_{k+1}, and will also itself be a product of $\ell_{k+1}^{e_k}$-th powers. But any such element of Φ must be trivial since the highest power of ℓ_{k+1} dividing Φ is not greater than $\ell_{k+1}^{e_k}$.

Note that $I + \ell_{k+1}^{\alpha-e_k}M \subset G_{\ell_{k+1}}$. If $e_k \geqslant 1$ then $\alpha \geqslant 2$ and so by repeated application of Lemma 1.5.2 with $\alpha = N$ we obtain that for any $A \in I+\ell_{k+1}^{\alpha}M$ there exists $Y \in I + \ell_{k+1}^{\alpha-e_k}M$ such that $Y^{\ell_{k+1}^{e_k}} = A$. It follows that

$$I + \ell_{k+1}^{\alpha}M \subset (I + \ell_{k+1}M) \cap Q. \tag{1.5.4}$$

If $e_k = 0$ then (1.5.4) is trivially true since in this case $Q = G_{\ell_{k+1}}$. We conclude

$$K_{B_k} \cap K_{\ell_{k+1}} = \mathbb{Q}(E[\ell_1 \cdots \ell_k]) \cap \mathbb{Q}(E[\ell_{k+1}^{\alpha}]).$$

Suppose now that $\ell_{k+1} = 2$, so that $k = n-1$. Note that in this case $I+\ell_1 \cdots \ell_{n-1}M$ need not map to the identity in G_2/N_2 since G_2 has quotients of order divisible by 3. We show however that

$$K_2 \cap K_{B_{n-1}} \subset \mathbb{Q}(E[3^{t+1}\ell_1 \cdots \ell_{n-2}]) \tag{1.5.5}$$

where $t \geqslant 1$ is denoting an integer such that 3^t is stable. Define

$$T_3 := \langle A^3 : A \in G_3 \rangle \leqslant G_3.$$

Since the order G_2/N_2 has at most one factor of 3, the map $G_3 \to G_2/N_2$ factors via $G_3/\big((I+3M)\cap T_3\big)$. Note also that $I + 3^tM \subset G_3$ and $t+1 \geqslant 2$, hence by Lemma 1.5.2 we have

$$(I + 3^{t+1}M) \subset (I + 3M) \cap T_3.$$

It follows that if we define

$$U'_{n-1} = \{A \in G_{B_{n-1}} : A \equiv I \pmod{3^{t+1}\ell_1 \cdots \ell_{n-2}}\}$$

then U'_{n-1} maps to the identity in G_2/N_2, hence (1.5.5) holds. Similarly as before we can also show that

$$K_2 \cap K_{B_{n-1}} \subset \mathbb{Q}(E[2^\alpha]).$$

The result now follows. □

1.6 Algorithm to compute $\rho_E(G_{\mathbb{Q}})$

We now have all the ingredients necessary to give a deterministic algorithm which, given an elliptic curve E, determines the image of ρ_E. We summarize it below.

Algorithm 1.6.1 (Determining the image of ρ_E)**.** *Given a non-CM elliptic curve over $\mathbb{Q}$, we may determine ρ_E as follows.*

1. Use Algorithm 1.4.3 to determine the set of primes S for which the mod ℓ image is not surjective.
2. Define the set $\mathcal{T} := \{2, 3, 5\} \cup S \cup \{\ell : \ell \mid N_E\}$.
3. For each $\ell \in \mathcal{T}$, use Algorithm 1.3.4 to determine G_ℓ.
4. For each $k = 1, \ldots, n-1$, use Proposition 1.5.3 to determine m_{k+1}. Note that this is possible as for each $\ell \in \mathcal{T}$ we have already computed t such that ℓ^t is stable. Also, using Algorithm 1.3.3 we may determine the largest power of ℓ dividing any of the finite groups $G(\ell_1 \cdots \ell_k)$.
5. Once determined m_n use Algorithm 1.3.3 to compute $G(m_n)$.

1.7 Practical considerations

As mentioned previously, Algorithm 1.6 is very slow in practice. Unless the set $\mathcal{T}$ contains only primes less than 7 and the stable powers of those primes are less than 2 this algorithm will take a very long time. There are several steps throughout which can be made much faster if we sacrifice having an unconditional algorithm. This is managed by instead at some steps having a heuristic algorithm using Frobenius statistics. In this section we briefly describe this approach.

The most time consuming step in our algorithm is the computation of $G(m)$ using Algorithm 1.3.3. If $m = \ell$ is prime, then there is a very fast algorithm due to Sutherland ([Sut13]) which computes the image of $\rho_{E,\ell}$ up to isomorphism, and usually up to conjugacy by using Frobenius statistics. If $\rho_{E,\ell}$ is surjective, then the algorithm proves this unconditionally. Otherwise its output is correct with a very high probability. This has been used to compute the mod ℓ image for every curve in the Cremona and Stein-Watkins databases for all $\ell < 60$.

Recall the notation of Section 1.3.1. We have used the Algorithm 1.3.3 to compute the smallest n such that the associated vector space to U_n has dimension 4. This is also quite time consuming when using Algorithm 1.3.3. Another way to do this would be to produce four elements $Y_i \in G_\ell$ such that

$$Y_i \equiv I + \ell^n X_i \pmod{\ell^{n+1}}$$

for $1 \leqslant i \leqslant 4$, and such that the X_i are linearly independent mod ℓ, and we can try to produce these elements via Frobenius elements at unramified primes. To be precise, let p be a prime of good reduction and as usual a_p denote the trace of Frobenius. Then one way to try to achieve this is by using the characteristic polynomial of Frob_p which we know is

$$\Phi_p(X) = X^2 - a_p X + p.$$

This can be done easily using machine computation, and in this manner we can explicitly write down reductions mod ℓ^n of matrices in G_ℓ, for suitable ℓ^n. If we are able to produce the four required elements Y_i then this shows unconditionally that ℓ^n is stable. This method however has the limitation that it does not work so well if the mod ℓ image is 'small'. See [LT74], §8 for one example of this method being used effectively.

We can conditionally determine the power n_ℓ such that ℓ^{n_ℓ} is stable, provided ℓ^{n_ℓ} is not too large. One method to do this is to use the density of primes $p \nmid N_E$ which split completely in $\mathbb{Q}(E[\ell^n])$ to determine the degree of $\mathbb{Q}(E[\ell^n])$ for different n, and increase n until $[\mathbb{Q}(E[\ell^n]) : \mathbb{Q}(E[\ell^{n-1}])] = \ell^4$. We illustrate this with an example.

1.7.1 Example: $Y^2 + XY + Y = X^3 + 4X - 6$

Consider the elliptic curve E over $\mathbb{Q}$ given by Weierstrass equation $Y^2+XY+Y = X^3+4X-6$. The discriminant of this Weierstrass model is $\Delta = -2^6 7^3$. Using Algorithm 1.4.3 and Sutherland's algorithm for the mod ℓ image we obtain that $\rho_{E,\ell}$ is surjective for all $\ell \neq 2, 3$ and $G(2) \simeq G(3) \simeq \{\pm 1\}$. This already implies that $G_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$ for all $\ell > 3$. The next step is to find G_2 and G_3 by finding exponents n_2 and n_3 such that 2^{n_2} and 3^{n_3} are stable. Here using Algorithm 1.3.3 is relatively fast for computing $G(2)$ and $G(4)$, however it quickly becomes infeasible to compute the 2^n-torsion for higher powers of 2. Also, the mod 2 and mod 3 images are too small for the method of Frobenius sampling outlined above to work.

Note that by Chebotarev, for each prime $p \nmid 14$ the density of primes splitting completely in $\mathbb{Q}(E[4])$ is $1/|G(4)|$. For each prime $p \nmid 14$ up to a chosen bound B we compute the observed density of primes such that the reduced curve $\tilde{E}(\mathbb{F}_p)$ has full 4-torsion. The observed density of primes $p \leqslant 10000000$ is 0.0311144 while $1/2^5 \simeq 0.03125$, so we can conditionally conclude that $[\mathbb{Q}(E[2^2]) : \mathbb{Q}(E[2])] = 2^4$. In the same manner one can determine that $[\mathbb{Q}(E[2^3]) : \mathbb{Q}(E[2^2])] = 2^3$ and $[\mathbb{Q}(E[2^4]) : \mathbb{Q}(E[2^3])] =$

2^4, hence 2^3 is stable. In the same way we can deduce that 3 is stable. In principle we may do the same thing to determine the degrees of the intersections between various torsion fields in such a way to determine $|G(2^3 \cdot 3 \cdot 7)|$, however this is quite time-consuming when the degrees of the fields in question are large.

The information we have obtained on the various mod ℓ images of ρ_E is, in this particular situation, already sufficient for us to determine m_E, using the same techniques we have used throughout this chapter. We first determine $G(8 \cdot 7)$, which is equivalent to determining $\mathbb{Q}(E[8]) \cap \mathbb{Q}(E[7])$. Note first of all that

$$\mathbb{Q}(E[2]) = \mathbb{Q}(\sqrt{\Delta}) \subset \mathbb{Q}(\zeta_7) \subset \mathbb{Q}(E[7]).$$

Let $L = \mathbb{Q}(E[8]) \cap \mathbb{Q}(E[7])$. We claim that $L = \mathbb{Q}(\sqrt{-7})$. Suppose otherwise that $\mathbb{Q}(\sqrt{-7})$ is strictly contained in L. As K_2 is a pro-2 tower of fields it follows that $L/\mathbb{Q}(\sqrt{-7})$ is a 2-power extension. Note that by the computations above we know that $G(7) \simeq \mathrm{GL}_2(\mathbb{F}_7)$. Let $\mathbb{Q}(E[7]_x)$ be the subfield of $\mathbb{Q}(E[7])$ fixed by $\{\pm 1\}$, so that

$$\mathrm{Gal}(\mathbb{Q}(E[7])_x/\mathbb{Q}(\zeta_7)) \simeq \mathrm{PSL}_2(\mathbb{F}_7).$$

Since L is Galois over $\mathbb{Q}(\sqrt{-7})$, it follows that $L \not\subset \mathbb{Q}(E[7]_x)$, for if it were then $L\mathbb{Q}(\zeta_7)$ would be a non-trivial Galois extension of $\mathbb{Q}(\zeta_7)$, and hence it would correspond to a non-trivial normal subgroup of $\mathrm{PSL}_2(\mathbb{F}_7)$, contradicting the simplicity of $\mathrm{PSL}_2(\mathbb{F}_\ell)$ for $\ell \geqslant 5$. Finally, if $L \not\subset \mathbb{Q}(E[7]_x)$, then $L\mathbb{Q}(\zeta_7)$ corresponds to a proper subgroup of $\mathrm{SL}_2(\mathbb{F}_7)$ which maps surjectively onto $\mathrm{PSL}_2(\mathbb{F}_7)$, contradicting Lemma 2, §3.4 in [Ser68]. This shows that $L = \mathbb{Q}(\sqrt{-7})$.

It remains then to compute the intersection $K_3 \cap (K_2K_7)$. Let Q be the Goursat quotient corresponding to this intersection. That is, $Q \simeq \mathrm{Gal}(M/\mathbb{Q})$ where $M = K_3 \cap K_2K_7$. Note that since $\mathbb{Q}(E[3]) = \mathbb{Q}(\zeta_3)$ is

totally ramified at 3, and $K_3/\mathbb{Q}(E[3])$ is pro-3, then Q is a 3- group. Let $U = \mathrm{Gal}(K_2K_7/\mathbb{Q}(E[7])$. Then every finite quotient of U has order divisible only by 2 and 7, hence U maps to the identity under $U \to Q$, and it follows that $M \subset \mathbb{Q}(E[7])$.

By replacing Q with a subgroup if necessary, we may assume Q is simple. By Lemma 1.2.6, the only simple non-abelian quotient of $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$ is $\mathrm{PSL}_2(\mathbb{Z}/7\mathbb{Z})$, hence it follows that Q must be abelian. We have then that the only possibility is $Q \simeq (\mathbb{Z}/7\mathbb{Z})^\times/\{\pm 1\}$.