Galois representations of elliptic curves and abelian entanglements

Brau Avila, Julio

Galois representations of elliptic curves and abelian entanglements

Proefschrift

ter verkrijging van
de graad van Doctor aan de Universiteit Leiden
op gezag van Rector Magnificus prof. mr. C.J.J.M. Stolker,
volgens besluit van het College voor Promoties
te verdedigen op [1/12/2015]
klokke [11:15] uur

door

Julio Brau Avila
geboren te Hermosillo
in 1985

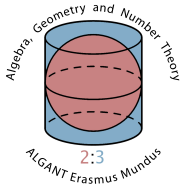
Samenstelling van de promotiecommissie:

Promotor: Prof. dr. Peter Stevenhagen (Universiteit Leiden)
Promotor: Prof. dr. Karim Belabas (Université Bordeaux I)

Overige leden:

Prof. dr. T. Dokchitser (University of Bristol)
Prof. dr. J. Top (Rijksuniversiteit Groningen)
Prof. dr. H. W. Lenstra, emeritus (Universiteit Leiden)
Prof. dr. B. de Smit (Universiteit Leiden)
Dr. M. Streng (Universiteit Leiden)

This PhD project was funded by the Erasmus Mundus program Algant-DOC, and was carried out at the Universiteit Leiden and the Université Bordeaux 1



THÈSE

présentée à

L'UNIVERSITÉ BORDEAUX I

ÉCOLE DOCTORALE DE MATHÉMATIQUES ET INFORMATIQUE

par Julio BRAU AVILA

POUR OBTENIR LE GRADE DE

DOCTEUR

SPECIALITÉ : Mathématiques Pures

Galois representations of elliptic curves and abelian entanglements

Directeurs de recherche : Peter STEVENHAGEN, Karim BELABAS

Soutenue le : Décembre 2015 à Leiden

Devant la commission d'examen formée de :

M STEVENHAGEN, Peter	Professeur	Universiteit Leiden	Directeur
M BELABAS, Karim	Professeur	Université Bordeaux I	Directeur
M DOKCHITSER, Tim	Professeur	University of Bristol	Rapporteur
M TOP, Jaap	Professeur	Rijksuniversiteit Groningen	Rapporteur
M LENSTRA, Hendrik	Professeur	Universiteit Leiden	Examinateur
M DE SMIT, Bart	Professeur	Universiteit Leiden	Examinateur
M STRENG, Marco	Docteur	Universiteit Leiden	Examinateur

Contents

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 $Q \simeq (\mathbb{Z}/7\mathbb{Z})^\times/\{\pm 1\}$.

Chapter 2

Entanglement correction factors as character sums

2.1 Introduction

The motivation for this chapter comes from the classical conjecture of Artin from 1927 which predicts the density of primes p for which a given rational number is a primitive root modulo p. More precisely, let g be an integer different from ± 1, and let h be the largest integer such that $g = g_0^h$ with $g_0 \in \mathbb{Z}$. The heuristic reasoning described by Artin was the following. If p is a prime number coprime to g, then g is a primitive root modulo p if and only if there is no prime ℓ dividing $p-1$ such that $g \equiv y^\ell \pmod{p}$ for some y. Note that this congruence condition can be given as a splitting condition on the prime p in the field $F_\ell := \mathbb{Q}(\zeta_\ell, \sqrt[\ell]{g})$. Indeed, the condition on p is equivalent to p not splitting completely in the aforementioned field. In other words, g is a primitive root modulo p if and only if for every prime $\ell < p$ we have that Frob_p is not the identity element in $\mathrm{Gal}(F_\ell/\mathbb{Q})$.

For a fixed ℓ, the density of primes which do not split completely in F_ℓ

is equal to

$$\delta_\ell := 1 - \frac{1}{[F_\ell : \mathbb{Q}]},$$

and this equals $1 - \frac{1}{\ell-1}$ for $\ell \mid h$ and $1 - \frac{1}{\ell(\ell-1)}$ otherwise. If we assume the splitting conditions in the various fields F_ℓ to be independent, then it is reasonable to expect that the density of primes p for which g is a primitive root modulo p is equal to $\prod_\ell \delta_\ell$. This was the density originally conjectured by Artin, however years later (see [Ste03]) he noticed that this assumption of independence is not correct, as the fields F_ℓ can have non-trivial intersections. If $F_2 = \mathbb{Q}(\sqrt{g})$ has discriminant $D \equiv 1 \pmod 4$, then F_2 is contained in the compositum of the fields F_ℓ with $\ell \mid D$. The corrected version of the conjecture was proven by Hooley under the assumption of the Generalized Riemann Hypothesis (GRH). He showed in [Hoo67] that, conditional on GRH, the density of primes such that g is a primitive root modulo p equals

$$C_g = \sum_{n=1}^{\infty} \frac{\mu(n)}{[F_n : \mathbb{Q}]} \tag{2.1.1}$$

where $F_n = \mathbb{Q}(\zeta_n, \sqrt[n]{g})$ and μ is the Möbius function. In the same paper Hooley shows that (2.1.1) can be rewritten as

$$C_g = \mathfrak{C}_g \prod_{\ell \mid h} \Big(1 - \frac{1}{\ell - 1}\Big) \prod_{\ell \nmid h} \Big(1 - \frac{1}{\ell(\ell-1)}\Big), \tag{2.1.2}$$

where $\mathfrak{C}_g$ is an *entanglement correction factor*, a rational number which depends on g. In fact it is given explicitly by

$$\mathfrak{C}_g := 1 - \prod_{\substack{\ell \mid D \\ \ell \mid h}} \frac{-1}{\ell - 2} \cdot \prod_{\substack{\ell \mid D \\ \ell \nmid h}} \frac{-1}{\ell^2 - \ell - 1}.$$

One advantage of having C_g in the form given by (2.1.2) is that it makes it easy to see when the density C_g vanishes. Vanishing of C_g implies that, con-

jecturally, there exist only finitely many primes p such that g is a primitive root modulo p, and the multiplicative structure of C_g and $\mathfrak{C}_g$ allows one to identify precisely what are the obstructions to this.

There are many interesting generalisations to Artin's conjecture on primitive roots. For instance, one could consider only primes p which lie in a prescribed congruence class modulo some integer f. One could also study the set of primes p such that g generates a subgroup of a given index in $(\mathbb{Z}/p\mathbb{Z})^\times$. As is shown in [Len77], in both of these cases one can again obtain a density under GRH via a formula similar to (2.1.1). However, it is not clear how to describe the non-vanishing criteria of such densities from such a sum.

In [LMS14], the authors develop an efficient method to compute entanglement correction factors $\mathfrak{C}_g$ for Artin's original conjecture and several of its generalisations. Their method consists in expressing $\mathfrak{C}_g$ as a sum of quadratic characters. More precisely, they show that $\mathfrak{C}_g$ has the form

$$\mathfrak{C}_g = 1 + \prod_{\ell} E_\ell$$

where each E_ℓ is the average value of a character χ_ℓ over an explicit set. One crucial fact used to arrive at this form is that when $D \equiv 1 \pmod 4$, then for n divisible by $2D$ we have that the subgroup

$$\mathrm{Gal}(F_n/\mathbb{Q}) \hookrightarrow \prod_{\ell \mid n} \mathrm{Gal}(F_\ell/\mathbb{Q})$$

is cut out by a quadratic character χ measuring the nature of the entanglement. The structure of C_g as an Euler product and the description of $\mathfrak{C}_g$ naturally lead to non-vanishing criteria.

In this chapter we attempt to generalize this method to the setting of elliptic curves. There are many problems concerning the study of the set of primes p such that the reduced curve $\tilde{E}(\mathbb{F}_p)$ satisfies a certain condition. One of these arises as a natural analogue of Artin's conjecture on

primitive roots. Namely, given an elliptic curve E over $\mathbb{Q}$, the problem is to determine the density of primes p such that $\tilde{E}(\mathbb{F}_p)$ is cyclic. The first thing to note is that the condition of $\tilde{E}(\mathbb{F}_p)$ being cyclic is completely determined by the splitting behaviour of p in the various torsion fields $\mathbb{Q}(E[\ell])$ for different ℓ. Given this, we can proceed similarly by defining local densities δ_ℓ and attempting to find the entanglement correction factor $\mathfrak{C}_E$, however one quickly runs into various difficulties which were not present in the case of classical Artin. One of these is that it is not necessarily true that $\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}) \hookrightarrow \prod_{\ell|m} \mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q})$ is a normal subgroup and even if so, the quotient need not be $\{\pm 1\}$ or even abelian for that matter.

This leads us to the study in Section 2.2 of so called *abelian entanglements*. If G is a subgroup of $G_1 \times \cdots \times G_n$ such that the projection maps $\pi_i : G \to G_i$ are surjective for $1 \leqslant i \leqslant n$, then we give a necessary and sufficient condition for G being normal in $G_1 \times \cdots \times G_n$ with abelian quotient.

In Section 2.3 we define elliptic curves with abelian entanglements to be those elliptic curves with the property that $G(m_E)$ has abelian entanglements in the sense of Section 2.2. We show that this definition is equivalent to $\mathbb{Q}(E[m_1]) \cap \mathbb{Q}(E[m_2])$ being an abelian extension of $\mathbb{Q}$ for every coprime m_1, m_2. It is for this class of curves that we will be able to apply our character sum method, with Theorem 2.3.4 being a crucial ingredient.

Section 2.4 applies Theorem 2.3.4 to the aforementioned problem of cyclic reduction of elliptic curves. We explicitly evaluate the density C_E as an Euler product $\prod_\ell \delta_\ell$ times an entanglement correction factor $\mathfrak{C}_E$. We then compute $\mathfrak{C}_E$ in the case of Serre curves and give examples of a few other elliptic curves with more complicated Galois Theory, as well as establishing non-vanishing criteria for these conjectural densities.

In Section 2.5 we study a variant of the problem of cyclic reduction on elliptic curves. Namely, we impose the additional condition that p lie in a prescribed congruence class modulo some integer f. This introduces new difficulties as the splitting conditions on p become more complicated, but it

also illustrates the way in which our method can be used to handle a variety of different scenarios. In the end the computation of $\mathfrak{C}_E$ is again reduced to fairly mechanical local computations. Again Serre curves and several other examples are treated in detail.

Section 2.6 we study a different type of problem. We look at a classical conjecture of Koblitz on the asymptotic behaviour of the number of primes p for which the cardinality of $\tilde{E}(\mathbb{F}_p)$ is prime. We see that the character sum approach can also be applied to describe the constant appearing in this asymptotic. In this case there are not even conditional results, and the constant computed is purely conjectural. However the constant we compute has previously been described via different methods by Zywina in [Zyw11c], where he provides some convincing numerical evidence for it.

The study of conjectural constants led us to investigate the class of elliptic curves with abelian entanglements, and naturally leads to the question of whether there exist elliptic curves with non-abelian entanglements. To be precise, can one classify the triples (E, m_1, m_2) with E an elliptic curve over $\mathbb{Q}$ and m_1, m_2 a pair of coprime integers for which the entanglement field $\mathbb{Q}(E[m_1]) \cap \mathbb{Q}(E[m_2])$ is non-abelian over $\mathbb{Q}$? In Chapter 3 we exhibit an infinite family of elliptic curves for which this is the case, and in doing so we obtain a complete set of modular curves which parametrize non-Serre curves.

2.2 Abelian entanglements

In this section we study the following question: if G is a subgroup of $G_1 \times \cdots \times G_n$ such that the projection maps $\pi_i : G \to G_i$ are surjective for $1 \leqslant i \leqslant n$, when does it happen that G is normal in $G_1 \times \cdots \times G_n$ with abelian quotient?

For a group G, we will denote by G' the commutator subgroup of G, and for $x, y \in G$, $[x, y] = x^{-1}y^{-1}xy$ will denote the commutator of x and y. For

a non-empty subset $S \subset \{1, \ldots, n\}$ we write π_S for the projection map

$$\pi_S : G_1 \times \cdots \times G_n \longrightarrow \prod_{i \in S} G_i$$

and let G_S denote the image of G under this projection map. Note that for each partition $\sqcup_j T_j = \{1, \ldots, n\}$ we have a canonical inclusion

$$G \hookrightarrow \prod_j G_{T_j}.$$

Let $\mathcal{P} := \{S, T\}$ be a partition of $\{1, \ldots, n\}$, so that $S \sqcup T = \{1, \ldots, n\}$. Then G is a subdirect product of $G_S \times G_T$ so by Goursat's lemma there is a group $Q_\mathcal{P}$ and a pair of homomorphisms $\psi_\mathcal{P} := (\psi_\mathcal{P}^{(1)}, \psi_\mathcal{P}^{(2)})$ with

$$\psi_\mathcal{P}^{(1)} : G_S \longrightarrow Q_\mathcal{P}$$
$$\psi_\mathcal{P}^{(2)} : G_T \longrightarrow Q_\mathcal{P}$$

such that $G = G_S \times_{\psi_\mathcal{P}} G_T$. We say that G has *abelian entanglements with respect to* $G_1 \times \cdots \times G_n$ if $Q_\mathcal{P}$ is abelian for each two-set partition $\mathcal{P}$ of $\{1, \ldots, n\}$. We will often write only that G has abelian entanglements, omitting with respect to which direct product of groups if this is clear from the context. The following proposition is the main result of this section and provides an answer to the question posed at the start.

Proposition 2.2.1. *Keeping the notation as above, G is a normal subgroup of $G_1 \times \cdots \times G_n$ if and only if G has abelian entanglements.*

The proof will use the following proposition, which is the case $n = 2$.

Proposition 2.2.2. *Let G be a subgroup of $G_1 \times G_2$ such that the projection maps $\pi_1 : G \to G_1$ and $\pi_2 : G \to G_2$ are surjective. Then $G \trianglelefteq G_1 \times G_2$ if and only if G has abelian entanglements.*

Proof. Suppose first that G has abelian entanglements, and let $x := (x_1, x_2) \in G$. We will show that for any $a \in G_1 \times \{1\}$ one has $axa^{-1} \in G$, and similarly for every $b \in \{1\} \times G_2$. The result will then follow. So take $a := (a_1, 1) \in G_1 \times \{1\}$. Let N_1 and N_2 be the corresponding Goursat subgroups associated to G, that is, $N_1 = (G_1 \times \{1\}) \cap G$ and $N_2 = (\{1\} \times G_2) \cap G$. Then because G has abelian entanglements we have that $(G_1 \times \{1\})/N_1$ is abelian, or equivalently $(G_1 \times \{1\})' \leqslant N_1$. It follows that $[(a_1, 1), (x_1, 1)] \in G$, however

$$\begin{aligned}[(a_1, 1), (x_1, 1)] &= (a_1, 1)(x_1, 1)(a_1, 1)^{-1}(x_1, 1)^{-1} \\ &= (a_1, 1)(x_1, x_2)(a_1, 1)^{-1}(x_1, x_2)^{-1}\end{aligned}$$

and $(x_1, x_2)^{-1}$ is in G, hence $(a_1, 1)(x_1, x_2)(a_1, 1)^{-1}$ is also in G, as claimed. Similarly one can show $(1, b_2)(x_1, x_2)(1, b_2)^{-1} \in G$ for any $b_2 \in G_2$, and we conclude G is normal in $G_1 \times G_2$.

For the converse, suppose that $G \trianglelefteq G_1 \times G_2$. We will show that $(G_1 \times \{1\})' \leqslant N_1$, from which it follows that G has abelian entanglements. Let $(x_1, 1)$ and $(y_1, 1)$ be arbitrary elements of $G_1 \times \{1\}$. Because $\pi_1 : G \to G_1$ is surjective, there exists $z \in G_2$ such that $(y_1, z) \in G$. As $G \trianglelefteq G_1 \times G_2$, we have $(x_1, 1)(y_1, z)(x_1, 1)^{-1}$ is in G and hence so is $[(x_1, 1), (y_1, z)]$. Using the fact that $[(x_1, 1), (y_1, 1)] = [(x_1, 1), (y_1, z)]$, we obtain $[(x_1, 1), (y_1, 1)] \in G$. However $[(x_1, 1), (y_1, 1)] = ([x_1, y_1], 1) \in G_1 \times \{1\}$, hence the result. □

Proof of Proposition 2.2.1. Again we suppose first that G has abelian entanglements, and we proceed similarly as in the case $n = 2$. Let $x := (x_1, \ldots, x_n) \in G$, and for $j \in \{1, \ldots, n\}$ let $a := (1, \ldots, 1, a_j, 1, \ldots, 1) \in \{1\} \times \cdots \times \{1\} \times G_j \times \{1\} \times \cdots \times \{1\}$ where the a_j is in the j-th position. Let $S_j := \{1, \ldots, n\} \backslash \{j\}$. Then $G \leqslant G_j \times G_{S_j}$ with surjective projection maps and the corresponding quotient $(G_j \times \{1\})/N_j$ is abelian. By Proposition 2.2.2, G is a normal subgroup of $G_j \times G_{S_j}$. But a is certainly an element of $G_j \times G_{S_j}$, hence $axa^{-1} \in G$. Since j was chosen arbitrarily we conclude

$G \trianglelefteq G_1 \times \cdots \times G_n$.

Conversely, suppose $G \trianglelefteq G_1 \times \cdots \times G_n$, and let $\mathcal{P} := \{S, T\}$ be a partition of $\{1, \ldots, n\}$. Then note that $G_S \times G_T$ may be viewed as a subgroup of $G_1 \times \cdots \times G_n$ and so $G \trianglelefteq G_S \times G_T$. By Proposition 2.2.2 the corresponding Goursat quotient $Q_{\mathcal{P}}$ is abelian, hence G has abelian entanglements. This completes the proof. □

In the proof we used the subset $S_j := \{1, \ldots n\} \backslash \{j\} \subset \{1, \ldots, n\}$. Here we have that G is a subdirect product of $G_j \times G_{S_j}$, so by Goursat's lemma there is a group Q_j and a pair of homomorphisms $\psi_j := (\psi_j^{(1)}, \psi_j^{(2)})$ such that $G = G_j \times_{\psi_j} G_{S_j}$. The following corollary tells us that these are all the partitions we need to consider in order to determine whether or not G has abelian entanglements.

Corollary 2.2.3. *With the notation above, G has abelian entanglements if and only if Q_j is abelian for every $j \in \{1, \ldots, n\}$.*

Proof. One implication is trivial. Suppose that Q_j is abelian for every $j \in \{1, \ldots, n\}$. Then by the proof of Proposition 2.2.1, G is a normal subgroup of $G_1 \times \cdots \times G_n$, and again using Proposition 2.2.1, G has abelian entanglements, as claimed. □

Proposition 2.2.4. *Suppose that G is a normal subgroup of $G_1 \times \cdots \times G_n$ such that the projection maps $\pi_i : G \to G_i$ are surjective for all i. Then the quotient $(G_1 \times \cdots \times G_n)/G$ is abelian.*

Proof. We will proceed by showing that $(G_1 \times \cdots \times G_n)' \leqslant G$. Let $x := (x_1, \ldots x_n) \in (G_1 \times \cdots \times G_n)'$. By Proposition 2.2.1 G has abelian entanglements, so for each j, to the inclusion $G \hookrightarrow G_j \times G_{S_j}$ there corresponds an abelian quotient $G_j/\pi_j(N_j)$, where $N_j = (G_j \times \{1\}) \cap G$. The composition

$$G_1 \times \cdots \times G_n \xrightarrow{\pi_j} G_j \longrightarrow G_j/\pi_j(N_j)$$

gives an abelian quotient of $G_1 \times \cdots \times G_n$, hence $x_j = \pi_j(x_1, \ldots, x_n)$ is contained in $\pi_j(N_j)$. It follows that $(1, \ldots, 1, x_j, 1 \ldots, 1) \in G$. As j was arbitrary, and $\prod_j (1, \ldots, 1, x_j, 1 \ldots, 1) = x$, we conclude $x \in G$. □

Proposition 2.2.5. *Suppose G has abelian entanglements with respect to $G_1 \times \cdots \times G_n$ and let $S \subseteq \{1, \ldots, n\}$. Then G_S has abelian entanglements with respect to $\prod_{i \in S} G_i$.*

Proof. We will show that G_S is normal in $\prod_{i \in S} G_i$. Note that

$$G \leqslant \pi_S^{-1}(G_S) \leqslant G_1 \times \cdots \times G_n$$

and by Proposition 2.2.4 the quotient $(G_1 \times \cdots \times G_n)/G$ is abelian. It follows then that $\pi_S^{-1}(G_S)$ is normal in $G_1 \times \cdots \times G_n$, and denote the quotient by Φ_S. Now $\ker \pi_S \subset \pi_S^{-1}(G_S)$ so the map $G_1 \times \cdots \times G_n \to \Phi_S$ factors via $\prod_{i \in S} G_i$. Let ψ_S be such that the following diagram commutes

$$\begin{array}{ccc} G_1 \times \cdots \times G_n & & \\ \downarrow{\scriptstyle \pi_S} & \searrow & \\ \prod_{i \in S} G_i & \xrightarrow{\psi_S} & \Phi_S \end{array} .$$

It is easy to see that the kernel of ψ_S is precisely G_S, hence G_S is normal in $\prod_{i \in S} G_i$ and by Proposition 2.2.1 G_S has abelian entanglements with respect to $\prod_{i \in S} G_i$, as claimed. □

2.3 Elliptic curves with abelian entanglements

We consider here a family of elliptic curves with the property that the intersections of the different torsion fields of each curve in this family are abelian extensions.

We say that an elliptic curve E has *abelian entanglements* if the corresponding group $G(m_E) \leqslant G(\ell_1^{\alpha_1}) \times \cdots \times G(\ell_n^{\alpha_n})$ has abelian entanglements in the sense of section 2.2, where m_E as usual denotes the smallest split and stable integer for E, and has prime factorisation $m_E = \ell_1^{\alpha_1} \dots \ell_n^{\alpha_n}$.

Lemma 2.3.1. *The following two conditions are equivalent:*

(i) *E has abelian entanglements.*

(ii) *For each $m_1, m_2 \in \mathbb{N}$ which are relatively prime, the intersection*

$$\mathbb{Q}([m_1]) \cap \mathbb{Q}([m_2])$$

is an abelian extension of $\mathbb{Q}$.

Proof. Suppose E has abelian entanglements, and let m_1, m_2 be relatively prime. If m_1 and m_2 both divide m_E, then by Proposition 2.2.5 $G(m_1 m_2)$ has abelian entanglements with respect to $G(m_1) \times G(m_2)$. This implies the Goursat quotient $Q_{m_1 m_2}$ is abelian, and by Lemma 1.2.8 $\mathbb{Q}([m_1]) \cap \mathbb{Q}([m_2])$ is an abelian extension of $\mathbb{Q}$. For general m_1, m_2, let

$$m_1' = (m_1, m_E), \quad m_2' = (m_2, m_E).$$

Then m_1' and m_2' are relatively prime integers dividing m_E so be the same argument $\mathbb{Q}([m_1']) \cap \mathbb{Q}([m_2'])$ is an abelian extension of $\mathbb{Q}$. From Serre's open image Theorem if n is any integer and d is coprime to nm_E then

$$G(nd) = G(n) \times \mathrm{GL}_2(\mathbb{Z}/d\mathbb{Z}).$$

It follows that $Q_{m_1 m_2}$ is isomorphic to $Q_{m_1' m_2'}$, hence the claim. □

Corollary 2.3.2. *If E has abelian entanglements, then for any $m := \prod_i q_i^{s_i}$ we have that $G(m) \leqslant \prod_i G(q_i^{s_i})$ has abelian entanglements.*

Proof. This follows immediately from Corollary 2.2.3 and Lemma 2.3.1. □

Assume now that E is an elliptic curve over $\mathbb{Q}$ with abelian entanglements, and let m be a positive integer with prime factorisation $m = \prod_\ell \ell^{\alpha_\ell}$. Since E has abelian entanglements, by Corollary 2.3.2 and Proposition 2.2.4 there are a map ψ_m and a finite abelian group Φ_m that fit into the exact sequence

$$1 \longrightarrow G(m) \longrightarrow \prod_{\ell|m} G(\ell^{\alpha_\ell}) \xrightarrow{\psi_m} \Phi_m \longrightarrow 1. \tag{2.3.1}$$

Note that the group Φ_m measures the extent to which there are entanglements between the various ℓ^{α_ℓ}-torsion fields. For instance Φ_m is trivial if and only if for any two coprime integers m_1, m_2 dividing m one has $\mathbb{Q}(E[m_1]) \cap \mathbb{Q}(E[m_2]) = \mathbb{Q}$. The following lemma tells us that Φ_{m_E} measures the full extent to which the distinct torsion fields of E have any entanglements.

Lemma 2.3.3. *Let m be a positive integer and d be a positive integer coprime to m_E. Then $\Phi_{md} \simeq \Phi_m$.*

Proof. Again there is a map ψ_{md} and an abelian group Φ_{md} which fit into the short exact sequence

$$1 \longrightarrow G(md) \longrightarrow \prod_{\ell^{\alpha_\ell}||md} G(\ell^{\alpha_\ell}) \xrightarrow{\psi_{md}} \Phi_{md} \longrightarrow 1.$$

As d is coprime to m_E, by Serre's open image Theorem we have that

$$G(md) = G(m) \times \prod_{\ell^{\alpha_\ell}||d} G(\ell^{\alpha_\ell}) \tag{2.3.2}$$

It follows that $G(\ell^{\alpha_\ell})$ is contained in the kernel of ψ_{md} for any $\ell \mid d$, hence $\Phi_{md} \simeq \Phi_m$. □

For each prime $\ell \mid m$, let $S(\ell)$ be a subset of $G(\ell^{\alpha_\ell})$, and define

$$\mathcal{S}_m := \prod_{\ell|m} S(\ell), \quad \mathcal{G}_m := \prod_{\ell|m} G(\ell^{\alpha_\ell}).$$

so that $\mathcal{S}_m \subset \mathcal{G}_m$. The following theorem allows us to compute the fraction of elements in $G(m)$ that belong to $\prod_{\ell|m} S(\ell)$. It will play a key role in the method we will develop for computing entanglement correction factors as character sums. If A is an abelian group, then $\widehat{A}$ denotes the group of characters $\chi : A \to \mathbb{C}^\times$.

Theorem 2.3.4. *Assume $E/\mathbb{Q}$ has abelian entanglements, and let Φ_m be as in (2.3.1). For each $\tilde{\chi} \in \widehat{\Phi}_m$ a character of Φ_m, let χ be the character of $\mathcal{G}_m$ obtained by composing $\tilde{\chi}$ with ψ_m, and let χ_ℓ the restriction of χ to the component $G(\ell^{\alpha_\ell})$. Then*

$$\frac{|\mathcal{S}_m \cap G(m)|}{|G(m)|} = \left(1 + \sum_{\tilde{\chi} \in \widehat{\Phi}_m - \{1\}} \prod_{\ell|m} E_{\chi,\ell}\right) \frac{|\mathcal{S}_m|}{|\mathcal{G}_m|},$$

where

$$E_{\chi,\ell} = \sum_{x \in S(\ell)} \frac{\chi_\ell(x)}{|S(\ell)|}.$$

Proof. Let $\mathbb{1}_{\mathcal{S}_m}$ be the indicator function of $\mathcal{S}_m$ in $\mathcal{G}_m$, and $\mathbb{1}_{G(m)}$ that of $G(m)$. Also, to simplify notation we will use Φ in place of Φ_m. Then we have that

$$\frac{|\mathcal{S}_m \cap G(m)|}{|G(m)|} = \frac{1}{|G(m)|} \sum_{x \in \mathcal{G}_m} \mathbb{1}_{\mathcal{S}_m}(x) \mathbb{1}_{G(m)}(x).$$

By the orthogonality relations of characters (see for instance §VI.1 of [Ser73]) we have that if $x \in \mathcal{G}_m$, then

$$\sum_{\tilde{\chi} \in \widehat{\Phi}} \chi(x) = \begin{cases} [\mathcal{G}_m : G(m)] & \text{if } x \in G(m) \\ 0 & \text{if } x \notin G(m). \end{cases}$$

This implies that

$$\mathbb{1}_{G(m)} = \frac{1}{[\mathcal{G}_m : G(m)]} \sum_{\tilde{\chi} \in \widehat{\Phi}} \chi,$$

so it follows that

$$\begin{aligned}
\frac{|\mathcal{S}_m \cap G(m)|}{|G(m)|} &= \frac{1}{|\mathcal{G}_m|} \Big(\sum_{x \in \mathcal{G}_m} \mathbb{1}_{\mathcal{S}_m}(x) + \sum_{x \in \mathcal{G}_m} \sum_{\tilde{\chi} \in \widehat{\Phi} \setminus \{1\}} \mathbb{1}_{\mathcal{S}_m}(x) \chi(x) \Big) \\
&= \frac{|\mathcal{S}_m|}{|\mathcal{G}_m|} \Big(1 + \sum_{x \in \mathcal{G}_m} \sum_{\tilde{\chi} \in \widehat{\Phi} \setminus \{1\}} \frac{\mathbb{1}_{\mathcal{S}_m}(x) \chi(x)}{|\mathcal{S}_m|} \Big) \\
&= \frac{|\mathcal{S}_m|}{|\mathcal{G}_m|} \Bigg(1 + \sum_{\tilde{\chi} \in \widehat{\Phi} \setminus \{1\}} \Big(\prod_{\ell \mid m} \sum_{x \in G(\ell)} \frac{\mathbb{1}_{S(\ell)}(x) \chi_\ell(x)}{|S(\ell)|} \Big) \Bigg) \\
&= \frac{|\mathcal{S}_m|}{|\mathcal{G}_m|} \Bigg(1 + \sum_{\tilde{\chi} \in \widehat{\Phi} \setminus \{1\}} \Big(\prod_{\ell \mid m} \sum_{x \in S(\ell)} \frac{\chi_\ell(x)}{|S(\ell)|} \Big) \Bigg)
\end{aligned}$$

where the third equality follows from the fact that $\mathbb{1}_{\mathcal{S}_m}$ and χ are products of functions $\mathbb{1}_{S(\ell)}$ and χ_ℓ defined on the components $G(\ell^{\alpha_\ell})$. The result now follows from letting $E_{\chi,\ell}$ be the average value of χ_ℓ on $S(\ell)$, that is

$$E_{\chi,\ell} = \sum_{x \in S(\ell)} \frac{\chi_\ell(x)}{|S(\ell)|}.$$

□

2.4 Cyclic reduction of elliptic curves

In this section we consider an elliptic curve analogue of Artin's classical conjecture on primitive roots. Recall that this conjecture predicts the density of primes p such that a given rational number is a primitive root modulo p. In [LT77], Lang and Trotter formulated an analogous conjecture for elliptic curves over $\mathbb{Q}$. Namely, if P is a point of $E(\mathbb{Q})$ of infinite order, then the

problem is to determine the density of primes p for which $\tilde{E}(\mathbb{F}_p)$ is generated by $\tilde{P}$, the reduction of P modulo p.

Note that for there to exist even one prime p of good reduction with this property, a necessary condition is that the group $\tilde{E}(\mathbb{F}_p)$ be cyclic, and that is the question we consider here. In [Ser86], Serre showed assuming the Generalized Riemann Hypothesis that the set of primes p such that $\tilde{E}(\mathbb{F}_p)$ is cyclic has a density. He did this by adapting Hooley's argument of conditionally proving Artin's conjecture on primitive roots. Namely, we have the following:

Theorem 2.4.1 (Serre, 1976)**.** *Let E be an elliptic curve defined over $\mathbb{Q}$ with conductor N_E. Assuming GRH we have that*

$$|\{p \leqslant x \text{ prime} : p \nmid N_E,\ \tilde{E}(\mathbb{F}_p) \text{ is cyclic}\}| \sim C_E \frac{x}{\log x}$$

as $x \to \infty$, where $C_E := \sum_{n \geqslant 1} \frac{\mu(n)}{[\mathbb{Q}(E[n]) : \mathbb{Q}]}$.

We explicitly evaluate this density C_E as an Euler product. Note that the condition of $\tilde{E}(\mathbb{F}_p)$ being cyclic is completely determined by $\rho_E(G_{\mathbb{Q}})$. Indeed, $\tilde{E}(\mathbb{F}_p)$ is cyclic if and only if p does not split completely in the field $\mathbb{Q}(E[\ell])$ for any $\ell \neq p$. Note that this condition is automatically satisfied when $\ell > p$, since p splitting completely in $\mathbb{Q}(E[\ell])$ implies $p \equiv 1 \pmod{\ell}$. In other words, if for each prime ℓ we define the set $S(\ell) := G(\ell) - \{1\}$, then for all $p \nmid N_E$ the group $\tilde{E}(\mathbb{F}_p)$ is cyclic if and only if $\rho_\ell(\mathrm{Frob}_p) \in S(\ell)$ for any $\ell < p$, i.e. if p does not split completely in $\mathbb{Q}(E[\ell])$.

By the Chebotarev density theorem, the set of primes p that do not split completely in $\mathbb{Q}(E[\ell])$ has density equal to

$$\delta_\ell := \frac{|S(\ell)|}{|G(\ell)|} = 1 - \frac{1}{[\mathbb{Q}(E[\ell]) : \mathbb{Q}]}.$$

If we assume that the various splitting conditions at each prime ℓ are in-

dependent, then it is reasonable to expect that the density of primes p for which $\tilde{E}(\mathbb{F}_p)$ is cyclic is equal to $\prod_\ell \delta_\ell$. However as we know, this assumption of independence is not correct, as different torsion fields may have non-trivial intersection. To be precise, for each square-free integer d let

$$\mathcal{S}_d := \prod_{\ell \mid d} S(\ell), \quad \mathcal{G}_d := \prod_{\ell \mid d} G(\ell).$$

By Chebotarev, the density of primes p such that $p \nmid N_E$ and $\rho_\ell(\mathrm{Frob}_p) \in S(\ell)$ for all $\ell \mid d$ and $\ell \neq p$ is equal to $|\mathcal{S}_d \cap G(d)|/|G(d)|$. If we let d increase to infinity ranging over square-free integers, then Serre's above result implies that, assuming GRH,

$$C_E = \lim_{d \to \infty} \frac{|\mathcal{S}_d \cap G(d)|}{|G(d)|} \tag{2.4.1}$$

where the limit will be seen to exist.

Now let $m = \prod_{\ell \mid m_E} \ell$ be the square-free part of m_E, and let d be a square-free integer coprime to m. By (2.3.2) we have

$$\frac{|\mathcal{S}_{md} \cap G(md)|}{|G(md)|} = \frac{|\mathcal{S}_m \cap G(m)|}{|G(m)|} \prod_{\ell \mid d} \frac{|S(\ell)|}{|G(\ell)|}.$$

For ℓ coprime to m_E, we have that $|S(\ell)|/|G(\ell)|$ is $1 + \mathcal{O}(1/\ell^4)$ so the limit in (2.4.1) does indeed exist. Letting d tend to infinity over the square-free numbers then gives

$$C_E = \frac{|\mathcal{S}_m \cap G(m)|}{|G(m)|} \prod_{\ell \nmid m} \frac{|S(\ell)|}{|G(\ell)|}.$$

The above discussion implies that if we do take into account entanglements,

then assuming GRH we have

$$C_E = \mathfrak{C}_E \prod_\ell \delta_\ell \tag{2.4.2}$$

where $\mathfrak{C}_E$ is an *entanglement correction factor*, and explicitly evaluating such densities amounts to computing the correction factors $\mathfrak{C}_E$. The entanglement correction factor $\mathfrak{C}_E$ arises as the factor by which C_E differs from the uncorrected value $\lim_{d\to\infty} |\mathcal{S}_d|/|\mathcal{G}_d| = \prod_\ell \delta_\ell$. We will use Theorem 2.3.4 for evaluating $\mathfrak{C}_E$ as a character sum for elliptic curves with abelian entanglements.

Theorem 2.4.2. *Assume $E/\mathbb{Q}$ has abelian entanglements, and let Φ_m be as in (2.3.1). Let $\tilde{\chi} \in \widehat{\Phi}_m$ be a character of Φ_m and let χ be the character of $\mathcal{G}_m$ obtained by composing $\tilde{\chi}$ with ψ_m. Define $E_{\chi,\ell}$ by*

$$E_{\chi,\ell} = \begin{cases} 1 & \text{if } \chi \text{ is trivial on } G(\ell), \\ \frac{-1}{[\mathbb{Q}(E[\ell]):\mathbb{Q}]-1} & \text{otherwise.} \end{cases}$$

Then

$$C_E = \mathfrak{C}_E \prod_\ell \delta_\ell$$

where the entanglement correction factor $\mathfrak{C}_E$ is given by

$$\mathfrak{C}_E = 1 + \sum_{\tilde{\chi} \in \widehat{\Phi} - \{1\}} \prod_{\ell | m} E_{\chi,\ell}.$$

Proof. By Theorem 2.3.4 we have that

$$\frac{|\mathcal{S}_m \cap G(m)|}{|G(m)|} = \frac{|\mathcal{S}_m|}{|\mathcal{G}_m|} \left(1 + \sum_{\tilde{\chi} \in \widehat{\Phi} \setminus \{1\}} \prod_{\ell | m} E_{\chi,\ell} \right),$$

where $E_{\tilde{\chi},\ell}$ is the average value of χ_ℓ on $S(\ell)$. By (2.4.2), we know that

$$\begin{aligned}\mathfrak{C}_E &= \frac{C_E}{\prod_\ell \delta_\ell} \\ &= \frac{|\mathcal{S}_m \cap G(m)|/|G(m)|}{|\mathcal{S}_m|/|\mathcal{G}_m|}.\end{aligned}$$

Finally, notice that if χ is non-trivial on $G(\ell)$ then χ_ℓ is non-trivial, hence

$$\sum_{x \in S(\ell)} \chi_\ell(x) = \Big(\sum_{x \in G(\ell)} \chi_\ell(x) \Big) - \chi_\ell(1) = -1.$$

This completes the proof. □

Remark 2.4.3. Note that in the above theorem we may replace m by any square-free multiple of it. Indeed, for any $\tilde{\chi}$, it follows from Lemma 2.3.3 that $E_{\chi,\ell} = 1$ for any $\ell \nmid m$, hence the product $\prod_{\ell|m} E_{\chi,\ell}$ does not change, and the quotient of $|\mathcal{S}_{md} \cap G(md)|/|G(md)|$ and $|\mathcal{S}_{md}|/|\mathcal{G}_{md}|$ is constant as d tends to infinity.

In what follows we will use Theorem 2.4.2 to compute $\mathfrak{C}_E$ for various elliptic curves over $\mathbb{Q}$.

2.4.1 Serre curves

Consider the representation $\rho_E : G_\mathbb{Q} \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$ given by the action of $G_\mathbb{Q}$ on $E(\overline{\mathbb{Q}})_{\mathrm{tors}}$. Serre has shown in [Ser72] that the image of ρ_E is always contained in a specific index 2 subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ and thus ρ_E is *never* surjective. Following Lang and Trotter, we define an elliptic curve E over $\mathbb{Q}$ to be a Serre curve if $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : G] = 2$.

It follows from the result of Serre that Serre curves are elliptic curves over $\mathbb{Q}$ whose Galois action on their torsion points is as large as possible. Jones has shown in [Jon10] that "most" elliptic curves over $\mathbb{Q}$ are Serre curves (see Section 3.1 for the more precise statement) . Thus they are prevalent over

$\mathbb{Q}$ and we also have complete understanding of their Galois theory, and this makes their entanglement factors particularly easy to handle in conjunction with Theorem 2.4.2.

First we briefly describe the index 2 subgroup H_E of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ (see [Ser72], page 311 for more details). To this end let $\chi_\Delta : G_\mathbb{Q} \to \{\pm 1\}$ be the character associated to $K := \mathbb{Q}(\sqrt{\Delta})$, where Δ is the discriminant of any Weierstrass model of E over $\mathbb{Q}$, and note that χ_Δ does not depend on the choice of model. Let

$$\varepsilon : \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \longrightarrow \{\pm 1\}$$

be the signature map under any isomorphism $GL_2(\mathbb{Z}/2\mathbb{Z}) \simeq S_3$. Then as $K \subset \mathbb{Q}(E[2])$, one can check that $\chi_\Delta = \varepsilon \circ \rho_{E,2}$.

Note that $K \subset \mathbb{Q}(\zeta_{|D|})$, where D is the discriminant of $\mathbb{Q}(\sqrt{\Delta})$. Then there exists a unique quadratic character $\alpha : (\mathbb{Z}/|D|\mathbb{Z})^\times \to \{\pm 1\}$ such that $\chi_\Delta = \alpha \circ \det \rho_{E,|D|}$. From this it follows that $\varepsilon \circ \rho_{E,2} = \alpha \circ \rho_{E,|D|}$. If we then define $M_E = \mathrm{lcm}(|D|, 2)$ and

$$H_{M_E} := \{A \in \mathrm{GL}_2(\mathbb{Z}/M_E\mathbb{Z}) \ : \ \varepsilon(A \bmod 2) = \alpha(\det(A \bmod |D|))\},$$

then it follows from the above discussion that H_{M_E} contains $G(M_E)$. If we let H_E be the inverse image of H_{M_E} in $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ under the reduction map, then H_E is clearly an index 2 subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ which contains G. We have then that G is a Serre curve if and only if $\rho_E(G_\mathbb{Q}) = H_E$. It follows from the above discussion that all Serre curves have abelian entanglements.

Proposition 2.4.4. *Let $E/\mathbb{Q}$ be a Serre curve. Let D be the discriminant of $\mathbb{Q}(\sqrt{\Delta})$ where Δ is the discriminant of any Weierstrass model of E over $\mathbb{Q}$. Then*

$$C_E = \mathfrak{C}_E \prod_\ell \left(1 - \frac{1}{(\ell^2 - 1)(\ell^2 - \ell)}\right)$$

where the entanglement correction factor $\mathfrak{C}_E$ *is given by*

$$\mathfrak{C}_E = \begin{cases} 1 & \text{if } D \equiv 0 \pmod 4 \\ 1 + \prod_{\ell \mid 2D} \frac{-1}{(\ell^2-1)(\ell^2-\ell)-1} & \text{if } D \equiv 1 \pmod 4 \end{cases}$$

Proof. Since E is a Serre curve, we have that $G(\ell) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ holds for all ℓ, hence $[\mathbb{Q}(E[\ell]) : \mathbb{Q}] = (\ell^2-1)(\ell^2-\ell)$.

Now suppose first that $D \equiv 0 \pmod 4$. Then $m_E = |D|$ is divisible by 4, hence we have that

$$G(m) = \prod_{\ell \mid m} G(\ell)$$

for all square-free m. It follows that $\Phi_m \simeq \{1\}$ hence its character group is trivial and $\mathfrak{C}_E = 1$.

Now suppose $D \equiv 1 \pmod 4$. In this case $m_E = 2|D|$ is square-free, hence $G(m_E)$ is an index 2 subgroup of $\prod_{\ell \mid m_E} G(\ell)$ and $\Phi \simeq \{\pm 1\}$. For each $\ell > 2$ dividing m_E, χ_ℓ is the character given by the composition $G(\ell) \xrightarrow{\det} (\mathbb{Z}/\ell\mathbb{Z})^* \to \{\pm 1\}$, that is $\chi_\ell = \left(\frac{\det}{\ell}\right)$, and $\chi_2 := \varepsilon$ is the signature map under an isomorphism $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \simeq S_3$. If we let $\chi := \prod_{\ell \mid m_E} \chi_\ell$ then we have an exact sequence

$$1 \longrightarrow G(m_E) \longrightarrow \prod_{\ell \mid m_E} G(\ell) \xrightarrow{\chi} \{\pm 1\} \longrightarrow 1.$$

Clearly each χ_ℓ is non-trivial on $G(\ell)$ for each ℓ dividing m_E so the result follows from Theorem 2.4.2 and using that $\Phi_{m_E} \simeq \{\pm 1\}$. □

2.4.2 Example: $Y^2 + Y = X^3 - X^2 - 10X - 20$

We now consider the elliptic curve over $\mathbb{Q}$ defined by the Weierstrass equation $Y^2 + Y = X^3 - X^2 - 10X - 20$. The Galois theory for this elliptic curve has been worked out by Lang and Trotter in [LT74], and in particular they have

shown that $m_E = 2 \cdot 5^2 \cdot 11$, and that the following properties hold:

- $G(2) = \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$.
- E has a rational 5-torsion point, and $\mathbb{Q}(E[5]) = \mathbb{Q}(\zeta_5)$.
- $[\mathbb{Q}(E[5^2]) : \mathbb{Q}(E[5])] = 5^4$, hence 5 is stable.
- $\mathbb{Q}(E[5^2]) \cap \mathbb{Q}(E[11]) = \mathbb{Q}(\zeta_{11})^+$, where $\mathbb{Q}(\zeta_{11})^+$ is the real quadratic subfield of $\mathbb{Q}(\zeta_{11})$. This implies there is a map

  $$\phi_5 : G(5^2) \longrightarrow (\mathbb{Z}/11\mathbb{Z})^\times/\{\pm 1\}.$$

  We make this map explicit. There is a basis for $E[5^2]$ over $\mathbb{Z}/25\mathbb{Z}$ under which we have

  $$G(5^2) = \left\{ \begin{pmatrix} 1+5a & 5b \\ 5c & u \end{pmatrix} : a, b, c, d \in \mathbb{Z}/25\mathbb{Z},\ u \in (\mathbb{Z}/25\mathbb{Z})^\times \right\}.$$

  Define the (surjective) homomorphism

  $$\begin{aligned} \psi : G(5^2) &\longrightarrow \mathbb{Z}/5\mathbb{Z} \\ \begin{pmatrix} 1+5a & 5b \\ 5c & u \end{pmatrix} &\longmapsto a \mod 5. \end{aligned}$$

  Then ϕ_5 is given by

  $$A \longmapsto (\pm 2)^{\psi(A)},$$

  where we note that ± 2 is a generator of $(\mathbb{Z}/11\mathbb{Z})^\times/\{\pm 1\}$.
- $\mathbb{Q}(E[2]) \cap \mathbb{Q}(E[11]) = \mathbb{Q}(\sqrt{-11})$.

From this we conclude that E has abelian entanglements and

$$G(2\cdot 5^2\cdot 11) = \Big\{(g_2, g_{25}, g_{11}) \in G(2)\times G(5^2)\times G(11) : \\ \varepsilon(g_2) = \left(\frac{\det(g_{11})}{11}\right),\ \phi_5(g_5) = \phi_{11}(g_{11})\Big\}.$$

Proposition 2.4.5. *Let $E/\mathbb{Q}$ be the elliptic curve given by Weierstrass equation $Y^2 + Y = X^3 - X^2 - 10X - 20$. Then we have*

$$C_E = \frac{3}{4}\mathfrak{C}_E \prod_{\ell\neq 5}\left(1 - \frac{1}{(\ell^2-\ell)(\ell^2-1)}\right) \\ \approx 0.611597,$$

where $\mathfrak{C}_E$ is given by

$$\mathfrak{C}_E = 1 + \frac{1}{65995}.$$

Proof. As before we take $m = 2\cdot 5\cdot 11$ to be the square-free part of m_E. Because E has abelian entanglements there is an exact sequence

$$1 \longrightarrow G(2\cdot 5\cdot 11) \longrightarrow G(2)\times G(5)\times G(11) \xrightarrow{\chi} \Phi_{110} \longrightarrow 1$$

From the description of $G(2\cdot 5^2\cdot 11)$ it follows that $G(2\cdot 5\cdot 11) = G(22)\times G(5)$, hence $\Phi_{110} \simeq \{\pm 1\}$. It follows that if we set χ_2 equal to the sign character ε, χ_{11} to $\left(\frac{\det(g_{11})}{11}\right)$ and χ_5 be trivial, then $\chi = \chi_2\chi_5\chi_{11}$.

By Theorem 2.4.2 we have

$$C_E = \mathfrak{C}_E \prod_{\ell} \delta_\ell.$$

where

$$\mathfrak{C}_E = 1 + E_{\chi_2}E_{\chi_5}E_{\chi_{11}}.$$

From the description of $G(\ell)$ it is then straightforward to compute δ_ℓ as well as E_{χ_ℓ} for every ℓ. □

Remark 2.4.6. Note that in this example, even though the Galois theory of E was considerably more complicated than that of a Serre curve, at the 'square-free' torsion level it was still very similar. Indeed, the subgroup $G(110) \leqslant G(2)\times G(5)\times G(11)$ was still cut out only by a quadratic character.

2.5 Cyclic reduction for primes in an arithmetic progression

We now consider a variant of the problem on cyclic reduction of elliptic curves. We have been looking at the density of primes p for which the reduction $\tilde{E}(\mathbb{F}_p)$ is cyclic. Here we impose the additional requirement that p lie in a prescribed residue class modulo some integer f. This is just one of many possible generalizations one could consider, and in many of them one should still obtain a density assuming GRH. One of the difficulties that arises however, is the explicit computation of the density as an Euler product. The character sum method we have given allows us to do this in a relatively simple manner.

If we keep the same setup as in Theorem 2.4.2, then note that the condition we are imposing on p being satisfied is again completely determined by $\rho_E(G_{\mathbb{Q}})$. In this case however, it is not necessarily enough to consider only the 'square-free' torsion fields $\mathbb{Q}(E[\ell])$. Suppose then that we are interested in primes p such that

(i) $\tilde{E}(\mathbb{F}_p)$ is cyclic,

(ii) $p \equiv a \pmod{f}$.

For each prime power ℓ^α, define

$$\mathcal{D}_a(\ell^\alpha) := \{A \in \mathrm{GL}_2(\mathbb{Z}/\ell^\alpha\mathbb{Z}) : \det A \equiv a \pmod{\ell^\alpha}\},$$
$$\left(I + \ell M_2(\mathbb{Z}/\ell^\alpha\mathbb{Z})\right)^c := \{A \in \mathrm{GL}_2(\mathbb{Z}/\ell^\alpha\mathbb{Z}) : A \not\equiv I \pmod{\ell}\}.$$

Let $f = \prod_\ell \ell^{e_\ell}$ be the prime factorisation of f, and for each $\ell \mid f$ set

$$\begin{aligned}\Psi_a(\ell^{e_\ell}) :&= \mathcal{D}_a(\ell^{e_\ell}) \cap \big(I + \ell M_2(\mathbb{Z}/\ell^{e_\ell}\mathbb{Z})\big)^c \\ &= \{A \in \mathrm{GL}_2(\mathbb{Z}/\ell^{e_\ell}\mathbb{Z}) : A \not\equiv I \pmod{\ell},\ \det A \equiv a \pmod{\ell^{e_\ell}}\}.\end{aligned}$$

Then set

$$S(\ell) := G(\ell^{e_\ell}) \cap \Psi_a(\ell^{e_\ell})$$

for those ℓ dividing f, and just as in the case of the previous subsection, set $S(\ell) := G(\ell) - \{1\}$ for all other ℓ. Then it follows that $p \nmid N_E$ satisfies conditions (i) and (ii) above if and only if for any $\ell \nmid p$ one has

(i) $\rho_\ell(\mathrm{Frob}_p) \in S(\ell)$ if $\ell \nmid f$,

(ii) $\rho_{\ell^{e_\ell}}(\mathrm{Frob}_p) \in S(\ell)$ if $\ell \mid f$.

Then the density of p having the 'right' local behaviour at ℓ equals

$$\delta_\ell = \begin{cases} |S(\ell)|/|G(\ell)| & \text{if } \ell \nmid f \\ |S(\ell)|/|G(\ell^{e_\ell})| & \text{if } \ell \mid f \end{cases}$$

and the naive density of primes satisfying conditions (i) and (ii) equals $\prod_\ell \delta_\ell$.

To account for entanglements, we proceed more or less along the same line as the case without the condition of p lying in a prescribed residue class, with some slight modifications. That is, let

$$m := \prod_{\ell \mid (f, m_E)} \ell^{e_\ell} \prod_{\substack{\ell \mid m_E \\ \ell \nmid f}} \ell$$

For any square-free d coprime to m, define

$$\mathcal{S}_{md} := \prod_{\ell \mid md} S(\ell), \quad \mathcal{G}_{md} := \prod_{\ell \mid (f,m)} G(\ell^{e_\ell}) \prod_{\substack{\ell \mid md \\ \ell \nmid f}} G(\ell).$$

By Corollary 2.3.2

$$G(md) \leqslant \mathcal{G}_{md}$$

has abelian entanglements, hence we have an exact sequence

$$1 \longrightarrow G(md) \longrightarrow \mathcal{G}_{md} \xrightarrow{\psi_{md}} \Phi_{md} \longrightarrow 1$$

for some abelian group Φ_{md}. We again have by (2.3.2) that $\Phi_{md} \simeq \Phi_m$ for any square-free d coprime to m, and the density we are looking for is then

$$C_E(a,f) = \lim_{d\to\infty} \frac{|\mathcal{S}_{md} \cap G(md)|}{|G(md)|} = \frac{|\mathcal{S}_m \cap G(m)|}{|G(m)|} \prod_{\ell\nmid m} \frac{|S(\ell)|}{|G(\ell)|}.$$

Theorem 2.5.1. *Let $\tilde{\chi} \in \widehat{\Phi}_m$ be a character of Φ_m and let χ be the character of $\mathcal{G}_m$ obtained by composing $\tilde{\chi}$ with ψ_m. Define $E_{\chi,\ell}$ by*

$$E_{\tilde{\chi},\ell} = \sum_{x\in S(\ell)} \frac{\chi_\ell(x)}{|S(\ell)|}.$$

Then

$$C_E(a,f) = \mathfrak{C}_E(a,f) \prod_\ell \delta_\ell$$

where the entanglement correction factor $\mathfrak{C}_E(a,f)$ is given by

$$\mathfrak{C}_E(a,f) = 1 + \sum_{\tilde{\chi}\in\widehat{\Phi}_m - \{1\}} \prod_{\ell|m} E_{\chi,\ell}.$$

Proof. The proof is exactly as that of Theorem 2.3.4 with the obvious modifications. □

It follows from the previous theorem that in order to evaluate the correction factors $\mathfrak{C}_E(a,f)$ it suffices to compute the order of $S(\ell)$ as well as the average value of the χ_ℓ on $S(\ell)$.

2.5.1 Serre curves

In what follows we again consider the example of Serre curves. To simplify the following proofs we will henceforth assume a and f are coprime integers. If not, then for a prime ℓ dividing (a, f) we obtain $|\Psi_a(\ell^{e_\ell})| = 0$ hence $|S(\ell)| = 0$ and $C_E(a, f) = 0$, which we take to mean the conditions imposed are satisfied for only finitely many p.

Lemma 2.5.2. *Let $E/\mathbb{Q}$ be a Serre curve, and let a and f be coprime positive integers. Let D be the discriminant of $\mathbb{Q}(\sqrt{\Delta})$ where Δ is the discriminant of any Weierstrass model of E over $\mathbb{Q}$. Suppose that $|D| \neq 4, 8$. Then*

$$\delta_\ell = \begin{cases} \frac{1}{\phi(\ell^{e_\ell})} & \text{if } a \not\equiv 1 \pmod{\ell} \text{ and } \ell \mid f \\ \frac{1}{\phi(\ell^{e_\ell})}\left(1 - \frac{1}{\ell(\ell-1)(\ell+1)}\right) & \text{if } a \equiv 1 \pmod{\ell} \text{ and } \ell \mid f \\ 1 - \frac{1}{(\ell^2-1)(\ell^2-\ell)} & \text{if } \ell \nmid f. \end{cases}$$

Proof. If $\ell \nmid f$ then as before we obtain the local density $\delta_\ell = 1 - 1/(\ell^2 - 1)(\ell^2 - \ell)$. At $\ell \mid f$ we consider the two cases. If $a \not\equiv 1 \pmod{\ell}$ then

$$S(\ell) = \mathcal{D}_a(\ell^{e_\ell})$$

since any element with determinant $a \not\equiv 1$ cannot be trivial mod ℓ. It follows that for such ℓ one has $\delta_\ell = 1/\phi(\ell^{e_\ell})$. If $a \equiv 1 \pmod{\ell}$ then we need to count the fraction of elements of $\mathcal{D}_a(\ell^{e_\ell})$ which are non-trivial mod ℓ. There is a surjective map $G(\ell) \to (\mathbb{Z}/\ell\mathbb{Z})^*$ of degree $\ell(\ell-1)(\ell+1)$, and $\mathbb{Q}(E[\ell]) \cap \mathbb{Q}(\zeta_{\ell^{e_\ell}}) = \mathbb{Q}(\zeta_\ell)$ (since $|D| \neq 4, 8$) so it follows that this fraction is precisely $1 - 1/\ell(\ell-1)(\ell+1)$, as desired. □

Lemma 2.5.3. *Let E, a and f be as in Lemma 2.5.2. Suppose further that*

$|D| = 4$. *Then*

$$\delta_2 = \begin{cases} \frac{1}{\phi(2^{e_2})} & \text{if } a \equiv 3 \pmod 4 \text{ and } 4 \mid f \\ \frac{1}{\phi(2^{e_2})}(1 - \frac{1}{3}) & \text{if } a \equiv 1 \pmod 4 \text{ and } 4 \mid f \\ \frac{5}{6} & \text{if } 4 \nmid f. \end{cases}$$

Proof. The assumption on D implies that $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(i)$ and $m_E = 4$. Recall that $2^{e_2} || f$ is the highest power of 2 dividing f. If $e_2 \geqslant 2$ then a is odd, hence is 1 or 3 mod 4. Note that $\mathbb{Q}(\zeta_{2^{e_2}}) \cap \mathbb{Q}(E[2]) = \mathbb{Q}(i)$. Now the fraction of elements $A \in G(2^{e_2})$ such that $A \in \mathcal{D}_a(2^{e_2})$ equals $1/\phi(2^{e_2})$. If $a \equiv 3 \pmod 4$ then any such $A \in \mathcal{D}_a(2^{e_2})$ acts non-trivially on $\mathbb{Q}(i)$, hence is non-trivial mod 2. It follows that $S(2) = \mathcal{D}_a(2^{e_2})$ and $\delta_2 = 1/\phi(2^{e_2})$. If $a \equiv 1 \pmod 4$, then because $[\mathbb{Q}(E[2]) : \mathbb{Q}(i)] = 3$ exactly $1 - 1/3$ of the elements in $A \in \mathcal{D}_a(2^{e_2})$ are in $S(2)$. Finally suppose $e_2 < 2$. Then the only condition at 2 is being non-trivial mod 2, and the conclusion follows. □

Lemma 2.5.4. *Let E, a and f be as in Lemma 2.5.2. Suppose further that $|D| = 8$. Then*

(i) If $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{2})$ then

$$\delta_2 = \begin{cases} \frac{1}{\phi(2^{e_2})} & \text{if } a \equiv 3 \text{ or } 5 \pmod 8 \text{ and } 8 \mid f \\ \frac{1}{\phi(2^{e_2})}(1 - \frac{1}{3}) & \text{if } a \equiv 1 \text{ or } 7 \pmod 8 \text{ and } 8 \mid f \\ \frac{5}{6} & \text{if } 8 \nmid f. \end{cases}$$

(ii) $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{-2})$ then

$$\delta_2 = \begin{cases} \frac{1}{\phi(2^{e_2})} & \text{if } a \equiv 5 \text{ or } 7 \pmod 8 \text{ and } 8 \mid f \\ \frac{1}{\phi(2^{e_2})}(1 - \frac{1}{3}) & \text{if } a \equiv 1 \text{ or } 3 \pmod 8 \text{ and } 8 \mid f \\ \frac{5}{6} & \text{if } 8 \nmid f. \end{cases}$$

Proof. We proceed similarly to Lemma 2.5.3. The assumption on D implies that $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{\pm 2})$. If $e_2 \geqslant 3$ then in this case $\mathbb{Q}(\zeta_{2^{e_2}}) \cap \mathbb{Q}(E[2]) = \mathbb{Q}(\sqrt{\pm 2})$. In case (i), elements in $\mathcal{D}_a(2^{e_2})$ act non-trivially on $\mathbb{Q}(\sqrt{2})$ if and only if $a \equiv 3$ or $5 \pmod 8$, hence the conclusion. Case (ii) follows from the same argument. □

In what remains of this section we will deduce the correction factor $\mathfrak{C}_E(a, f)$. In the following lemmas we compute the local factors E_ℓ for the different primes ℓ dividing m_E. As is often the case, the prime 2 requires special consideration and we split the computation of the local correction factor E_2 into various cases. Keep the same notation for E, a, f and D, and suppose further that $|D| \neq 4, 8$. Then m_E contains at least one odd prime factor and we have an exact sequence

$$1 \longrightarrow G(m) \longrightarrow \prod_{\ell | (f, m_E)} G(\ell^{e_\ell}) \prod_{\substack{\ell | m_E \\ \ell \nmid f}} G(\ell) \xrightarrow{\chi} \{\pm 1\} \longrightarrow 1$$

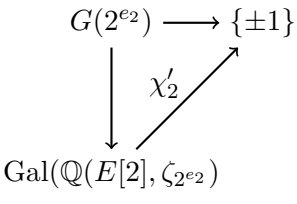
where $\chi = \prod_\ell \chi_\ell$ is a product of characters χ_ℓ. Here χ_ℓ is given by the composition $G(\ell^{e_\ell}) \to G(\ell) \xrightarrow{\det} (\mathbb{Z}/\ell\mathbb{Z})^* \to \{\pm 1\}$ and χ_2 is the character corresponding to the quadratic extension $\mathbb{Q}(E[2^{\alpha_2}]) \cap \mathbb{Q}(E[m/2^{\alpha_2}])$, where $2^{\alpha_2} || m$. When $e_2 = 1$ for instance, χ_2 is the signature map $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \to \{\pm 1\}$, corresponding to the quadratic extension $\mathbb{Q}(\sqrt{\Delta})$.

Lemma 2.5.5. *Suppose* $\mathrm{ord}_2(D) = 0$. *Then* $E_2 = -1/5$.

Proof. Since $D \equiv 1 \pmod 4$ it follows that $m_E = 2|D|$ and χ_2 is the signature map. Let $2^{e_2} || f$ be the largest power of 2 dividing f. If $e_2 \leqslant 0$ then $E_2 = -1/5$ by the same argument as in Proposition 2.4.1. If $e_2 > 1$, then $S(2) \subset G(e^{e_2})$ consists of the elements of $\mathcal{D}_a(2^{e_2})$ which are non-trivial mod 2.

Because $m_E = 2|D|$ with D odd, χ_2 is the signature map, hence it factors through the surjection $G(2^{e_2}) \to \mathrm{Gal}(\mathbb{Q}(E[2]), \zeta_{2^{e_2}})$, so we have a

commutative diagram



.

Let $S'(2)$ be the image of $S(2)$ under the surjection $G(2^{e_2}) \to \mathrm{Gal}(\mathbb{Q}(E[2]), \zeta_{2^{e_2}})$. Then note that because $\mathbb{Q}(\zeta_{2^{e_2}}) \cap \mathbb{Q}(E[2]) = \mathbb{Q}$, for each $\sigma \in G(2)$ there is a unique $\sigma' \in \mathrm{Gal}(\mathbb{Q}(E[2]), \zeta_{2^{e_2}})$ such that $\sigma(\zeta_{2^{e_2}}) = \zeta_{2^{e_2}}^a$ and $\sigma' \equiv \sigma \pmod 2$. It follows that

$$\sum_{x \in S'(2)} \chi'(x) = -1$$

and the conclusion follows. □

Lemma 2.5.6. *Suppose* $\mathrm{ord}_2(D) = 2$. *We have*

(i) If $|D| \neq 4$ *and* $4 \mid f$ *then*

$$E_2 = -\left(\frac{a}{4}\right)\frac{1}{5}.$$

(ii) If $|D| = 4$ *or* $4 \nmid f$ *then*

$$E_2 = 0.$$

Proof. If $4 \nmid f$ then because $m_E = |D|$ it follows that $m_E \nmid m$, hence

$$G(m) = \prod_{\ell \mid (f, m_E)} G(\ell^{e_\ell}) \prod_{\substack{\ell \mid m_E \\ \ell \nmid f}} G(\ell)$$

and $\Phi_m \simeq \{1\}$, so $E_2 = 0$. Similarly if $|D| = 4$ then m_E has no odd prime factors and we again conclude $E_2 = 0$.

Now suppose $|D| \neq 4$ and $4 \mid f$. If we let Δ_{sf} denote the square-free part of Δ, then the assumption on $\mathrm{ord}_2(D)$ implies that $\Delta_{\mathrm{sf}} \equiv 3 \pmod 4$. Also, because $4 \mid f$, we have that $\mathbb{Q}(i) \subset \mathbb{Q}(E[2^{e_2})$, hence

$$\mathbb{Q}(\sqrt{i\Delta_{\mathrm{sf}}}) = \mathbb{Q}(E[2^{e_2}]) \cap \mathbb{Q}(E[m/2^{e_2}])$$

and χ_2 is the character corresponding to this quadratic extension. If we define

$$\chi_i : G(2^{e_2}) \to \{\pm 1\}, \quad \chi_\Delta : G(2^{e_2}) \to \{\pm 1\}$$

to be the characters corresponding to the quadratic extensions $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{\Delta})$, respectively, then $\chi_2 = \chi_i\chi_\Delta$. Now χ_i has constant value equal to $(\frac{a}{4})$ on $S(2)$, and by the same argument as in Lemma 2.5.5 χ_Δ has average value $-1/5$ on $S(2)$. It follows then that

$$\begin{aligned} E_2 &= \frac{1}{S(2)} \sum_{x \in S(2)} \chi_2(x) \\ &= \frac{1}{S(2)} \sum_{x \in S(2)} \chi_i(x)\chi_\Delta(x) \\ &= -\left(\frac{a}{4}\right)\frac{1}{5}. \end{aligned}$$

□

To deal with the case of $\mathrm{ord}_2(D) = 3$, we establish the following notation. Note that if $\mathrm{ord}_2(D) = 3$ then we must have that $2 \mid \Delta_{\mathrm{sf}}$. Let Δ' be such that $\Delta_{\mathrm{sf}} = 2\Delta'$.

Lemma 2.5.7. *Suppose* $\mathrm{ord}_2(D) = 3$*, and keep the notation above. We have*

(i) If $|D| \neq 8,\ 8 \mid f$ *and* $\Delta' \equiv 1 \pmod 4$ *then*

$$E_2 = \begin{cases} 1/5 & \text{if } a \equiv 1 \text{ or } 7 \pmod 8 \\ -1/5 & \text{if } a \equiv 3 \text{ or } 5 \pmod 8 \end{cases}.$$

(ii) If $|D| \neq 8,\ 8 \mid f$ *and* $\Delta' \equiv 3 \pmod 4$ *then*

$$E_2 = \begin{cases} 1/5 & \text{if } a \equiv 1 \text{ or } 3 \pmod 8 \\ -1/5 & \text{if } a \equiv 5 \text{ or } 7 \pmod 8 \end{cases}.$$

(iii) If $|D| = 8$ *or* $8 \nmid f$ *then*

$$E_2 = 0.$$

Proof. If $|D| = 8$ or $8 \nmid f$ then by the same reasoning as in Lemma 2.5.6 we conclude $E_2 = 0$. Assume then that $|D| \neq 8$ and $8 \mid f$. Because $8 \mid f$, we have that $\mathbb{Q}(\sqrt{\pm 2}) \subset \mathbb{Q}(E[2^{e_2}])$. Let

$$\chi_{\sqrt{2}} : G(2^{e_2}) \to \{\pm 1\}, \quad \chi_{\sqrt{-2}} : G(2^{e_2}) \to \{\pm 1\}, \quad \chi_\Delta : G(2^{e_2}) \to \{\pm 1\}$$

to be the characters corresponding to the quadratic extensions $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{\Delta})$, respectively. If $\Delta' \equiv 1 \pmod 4$ then

$$\mathbb{Q}(\sqrt{\Delta'}) = \mathbb{Q}(E[2^{e_2}]) \cap \mathbb{Q}(E[m/2^{e_2}])$$

and χ_2 is the quadratic character corresponding to this extension, with $\chi_2 = \chi_{\sqrt{2}}\chi_\Delta$. If $\Delta' \equiv 3 \pmod 4$ then

$$\mathbb{Q}(\sqrt{-\Delta'}) = \mathbb{Q}(E[2^{e_2}]) \cap \mathbb{Q}(E[m/2^{e_2}])$$

and χ_2 is the quadratic character corresponding to this extension, with $\chi_2 = \chi_{\sqrt{-2}}\chi_\Delta$. Now note that $\chi_{\sqrt{2}}$ has constant value on $S(2)$ equal to 1 if $a \equiv 1$ or $7 \pmod 8$, and -1 if $a \equiv 3$ or $5 \pmod 8$, and $\chi_{\sqrt{-2}}$ has constant value on $S(2)$ equal to 1 if $a \equiv 1$ or $3 \pmod 8$, and -1 if $a \equiv 5$ or $7 \pmod 8$ We conclude exactly as in Lemma 2.5.6. □

Proposition 2.5.8. *Let* $E/\mathbb{Q}$ *be a Serre curve, and let* a *and* f *be coprime positive integers. Let* D *be the discriminant of* $\mathbb{Q}(\sqrt{\Delta})$ *where* Δ *is the dis-*

criminant of any Weierstrass model of E over $\mathbb{Q}$. Suppose that $|D| \neq 4, 8$. Then

$$C_E(a,f) = \mathfrak{C}_E(a,f)\frac{1}{\phi(f)}\prod_{\ell\mid(a-1,f)}\left(1-\frac{1}{\ell(\ell-1)(\ell+1)}\right)\prod_{\ell\nmid f}\left(1-\frac{1}{(\ell^2-1)(\ell^2-\ell)}\right)$$

where the entanglement correction factor $\mathfrak{C}_E(a,f)$ is given by

$$\mathfrak{C}_E(a,f) = 1 + E_2\prod_{\substack{\ell\mid(D,f)\\ \ell\neq 2}}\left(\frac{a}{\ell}\right)\prod_{\substack{\ell\mid D\\ \ell\nmid 2f}}\frac{-1}{(\ell^2-1)(\ell^2-\ell)-1}.$$

Here E_2 is given by Lemmas 2.5.5, 2.5.6 and 2.5.7,

Proof. Since $|D| \neq 4, 8$, the equality involving $C_E(a,f)$ follows from using Lemma 2.5.2 for all ℓ. The form of the entanglement correction factor at 2 follows from Lemmas 2.5.5, 2.5.6 and 2.5.7. It remains to consider $\ell \neq 2$. By Theorem 2.5.1 if $\ell \nmid f$ and $\ell \mid D$ then $S(\ell) = G(\ell) - \{1\}$ and so

$$E_\ell = \frac{-1}{(\ell^2-1)(\ell^2-\ell)-1}.$$

Ir $\ell \mid (D,f)$ then because $\mathbb{Q}(E[\ell]) \cap \mathbb{Q}(\zeta_{\ell^{e_\ell}}) = \mathbb{Q}(\zeta_\ell)$ we have that χ_ℓ has constant value $(\frac{a}{\ell})$ on $S(\ell)$ and the result follows. □

Corollary 2.5.9. *For any (a,f) coprime integers, we have $C_E(a,f) > 0$.*

Proof. It is clear that the naive density $\prod_\ell \delta_\ell$ does not vanish, hence in order for $C_E(a,f)$ to be zero, we would need the correction factor $\mathfrak{C}_E(a,f)$ to be zero, which happens if and only if $\prod_\ell E_\ell = -1$. This is impossible as E_2 is always $\pm 1/5$ or 0. □

Corollary 2.5.10. *The correction factor $\mathfrak{C}_E(a,f)$ equals 1 if and only if* $\mathrm{ord}_2(D) > \mathrm{ord}_2(f)$.

Proof. From the form of the correction factor it follows that $\mathfrak{C}_E(a,f) = 1$ if and only if $E_2 = 0$, and the result follows. □

2.5.2 Example: $Y^2 = X^3 + X^2 + 4X + 4$

We look now at an example of a non-Serre curve where the constant $C_E(a, f)$ can vanish. This implies that conjecturally, there should only exist finitely many primes p such that $\tilde{E}(\mathbb{F}_p)$ is cyclic and $p \equiv a \pmod{f}$. Let E be the elliptic curve over $\mathbb{Q}$ given by the Weierstrass equation $Y^2 = X^3 + X^2 + 4X + 4$. In [Bra09], a description of the Galois theory of E is worked out. In particular, for this curve we have that $m_E = 120$, and the following properties hold:

- E has a rational 3-torsion point, and $G(3) \simeq S_3$.
- E has a rational two-torsion point, and $\mathbb{Q}(E[2]) = \mathbb{Q}(i)$.
- $G(4)$ has order 16, and $\mathbb{Q}(E[4]) \cap \mathbb{Q}(E[5]) = \mathbb{Q}(\sqrt{5})$.
- $G(8)$ has order 128, and $\mathbb{Q}(E[8]) \cap \mathbb{Q}(E[5]) = \mathbb{Q}(\zeta_5)$.
- $G(5) = \mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z})$
- $\mathbb{Q}(E[3]) \cap \mathbb{Q}(E[40]) = \mathbb{Q}$, hence $G(120) = G(3) \times G(40)$.

From all of this we conclude that

$$G(120) = \{(g_8, g_3, g_5) \in G(8) \times G(3) \times G(5) : g_8(\zeta_5) = \zeta_5^{\det g_5}\}$$

hence E has abelian entanglements and $G(120)$ fits into the exact sequence

$$1 \longrightarrow G(120) \longrightarrow G(8) \times G(3) \times G(5) \longrightarrow \Phi_{120} \longrightarrow 1,$$

where $\Phi_{120} \simeq (\mathbb{Z}/5\mathbb{Z})^\times$. Also, given coprime integers a and $f = \prod_\ell \ell^{e_\ell}$ we again set

$$m := \prod_{\ell \mid (f, 120)} \ell^{e_\ell} \prod_{\substack{\ell \mid 120 \\ \ell \nmid f}} \ell.$$

Lemma 2.5.11. *For any $\tilde{\chi} \in \widehat{\Phi}_m - \{1\}$ we have $E_{\chi,2} = 0$.*

Proof. Suppose first that $4 \nmid f$. Then m is square-free, and because

$$G(30) = G(2) \times G(3) \times G(5)$$

it follows that $\Phi_m \simeq \{1\}$, hence $E_{\chi,2} = 0$. Suppose now that $4 \mid f$, and let $\tilde{\eta}$ be a generator of $\tilde{\Phi}_{120}$. If $8 \mid f$, then $120 \mid m$, hence $\Phi_m \simeq \Phi_{120} \simeq (\mathbb{Z}/5\mathbb{Z})^\times$. Any $\tilde{\chi} \in \widehat{\Phi}_m - \{1\}$ is equal to $\tilde{\eta}^j$ for some $j \in \{1, 2, 3\}$ and χ_2 is equal to η_2^j, where

$$\eta_2 : G(2^{e_2}) \longrightarrow (\mathbb{Z}/5\mathbb{Z})^\times$$

is the character corresponding to the subfield $\mathbb{Q}(\zeta_5) \subset \mathbb{Q}(E[2^{e_2}])$. Now because $\mathbb{Q}(E[2]) = \mathbb{Q}(i) \subset \mathbb{Q}(\zeta_{2^{e_2}})$ it follows that $\mathbb{Q}(E[2], \zeta_{2^{e_2}}) \cap \mathbb{Q}(\zeta_5) = \mathbb{Q}$, hence

$$\begin{aligned} \sum_{g \in S(2)} \eta_2^j(g) &= \sum_{x \in (\mathbb{Z}/5\mathbb{Z})^\times} x \\ &= 0. \end{aligned}$$

We conclude that $E_{\chi,2} = 0$. If $4 || f$, then $\Phi_m \simeq \{\pm 1\}$ and we can use the same argument given that $\mathbb{Q}(i) \cap \mathbb{Q}(\zeta_5) = \mathbb{Q}$. This proves the claim. □

Proposition 2.5.12. *For any coprime (a, f) we have that $\mathfrak{C}_E(a, f) = 1$. Further,*

$$C_E(a, f) = 0 \iff 4 \mid f \text{ and } a \equiv 1 \pmod 4.$$

Proof. That $\mathfrak{C}_E(a, f) = 1$ follows directly from Theorem 2.5.1 and Lemma 2.5.11. It follows from this that

$$C_E(a, f) = \prod_\ell \delta_\ell.$$

For $\ell \neq 2$ we have that $\delta_\ell \neq 0$. Indeed,

$$\delta_3 = \begin{cases} \frac{1}{\phi(3^{e_3})} & \text{if } a \equiv 2 \pmod 3 \text{ and } 3 \mid f \\ \frac{1}{\phi(3^{e_3})}(1 - \frac{1}{3}) & \text{if } a \equiv 1 \pmod 3 \text{ and } 3 \mid f \\ \frac{5}{6} & \text{if } 3 \nmid f \end{cases},$$

and

$$\delta_\ell = \begin{cases} \frac{1}{\phi(\ell^{e_\ell})} & \text{if } a \not\equiv 1 \pmod \ell \text{ and } \ell \mid f \\ \frac{1}{\phi(\ell^{e_\ell})}\left(1 - \frac{1}{\ell(\ell-1)(\ell+1)}\right) & \text{if } a \equiv 1 \pmod \ell \text{ and } \ell \mid f \\ 1 - \frac{1}{(\ell^2-1)(\ell^2-\ell)} & \text{if } \ell \nmid f. \end{cases}$$

Finally, given that $\mathbb{Q}(E[2]) = \mathbb{Q}(i)$, it follows that $\delta_2 = 0$ if and only if $4 \mid f$ and $a \equiv 1 \pmod 4$, and the conclusion follows. □

Remark 2.5.13. Suppose a and f are coprime integers such that $a \equiv 1 \pmod 4$. The above proposition is saying that the only obstruction to the existence of infinitely many primes p such that $\tilde{E}(\mathbb{F}_p)$ is cyclic and $p \equiv a \pmod f$ is a local one at the prime 2. Meaning, for any prime p it is impossible for it to satisfy the required condition at the prime 2, that is, for Frob_p to lie in the set $S(2)$, which is the empty set. Note also that even when f is divisible by 4, we still have $E_{\chi,2} = 0$ and hence $\mathfrak{C}_E(a, f) = 1$. What this is encoding is the fact that $\mathbb{Q}(\zeta_{2^{e_2}}) \cap \mathbb{Q}(\zeta_5) = \mathbb{Q}$ for any e_2. The only entanglement of E occurs in the subfield $\mathbb{Q}(\zeta_5)$, and this field is disjoint from $\mathbb{Q}(\zeta_{2^\infty})$.

2.5.3 Example: $Y^2 + XY + Y = X^3 - X^2 - 91X - 310$

So far we have only considered examples where the constant $C_E(a, f)$ either does not vanish, or vanishes because there is a condition at some prime ℓ which cannot be satisfied. Another interesting possibility is when all δ_ℓ are

non-zero, yet the constant $C_E(a,f)$ still vanishes. This occurs if and only if the entanglement correction factor $\mathfrak{C}_E(a,f)$ vanishes and its expression as a product of local correction factors makes it easy to determine when this happens. The entanglement correction factor being zero means there is an obstruction coming from the entanglement fields which prevent there being infinitely many primes p satisfying the imposed conditions. We will now analyse an example when this occurs.

Consider the elliptic curve E over $\mathbb{Q}$ given by Weierstrass equation $Y^2 + XY + Y = X^3 - X^2 - 91X - 310$. The discriminant of our Weierstrass model is $\Delta = 17$. This curve has one rational torsion point of order 2 and $\mathbb{Q}(E[2]) = \mathbb{Q}(\sqrt{17})$. In fact, machine computation shows that $m = 34$, where m is the square-free part of m_E, and

$$G(34) = \{(g_2, g_{17}) \in G(2) \times \mathrm{GL}_2(\mathbb{Z}/17\mathbb{Z}) : \varepsilon(g_2) = \theta_{17} \circ \det(g_{17})\}$$

where as usual ε denotes the signature map and $\theta_{17} : (\mathbb{Z}/17\mathbb{Z})^* \to \{\pm 1\}$ denotes the unique quadratic character of $(\mathbb{Z}/17\mathbb{Z})^*$.

If we let D denote the discriminant of $\mathbb{Q}(\sqrt{\Delta})$, then $D = 17 \equiv 1 \pmod 4$, hence by a similar argument to Lemma 2.5.2 we obtain that

$$\prod_{\ell} \delta_\ell = \frac{1}{2}\frac{1}{\phi(f)} \prod_{\substack{\ell \mid (a-1,f) \\ \ell \neq 2}} \left(1 - \frac{1}{\ell(\ell-1)(\ell+1)}\right) \prod_{\substack{\ell \nmid f \\ \ell \neq 2}} \left(1 - \frac{1}{(\ell^2-\ell)(\ell^2-1)}\right)$$

which is non-zero for all a and f. By Theorem 2.5.1 we have that

$$C_E(a,f) = \mathfrak{C}_E(a,f)\frac{1}{2}\frac{1}{\phi(f)} \prod_{\substack{\ell \mid (a-1,f) \\ \ell \neq 2}} \left(1 - \frac{1}{\ell(\ell-1)(\ell+1)}\right) \prod_{\substack{\ell \nmid f \\ \ell \neq 2}} \left(1 - \frac{1}{(\ell^2-\ell)(\ell^2-1)}\right)$$

with

$$\mathfrak{E}_E(a,f) = 1 + \prod_{\ell \mid 34} E_\ell.$$

We conclude then the following.

Proposition 2.5.14. *For the above elliptic curve we have that $C_E(a, f) = 0$ if and only if $17 \mid f$ and a is a quadratic residue modulo 17.*

Proof. The naive density $\prod_\ell \delta_\ell$ is non-vanishing, hence $C_E(a, f) = 0$ if and only if $\mathfrak{C}_E(a, f) = 0$. Using the same argument as in Lemma 2.5.5, we deduce $E_2 = -1$ for all a, f. We have then that

$$\mathfrak{C}_E(a, f) = 0 \iff E_{17} = 1.$$

If $17 \nmid f$ then $E_{17} = -1/78335$. If $17 \mid f$ then $E_{17} = \left(\frac{a}{17}\right)$ and the conclusion follows. □

Remark 2.5.15. Note that if $17 \mid f$ and a is a quadratic residue mod 17, then for any prime $p \equiv a \pmod f$ we have that p splits in $\mathbb{Q}(\sqrt{17}) = \mathbb{Q}(E[2])$, so Frob_p would not satisfy the condition at the prime 2. The obstruction to the existence of infinitely many primes p such that $\tilde{E}(\mathbb{F}_p)$ is cyclic and $p \equiv a \pmod f$ is precisely the entanglement between the 2 and 17 torsion fields. The above proposition is saying that this the only obstruction that exists.

2.6 Koblitz's conjecture

In [Kob88], N. Koblitz made a conjecture on the asymptotic behaviour of the number of primes p for which the cardinality of the group $\tilde{E}(\mathbb{F}_p)$ is prime. In this section we use our character sum method to give a description of the constants appearing in this asymptotic.

Conjecture 2.6.1 (Koblitz)**.** *Let $E/\mathbb{Q}$ be a non-CM curve and let Δ be the discriminant of any Weierstrass model of E over $\mathbb{Q}$. Suppose that E is not $\mathbb{Q}$-isogenous to a curve with non-trivial $\mathbb{Q}$-torsion. Then*

$$|\{\text{primes } p \leqslant x : p \nmid \Delta, |\tilde{E}(\mathbb{F}_p)| \text{ is prime}\}| \sim C_E \frac{x}{(\log x)^2}$$

as $x \to \infty$ where C_E is an explicit positive constant.

In [Zyw11c], Zywina shows that the description of the constant C_E given by Koblitz is not always correct, and he gives a corrected description of the constant along with providing several interesting examples and numerical evidence for the refined conjecture. In particular the constant described by Zywina is not necessarily positive. The reason the original constant is not always correct is that it does not take into account that divisibility conditions modulo distinct primes need not be independent. Put another way, it could occur that there are non-trivial intersections between distinct ℓ-power torsion fields of E. The following is the refined Koblitz conjecture given by Zywina, which here we state restricted to non-CM curves over $\mathbb{Q}$.

Conjecture 2.6.2. *Let $E/\mathbb{Q}$ be a non-CM elliptic curve of discriminant Δ, and let t be a positive integer. Then there is an explicit constant $C_{E,t} \geqslant 0$ such that*

$$|\{\textit{primes } p \leqslant x : p \nmid \Delta, |\tilde{E}(\mathbb{F}_p)|/t \textit{ is prime}\}| \sim C_{E,t} \frac{x}{(\log x)^2}$$

as $x \to \infty$.

The condition on p that $|\tilde{E}(\mathbb{F}_p)|/t$ be prime can be given as a splitting condition in the various ℓ-torsion fields, so the character sum method we have developed again seems well suited to compute $C_{E,t}$. In his paper Zywina computes the constants $C_{E,t}$ via a different method than the one we use here, both in the CM and non-CM cases. Here we will restrict ourselves to non-CM curves with abelian entanglements over the rationals.

For each prime power ℓ^α, define

$$\Psi_t(\ell^\alpha) := \left\{ A \in \mathrm{GL}_2(\mathbb{Z}/\ell^\alpha\mathbb{Z}) : \ \det(I - A) \in t \cdot (\mathbb{Z}/\ell^\alpha\mathbb{Z})^\times \right\}.$$

For a prime $p \nmid N_E \ell$ note that $\tilde{E}(\mathbb{F}_p)/t$ is invertible modulo $\ell^\alpha/(\ell^\alpha, t)$ if and only if $\rho_{\ell^\alpha}(\mathrm{Frob}_p) \in G(\ell^\alpha) \cap \Psi_t(\ell^\alpha)$. Suppose that t has prime factorisation

$t = \prod_\ell \ell^{e_\ell}$. With this in mind, define the set of 'good' Frobenius elements to be

$$S_t(\ell) = \begin{cases} G(\ell^{e_\ell+1}) \cap \Psi_t(\ell^{e_\ell+1}) & \text{if } \ell \mid t \\ G(\ell) \cap \Psi_t(\ell) & \text{if } \ell \nmid t \ . \end{cases}$$

We now give a description of the constant $C_{E,t}$ in terms of our sets $S_t(\ell)$ as well as a crude heuristic of justifying it. This heuristic follows the same lines as that of Koblitz and Zywina. The key argument relies on the Cramer's model which asserts that, roughly speaking, the primes behave as if every random integer n is prime with probability $1/\log n$. If the sequence $\{|\tilde{E}(\mathbb{F}_p)|/t\}_{p \nmid N_E}$ were assumed to behave like random integers, then the proability that $|\tilde{E}(\mathbb{F}_p)|/t$ is prime would be

$$\frac{1}{\log\left(|\tilde{E}(\mathbb{F}_p)|/t\right)} \approx \frac{1}{\log(p+1) - \log t}.$$

The last approximation uses the fact that by Hasse's bound, $\tilde{E}(\mathbb{F}_p)$ is close to $p+1$.

It is not true however, that the $|\tilde{E}(\mathbb{F}_p)|/t$ behave like random integers with respect to congruences, and in order to get a better approximation we need to take these congruences into account. If we fix a prime ℓ, then for all but finitely many p. if $|\tilde{E}(\mathbb{F}_p)|/t$ is prime then it is invertible modulo ℓ. If ℓ does not divide t, then by Chebotarev, the density of primes $p \nmid N_E$ such that $\tilde{E}(\mathbb{F}_p)/t$ is invertible modulo ℓ is $|S_t(\ell)|/|G(\ell)|$. If $\ell \mid t$, then similarly the density of primes $p \nmid N_E$ such that $\tilde{E}(\mathbb{F}_p)$ is divisible by ℓ^{e_ℓ} *and* $\tilde{E}(\mathbb{F}_p)/t$ is invertible modulo ℓ equals $|S_t(\ell)|/|G(\ell^{e_\ell+1})|$. Meanwhile the density of natural numbers that are invertible mod ℓ is $(1 - 1/\ell)$. If we let d be a square-free integer coprime to t, then

$$\prod_{\ell \mid td} \frac{1}{1-1/\ell} \prod_{\ell \mid t} \frac{|S_t(\ell)|}{|G(\ell^{e_\ell+1})|} \prod_{\ell \mid d} \frac{|S_t(\ell)|}{|G(\ell)|} \cdot \frac{1}{\log(p+1) - \log t}$$

should constitute a better approximation to the probability that $|\tilde{E}(\mathbb{F}_p)|/t$ is prime, as it takes into account the congruences modulo all primes $\ell \mid td$. Taking into account all congruences amounts to letting d tend to infinity, hence this model suggests that for a randomly chosen p, $|\tilde{E}(\mathbb{F}_p)|/t$ is prime with probability

$$\prod_{\ell} \frac{\delta_\ell}{1-1/\ell} \cdot \frac{1}{\log(p+1) - \log t}$$

where

$$\delta_\ell = \begin{cases} |S_t(\ell)|/|G(\ell)| & \text{if } \ell \nmid t \\ |S_t(\ell)|/|G(\ell^{e_\ell+1})| & \text{if } \ell \mid t \ . \end{cases}$$

This is the constant that was given by Koblitz with $t = 1$ and later refined by Zywina. The problem that still remained with the approximation given by Koblitz, is that while it does take into account congruences modulo ℓ, is assumes that divisibility conditions modulo distinct primes are independent. In order to deal with this we take a similar approach as in the previous sections. That is, we let

$$m := \prod_{\ell \mid t} \ell^{e_\ell+1} \prod_{\substack{\ell \mid m_E \\ \ell \nmid t}} \ell$$

and for each square-free d coprime to m, let

$$\mathcal{S}_{md} := \prod_{\ell \mid md} S_t(\ell), \quad \mathcal{G}_{md} := \prod_{\ell \mid t} G(\ell^{e_\ell+1}) \prod_{\substack{\ell \mid md \\ \ell \nmid t}} G(\ell).$$

By Corollary 2.3.2

$$G(md) \leqslant \mathcal{G}_{md}$$

has abelian entanglements, hence we have an exact sequence

$$1 \longrightarrow G(md) \longrightarrow \mathcal{G}_{md} \xrightarrow{\psi_{md}} \Phi_{md} \longrightarrow 1$$

for some abelian group Φ_{md}. By (2.3.2) we have that $\Phi_{md} \simeq \Phi_m$ for any square-free d coprime to m. Note now that $|\mathcal{S}_{md} \cap G(md)|/|G(md)|$ is the density of p for which $|\tilde{E}(\mathbb{F}_p)|/t$ is an integer and invertible modulo md, hence by letting d tend to infinity over the square free integers coprime to m, the refined constant is

$$\begin{aligned} C_{E,t} &= \lim_{d\to\infty} \frac{|\mathcal{S}_{md} \cap G(md)|/|G(md)|}{1-1/\ell} \\ &= \left(\prod_{\ell|m} \frac{1}{1-1/\ell}\right) \cdot \frac{|\mathcal{S}_m \cap G(m)|}{|G(m)|} \prod_{\ell\nmid m} \frac{\delta_\ell}{1-1/\ell}. \end{aligned}$$

It follows by the prime number theorem that the expected number of primes p such that $|\tilde{E}(\mathbb{F}_p)|/t$ is prime is asymptotic to $C_{E,t} \cdot x/(\log x)^2$.

Applying Theorem 2.3.4 with m defined as above we obtain

$$C_{E,t} = \mathfrak{C}_{E,t} \prod_{\ell} \frac{\delta_\ell}{1-1/\ell} \tag{2.6.1}$$

where the entanglement correction factor $\mathfrak{C}_{E,t}$ is given by

$$\mathfrak{C}_{E,t} = 1 + \sum_{\tilde{\chi}\in\widehat{\Phi}_m - \{1\}} \prod_{\ell|m} E_{\chi,\ell}.$$

2.6.1 Serre curves

In this section we compute the constants $C_{E,1}$ in Conjecture 2.6.2 for Serre curves. This will amount to finding the average value of various quadratic characters on $S(\ell)$. In the case of Serre curves, the sets $S(\ell)$ are particularly easy to treat.

Proposition 2.6.3. *Let $E/\mathbb{Q}$ be a Serre curve. Let D be the discriminant of $\mathbb{Q}(\sqrt{\Delta})$ where Δ is the discriminant of any Weierstrass model of E over*

$\mathbb{Q}$. *Then*

$$C_{E,1} = \mathfrak{C}_{E,1} \prod_{\ell} \left(1 - \frac{\ell^2 - \ell - 1}{(\ell-1)^3(\ell+1)}\right)$$

where the entanglement correction factor $\mathfrak{C}_{E,1}$ *is given by*

$$\mathfrak{C}_{E,1} = \begin{cases} 1 & \text{if } D \equiv 0 \pmod 4 \\ 1 + \prod_{\ell \mid D} \dfrac{1}{\ell^3 - 2\ell^2 - \ell + 3} & \text{if } D \equiv 1 \pmod 4 \end{cases}$$

Proof. We begin by noting that, for Serre curves,

$$S_1(\ell) = \left\{ A \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \ \det(I - A) \in (\mathbb{Z}/\ell\mathbb{Z})^{\times} \right\}.$$

We have then that

$$\begin{aligned} \delta_\ell &= \frac{|S_1(\ell)|}{|G(\ell)|} \\ &= 1 - \frac{|S_1(\ell)^c|}{|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})|} \end{aligned}$$

where $S_1(\ell)^c = \{A \in \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \ \det(I - A) = 0\}$. Thus $S_1(\ell)^c$ consists of those matrices whose eigenvalues are 1 and λ for some $\lambda \in (\mathbb{Z}/\ell\mathbb{Z})^{\times}$. It follows from Table 12.4 in §12, Chapter XVIII of [Lan02], that there are ℓ^2 elements of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ with both eigenvalues equal to 1, and $\ell^2 + \ell$ elements with eigenvalues 1 and $\lambda \neq 1$. We obtain then that $|S_1(\ell)^c| = \ell^2 + (\ell-2)(\ell^2+\ell)$, hence we have that

$$\delta_\ell = 1 - \frac{\ell^2 + (\ell-2)(\ell^2+\ell)}{(\ell^2-\ell)(\ell^2-1)}$$

and a calculation yields that

$$\frac{\delta_\ell}{1 - 1/\ell} = 1 - \frac{\ell^2 - \ell - 1}{(\ell-1)^3(\ell+1)}.$$

From (2.6.1) it rests only to compute $\mathfrak{C}_{E,1}$. Because $t = 1$, m equals the square-free part of m_E, and we may proceed just as in the proof of Proposition 2.4.4. That is, when $D \equiv 0 \pmod 4$ then $\mathfrak{C}_{E,1} = 1$. If $D \equiv 1 \pmod 4$, then for each $\ell \mid 2D$ it suffices to compute the average value of χ_ℓ on $S_1(\ell)$.

Note that since the χ_ℓ are non-trivial, then $\sum_{x \in G(\ell)} \chi_\ell(x) = 0$. For $\ell > 2$ recall that $\chi_\ell = \left(\frac{\det}{\ell}\right)$, hence given an element $x \in S_1(\ell)^c$ with eigenvalues 1 and λ, we have that $\chi_\ell(x) = \left(\frac{\lambda}{\ell}\right)$. There are an equal number of squares and non-squares in $(\mathbb{Z}/\ell\mathbb{Z})^\times$, so we conclude then

$$\begin{aligned}
\sum_{x \in S_1(\ell)} \chi_\ell(x) &= -\sum_{x \in S_1(\ell)^c} \chi_\ell(x) \\
&= -\left(\ell^2 \left(\frac{1}{\ell}\right) + (\ell^2 + \ell) \sum_{\substack{\lambda \in (\mathbb{Z}/\ell\mathbb{Z})^\times \\ \ell \neq 1}} \left(\frac{\lambda}{\ell}\right)\right) \\
&= -(\ell^2 - (\ell^2 + \ell)) \\
&= \ell.
\end{aligned}$$

From this we obtain

$$\begin{aligned}
E_\ell &= \frac{\ell}{|G(\ell)| - |S_1(\ell)|} \\
&= \frac{\ell}{(\ell^2 - \ell)(\ell^2 - 1) - (\ell^2 + \ell)(\ell - 2) - \ell^2} \\
&= \frac{1}{\ell^3 - 2\ell^2 - \ell + 3}.
\end{aligned}$$

For $\ell = 2$ one can directly compute $S_1(2)$. It consists of the 2 matrices $\left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$ both of which have order 3 and hence are even permutations. Since χ_2 is the signature character we conclude $E_2 = 1$, and this completes the proof. □

Chapter 3

Non-Serre curves

3.1 Introduction

Let E be a non-CM elliptic curve over a number field K. As we have seen in chapters 1 and 2, understanding the image of ρ_E in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ amounts to understanding the ℓ-adic images $\rho_{E,\ell^\infty}(G_K)$ for every prime ℓ as well as the entanglement fields

$$K(E[m_1]) \cap K(E[m_2])$$

for each pair $m_1, m_2 \in \mathbb{N}$ which are relatively prime. We have also seen such entanglement fields appear prominently in Chapter 2. Indeed, using Lemma 2.3.1 we see that the character sum method for the study of conjectural constants can only be applied to the class of elliptic curves whose entanglement fields are abelian extensions of K. This naturally leads to the question: given a number field K, can one classify the triples (E, m_1, m_2) with E an elliptic curve over K and m_1, m_2 a pair of coprime integers for which the entanglement field $K(E[m_1]) \cap K(E[m_2])$ is non-abelian over K? The study of correction factors done in Chapter 2 illustrates why it would be of interest to obtain a complete classification of such examples.

In this chapter we show that there does indeed exist at least one infi-

nite family of curves such that the curves in it do not satisfy the abelian entanglements property. The character sum method as we have developed it cannot be applied to the curves in this family, however we will see that with some additional restrictions it still can be. The family of curves we have found appears to be of a very idiosyncratic nature.

Let us restrict our attention now to elliptic curves over $\mathbb{Q}$. With respect to understanding the entanglement fields, the case $K = \mathbb{Q}$, although it is usually the first case considered, has a complication which doesn't arise over any other number field. Indeed, when the base field is $\mathbb{Q}$, the Kronecker-Weber theorem, together with the containment $\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(E[n])$, *forces* the occurrence of non-trivial entanglement fields. Recall from Section 2.4.1 that for any elliptic curve E over $\mathbb{Q}$ one has

$$\mathbb{Q}(\sqrt{\Delta_E}) \subseteq \mathbb{Q}(E[2]) \cap \mathbb{Q}(\zeta_n), \tag{3.1.1}$$

where $n = 4|\Delta_E|$, and that a Serre curve is one whose Galois action on its torsion points is as large as possible. That is, it satisfies that $[\mathrm{GL}_2(\hat{\mathbb{Z}}) : \rho_E(G_{\mathbb{Q}})] = 2$. These are precisely the curves E over $\mathbb{Q}$ for which the entanglement (3.1.1) is the only obstruction to surjectivity of ρ_E. It is also shown in Section 2.4 that Serre curves have abelian entanglements.

Let $E_{r,s}$ denote the curve given by the equation

$$E_{r,s} : Y^2 = X^3 + rX + s.$$

For a varying parameter x let $R(x)$ and $S(x)$ be a given length and width that grow with x and define

$$C(x) := \{E_{r,s} : (r,s) \in \mathbb{Z}^2, |r| \leqslant R(x), |s| \leqslant S(x) \text{ and } 4r^3 + 27s^2 \neq 0\}.$$

In [Jon10] Nathan Jones proves a theorem bounding the mean-square error in the Chebotarev theorem for division fields of elliptic curves and uses this

to count the elliptic curves over $\mathbb{Q}$ which are Serre curves. More precisely, he proves the following theorem (Theorem 4 in [Jon10]).

Theorem 3.1.1 (Jones). *Let $C_{Serre}(x)$ denote the set*

$$\{E_{r,s} \in C(x) : E_{r,s} \text{ is a Serre curve}\}.$$

Assuming that $\min\{R(x), S(x)\} \geqslant x^2$, one has

$$|C(x) - C_{Serre}(x)| \ll \frac{|C(x)| \log^B x}{x},$$

where B is an explicit constant. Thus, in particular,

$$\lim_{x\to\infty} \frac{|C_{Serre}(x)|}{C(x)|} = 1.$$

The main algebraic ingredient used by Jones in his proof is the following lemma (Lemma 5 in [Jon10]) which gives a sufficient condition for an elliptic curve E to be a Serre curve.

Lemma 3.1.2 (Jones). *Suppose E is an elliptic curve over $\mathbb{Q}$ such that:*

1. *For all primes ℓ we have that $\rho_{E,\ell}(G_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$,*
2. *$\rho_{E,72}(G_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{Z}/72\mathbb{Z})$.*

Then E is a Serre curve.

In [Zyw10], Zywina generalizes Theorem 3.1.1 to the case $K \neq \mathbb{Q}$ (see also [Rad08], which sharpens the upper bound to an asymptotic formula). In [GJ11], different ideas are used to deduce stronger upper bounds for the number of elliptic curves in *one-parameter* families which are not Serre curves. These results are obtained by viewing non-Serre curves as coming from rational points on modular curves. More precisely, there is a family

$\mathcal{X} = \{X_1, X_2, \dots\}$ of modular curves with the property that, for each elliptic curve E, one has

$$E \text{ is not a Serre curve} \iff j(E) \in \bigcup_{X \in \mathcal{X}} j(X(\mathbb{Q})), \tag{3.1.2}$$

where j denotes the natural projection followed by the usual j-map:

$$j : X \longrightarrow X(1) \longrightarrow \mathbb{P}^1.$$

In [GJ11], the authors use (3.1.2) together with geometric methods to bound the number of non-Serre curves in a given one-parameter family. This brings us to the following question, which serves as additional motivation for the present chapter.

Question 3.1.3. *What is an explicit list of modular curves in a family* $\mathcal{X} = \{X_1, X_2, \dots\}$ *satisfying* (3.1.2)*?*

In order to answer this question it will be essential to have a necessary and sufficient condition for an elliptic curve to be a Serre curve. Lemma 3.1.2 above gives a sufficient condition, and this was furthered strengthened by Jones (Corollary 2.12 in [Jon]) to provide a necessary condition as well.

Proposition 3.1.4 (Jones)**.** *Let E be an elliptic curve over $\mathbb{Q}$. Then E is a Serre curve if and only if the following two conditions hold.*

1. *For each prime $\ell \geqslant 5$, $\rho_{E,\ell}(G_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.*
2. *One has $[\rho_{E,36}(G_{\mathbb{Q}}), \rho_{E,36}(G_{\mathbb{Q}})] = [\mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z}), \mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z})]$.*

Let $\mathcal{E}_\ell$ be the set of modular curves whose rational points correspond to j-invariants of elliptic curves E for which $\rho_{E,\ell}$ is not surjective. Then we have seen in Section 1.2.3 that

$$\mathcal{E}_\ell \subseteq \left\{X_0(\ell), X^+_{\text{split}}(\ell), X^+_{\text{non-split}}(\ell), X_{A_4}(\ell), X_{S_4}(\ell), X_{A_5}(\ell)\right\} \tag{3.1.3}$$

where each of the modular curves $X_{A_4}(\ell)$, $X_{S_4}(\ell)$, and $X_{A_5}(\ell)$ corresponding to the exceptional groups A_4, S_4 and A_5 only occurs for certain primes ℓ. We have then

$$\bigcup_{\ell \text{ prime}} \mathcal{E}_\ell \subseteq \mathcal{X}.$$

If $\rho_{E,\ell}$ is surjective for all primes ℓ and E is not a Serre curve then by Proposition 3.1.4 the obstruction must be coming from the mod 36 representation. By Corollary 1.2.4 we have that if $\rho_{E,\ell}$ is surjective then so is the ℓ-adic representation ρ_{E,ℓ^∞}, however this is not necessarily true for $\ell = 2, 3$. These obstructions are described by two other modular curves $X'(4)$ and $X''(4)$ of level 4, and another $X'(9)$ of level 9, which have been considered in [DD12] and [Elk06], respectively.

Here we consider a modular curve $X'(6)$ of level 6 which, taken together with those listed above, completes the set $\mathcal{X}$ of modular curves occurring in (3.1.2), answering Question 3.1.3. Let $X(n)$ denote the complete modular curve of level n, and let $H \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ be a subgroup containing $-I$ for which the determinant map

$$\det\colon H \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$$

is surjective. Recall from Section 1.2.3 that for any $x \in \mathbb{P}^1(\mathbb{Q})$, we have that

$$x \in j(X_H(\mathbb{Q})) \iff \begin{array}{c}\exists \text{ an elliptic curve } E \text{ over } \mathbb{Q} \text{ and } \exists g \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \\ \text{with } j(E) = x \text{ and } \rho_{E,n}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) \subseteq g^{-1}Hg.\end{array} \tag{3.1.4}$$

Thus, to describe $X'(6)$, it suffices to describe the corresponding subgroup $H \subseteq \mathrm{GL}_2(\mathbb{Z}/6\mathbb{Z})$.

There is exactly one index 6 normal subgroup $\mathcal{N} \subseteq \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$, defined

by

$$\mathcal{N} := \left\{ \begin{pmatrix} x & -y \\ y & x \end{pmatrix} : \ x^2 + y^2 \equiv 1 \mod 3 \right\} \sqcup \left\{ \begin{pmatrix} x & y \\ y & -x \end{pmatrix} : \ x^2 + y^2 \equiv -1 \mod 3 \right\}. \quad (3.1.5)$$

This subgroup fits into an exact sequence

$$1 \longrightarrow \mathcal{N} \longrightarrow \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \longrightarrow 1, \quad (3.1.6)$$

and we denote by

$$\theta \colon \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \quad (3.1.7)$$

the (non-canonical) surjective map in the above sequence. We take $H \subseteq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ to be the graph of θ, viewed as a subgroup of $\mathrm{GL}_2(\mathbb{Z}/6\mathbb{Z})$ via the Chinese Remainder Theorem. The modular curve $X'(6)$ is then defined by

$$X'(6) := X_{H'_6}, \ \text{ where } \ H'_6 := \{(g_2, g_3) \in \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) : g_2 = \theta(g_3)\} \subseteq \mathrm{GL}_2(\mathbb{Z}/6\mathbb{Z}). \quad (3.1.8)$$

Unravelling (3.1.4) in this case, we find that, for every elliptic curve E over $\mathbb{Q}$,

$$j(E) \in j(X'(6)(\mathbb{Q})) \iff E \simeq_{\overline{\mathbb{Q}}} E' \ \text{ for some } E' \text{ over } \mathbb{Q} \text{ for which } \mathbb{Q}(E'[2]) \subseteq \mathbb{Q}(E'[3]). \quad (3.1.9)$$

By considering the geometry of the natural map $X'(6) \longrightarrow X(1)$, the curve $X'(6)$ is seen to have genus zero and one cusp. Since $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the

cusps, the single cusp must be defined over $\mathbb{Q}$, thus endowing $X'(6)$ with a rational point. Therefore $X'(6) \simeq_{\mathbb{Q}} \mathbb{P}^1$. We prove the following theorem, which gives an explicit model of $X'(6)$.

Theorem 3.1.5. *There exists a parameter $t\colon X'(6) \longrightarrow \mathbb{P}^1$, whose inverse is a uniformizer at the cusp, and which has the property that*

$$j = 2^{10}3^3t^3(1-4t^3),$$

where $j\colon X'(6) \longrightarrow X(1) \simeq \mathbb{P}^1$ is the usual j-map.

Remark 3.1.6. By (3.1.9), Theorem 3.1.5 is equivalent to the following statement: for any elliptic curve E over $\mathbb{Q}$, E is isomorphic over $\overline{\mathbb{Q}}$ to an elliptic curve E' satisfying

$$\mathbb{Q}(E'[2]) \subseteq \mathbb{Q}(E'[3])$$

if and only if $j(E) = 2^{10}3^3t^3(1-4t^3)$ for some $t \in \mathbb{Q}$.

Furthermore, we prove the following theorem, which answers Question 3.1.3. For each prime ℓ, consider the set $\mathcal{G}_{\ell,\max}$ of maximal proper subgroups of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$, which surject via determinant onto $(\mathbb{Z}/\ell\mathbb{Z})^\times$:

$$\mathcal{G}_{\ell,\max} := \{H \subsetneq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) :\ \det(H) = (\mathbb{Z}/\ell\mathbb{Z})^\times \\ \text{and } \nexists H_1 \text{ with } H \subsetneq H_1 \subsetneq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})\}. \quad (3.1.10)$$

The group $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ acts on $\mathcal{G}_{\ell,\max}$ by conjugation, and let $\mathcal{R}_\ell$ be a set of representatives of $\mathcal{G}_{\ell,\max}$ modulo this action. By (3.1.4), the collection $\mathcal{X}$ occurring in (3.1.2) must contain as a subset

$$\mathcal{E}_\ell := \{X_H :\ H \in \mathcal{R}_\ell\}, \quad (3.1.11)$$

the set of modular curves attached to subgroups $H \in \mathcal{R}_\ell$ (this gives a more precise description of the set $\mathcal{E}_\ell$ in (3.1.3)). Furthermore, the previously mentioned modular curves $X'(4)$, $X''(4)$, and $X'(9)$ correspond to the following

subgroups. Let $\varepsilon : \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \longrightarrow \{\pm 1\}$ denote the unique non-trivial character, and we will view $\det\colon \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \longrightarrow (\mathbb{Z}/4\mathbb{Z})^\times \simeq \{\pm 1\}$ as taking the values ± 1.

$$\begin{aligned} X'(4) = X_{H_4'}, \quad \text{where} \quad H_4' &:= \{g \in \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) : \\ &\qquad \det g = \varepsilon(g \bmod 2)\} \subseteq \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}), \\ X''(4) = X_{H_4''} \quad \text{where} \quad H_4'' &:= \left\langle \begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\rangle \subseteq \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}), \\ X'(9) = X_{H_9'} \quad \text{where} \quad H_9' &:= \left\langle \begin{pmatrix} 0 & 2 \\ 4 & 0 \end{pmatrix}, \begin{pmatrix} 4 & 1 \\ -3 & 4 \end{pmatrix}, \right. \\ &\qquad \left. \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle \subseteq \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z}). \end{aligned} \tag{3.1.12}$$

For more details on these modular curves, see [DD12] and [Elk06].

Theorem 3.1.7. *Let $\mathcal{X}$ be defined by*

$$\mathcal{X} = \{X'(4), X''(4), X'(9), X'(6)\} \cup \bigcup_{\ell \text{ prime}} \mathcal{E}_\ell,$$

where $X'(4)$, $X''(4)$ and $X'(9)$ are defined by (3.1.12)*, $X'(6)$ is defined by* (3.1.8)*, and $\mathcal{E}_\ell$ is as in* (3.1.11)*. Then, for any elliptic curve E over $\mathbb{Q}$,*

$$E \text{ is not a Serre curve} \iff j(E) \in \bigcup_{X \in \mathcal{X}} j(X(\mathbb{Q})).$$

3.2 Proofs

We now prove Theorems 3.1.5 and 3.1.7.

Proof of Theorem 3.1.5. Consider the elliptic curve $\mathbb{E}$ over $\mathbb{Q}(t)$ given by

$$\mathbb{E}:\ y^2 = x^3 + 3t\left(1-4t^3\right)x + \left(1-4t^3\right)\left(\frac{1}{2}-4t^3\right),$$

with discriminant and j-invariant $\Delta_{\mathbb{E}}, j(\mathbb{E}) \in \mathbb{Q}(t)$ given, respectively, by

$$\Delta_{\mathbb{E}} = -2^6 3^3 (1-4t^3)^2 \quad \text{and} \quad j(\mathbb{E}) = 2^{10}3^3 t^3 (1-4t^3). \tag{3.2.1}$$

For every $t \in \mathbb{Q}$, the specialization $\mathbb{E}_t$ is an elliptic curve over $\mathbb{Q}$ whose discriminant $\Delta_{\mathbb{E}_t} \in \mathbb{Q}$ and j-invariant $j(\mathbb{E}_t) \in \mathbb{Q}$ are given by evaluating (3.2.1) at t. We will show that, for any $t \in \mathbb{Q}$, one has

$$\mathbb{Q}(\mathbb{E}_t[2]) \subseteq \mathbb{Q}(\mathbb{E}_t[3]). \tag{3.2.2}$$

By (3.1.9) and (3.2.1), it then follows that

$$\forall t \in \mathbb{Q}, \quad 2^{10}3^3 t^3 (1-4t^3) \in j(X'(6)(\mathbb{Q})).$$

Since the natural j-map $j\colon X'(6) \longrightarrow \mathbb{P}^1$ and the map $t \mapsto 2^{10}3^3t^3(1-4t^3)$ both have degree 6, Theorem 3.1.5 will then follow. To verify (3.2.2), we will show that, for every $t \in \mathbb{Q}$, one has

$$\mathbb{Q}(\mathbb{E}_t[2]) \subseteq \mathbb{Q}(\zeta_3, \Delta_{\mathbb{E}_t}^{1/3}). \tag{3.2.3}$$

It is a classical fact that, for any elliptic curve E over $\mathbb{Q}$, one has $\mathbb{Q}(\zeta_3, \Delta_E^{1/3}) \subseteq \mathbb{Q}(E[3])$ (for details, see for instance [LT74, p. 181] and the references given there). Thus, the containment (3.2.2) follows from (3.2.3). Finally, (3.2.3) follows immediately from the factorization

$$(x-e_1(t))\,(x-e_2(t))\,(x-e_3(t)) = x^3 + 3t\left(1-4t^3\right)x + \left(1-4t^3\right)\left(\frac{1}{2}-4t^3\right)$$

of the 2-division polynomial $x^3+3t\left(1-4t^3\right)x+\left(1-4t^3\right)\left(\frac{1}{2}-4t^3\right)$, where

$$\begin{aligned} e_1(t) &:= \frac{1}{6}\Delta_{\mathbb{E}_t}^{1/3} + \frac{t}{18(1-4t^3)}\Delta_{\mathbb{E}_t}^{2/3}, \\ e_2(t) &:= \frac{\zeta_3}{6}\Delta_{\mathbb{E}_t}^{1/3} + \frac{\zeta_3^2 t}{18(1-4t^3)}\Delta_{\mathbb{E}_t}^{2/3}, \quad \text{and} \\ e_3(t) &:= \frac{\zeta_3^2}{6}\Delta_{\mathbb{E}_t}^{1/3} + \frac{\zeta_3 t}{18(1-4t^3)}\Delta_{\mathbb{E}_t}^{2/3}. \end{aligned}$$

This finishes the proof of Theorem 3.1.5. □

Remark 3.2.1. Our proof shows that, viewing $\mathbb{E}_t$ as an elliptic curve over $\mathbb{Q}(t)$, we have a containment of function fields

$$\mathbb{Q}(t)(\mathbb{E}_t[2]) \subseteq \mathbb{Q}(t)(\mathbb{E}_t[3]).$$

We will now turn to Theorem 3.1.7, whose proof employs the following group theoretic lemma. Recall from Section 1.2.2 that if ψ is the abbreviation for the ordered pair (ψ_0, ψ_1), then the group G given by

$$G_1 \times_\psi G_2 := \{(g_1, g_2) \in G_1 \times G_2 : \psi_1(g_1) = \psi_2(g_2)\} \tag{3.2.4}$$

is called the *fibered product of* G_0 *and* G_1 *over* ψ, and is commonly denoted by $G_0 \times_\psi G_1$. Notice that, for a surjective group homomorphism $f\colon Q \to Q_1$, if $f \circ \psi$ denotes the ordered pair $(f \circ \psi_0, f \circ \psi_1)$ and $G_0 \times_{f\circ\psi} G_1$ denotes the corresponding fibered product, then one has

$$G_0 \times_\psi G_1 \subseteq G_0 \times_{f\circ\psi} G_1. \tag{3.2.5}$$

Lemma 3.2.2. *Let* G_0 *and* G_1 *be groups, let* $\psi_0\colon G_0 \to Q$ *and* $\psi_1\colon G_1 \to Q$ *be a pair of surjective homomorphisms onto a common quotient group* Q*, and let* $H = G_0 \times_\psi G_1$ *be the associated fibered product. If* Q *is cyclic, then*

one has the following equality of commutator subgroups:

$$[H, H] = [G_0, G_0] \times [G_1, G_1].$$

Proof. See [LT74, Lemma 1, p. 174] (the hypothesis of this lemma is readily verified when Q is cyclic). □

Proof of Theorem 3.1.7. Using Proposition 3.1.4 one has

$$E \text{ is not a Serre curve} \iff \begin{array}{c} \exists \text{ a prime } \ell \geq 5 \text{ with} \\ \rho_{E,\ell}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) \subsetneq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}), \\ \text{or } [\rho_{E,36}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})), \rho_{E,36}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))] \\ \subsetneq [\mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z}), \mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z})]. \end{array}$$

For each divisor d of 36, let

$$\pi_{36,d} \colon \mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/d\mathbb{Z}) \tag{3.2.6}$$

denote the canonical projection. One checks that, for $\ell \in \{2, 3\}$, any proper subgroup $H \subsetneq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ for which $\det(H) = (\mathbb{Z}/\ell\mathbb{Z})^\times$ must satisfy $[H, H] \subsetneq [\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}), \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})]$. We then define

$$\mathcal{G}_{36} := \left\{ H \subseteq \mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z}) : \begin{array}{c} \forall d \in \{2, 3\},\ \pi_{36,d}(H) = \mathrm{GL}_2(\mathbb{Z}/d\mathbb{Z}), \\ \det(H) = (\mathbb{Z}/36\mathbb{Z})^\times, \\ \text{and } [H, H] \subsetneq [\mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z}), \mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z})] \end{array} \right\}, \tag{3.2.7}$$

and note that

$$E \text{ is not a Serre curve} \iff \begin{array}{c} \exists \text{ a prime } \ell \text{ and } H \in \mathcal{G}_{\ell,\max} \text{ for which} \\ \rho_{E,\ell}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) \subseteq H, \\ \text{or } \exists H \in \mathcal{G}_{36} \text{ for which} \\ \rho_{E,36}(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) \subseteq H. \end{array} \tag{3.2.8}$$

As in the prime level case, we need only consider *maximal* subgroups $H \in \mathcal{G}_{36}$, and because of (3.1.4), only up to conjugation by $\mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z})$. Thus, we put

$$\mathcal{G}_{36,\max} := \{H \in \mathcal{G}_{36} : \nexists H_1 \in \mathcal{G}_{36} \text{ with } H \subsetneq H_1 \subsetneq \mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z})\},$$

we let $\mathcal{R}_{36} \subseteq \mathcal{G}_{36,\max}$ be a set of representatives of $\mathcal{G}_{36,\max}$ modulo $\mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z})$-conjugation, and we set

$$\mathcal{E}_{36} := \{X_H : H \in \mathcal{R}_{36}\}.$$

The equivalence (3.2.8) now becomes (see (3.1.11))

$$E \text{ is not a Serre curve} \iff \begin{array}{r} \exists \text{ a prime } \ell \text{ and } X_H \in \mathcal{E}_\ell \text{ for which} \\ j(E) \in j(X_H(\mathbb{Q})), \text{or } \exists X_H \in \mathcal{E}_{36} \text{ for which} \\ j(E) \in j(X_H(\mathbb{Q})). \end{array}$$

Thus, Theorem 3.1.7 will follow from the next proposition.

Proposition 3.2.3. *With the above notation, one may take*

$$\mathcal{R}_{36} = \{\pi_{36,4}^{-1}(H_4'), \pi_{36,4}^{-1}(H_4''), \pi_{36,9}^{-1}(H_9'), \pi_{36,6}^{-1}(H_6')\},$$

where $\pi_{36,d}$ is as in (3.2.6) *and the groups H_4', H_4'', H_9' and H_6' are given by* (3.1.12) *and* (3.1.8).

Proof. Let $H \in \mathcal{G}_{36,\max}$. If $\pi_{36,4}(H) \neq \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$, then [DD12] shows that $\pi_{36,4}(H) \subseteq H_4'$ or $\pi_{36,4}(H) \subseteq H_4''$, up to conjugation in $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$. If $\pi_{36,9}(H) \neq \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$, then [Elk06] shows that, up to $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$-conjugation, one has $\pi_{36,9}(H) \subseteq H_9'$. Thus, we may now assume that $\pi_{36,4}(H) = \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ and $\pi_{36,9}(H) = \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$. By Lemma 1.2.7, this implies that there exists

a group Q and a pair of surjective homomorphisms

$$\begin{aligned}\psi_4 &\colon \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \longrightarrow Q\\ \psi_9 &\colon \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z}) \longrightarrow Q\end{aligned}$$

for which $H = \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \times_\psi \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$. We will now show that in this case, up to $\mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z})$-conjugation, we have

$$H \subseteq \{(g_4, g_9) \in \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \times \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z}) : \ \theta(g_9 \bmod 3) = g_4 \bmod 2\}, \tag{3.2.9}$$

where $\theta\colon \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ is the map given in (3.1.7), whose graph determines the level 6 structure defining the modular curve $X'(6)$. This will finish the proof of Proposition 3.2.3.

Let us make the following definitions:

$$\begin{aligned} N_4 &:= \ker \psi_4 \subseteq \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}), & N_9 &:= \ker \psi_9 \subseteq \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})\\ N_2 &:= \pi_{4,2}(N_4) \subseteq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}), & N_3 &:= \pi_{9,3}(N_9) \subseteq \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})\\ Q_2 &:= \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})/N_2, & Q_3 &:= \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})/N_3, \end{aligned}$$

where $\pi_{4,2}\colon \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ and $\pi_{9,3}\colon \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ denote the canonical projections. We then have the following exact sequences:

$$\begin{aligned} 1 &\longrightarrow N_9 \longrightarrow \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z}) \longrightarrow Q \longrightarrow 1\\ 1 &\longrightarrow N_4 \longrightarrow \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \longrightarrow Q \longrightarrow 1\\ 1 &\longrightarrow N_3 \longrightarrow \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) \longrightarrow Q_3 \longrightarrow 1\\ 1 &\longrightarrow N_2 \longrightarrow \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \longrightarrow Q_2 \longrightarrow 1, \end{aligned} \tag{3.2.10}$$

as well as

$$\begin{aligned} 1 &\longrightarrow K_2 \longrightarrow Q \longrightarrow Q_2 \longrightarrow 1\\ 1 &\longrightarrow K_3 \longrightarrow Q \longrightarrow Q_3 \longrightarrow 1, \end{aligned} \tag{3.2.11}$$

where for each $\ell \in \{2,3\}$, the kernel $K_\ell \simeq \dfrac{\ker \pi_{\ell^2,\ell}}{N_{\ell^2} \cap \ker \pi_{\ell^2,\ell}} \subseteq \dfrac{\mathrm{GL}_2(\mathbb{Z}/\ell^2\mathbb{Z})}{N_{\ell^2}} \simeq Q$ is evidently abelian (since $\ker \pi_{\ell^2,\ell}$ is), and has order dividing $\ell^4 = |\ker \pi_{\ell^2,\ell}|$. We will proceed to prove that

$$Q_2 \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \quad \text{and} \quad Q_3 \simeq Q, \tag{3.2.12}$$

which is equivalent to

$$N_4 \subseteq \ker \pi_{4,2} \quad \text{and} \quad \ker \pi_{9,3} \subseteq N_9.$$

Writing $\tilde{\psi}_4 \colon \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \to Q \to Q_2 \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ and $\tilde{\psi}_9 \colon \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z}) \to Q \to Q_2 \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$, we then see by (3.2.5) that

$$H = \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \times_\psi \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z}) \subseteq \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \times_{\tilde{\psi}} \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z}).$$

Furthermore, it follows from $Q \simeq Q_3$ that $\tilde{\psi}_9$ factors through the projection $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$. This, together with the uniqueness of $\mathcal{N}$ in (3.1.6) and the fact that every automorphism of $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ is inner, implies that (3.2.9) holds, up to $\mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z})$-conjugation. Thus, the proof of Proposition 3.2.3 is reduced to showing that (3.2.12) holds.

We will first show that $Q_2 \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$. Suppose on the contrary that $Q_2 \subsetneq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$. Looking at the first exact sequence in (3.2.11), we see that Q must then be a 2-group, and since K_3 has order a power of 3 (possibly 1), we see that $Q \simeq Q_3$, and the third exact sequence in (3.2.10) becomes

$$1 \longrightarrow N_3 \longrightarrow \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) \longrightarrow Q \longrightarrow 1.$$

The kernel N_3 must contain an element σ of order 3, and by considering $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$-conjugates of σ, we find that $|N_3| \geq 8$. Since 3 also divides $|N_3|$, we see that $|N_3| \geq 12$, and so Q must be abelian, having order at most 4. Furthermore, since $[\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}), \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})] = \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$, we find that Q

has order at most 2, and thus is cyclic. Applying Lemma 3.2.2, we find that $[H, H] = [\mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z}), \mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z})]$, contradicting (3.2.7). Thus, we must have that $Q_2 \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$.

We will now show that $Q_3 \simeq Q$. To do this, we will first take a more detailed look at the structure of the group $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$. Note the embedding of groups $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \hookrightarrow \mathrm{GL}_2(\mathbb{Z})$ given by

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \mapsto \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix},$$
$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}.$$

This embedding, followed by reduction modulo 4, splits the exact sequence

$$1 \to \ker \pi_{4,2} \to \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \to 1.$$

Also note the isomorphism $(\ker \pi_{4,2}, \cdot) \to (M_{2\times 2}(\mathbb{Z}/2\mathbb{Z}), +)$ given by $I + 2A \mapsto A \pmod 2$. These two observations realize $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ as a semi-direct product

$$\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \ltimes M_{2\times 2}(\mathbb{Z}/2\mathbb{Z}), \tag{3.2.13}$$

where the right-hand factor is an additive group and the action of $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ on $M_{2\times 2}(\mathbb{Z}/2\mathbb{Z})$ is by conjugation. Since $Q_2 \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$, we see that, under (3.2.13), one has

$$N_4 \subseteq M_{2\times 2}(\mathbb{Z}/2\mathbb{Z}),$$

and since it is a normal subgroup of $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$, we see that N_4 must be a $\mathbb{Z}/2\mathbb{Z}$-subspace which is invariant under $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$-conjugation. This

implies that we must be in one of the following 5 cases.

N_4	Q
$M_{2\times 2}(\mathbb{Z}/2\mathbb{Z})$	$\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$
$\{A \in M_{2\times 2}(\mathbb{Z}/2\mathbb{Z}) : \mathrm{tr}A = 0\}$	$\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \times \{\pm 1\}$
$\left\{\begin{pmatrix}0&0\\0&0\end{pmatrix}, \begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\1&0\end{pmatrix}, \begin{pmatrix}0&1\\1&1\end{pmatrix}\right\}$	$\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \ltimes (\mathbb{Z}/2\mathbb{Z})^2$
$\left\{\begin{pmatrix}0&0\\0&0\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\1&1\end{pmatrix}, \begin{pmatrix}0&1\\1&0\end{pmatrix}\right\}$	$\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \ltimes (\mathbb{Z}/2\mathbb{Z})^2$
$\left\{\begin{pmatrix}0&0\\0&0\end{pmatrix}, \begin{pmatrix}1&0\\0&1\end{pmatrix}\right\}$	$\mathrm{PGL}_2(\mathbb{Z}/4\mathbb{Z})$

(We have omitted from the table the case that N_4 is trivial, since then $Q \simeq \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$, which has order $2^5 \cdot 3$ and thus cannot be a quotient of $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$.) In the third row of the table, the action of $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ on $(\mathbb{Z}/2\mathbb{Z})^2$ defining the semi-direct product is the usual action by matrix multiplication on column vectors, while in the fourth row of the table, the action is defined via

$$g \cdot \begin{pmatrix}x\\y\end{pmatrix} = \begin{cases} \begin{pmatrix}x\\y\end{pmatrix} & \text{if } g \in \left\{\begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\1&0\end{pmatrix}, \begin{pmatrix}0&1\\1&1\end{pmatrix}\right\}, \\ \begin{pmatrix}y\\x\end{pmatrix} & \text{if } g \in \left\{\begin{pmatrix}1&1\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\1&1\end{pmatrix}, \begin{pmatrix}0&1\\1&0\end{pmatrix}\right\}. \end{cases}$$

Since 9 does not divide $|Q|$, the degree of the projection $Q \twoheadrightarrow Q_3$ is either 1 or 3. Inspecting the table above, we see that in all cases except $Q = \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$, either Q has no normal subgroup of order 3, or for each normal subgroup $K_3 \trianglelefteq Q$ of order 3, $Q_3 \simeq Q/K_3$ has $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ as a quotient group. Since $[\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}), \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})] = \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$, the group $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ cannot have $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ as a quotient group, and so we must have $Q \simeq Q_3$ in these

cases, as desired.

When $Q = \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$, we must proceed differently. Suppose that $Q = \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ and (for the sake of contradiction) that $Q \neq Q_3$, so that the projection $Q \twoheadrightarrow Q_3$ has degree 3. Then $Q_3 \simeq \mathbb{Z}/2\mathbb{Z}$, which implies that $N_3 = \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$, so that

$$N_9 \subseteq \pi_{9,3}^{-1}(\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})) \subseteq \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z}).$$

Furthermore, the quotient group $\pi_{9,3}^{-1}(\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z}))/N_9 \simeq \mathbb{Z}/3\mathbb{Z}$, and in particular is abelian. A commutator calculation shows that

$$[\pi_{9,3}^{-1}(\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})), \pi_{9,3}^{-1}(\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z}))] = \pi_{9,3}^{-1}(\mathcal{N}) \cap \mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z}),$$

(see (3.1.5)) and that the corresponding quotient group satisfies

$$\pi_{9,3}^{-1}(\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z}))/[\pi_{9,3}^{-1}(\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})), \pi_{9,3}^{-1}(\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z}))] \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

Furthermore, fixing a pair of isomorphisms

$$\begin{aligned}
\eta_1 &\colon \left(\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \right\}, \cdot \right) \longrightarrow (\mathbb{Z}/3\mathbb{Z}, +), \\
\eta_2 &\colon (1 + 3 \cdot \mathbb{Z}/9\mathbb{Z}, \cdot) \longrightarrow (\mathbb{Z}/3\mathbb{Z}, +),
\end{aligned}$$

and defining the characters

$$\begin{aligned}
\chi_1 &\colon \pi_{9,3}^{-1}(\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})) \longrightarrow \mathbb{Z}/3\mathbb{Z}, \\
\chi_2 &\colon \pi_{9,3}^{-1}(\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})) \longrightarrow \mathbb{Z}/3\mathbb{Z}
\end{aligned}$$

by $\chi_1 = \eta_1 \circ \theta \circ \pi_{9,3}$ and $\chi_2 = \eta_2 \circ \det$, we have that every homomorphism $\chi \colon \pi_{9,3}^{-1}(\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})) \to \mathbb{Z}/3\mathbb{Z}$ must satisfy

$$\chi = a_1\chi_1 + a_2\chi_2,$$

for appropriately chosen $a_1, a_2 \in \mathbb{Z}/3\mathbb{Z}$. In particular,

$$N_9 = \ker(a_1\chi_1 + a_2\chi_2) \tag{3.2.14}$$

for some choice of $a_1, a_2 \in \mathbb{Z}/3\mathbb{Z}$. One checks that

$$\exists g \in \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z}),\ x \in \pi_{9,3}^{-1}(\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z}))\ \text{ for which }\ \chi_1(gxg^{-1}) \neq \chi_1(x),$$

whereas $\chi_2(gxg^{-1}) = \chi_2(x)$ for any such choice of g and x. Since N_9 is a normal subgroup of $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$, it follows that $a_1 = 0, a_2 \neq 0$ in (3.2.14). This implies that $N_9 = \mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$, which contradicts the fact that $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})/N_9 \simeq Q \simeq \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ is non-abelian. This contradiction shows that we must have $Q \simeq Q_3$, and this verifies (3.2.12), completing the proof of Proposition 3.2.3. □

As already observed, the proof of Proposition 3.2.3 completes the proof of Theorem 3.1.7. □

3.3 Elliptic curves without abelian entanglements

Let us study in more detail one example coming from the family of curves in Theorem 3.1.5. Consider the curve $E/\mathbb{Q}$ given by minimal Weierstrass equation $Y^2 = X^3 - 63504X + 6223392$. This curve has $j(E) = -2^{10}3^4$, as well as $\Delta = -2^4 3^{11} 7^6$. Machine computation shows that $G(\ell) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ and $\mathbb{Q}(E[2]) \subset \mathbb{Q}(E[3])$. We also have that $\mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{-3})$, which is what we expect since the maximal abelian extension inside $\mathbb{Q}(E[3])$ is precisely $\mathbb{Q}(\sqrt{-3})$.

Suppose we wish to compute the conjectural density of primes p such that $\tilde{E}(\mathbb{F}_p)$ is cyclic. As we have seen, the naive density of this is $\prod_\ell \delta_\ell$, however a correction factor is needed. As the only critical primes are $2, 3$

and 7, the density we are looking for is

$$C_E = \frac{|G(42) \cap \mathcal{S}_{42}|}{G(42)|} \prod_{\ell \neq 2,3,7} \delta_\ell,$$

where we are using the notation of Section 2.4. Now $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ and $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$ have no simple non-abelian quotients, hence any entanglement between the fields $\mathbb{Q}(E[3])$ and $\mathbb{Q}(E[7])$ would have to contain a non-trivial abelian subfield. However the maximal abelian extensions of $\mathbb{Q}(E[3])$ and $\mathbb{Q}(E[7])$ are $\mathbb{Q}(\zeta_3)$ and $\mathbb{Q}(\zeta_7)$, hence we conclude $\mathbb{Q}(E[3]) \cap \mathbb{Q}(E[7]) = \mathbb{Q}$. This implies that $G(42) = G(6) \times G(7)$, hence

$$C_E = \frac{|G(6) \cap \mathcal{S}_6|}{|G(6)|} \prod_{\ell \neq 2,3} \delta_\ell,$$

Finally, note that because $G(6) = G(3)$ and $G(2)$ is a quotient of $G(6)$, then

$$\frac{|G(6) \cap \mathcal{S}_6|}{|G(6)|} = \frac{|S(2)|}{|G(2)|}.$$

Using machine computation we find that the observed density of primes $p \leqslant 100000000$ is 0.831069 while our computation yields

$$\begin{aligned} C_E &= \prod_{\ell \neq 3} \delta_\ell \\ &\approx 0.831066. \end{aligned}$$

As mentioned in the introduction, another natural question which arises from this is whether one can one classify the triples (E, m_1, m_2) with E an elliptic curve over $\mathbb{Q}$ and m_1, m_2 a pair of coprime integers for which the entanglement field $\mathbb{Q}(E[m_1]) \cap \mathbb{Q}(E[m_2])$ is non-abelian over $\mathbb{Q}$. We are not sure if any other families exist, however one systematic way one could possibly rule out other examples is via the following steps.

(i) Classify the non-abelian groups which arise as common quotients of subgroups H_{m_1} and H_{m_2}, where $H_{m_i} \subset \mathrm{GL}_2(\mathbb{Z}/m_i\mathbb{Z})$ and $\det(H_{m_i}) = (\mathbb{Z}/m_i\mathbb{Z})^\times$ for $i = 1, 2$.

(ii) For each example in step (i), compute the genus of the associated modular curve.

(iii) For each modular curve in step (ii), decide whether or not it has any rational points.

For each of these families of curves it would also be of interest to find a systematic way to compute their entanglement correction factors. For the family we have described here this is easy to do because one of the torsion fields is fully contained in another one. It may occur however, at least in theory, that a curve could have many non-abelian intersections between various of its torsion fields. However it seems unlikely many examples of this type exist.

Bibliography

[BP11] Yuri Bilu and Pierre Parent, *Serre's uniformity problem in the split Cartan case*, Ann. of Math. **173** (2011), no. 1, 569–584.

[BPR11] Yuri Bilu, Pierre Parent, and Marusia Rebolledo, *Rational points on $X_0^+(p^r)$*, arXiv:1104.4641, 2011.

[Bra09] J. Brau, *Congruence conditions on supersingular primes*, Master's thesis, Universiteit Leiden, 2009.

[Coh93] H. Cohen, *A course in computational algebraic number theory*, 2nd ed., Graduate Texts in Mathematics, vol. 138, Springer-Verlag, 1993.

[DD12] T. Dokchitser and V. Dokchitser, *Surjectivity of mod 2^n representations of elliptic curves*, Math. Z. **272** (2012), 961–964.

[DR73] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular Functions of One Variable II, vol. 349, 1973, pp. 143–316.

[Elk06] N. Elkies, *Elliptic curves with 3-adic Galois representation surjective mod 3 but not mod 9*, preprint, 2006.

[GJ11] A.C. Cojocaru, D. Grant and N. Jones, *One-parameter families of elliptic curves over $\mathbb{Q}$ with maximal Galois representations*, Proc. Lond. Math. Soc. **103** (2011), no. 3, 654–675.

[Hoo67] C. Hooley, *On Artin's conjecture for primitive roots*, J. Reine Angew. Math. **225** (1967), 209–220.

[Jon] N. Jones, *GL_2-representations with maximal image*, To appear in Math. Res. Lett.

[Jon10] Nathan Jones, *Almost all elliptic curves are Serre curves*, Trans. Amer. Math. Soc. (2010), no. 362, 1547–1570.

[Kob88] Neil Koblitz, *Primality of the number of points on an elliptic curve over a finite field*, Pacific J. Math. **131** (1988), no. 1, 157–168.

[Lan02] S. Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, 2002.

[Len77] H.W. Lenstra, *On Artin's conjecture and Euclid's algorithm in global fields*, Invent. Math. **42** (1977), 201–224.

[LMS14] H.W. Lenstra, P. Moree, and P. Stevenhagen, *Character sums for primitive root densities*, Math. Proc. of the Cambridge Philos. Soc. **157** (2014), 489–511.

[LT74] S. Lang and H. Trotter, *Frobenius distributions in GL_2-extensions*, Springer, 1974.

[LT77] ———, *Primitive points on elliptic curves*, Bull. Amer. Math. Soc. **83** (1977), 289–292.

[Maz78] Barry Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), no. 2, 129–162.

[Rad08] V. Radhakrishnan, *Asymptotic formula for the number of non-Serre curves in a two-parameter family*, Ph.D. thesis, University of Colorado at Boulder, 2008.

[RZB14] J. Rouse and D. Zureick-Brown, *Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois*, arXiv:1402.5997, 2014.

[Ser64] J.-P. Serre, *Groupes de Lie ℓ-Adiques Attachés aux Courbes Elliptique*, Colloque de Clermont-Ferrand, IHES (1964).

[Ser68] J.-P Serre, *Abelian ℓ-adic representations and elliptic curves*, Benjamin, 1968.

[Ser72] ———, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Inventiones mathematicae **15** (1972), 259–331.

[Ser73] Jean-Pierre Serre, *A course in arithmetic*, Springer-Verlag, 1973.

[Ser81] ———, *Quelques applications du théoréme de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math. **54** (1981), 323–401.

[Ser86] ———, *Resumé de cours de 1977-1978*, Oeuvres, Springer, 1986.

[Sil09] J. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Springer, 2009.

[Ste03] Peter Stevenhagen, *The correction factor in Artin's primitive root conjecture*, J. Théor. Nombres Bordeaux **15** (2003), no. 1, 383–391.

[Sut13] Andrew V. Sutherland, *Computing the image of Galois representations attached to an elliptic curve*, `http://math.mit.edu/~drew/AMSEast2013.pdf`, 2013.

[Zyw10] D. Zywina, *Elliptic curves with maximal Galois action on their torsion points*, Bull. Lond. Math. Soc. **42** (2010), 811–826.

[Zyw11a] David Zywina, *Bounds for Serre's open image theorem*, arXiv:1102.4656, 2011.

[Zyw11b] ———, *On the surjectivity of mod ℓ representations associated to elliptic curves*, `http://www.mast.queensu.ca/~zywina/papers/EffectiveModl.pdf`, 2011.

[Zyw11c] ———, *A refinement of Koblitz's conjecture*, Int. J. Number Theory **7** (2011), no. 3, 739–769.

Summary

This thesis deals primarily with the study of Galois representations attached to torsion points on elliptic curves. In the first chapter we consider the problem of determining the image of the Galois representation ρ_E attached to a non-CM elliptic curve over the rational number field $\mathbb{Q}$. We give a deterministic algorithm that determines the image of ρ_E as a subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, where the output is given as an integer m together with a finite subgroup $G(m) \subset \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. The image of ρ_E is then the subgroup of all elements of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ whose reduction modulo m belongs to $G(m)$.

In the second part we develop a method using character sums that uses the image of ρ_E to describe densities of sets of primes p for which $\tilde{E}(\mathbb{F}_p)$ has certain prescribed properties. If E is an elliptic curve over $\mathbb{Q}$, then it follows by work of Serre and Hooley that, under the assumption of the Generalized Riemann Hypothesis, the density of primes p such that the group of $\mathbb{F}_p$-rational points of the reduced curve $\tilde{E}(\mathbb{F}_p)$ is cyclic can be written as an infinite product $\prod \delta_\ell$ of local factors δ_ℓ reflecting the degree of the ℓ-torsion fields, multiplied by a factor that corrects for the entanglements between the various torsion fields. We show that this correction factor can be interpreted as a character sum, and the resulting description allows us to easily determine non-vanishing criteria for it. We apply our character sum method to a variety of other settings. Among these, we consider the aforementioned problem with the additional condition that the

primes p lie in a given arithmetic progression. We also study the conjectural constants appearing in Koblitz's conjecture, a conjecture which relates to the density of primes p for which the cardinality of the group of $\mathbb{F}_p$-points of E is prime. The unifying theme in all these settings is that the constants we are interested in are completely determined by the image of ρ_E.

The final chapter deals with the classification of non-Serre curves. An elliptic curve over $\mathbb{Q}$ is a *Serre curve* if its attached Galois representation is as large as possible, and it is known that most elliptic curves over $\mathbb{Q}$ are of this type. We exhibit a modular curve of level 6 that completes a set of modular curves which parametrise non-Serre curves. This modular curve also gives an infinite family of elliptic curves with non-abelian "entanglement fields". Exhibiting such a family is naturally motivated by questions arising in the previous chapter regarding the classification of elliptic curves to which we can apply the character sum method described above.

Samenvatting

Dit proefschrift richt zich in hoofdzaak op de studie van Galoisrepresentaties geassocieerd met de torsiepunten van elliptische krommen. In het eerste hoofdstuk beschouwen we het probleem om het beeld te bepalen van de Galoisrepresentatie ρ_E van een elliptische kromme zonder CM over het lichaam van de rationale getallen $\mathbb{Q}$. We geven een deterministische algoritme dat het beeld van ρ_E bepaalt als ondergroep van $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, waarbij de output gegeven wordt als een geheel getal m tesamen met een eindige ondergroep. Het beeld van ρ_E is dan de ondergroep van alle elementen van $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ waarvan de reductie modulo m to $G(m)$ behoort.

In het tweede deel ontwikkelen we een methode die van karaktersommen gebruik maakt om uitgaande van het beeld van ρ_E dichtheden te beschrijven van verzamelingen van priemen p waarvoor zekere voorgeschreven eigenschappen heeft. Als E een elliptische kromme over $\mathbb{Q}$ is, dan volgt uit werk van Serre en Hooley dat, onder aanname van de Gegeneraliseerde Riemannhypothese, de dichtheid van de verzameling priemen p waarvoor de groep van $\mathbb{F}_p$-rationale punten van de gereduceerde kromme cyclisch is, geschreven kan worden als een oneindig product $\prod \delta_\ell$ van locale factoren δ_ℓ die de graad van de ℓ-torsielichamen reflecteren, vermenigvuldigd met met een factor die corrigeert voor de verstrengeling tussen de torsielichamen. We laten zien dat deze correctiefactor geïnterpreteerd kan worden als een karaktersom, en de resulterende beschrijving stelt ons in staat om

op eenvoudige wijze criteria voor het verdwijnen van de correctiefactor te bepalen. We passen onze karaktersommethode toe in een aantal andere situaties. Hieronder is het hiervoor genoemde probleem met de aanvullende voorwaarde dat de priemen in een gegeven meetkundige reeks liggen. We bestuderen ook de vermoede constanten die voorkomen in een vermoeden van Koblitz betreffende de dichtheid van priemen waarvoor de cardinaliteit van de groep van $\mathbb{F}_p$-punten van E een priemgetal is. Het unificerende thema in al deze situaties is dat de constanten waarin we geïnteresseerd zijn, geheel bepaald worden door het beeld van ρ_E.

Het laatste hoofdstuk gaat in op de classificatie van niet-Serre-krommen. Een elliptische kromme over $\mathbb{Q}$ is een *Serre-kromme* als de ermee geassocieerde Galoisrepresentatie zo groot mogelijk is, en het is bekend dat de meeste elliptische krommen over $\mathbb{Q}$ van dit type zijn. We presenteren een modulaire kromme van niveau 6 die een verzameling van modulaire krommen die niet-Serre-krommen parmetriseren completeert. Deze modulaire kromme geeft ook een oneindige familie van elliptische krommen met niet-abelse "verstrengelingslichamen". Het aangeven van zo'n familie komt op natuurlijke wijze naar voren in relatie tot de vragen in het vorige hoofstuk met betrekking tot de classificatie van elliptische krommen waarvoor we de karaktersommethode toe kunnen passen.

Resume

Cette thèse étudie principalement les représentations galoisiennes attachées aux points de torsion des courbes elliptiques. Dans le premier chapitre, nous considérons le problème de déterminer l'image de la représentation ρ_E attachée à une courbe elliptique E définie sur $\mathbb{Q}$, sans multiplication complexe. Nous donnons un algorithme déterministe qui calcule l'image de ρ_E comme sous-groupe de $\mathrm{GL}_2(\widehat{\mathbb{Z}})$, dont la sortie est un entier m et un sous-groupe fini $G(m) \subset \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. L'image de ρ_E est le sous-groupe des éléments de $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ dont la réduction modulo m appartient à $G(m)$.

Dans une seconde partie, nous développons une méthode utilisant des sommes de caractères, qui exploite l'image de ρ_E pour décrire les densités d'ensembles de premiers p pour lesquels la courbe réduite $\tilde{E}(\mathbb{F}_p)$ a certaines propriétés. Si E est une courbe elliptique définie sur $\mathbb{Q}$, il suit des travaux de Serre et Hooley que, sous l'Hypothèse de Riemann Généralisée, la densité des premiers p tels que le groupe des points $\mathbb{F}_p$-rationnels de la courbe réduite $\tilde{E}(\mathbb{F}_p)$ est cyclique s'écrit comme un produit infini $\prod \delta_\ell$ de facteurs locaux δ_ℓ liés au degré du corps contenant la ℓ-torsion, multiplié par un facteur correctif prenant en compte l'intrication de ces différents corps. Nous montrons que ce facteur correctif s'interprète comme somme de caractères et cette description nous permet de déterminer facilement s'il s'annule ou non. Nous appliquons notre méthode à d'autres situations, par exemple en restreignant p à une progression arithmétique fixée. Nous étudions

aussi les constantes apparaissant dans la conjecture de Koblitz, liée à la densité des p pour lesquels le groupe des $\mathbb{F}_p$-points de E est un nombre premier. Dans toutes ces applications, le thème unificateur sous-jacent est que les densités étudiées sont entièrement déterminées par l'image de ρ_E.

Une courbe elliptique sur $\mathbb{Q}$ est une *courbe de Serre* si l'image de la représentation galoisienne associée est aussi grande que possible, et la plupart des courbes elliptiques définies sur $\mathbb{Q}$ sont de ce type. Notre dernier chapitre se préoccupe de la classification des courbes qui ne sont pas courbes de Serre : nous exhibons une courbe modulaire de niveau 6 qui complète la liste des courbes modulaires paramétrant ces courbes. Cette courbe modulaire définit aussi une famille infinie de courbes elliptiques dont les «corps d'intrication» sont non abéliens. Les questions en suspens après le chapitre précédent, sur la classification des courbes elliptiques auxquelles nous pouvons appliquer la méthode des sommes de caractères, fournissent une motivation supplémentaire pour cette famille.

Acknowledgements

I would like to express my gratitude to everyone who contributed in making this work possible. First and foremost I would like to thank Peter Stevenhagen. Without his constant encouragement, support and excellent guidance this work would not have been possible. Thank you also to Karim for being my co-supervisor, and for his hospitality while I was in Bordeaux.

I would like to express my gratitude to Hendrik Lenstra for his careful reading of the manuscript and for his many helpful comments and suggestions for improvements. Thank you as well to Tim Dokchister, Jaap Top, Bart de Smit and Marco Streng for being members of the examination committee. Thanks also to Nathan Jones for allowing me to use our joint work for the material in Chapter 3.

A big thank you to all my friends in Leiden who made this a great experience. A special thanks to Kolyan and Athananasios for all your help with the preparations. Finally, I would like to thank my family for their unwavering support and encouragement throughout these four years. Thanks to my parents Agustin and Lupita, to my brothers Ernesto and Agustin, and my nephew Ernesto. It is an understatement to say that I could not have done this without you.

Curriculum Vitae

Julio Brau Avila was born in Hermosillo, Mexico on September 17, 1985. He spent much of his childhood in Tucson, Arizona, and his teenage years in Mexico. He moved to Bordeaux as part of the first year of the Algant MSc program, and spent his second year in Leiden. Afterwards he completed Part III of the Math Tripos at the University of Cambridge. In his free time he enjoys cooking, playing chess and dancing tango.

Printed and Lay Out by: Proefschriftmaken.nl II Uitgeverij BOXPress
Published by: Uitgeverij BOXPress, 's-Hertogenbosch