



Universidad Autónoma
de Madrid

Biblos-e Archivo
Repositorio Institucional UAM

Repositorio Institucional de la Universidad Autónoma de Madrid

<https://repositorio.uam.es>

Esta es la **versión de autor** del artículo publicado en:
This is an **author produced version** of a paper published in:

Experimental Mathematics 31.2 (2022): 518-536

DOI: <https://doi.org/10.1080/10586458.2019.1655816>

Copyright: © 2019 Taylor & Francis Group, LLC.

El acceso a la versión del editor puede requerir la suscripción del recurso
Access to the published version may require subscription

SERRE'S CONSTANT OF ELLIPTIC CURVES OVER THE RATIONALS

HARRIS B. DANIELS AND ENRIQUE GONZÁLEZ-JIMÉNEZ

ABSTRACT. Let E be an elliptic curve without complex multiplication defined over the rationals. The purpose of this article is to define a positive integer $A(E)$, that we call the *Serre's constant associated to E* , that gives necessary conditions to conclude that $\rho_{E,m}$, the mod m Galois representation associated to E , is non-surjective. In particular, if there exists a prime factor p of m satisfying $\text{val}_p(m) > \text{val}_p(A(E)) > 0$ then $\rho_{E,m}$ is non-surjective. Conditionally under Serre's Uniformity Conjecture, we determine all the Serre's constants of elliptic curves without complex multiplication over the rationals that occur infinitely often. Moreover, we give all the possible combination of mod p Galois representations that occur for infinitely many non-isomorphic classes of non-CM elliptic curves over \mathbb{Q} , and the known cases that appear only finitely. We obtain similar results for the possible combination of maximal non-surjective subgroups of $\text{GL}_2(\mathbb{Z}_p)$. Finally, we conjecture all the possibilities of these combinations and in particular all the possibilities of these Serre's constant.

1. INTRODUCTION

Let E/\mathbb{Q} be an elliptic curve and n a positive integer. We denote by $E[n]$ the n -torsion subgroup of $E(\overline{\mathbb{Q}})$, where $\overline{\mathbb{Q}}$ is a fixed algebraic closure of \mathbb{Q} . The absolute Galois group $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $E[n]$ by its action on the coordinates of the points, inducing a Galois representation

$$\rho_{E,n} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \text{Aut}(E[n]),$$

called the *mod n Galois representation associated to E* . Notice that since $E[n]$ is a free $\mathbb{Z}/n\mathbb{Z}$ -module of rank 2, fixing a \mathbb{Z} -basis of $E[n]$, we identify $\text{Aut}(E[n])$ with $\text{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Then we rewrite the above Galois representation as

$$\rho_{E,n} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \text{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

Therefore we can view $\rho_{E,n}(\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ as a subgroup of $\text{GL}_2(\mathbb{Z}/n\mathbb{Z})$, determined uniquely up to conjugacy, and denoted by $G_E(n)$ in the sequel.

Fixing a prime p and choosing compatible bases for $E[p^k]$ for all k , one can take the inverse limit of these mod p^k Galois representations and construct a new map

$$\rho_{E,p^\infty} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{Z}_p),$$

called the *p -adic Galois representation associated to E* . Let us denote by $G_E^\infty(p)$ the image of ρ_{E,p^∞} , which is determined uniquely up to conjugacy. In certain instances we will say that $G_E(n) = G$ or $G_E^\infty(p) = G$ for some group G ; this will always mean that we have fixed a basis so that we remove ambiguity of working up to conjugacy.

Suppose that E does not have complex multiplication (CM in the sequel), then one of the first major results about the images of Galois representation associated to an elliptic curve is a renowned theorem of Serre [36, Théorème 2] that asserts that $\rho_{E,p}$ is not surjective for a finite number of primes p , called exceptional primes (Duke [21] showed that almost all non-CM elliptic curves has no exceptional primes). In other words, there exists a positive integer C_E , depending on E , such that $\rho_{E,p}$ is surjective for any prime $p > C_E$. After proving this theorem, Serre immediately asked [36, §4.3] if it was possible to make the constant C_E independent of E . Moreover, Serre in [37, page 399] asked if $C_E < 41$ always holds. That is, he asked the following question:

Serre's Uniformity Question. *If E/\mathbb{Q} is a non-CM elliptic curve, then must it be that $\rho_{E,p}$ is surjective for any prime $p \geq 41$?*

Nowadays, an affirmative answer to the above question has received the name of *Serre's Uniformity Conjecture* (or sometimes just *Uniformity Conjecture*) despite the fact that Serre himself never conjectured it to be true.

Date: April 11, 2019.

2010 Mathematics Subject Classification. Primary: 11G05; Secondary: 11F80.

Key words and phrases. Elliptic curves, rationals, Galois representation.

The second author was partially supported by the grant MTM2015-68524-P.

Since Serre first asked the question there has been much progress towards to proving it. A summary of these results can be found in the following theorem (see [3, 7, 8, 33, 36, 41] for more details):

Theorem 1. *Let E/\mathbb{Q} be a non-CM elliptic curve and p a prime. Then one the following possibilities occurs:*

- (i) $G_E(p) = \mathrm{GL}_2(\mathbb{F}_p)$.
- (ii) $p \in \{2, 3, 5, 7, 11, 13, 17, 37\}$, and $G_E(p)$ is conjugate in $\mathrm{GL}_2(\mathbb{F}_p)$ to one of the groups in Tables 1 and 2.
- (iii) $p \geq 17$: $G_E(p)$ is conjugate to a subgroup of the normalizer of a non-split Cartan subgroup of level p .

Beside the above theorem, Lemos ([28, Theorem 1.1], [29, Theorem 1.4]) has recently obtained partial results in the direction of a complete proof of the Serre's Uniformity Conjecture:

Theorem 2. *Let E/\mathbb{Q} be a non-CM elliptic curve. Suppose that one the following possibilities occurs:*

- (i) E admits a non-trivial cyclic isogeny defined over \mathbb{Q} .
- (ii) There exists a prime q for which $G_E(q)$ is contained in the normalizer of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_q)$.

Then $\rho_{E,p}$ is surjective for any prime $p > 37$.

Zywina conjectures [41, Conjecture 1.12] that Theorem 1 (iii) is not possible. This is what we call the Strong Uniformity Conjecture.

Strong Uniformity Conjecture. *Let E be a non-CM elliptic curve defined over \mathbb{Q} and j_E its j -invariant. If $p \geq 17$ be a prime such that*

$$(p, j_E) \notin \{(17, -17 \cdot 373^3/2^{17}), (17, -17^2 \cdot 101^3/2), (37, -7 \cdot 11^3), (37, -7 \cdot 137^3 \cdot 2083^3)\},$$

then $G_E(p) = \mathrm{GL}_2(\mathbb{F}_p)$.

Zywina classifies all of the possible images of the mod p images of non-CM elliptic curves defined over \mathbb{Q} given the corresponding moduli spaces for $p \leq 13$, except the case when the image of $G_E(13)$ in $\mathrm{PGL}_2(\mathbb{F}_{13})$ is isomorphic to S_4 (the permutation group of 4 elements) (see [41, 3, 5]).

Conjecture 3. *Let E be a non-CM elliptic curve defined over \mathbb{Q} and j_E its j -invariant. Then the image of $G_E(13)$ in $\mathrm{PGL}_2(\mathbb{F}_{13})$ is isomorphic to S_4 if and only if*

$$j_E \in \left\{ \frac{2^4 \cdot 5 \cdot 13^4 \cdot 17^3}{3^{13}}, -\frac{2^{12} \cdot 5^3 \cdot 11 \cdot 13^4}{3^{13}}, \frac{2^{18} \cdot 3^3 \cdot 13^4 \cdot 127^3 \cdot 139^3 \cdot 157^3 \cdot 283^3 \cdot 929}{5^{13} \cdot 61^{13}} \right\}.$$

Assuming Conjecture 3 and the Strong Uniformity Conjecture, Zywina gives all the possible groups $G_E(p)$ for E/\mathbb{Q} and the corresponding moduli spaces. This data can be found in Tables 1 and 2.

Remark 4. Let E/\mathbb{Q} be a non-CM elliptic curve and p a prime. Serre [38, IV] showed that if $p \geq 5$ then $\rho_{E,p}$ is surjective if and only if ρ_{E,p^∞} is surjective. But when $p = 2$ or 3 it is not the case. The reason is that there are proper subgroups of $\mathrm{SL}_2(\mathbb{Z}/4\mathbb{Z})$ and $\mathrm{SL}_2(\mathbb{Z}/8\mathbb{Z})$ that surject onto $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ under the standard reduction map as well as a proper subgroup of $\mathrm{SL}_2(\mathbb{Z}/9\mathbb{Z})$ that surjects onto $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$. These groups and the corresponding moduli spaces of elliptic curves can be found in [22] or [31] and [20] or [35] and are available in Table 4.

In view of the above remark we make the following definition:

Definition 5. *Let E/\mathbb{Q} be a non-CM elliptic curve and p a prime. We say that p is adically-exceptional for E if ρ_{E,p^∞} is not surjective.*

Remark 4 asserts that if $p \geq 5$ then p is exceptional if and only if it is adically-exceptional, and that the only possible primes that could be non-exceptional but adically-exceptional are $p = 2$ and $p = 3$.

An affirmative answer to the Serre's uniformity question does not give any information about the possible combinations of exceptional primes (or adically-exceptional primes) may occur for a given non-CM elliptic curve defined over \mathbb{Q} . In attempt to study this question, we give the following definition¹.

Definition 6. *Let E/\mathbb{Q} be a non-CM elliptic curve, then we define Serre's constant associated to E to be*

$$A(E) = \prod_{p \text{ prime}} p^k$$

where k is the smallest positive integer such that ρ_{E,p^k} is non-surjective if such an integer exists or 0 otherwise.

¹The definition of Serre's constant that appears in this paper is a generalization of the one that Cojocaru defined at [13].

Note that if p is not adically-exceptional then $\text{val}_p(A(E)) = 0$. In particular, if any prime is not adically-exceptional for E then $A(E) = 1$. Moreover, Jones [23] has proved that almost all non-CM elliptic curve over \mathbb{Q} have $A(E) = 1$. On the other hand, if m is a positive integer, $A(E)$ gives necessary conditions to conclude that $\rho_{E,m}$ is non-surjective.

Proposition 7. *Let E/\mathbb{Q} be a non-CM elliptic curve and $m \in \mathbb{N}$. If there exists a prime factor p of m satisfying $\text{val}_p(m) > \text{val}_p(A(E)) > 0$ then $\rho_{E,m}$ is non-surjective.*

Remark 8. The hypothesis of above proposition is a necessary but not sufficient condition. Let E/\mathbb{Q} be the elliptic curve with Cremona label 3891b1. Then E is a Serre curve, so all the p -adic Galois representations are surjective. Therefore $A(E) = 1$. In this case if $m = 2 \cdot 3 \cdot 1297$, then the mod m Galois representation is non-surjective. The reason is that this curve has entanglement: $\mathbb{Q}(E[2]) \cap \mathbb{Q}(E[3891]) = \mathbb{Q}(\sqrt{\Delta_E})$, where Δ_E is the discriminant of the minimal model of E , and $[\text{GL}_2(\mathbb{Z}/m\mathbb{Z}) : G_E(m)] = 2$ (cf. [15]).

We will use the following notation:

- Let \mathcal{A} be the set of the integers $A(E)$ where E runs over all non-CM elliptic curve over \mathbb{Q} .
- Let \mathcal{A}_∞ be the subset of \mathcal{A} that occur infinitely often. More precisely, $N \in \mathcal{A}_\infty$ if there are infinitely many non-CM elliptic curves E , non isomorphic over $\overline{\mathbb{Q}}$, such that $A(E) = N$.

Remark 9. Notice that Serre's Uniformity Conjecture is equivalent to the finiteness of the set \mathcal{A} .

The first theorem of this paper is the following:

Theorem 10. *Assuming the Uniformity Conjecture:*

$$\mathcal{A}_\infty = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 20, 21, 24, 28, 40, 56, 104\}.$$

Remark 11. We need to assume the Uniformity Conjecture in the proof of the complete classification of \mathcal{A}_∞ at Theorem 10 in order to ensure that there are infinitely many non-isomorphic curves with the Serre's constant that we want. Without assuming uniformity we can not be sure that for all but finitely many of the $\overline{\mathbb{Q}}$ -isomorphism classes the associated Serre's constant does not contain some unexpected prime factors. Using Theorem 2, much of Theorem 10 can be made independent of the Uniformity Conjecture. In fact, only 4, 8, 9, 11, 20 and 21 are conditionally under uniformity.

In Section 2, Theorem 16 classifies the possible combinations of mod p Galois representations that occur for infinitely many non-isomorphic classes of non-CM elliptic curves over \mathbb{Q} , and the known cases that appear only finitely. We obtain similar results in Theorem 18 for the possible combinations of maximal non-surjective subgroups of $\text{GL}_2(\mathbb{Z}_p)$. Theorem 10 is a direct consequence of the Theorem 16 and 18. Besides classifying which numbers occur as Serre's constant for infinitely many elliptic curve we give construct the moduli space for each of the possible combinations of images and determine all of the points on the corresponding modular curves when the genus ≤ 2 . Further, for each curve of genus ≥ 3 we do a point search to find all easily visible points and we compute Serre's constant for each curve in the LMFDB. The resulting data is compiled in tables at the Appendix. These results and the previous search motivate the following conjecture.

Conjecture 12. $\mathcal{A} = \mathcal{A}_\infty \cup \{17, 36, 37, 44, 60, 120, 168\}$.

The above conjecture is being treated in an ongoing continuation of this paper at [17].

Acknowledgements. The authors would like to thank Alina Cojocaru, Álvaro Lozano-Robledo, Filip Najman, Andrew Sutherland, Xavier Xarles and David Zywinia for help in the preparation of this article. We would like to thank to John Cremona for providing access to computer facilities on the Number Theory Warwick Grid at University of Warwick, where the main part of the computations were done.

Notation. Through out the paper we will refer to conjugacy classes of subgroups of $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ using the notation established by Sutherland in [39, Section 6.4] and used throughout the LMFDB database [30]. Notice that Zywinia [41] uses different notation for such conjugacy classes, in Tables 1 and 2 we give the translation between Sutherland's and Zywinia's labels. Any specific elliptic curves mentioned in this paper will be referred to by Cremona label [14, 9] and a link to the corresponding LMFDB page [30] for the ease of the reader.

2. RESULTS FOR COMBINATIONS OF GALOIS REPRESENTATIONS FOR NON-CM ELLIPTIC CURVES OVER \mathbb{Q}

One of the goals of this paper is to classify all the possible combinations of mod p Galois representations attached to elliptic curves defined over \mathbb{Q} . We wish to point out here that Morrow [34] began the study of the possible combinations of mod $n_1 n_2$ Galois representations such that n_1 is a power of 2 and $n_2 < 17$ is a prime. Then Camacho-Navarro et al. [12] are continuing this study to the case of subgroups of $\mathrm{GL}_2(\mathbb{Z}/n_1 n_2 \mathbb{Z})$ where the corresponding modular curve has low genus, and/or is hyperelliptic.

In order to establish the appropriate language to study the possible combinations of images that can occur we give the following definitions.

Definition 13. Let E/\mathbb{Q} be a non-CM elliptic curve and S_E be the set of exceptional primes of E . Let $S \subseteq S_E$ and for each $p \in S$ let G_p be a proper subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. We say that E is of exceptional type (or type for short) $[G_p : p \in S]$ if for every $p \in S$ the group $G_E(p)$ is conjugate to a subgroup of G_p . We say that the exact exceptional type (or exact type) of E is $[G_p : p \in S]$ if $S = S_E$ and $G_E(p)$ is conjugate to G_p (not a proper subgroup of G_p) for every $p \in S$.

Here we consider two possible types $[G_p : p \in S]$ and $[H_p : p \in T]$ equal if $S = T$ and for every $p \in S$, G_p is conjugate to H_p in $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. Similarly, we say that $[G_p : p \in S]$ is a *smaller type* than (or subtype of) $[H_p : p \in T]$ if $S \subseteq T$ and G_p is conjugate to a subgroup of H_p for every $p \in S$. We will refer to $\#S$ as the *length* of type $[G_p : p \in S]$. With these conventions, the exact type of E/\mathbb{Q} is unique and equal to $[G_E(p) : p \in S_E]$. We also define the level of a given type $[G_p : p \in S]$ to be $\prod_{p \in S} p$. We say a type $[G_p : p \in S]$ is *maximal* if it is not a subtype of any other type of the same level. We point here out that for almost all elliptic curves E/\mathbb{Q} the set $S_E = \emptyset$ (cf. [21]). In this case we say that the exact type of E is $[\]$ and refer to this as the trivial type.

Before moving on we introduce the concept of a modular curve and explore the relationship between these curves and certain types. Let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ satisfying $-I \in G$ and $\det(G) = (\mathbb{Z}/n\mathbb{Z})^\times$. There is a *modular curve* X_G associated to G . This curve is defined over \mathbb{Q} , smooth, projective and geometrically irreducible. Moreover, there is a non-constant morphism $j_G : X_G \rightarrow \mathbb{P}^1(\mathbb{Q})$, called the j -map of G . Moreover, given another group $G' \subseteq G \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ satisfying $-I \in G'$ and $\det(G') = (\mathbb{Z}/n\mathbb{Z})^\times$, there exists a non-constant morphism $X_G \rightarrow X_{G'}$. One of the main properties of the pair (X_G, j_G) is that for an elliptic curve E/\mathbb{Q} with j -invariant $j_E \notin \{0, 1728\}$, $G_E(n)$ is conjugate in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ to a subgroup of G if and only if $j_E \in j_G(X_G(\mathbb{Q})) \cap \mathbb{Q}$.

The relationship between modular curves arising from the fact that given a type $[G_p : p \in S]$ of level N we can associate a group $G \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, where G is the largest group (by containment) such that $\pi_p(G) = G_p$ for all $p \in S$. Here $\pi_p : \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \rightarrow \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ is the standard componentwise reduction map which is well-defined since p divides N by construction. Associated to the group G is the modular curve X_G whose rational points correspond to $\overline{\mathbb{Q}}$ -isomorphism classes of elliptic curves over \mathbb{Q} of type $[G_p : p \in S]$.

In the other direction, given a group $G \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ we can associate a type $[\pi_p(G) : p \text{ divides } N]$ of level $\mathrm{rad}(N)$. Again, the $\overline{\mathbb{Q}}$ -isomorphism classes of curves coming from points in $X_G(\mathbb{Q})$ all have type $[\pi_p(G) : p \text{ divides } N]$. In fact, every $\overline{\mathbb{Q}}$ -isomorphism classes of curves of type $[\pi_p(G) : p \text{ divides } N]$ arises as a point on X_G exactly when N is squarefree and G is maximal among the groups of level N corresponding to the type $[\pi_p(G) : p \text{ divides } N]$.

This association of types with groups, and hence modular curves, will be extremely useful in studying what combinations of images can occur. We will use it intimately in the remaining sections.

Next we give a definition of *adic-type* and *exact adic-type*.

Definition 14. Let E/\mathbb{Q} be a non-CM elliptic curve and S_E^∞ be the set of adically exceptional primes. Let $S \subseteq S_E^\infty$. For each $p \in S$, let G_p be a proper subgroup of $\mathrm{GL}_2(\mathbb{Z}_p)$. We say that E is of adically-exceptional type (or adic-type for short) $[G_p : p \in S]$ if for every $p \in S$ the group $G_E^\infty(p)$ is conjugate to a subgroup of G_p . We say that the exact adically-exceptional type (or exact adic-type) of E is $[G_p : p \in S]$ if $S = S_E^\infty$ and $G_E^\infty(p)$ is conjugate to G_p (not a proper subgroup group of G_p) for every $p \in S$.

We adopt similar conventions as above to compare two adic-types so that everything is well-defined changing what is necessary. For a given adic-type $[G_p : p \in S]$ we define the *level* of that type to be $\prod_{p \in S} p^{k_p}$ where k_p is the minimum integer such that the standard componentwise reduction map $G_p \rightarrow \mathrm{GL}_2(\mathbb{Z}/p^{k_p}\mathbb{Z})$ is not surjective. For the sake of notational brevity, for each $G_p \subseteq \mathrm{GL}_2(\mathbb{Z}_p)$ that occurs in an adic-type we will denote G_p by a subgroup $\tilde{G}_p \subseteq \mathrm{GL}_2(\mathbb{Z}/p^k\mathbb{Z})$ for some k such that $G_p = \pi^{-1}(\tilde{G}_p)$ where $\pi : \mathrm{GL}_2(\mathbb{Z}_p) \rightarrow \mathrm{GL}_2(\mathbb{Z}/p^k\mathbb{Z})$ is again the standard componentwise reduction map.

Remark 15. Let E/\mathbb{Q} be an elliptic curve and $\rho_E : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\widehat{\mathbb{Z}})$ be the adelic Galois representation associated to E constructed choosing bases for $E[n]$ compatible with divisibility and taking inverse limits. It is tempting to think that knowing the exact adic-type of E is equivalent to knowing the image of ρ_E upto conjugation, but this is not the case. The gap is that the exact adic-type does not contain any information about the entanglements between the field of definition of each Tate module. Serre showed that there must be *some* entanglement between these fields using the Weil paring and the Kronecker–Weber theorem and so we usually cannot recover the image of the adelic Galois representation attached to E just from the exact adic-type of E .

The following theorem gives the set of possible exceptional types that occur for infinitely many non-isomorphic classes of non-CM elliptic curves over \mathbb{Q} , and the known cases that appear only finitely.

Theorem 16. (A) *The following nontrivial exceptional types occur for infinitely many non-isomorphic classes of non-CM elliptic curves over \mathbb{Q} :*

- $[G_p]$ for any G_p in Tables 1 and 2 except 7Ns.3.1, 11B.10.4, 11B.10.5, 13S4, 17B.4.2, 17B.4.6, 37B.8.1 and 37B.8.2 (that appear only for finitely many \mathbb{Q} -isomorphic classes).
- $[G_2, G_p]$, where G_2 is:
 - ★ 2B and G_p is 3B, 3B.1.1, 3B.1.2, 3Cs, 3Cs.1.1, 3Nn, 3Ns, 5B, 5B.4.1, 5B.1.1, 5B.1.4, 5B.4.2, 5B.1.2, or 5B.1.3.
 - ★ 2Cn and G_p is 3B, 3B.1.1, 3B.1.2, 5S4, 7B, 7B.2.1, or 7B.2.3.
 - ★ 2Cs and G_p is 3B, 3B.1.1, or 3B.1.2.
- $[G_3, G_5]$, where G_3 is 3Nn and G_5 is 5B, or 5Ns.
- $[G_3, G_p]$, where G_3 is 3Nn and G_p is 5Nn, or 7Nn.

(B) *For the following exceptional types there are only a finite number of $\overline{\mathbb{Q}}$ -isomorphic classes:*

- $[G_p]$ where G_p is 7Ns.3.1, 11B.10.4, 11B.10.5, 13S4, 17B.4.2, 17B.4.6, 37B.8.1 or 37B.8.2.
- $[G_3, G_p]$, where $G_E(3)$ is:
 - ★ 3B and G_p is 5B, 5B.4.1, 5B.1.1, 5B.4.2, 5B.1.2, 5S4, 7B, 7B.2.1, or 7B.2.3.
 - ★ 3B.1.1 or 3B.1.2 and G_p is 5B.1.3, 5B.1.4, 5B.4.1, 5B.4.2, 5S4, 7B, 7B.2.1, or 7B.2.3.
 - ★ 3Ns and G_p is 5B.

Moreover, we give unconditionally the moduli space for each of the possible exceptional types (see Tables 1, 2, 3, 6, 7, 9, 11, 12), except for the cases of level 13, 17 and 37 which are conditionally under Conjecture 3 and the Strong Uniformity Conjecture.

Corollary 17. *Assuming Serre's Uniformity Conjecture, the set of nontrivial exact types such that there exist infinitely many non-isomorphic classes of non-CM elliptic curves over \mathbb{Q} correspond to the cases that appear at Theorem 16 (A).*

We postpone the proof of Theorem 16 to section 5. We include the proof of Corollary 17 here.

Proof. The proof of this corollary breaks down into two cases. Given a group $G \subseteq \text{GL}_2(\mathbb{Z}/n\mathbb{Z})$ with n squarefree satisfying $-I \in G$ and $\det(G) = (\mathbb{Z}/n\mathbb{Z})^\times$ there can only be infinitely many $\overline{\mathbb{Q}}$ -isomorphism classes of elliptic curves over \mathbb{Q} of type G if the corresponding modular curve X_G is genus 0 with a rational point or if it is an elliptic curve with positive rank over \mathbb{Q} .

For the first case, assume $X_G \simeq \mathbb{P}^1$ over \mathbb{Q} . Under the assumption of uniformity we may assume that p divides n if and only if there exists some elliptic curve over \mathbb{Q} for which p is exceptional. This is because if p did not already divide n , we can lift the group G to be a subgroup of $\text{GL}_2(\mathbb{Z}/pn\mathbb{Z})$ and by taking its preimage under the standard reduction map. This processes does not affect the modular curve X_G or its moduli interperetaion.

By [41, Lemma 3.5] we have that there are infinitely $\overline{\mathbb{Q}}$ -isomorphism classes of elliptic curves with $\pm G_E(n)$ conjugate to G . For each of these isomorphism classes, the curves in them cannot have any additional exceptional primes by the assumption that any prime that could potentially be exceptional (under the assumption of uniformity) is already accounted for since it divides n . Thus, for each of the infinitely many $\overline{\mathbb{Q}}$ -isomorphism classes of elliptic curves guaranteed to exist by [41, Lemma 3.5], we have that the associated Serre's constant is the product of primes p such that $\pi_p(G) \neq \text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ and the image is exactly what we wanted it to be.

Finally, assume that the corresponding modular curve X_G has genus 1 and positive rank. For every p dividing n let $G_p = \pi_p(G)$ where $\pi_p : \text{GL}_2(\mathbb{Z}/n\mathbb{Z}) \rightarrow \text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ is the standard componentwise reduction map. Then every point in $X_G(\mathbb{Q})$ correspond to a $\overline{\mathbb{Q}}$ -isomorphism class of elliptic curves with type $[G_p : p \text{ dividing } n]$.

Suppose that E has type $[G_p : p \text{ dividing } n]$ but its exact type is not $[G_p : p \text{ dividing } n]$. Then at least one of the following must be true:

- The level of the type of E is larger than n .
- There is a prime p that divides n such that $G_E(p)$ is conjugate to a proper subgroup of G_p .

Assuming uniformity, we have that there are only finitely many additional primes that one can add to the level of the exact type of E and the computations described in Section 4 show that that all of the modular curves with additional exceptional primes have genus strictly greater than 1 and thus have only finitely many rational points.

Next, checking every possible subtype shows that there are only 2 types whose corresponding modular curves are of genus 1 and have positive rank over \mathbb{Q} that also have a subtype with a genus 1 positive rank corresponding modular curve. Those types are $[8X5, 3Nn]$ and $[3Nn, 5S4]$ and we deal with these at the beginning of Section 5.

Therefore, under the assumption of uniformity there are only finitely many possibilities for the exact type of E and for each of the possible exact types there are only finitely many possible j -invariant. Thus, there can only be finitely many \mathbb{Q} -isomorphism classes of elliptic curves with type $[G_p : p \text{ dividing } n]$ and different exact type $[G_p : p \text{ dividing } n]$.

Since $X_G(\mathbb{Q})$ is infinite and the j -map from $X_G \rightarrow \mathbb{P}^1(\mathbb{Q})$ is finite-to-one, we know that there are infinitely many \mathbb{Q} -isomorphism classes of elliptic curves with type $[G_p : p \text{ dividing } n]$. Therefore it must be that there are infinitely many \mathbb{Q} -isomorphism classes of elliptic curves with exact type $[G_p : p \text{ dividing } n]$. \square

The next result is similar to Theorem 16 but we do not obtain a complete characterization, instead we obtain only maximal adically exceptional types that can occur.

Theorem 18. (A) *The following list of maximal adically-exceptional types occur for infinitely many non-isomorphic classes of non-CM elliptic curves over \mathbb{Q} :*

- $[G_p]$ where G_p is 2B, 2Cn, 3B, 3Nn, 5Nn, 5B, 5S4, 7Ns, 7Nn, 7B, 11Nn or 13B.
- $[G_p]$ where G_p is 4X3, 4X7, 8X4, 8X5, or 9XE.
- $[G_2, G_p]$, where G_2 is:
 - ★ 2B and G_p is 3B, 3Nn, or 5B.
 - ★ 2Cn and G_p is 3B, 5S4, or 7B.
 - ★ 4X3 and G_p is 3B, 5S4, or 7B.
 - ★ 4X7 and G_p is 3Nn.
 - ★ 8X4 and G_p is 3B, 5S4, 7B, 5B, or 13B.
 - ★ 8X5 and G_p is 3B, 5S4, or 7B.
- $[G_3, G_5]$, where G_3 is 3Nn and G_5 is 5B.
- $[G_2, G_5]$, where G_2 is 4X7 (resp. 8X5) and G_5 is 5S4 (resp. 5Nn).
- $[G_3, G_p]$, where G_3 is 3Nn and G_p is 5Nn, or 7Nn.

(B) *There is only a finite number of \mathbb{Q} -isomorphic classes of elliptic curves with the following maximal adic-types:*

- $[G_p]$ where G_p is 13S4, 17B.4.2, 17B.4.6, 37B.8.1 or 37B.8.2.
- $[G_2, G_p]$, where G_2 is:
 - ★ 4X3 and G_p is 11B.10.4, or 11B.10.5.
 - ★ 4X7 and G_p is 9XE, 3B, 5B, or 7B.
 - ★ 8X5 and G_7 is 7Ns.3.1.
- $[G_3, G_p]$, where G_3 is 3B and G_p is 5B, 5S4, or 7B.
- $[G_2, G_3, G_5]$, where G_2 (resp. G_3, G_5) is 4X3 (resp. 3B, 5S4).
- $[G_2, G_3, G_5]$, where G_2 (resp. G_3, G_5) is 8X4 (resp. 3B, 5B).
- $[G_2, G_3, G_7]$, where G_2 (resp. G_3, G_7) is 8X4 (resp. 3B, 7B).

Moreover, we give unconditionally the moduli space for each of the possible maximal adic-types above (see Tables 1, 4, 5, 6, 9, 11 and Remark 24), except (maybe) the case $[4X7, 9XE]$ and for the cases of level 13, 17 and 37 that are conditionally under Conjecture 3 and the Strong Uniformity Conjecture.

Corollary 19. *Assuming Serre's Uniformity Conjecture, the set of maximal adically-exceptional types such that there exist infinitely many non-isomorphic classes of non-CM elliptic curves over \mathbb{Q} correspond to the cases that appear at Theorem 18 (A).*

Since we do not require that the types be exact in Corollary 19, the result follows from a genus and rank computation that is described in Section 5 as well as an argument similar to that of the proof of Corollary 17.

3. INVARIANCE OF THE SERRE'S CONSTANT UNDER QUADRATIC TWISTS

The purpose of this section is to prove that $A(E)$ is an invariant of the isomorphism class of a non-CM elliptic curve.

Proposition 20. *Let E/\mathbb{Q} be a non-CM elliptic curve and let p be a prime. If E'/\mathbb{Q} is a quadratic twist of E , then $\rho_{E,p}$ is surjective if and only if $\rho_{E',p}$ is surjective.*

Proof. Notice that it is enough to show that if $\rho_{E,p}$ is surjective, then $\rho_{E',p}$ is surjective. Now, if E' is a quadratic twist of E , then there is a square free $D \in \mathbb{Z}$ such that E and E' are isomorphic over $\mathbb{Q}(\sqrt{D})$. Assume that $G_E(p) = \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. Then, it must be that either $G_{E'}(p) = \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ or $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) \simeq G_{E'}(p) \rtimes \mathbb{Z}/2\mathbb{Z}$. In the last case, we would have that $G_{E'}(p)$ is a subgroup of index 2 inside of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. We have that $\det \rho_{E,p}$ is the cyclotomic character, a standard consequence of the Weil pairing says that $\det : G_{E'}(p) \rightarrow (\mathbb{Z}/p\mathbb{Z})^\times$ is surjective. According to [1, Figure 5.1] there are no such groups unless $p = 2$ and $G_{E'}(p)$ is conjugate to $2\mathrm{Cn}$, but the property that $G_{E'}(p)$ is conjugate to $2\mathrm{Cn}$ is equivalent to E' having a square discriminant which is invariant under quadratic twists. This would mean that $G_E(p)$ is not surjective giving a contradiction. \square

Corollary 21. *Let E/\mathbb{Q} be a non-CM elliptic curve. Then $A(E)$ is invariant under $\overline{\mathbb{Q}}$ -isomorphism. In other words, $A(E)$ only depends on j_E .*

Proof. All that is left is to prove is that if p is adically-exceptional for E , then it is adically-exceptional with the same exponent for all of the quadratic twists of E . This follows from the exact same argument as above together with the fact that the 5 maximal groups that surject onto $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ but are not all $\mathrm{GL}_2(\mathbb{Z}/p^k\mathbb{Z})$ for some $k \geq 2$, all contain $-I$ and thus can not be quadratic twisted into. That is, because they contain $-I$, if $G_E^\infty(p)$ is not in one of these groups and E' is a quadratic twist of E , then $G_{E'}^\infty(p)$ is not in one of these groups either. \square

Corollary 21 allow us to take representatives of each of the finitely many $\overline{\mathbb{Q}}$ -isomorphism classes of elliptic curves and compute their Serre's constant.

4. OUTLINE OF THE COMPUTATIONS: FIBER PRODUCTS OF PAIRS OF MODULAR CURVES

We are now ready to fully leverage the connection between types and subgroups of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ and their corresponding modular curves. To start we survey some of the results about modular curves that will form the foundation for our computations. For $n = p \leq 11$ prime, Zywinia [41] classifies all of the possible subgroups $G_E(p) \subseteq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ for elliptic curves E/\mathbb{Q} . The case $p = 13$ is the first prime for which Zywinia does not have a complete description. He classifies all the possible subgroups $G_E(13)$ except the cases concerning subgroups of $13\mathrm{Nn}$, $13\mathrm{Ns}$ and $13\mathrm{S4}$. Baran [5] showed that the modular curves $X_{13\mathrm{Nn}}$ and $X_{13\mathrm{Ns}}$ are both isomorphic to a genus 3 curve, and recently Balakrishnan et al. [3] have determined that this genus 3 curve has no non-singular, non-CM rational points. Therefore there are no non-CM elliptic curves E/\mathbb{Q} such that $G_E(13)$ is a subgroup of $13\mathrm{Nn}$ neither $13\mathrm{Ns}$. The remaining case is the curve $X_{13\mathrm{S4}}$. Banwait and Cremona [6] have shown that this curve has genus 3 and at least three non-singular, non-CM points corresponding to the three j -invariants that appear in Conjecture 3. Finally, thanks to Theorem 1 we have that if $p \geq 17$ and $\rho_{E,p}$ is non-surjective then $G_E(p)$ appears in Table 1 or $G_E(p) = \mathrm{pNn}$. In the later case, Baran [4] has showed that the genus of $X_{\mathrm{pNn}} \geq 2$. On the other hand, by Remark 4 if $p \geq 5$ we have $G_E^\infty(p) = \mathrm{GL}_2(\mathbb{Z}_p)$ if and only if $G_E(p) = \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ while when $p = 2$ or 3 , $G_E^\infty(p) = \mathrm{GL}_2(\mathbb{Z}_p)$ if and only if $G_E(p^k)$ is not conjugate to a subgroup of one of the groups listed in Table 4.

Let G be a proper subgroup of $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ satisfying $-I \in G$, $\det(G) = (\mathbb{Z}/p\mathbb{Z})^\times$ and $X_G(\mathbb{Q})$ contains points corresponding to non-CM j -invariants, and the group $G = \mathrm{pNn}$. The following table summarizes the genus of the modular curves of the form X_G from [41] and whether or not the modular curve has infinitely many points:

	Genus X_G	$G = G_E^\infty(p)$
$\#X_G(\mathbb{Q}) < \infty$	> 1	13S4, 37B.8.1, 37B.8.2; pNn , $p \geq 17$
	1	7Ns.3.1, 11B.10.4, 11B.10.5, 17B.4.2, 17B.4.6
$\#X_G(\mathbb{Q}) = \infty$	1	11Nn
	0	otherwise

The main goal of our project is to characterizes the exceptional and adically-exceptional types of non-CM elliptic curves defined over \mathbb{Q} .

Let E be a non-CM elliptic curve defined over \mathbb{Q} . Let $S \subseteq S_E$ be a subset of the set of exceptional primes for E and $[\pm G_E(p) : p \in S]$ be the exceptional type associated to E and S where we add $-I$ to each component if it is not already there. Letting $G \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ be the group corresponding to the type $[G_E(p) : p \in S]$, where n is the product of $p \in S$ (i.e. the level of $[G_E(p) : p \in S]$). The group G satisfies $-I \in G$ since we added $-I$ to each $G_E(p)$ and $\det(G) = (\mathbb{Z}/n\mathbb{Z})^\times$ and as discussed before we can associated a modular curve X_G . Using the correspondence established in Section 2, there exist a non-CM elliptic curve with mod p image in $\pm G_E(p)$ for all $p \in S$ exactly when there exists a non-cuspidal, non-CM rational point in $X_G(\mathbb{Q})$. The case of adically-exceptional types is equivalent. We are primarily interested in those groups G coming from (adically-)exceptional types such that $\#X_G(\mathbb{Q}) = \infty$. That is, when X_G is a genus 0 curve with a rational point, i.e. $X_G(\mathbb{Q}) \simeq \mathbb{P}^1(\mathbb{Q})$, or X_G is an elliptic curve defined over \mathbb{Q} with positive rank over \mathbb{Q} . Although we treat the whole problem in this paper trying to build the bases to finalize the characterization of the (adic-)types that can occur for non-CM elliptic curves over \mathbb{Q} , as well as the combinations of primes that can be (adically-)exceptional for a given non-CM elliptic curve E/\mathbb{Q} . This project will have a second component [17].

Let G be a group in Table 1 such that $\#X_G(\mathbb{Q}) < \infty$. Thanks to Corollary 21 we know that Serre's constant is an invariant of the $\overline{\mathbb{Q}}$ -isomorphism class. For each j -invariant j_0 , it is enough to take one elliptic curve E/\mathbb{Q} with $j_E = j_0$ and then compute the set S_E of exceptional primes. Zywinia [42] gave an algorithm to compute S_E and combined with his classification in Table 1 allow us to determine the exceptional type of the $\overline{\mathbb{Q}}$ -isomorphic class of E . We can compute the set of adically-exceptional primes S_E^∞ in an analagous manner. Then we obtain that the possible (adically-)exceptional types are the ones that appear in Table 5. Assuming Conjecture 3 and Strong Uniformity gives that Table 5 is complete.

Let p be prime, after the above sieve, we have 29 groups G of the form $G_E(p)$ (see Table 1) and 5 of the form $G_E(p^k)$ for $k \geq 2$ (Table 4) such that $-I \in G$ and $\#X_G(\mathbb{Q}) = \infty$. Moreover, all those curves have genus 0, except for $G = 11\mathrm{Nn}$, that is an elliptic curve with positive rank. Of these 34 images that occur for infinitely many $\overline{\mathbb{Q}}$ -isomorphism classes, there levels are broken down in the following table.

Level	2	3	4	5	7	8	9	11	13
# of groups	3	4	2	9	6	2	1	1	6

4.1. Pairs of non-surjective Galois representations. For the remainder of this section any group G is on the above 34 groups. In the next sections we treat separately the cases of exceptional primes and adically-exceptional primes. Note that we are trying to characterize the complete set of possible combination of mod p Galois representations, but in the p -adic case we are only interested up to conjugation of a subgroup of a maximal group in $\mathrm{GL}_2(\mathbb{Z}_p)$.

4.1.1. Exceptional pairs. Let E/\mathbb{Q} be an elliptic curve with two distinct exceptional primes $p < q$ and let $G_p = G_E(p)$ and $G_q = G_E(q)$. The next sieve comes from the classification of rational n -cyclic isogenies given by Mazur and Kenku (cf. [33, 24, 25, 26, 27]) and torsion structure given by Mazur (cf. [32]). For the special case of a non-CM elliptic curve E/\mathbb{Q} we have:

- if E has a cyclic n -isogeny, then $n \in \{1, \dots, 13, 15, 16, 17, 18, 21, 25, 37\}$, and
- $E(\mathbb{Q})_{\mathrm{tors}} \in \{\mathbb{Z}/m\mathbb{Z} : m = 1, \dots, 10, 12\} \cup \{\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} : m = 1, \dots, 4\}$.

Using the above classifications we can immediately eliminate some pairs G_1, G_2 . For example, any combinations of groups $G_5 \subseteq 5\mathrm{B}$ and $G_7 \subseteq 7\mathrm{B}$ can be eliminated, since such a elliptic curve would have a 35-isogeny. After using these results to eliminate combinations of groups that would violate these classifications, we are left with 206 possible pairs to consider. For each of these possibilities, we compute the corresponding group $G \subseteq \mathrm{GL}_2(\mathbb{Z}/pq\mathbb{Z})$, and we compute the genus of the corresponding modular curve X_G group theoretically (see [40, Lemma 2.4]). Note that $X_G = X_{G_p} \times_{\mathbb{P}^1} X_{G_q}$, the fiber product:

$$\begin{array}{ccc}
 & X_G & \\
 \swarrow & & \searrow \\
 X_{G_p} & & X_{G_q} \\
 \searrow j_{G_p} & & \swarrow j_{G_q} \\
 & \mathbb{P}^1 &
 \end{array}$$

Therefore,

$$X_G(\mathbb{Q}) = \{(R_p, R_q) \in X_{G_p}(\mathbb{Q}) \times X_{G_q}(\mathbb{Q}) : j_{G_p}(R_p) = j_{G_q}(R_q)\}.$$

The simplest case is that the modular curves associated to the groups G_p and G_q both have genus 0. That is $G_p, G_q \neq 11\mathbf{Nn}$. In this case, both curves X_{G_p} and X_{G_q} are isomorphic to \mathbb{P}_1 and an equation of the fiber product X_G is just the numerator of $j_{G_p}(x) - j_{G_q}(y) = 0$. This model for this curve is usually singular, but give an initial model to work with in order to classify all the rational points.

The next case we considered is when, say $G_q = 11\mathbf{Nn}$. In [41, §4.5.5], Zywinia gives polynomials $A(x), B(x), C(x)$ in $\mathbb{Z}[x]$ such that an elliptic curve E has $G_E(11)$ conjugate to a subgroup of $11\mathbf{Nn}$ exactly when the polynomial $j_E^2 A(x) + j_E B(x) + C(x)$ has a rational root, where j_E denotes the j -invariant of E . Thus, in order to construct a plane curve model for the modular curve that parameterizes elliptic curves over whose image mod p image is conjugate to a subgroup of G_p and whose mod 11 image is conjugate to a subgroup of $11\mathbf{Nn}$ on can consider the curve given by the equation $j_{G_p}(y)^2 A(x) + j_{G_p}(y) B(x) + C(x) = 0$.

The largest genus that occurs in this computation is genus 246, and of the 206 curves 141 of these curves have genus less than 20. The counts of genus curves are listed in the table below.

g	0	1	2	3	4	5	6	7	8	9	10	11	13	14	15	16	18	19	≥ 20
# Curves of genus g	12	25	14	15	12	8	5	9	7	7	2	2	4	5	4	3	1	6	65

Here we point out that the genus of the modular curve X_G can computed without ever computing a module for the curve. This is because the genus of X_G can be computed by counting elliptic points and cusps on X_G (see [19, Theorem 3.1.1] for example) which can be done using just G . The code for the computation of the genus of these curves was taken from [40].

We obtain the following data depending on the genus of the fiber product:

- Genus 0: For each of the genus 0 curves we are able to compute the j -maps and thus completely classify all of the elliptic curves with those exceptional types. This data can be found in Table 6 and the corresponding parametrization to obtain the fine moduli in Table 7.
- Genus 1: For the 25 genus 1 curves (see Table 8) there are 24 elliptic curves and 1 curve that do not have a single rational point. Of the 24 elliptic curves, 20 have rank 0 and 4 have positive rank. For the curves with rank 0, we compute all of the rational points and their corresponding j -invariants to see that only 6 curves have points that correspond to non-CM elliptic curves. These curves, their points and representatives of the corresponding non-CM \mathbb{Q} -isomorphism classes can be found in Table 11 and the finitely many elliptic curve that correspond to the fine moduli in Table 12. Lastly, the modular curves that are genus 1 and have positive rank we give the j -maps and the Cremona label for the corresponding model in Table 9 (except for the case $[3\mathbf{Nn}, 5\mathbf{S4}]$, see Section 5).
- Genus 2: For each of the genus 2 curves the rank of their jacobian have rank 0 or 1, then we can apply Chabauty to obtain all the rational points. We have obtained that all the rational points, if there are, correspond to CM j -invariants. This data can be found in Table 13.
- Genus > 2 : There are 155 curve of genus > 2 . For the corresponding groups, there are 28 maximal groups. Now, thanks to the non-constant morphism $X_G \rightarrow X_{G'}$ when $G \subseteq G'$, we have that it is enough to compute the rational points of the curves corresponding to these 28 curves. First we checked for CM-points and then we looking for points of bounded height. For the cases that $G_i \neq 11\mathbf{Nn}$, $i = 1, 2$ with bound 10^6 , otherwise with bound 100 or until the computer used more than 50GB of memory. In all those maximal curves we have not found any non-CM rational point. For each type we add a subscript indicating the genus of the corresponding modular curve, a superscript of cm when the only points we have found correspond to elliptic curves with CM or a superscript of \emptyset in the case that we have not found any rational point. This data can be found in Table 14.

4.1.2. Adically-exceptional pairs. In the case of p -adic Galois representations, our objective in this paper is only to characterize the possible combinations of maximal p -adic images. That is up to conjugation of a subgroup of a maximal group in $\mathrm{GL}_2(\mathbb{Z}_p)$.

Let E/\mathbb{Q} be an elliptic curve with at least one adically-exceptional prime p such that p is not exceptional. That is $G_E^\infty(p) \neq \mathrm{GL}_2(\mathbb{Z}_p)$ and $G_E(p) = \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. Therefore $G_1 = G_E^\infty(p)$ is conjugate to a subgroup of one of the groups listed in Table 4. Now, let $q \neq p$ a prime and $G_2 = G_E^\infty(q)$ one of the groups in Table 1 such that the corresponding modular curve has infinitely many points or in Table 4 such that it is maximal. All the groups in Table 4 are maximal, meanwhile the maximal groups in Table 1 are $2\mathbf{B}$, $2\mathbf{Cn}$, $3\mathbf{B}$, $3\mathbf{Nn}$, $5\mathbf{B}$, $5\mathbf{Nn}$, $5\mathbf{S4}$, $7\mathbf{B}$, $7\mathbf{Nn}$, $7\mathbf{Ns}$, $11\mathbf{Nn}$ and $13\mathbf{B}$. Let $G_1 = G_E^\infty(p)$ and $G_2 = G_E^\infty(q)$. Similarly to the exceptional case at section

4.1.1, for each of these possibilities, we compute the corresponding group $G \subseteq \mathrm{GL}_2(\mathbb{Z}/p^kq\mathbb{Z})$, the genus and a model of the corresponding modular curve X_G . In this case we obtain 54 curves, and the largest genus is 111. Note that for these computations we have not made the cases when G_1 and G_2 belong to Table 1, since those computations have been done in the previous section. The counts of genus curves are listed in the table below.

g	0	1	2	3	4	6	7	8	10	13	14	18	26	40	54	111
# Curves of genus g	10	15	6	7	2	2	3	1	1	1	1	1	1	1	1	1

We obtain the following data depending on the genus of the fiber product:

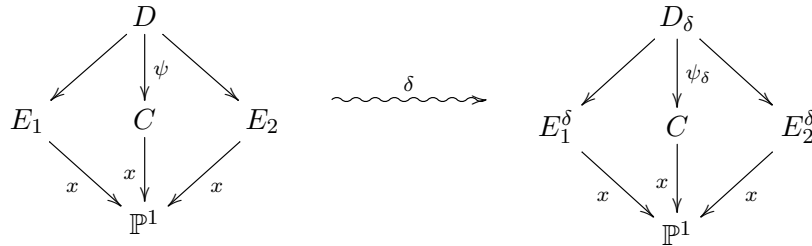
- Genus 0: Similar to the Section 4.1.1 although in this case we do not consider the fine moduli spaces. The data can be found in Table 6.
- Genus 1: There are 15 genus 1 curves (see Table 8), only 2 of them without rational points. For the remaining elliptic curves there are 8 with rank 0 and 5 with positive rank, and the corresponding data appear in Table 11 and Table 9 respectively.
- Genus 2: There are 6 genus 2 curves. One of them has not any rational point, 4 have jacobian with rank 0 or 1 and then we obtain all their rational points applying Chabauty. The remaining curve is the modular curve associated to the pair $[4X7, 5Nn]$ whose jacobian has rank 2. Then in order to obtain its rational points we apply 2-cover descent and elliptic Chabauty. This computation has been realized with the help of Xavier Xarles. Let C be the following hyperelliptic model associated to the modular curve corresponding to the pair $[4X7, 5Nn]$:

$$C : y^2 = f(x), \quad f(x) = (x-2)(x^2+1)(4x^3-4x^2+3x-2).$$

First we do a point search to find all easily visible points and we compute that in projective coordinates

$$S_1 := \{[0 : \pm 2 : 1], [3/4 : \pm 50/4 : 1], [2 : 0 : 1], [1 : \pm 2 : 0]\} \subseteq C(\mathbb{Q}).$$

Our purpose is to prove $C(\mathbb{Q}) = S_1$. Let us determine an unramified two covering $\psi : D \rightarrow C$ defined over \mathbb{Q} such that the associated covering collection $\psi_\delta : D_\delta \rightarrow C$ satisfies that any rational point $P \in C(\mathbb{Q})$ on the curve lifts to one of the covers $D_\delta(\mathbb{Q})$. The idea is to factorize the polynomial $f(x)$ as the product of two polynomials (over some number field K) of even degree. Let be $f(x) = f_1(x)f_2(x)$, where $f_1(x), f_2(x) \in K[x]$ for some number field K . We get the subcovers $E_1 : y_1^2 = f_1(x)$ and $E_2 : y_2^2 = f_2(x)$ and the unramified two covering $\psi : D \rightarrow C$, $\psi(x_0, y_1, y_2) = (x_0, y_1y_2)$ where $D : \{y_1^2 = f_1(x), y_2^2 = f_2(x)\}$:



Now if we can determine $D_\delta(\mathbb{Q})$ we determine $C(\mathbb{Q})$. Since $D_\delta(\mathbb{Q})$ maps to $\{P \in E_i^\delta(K) : x(P) \in \mathbb{P}^1(\mathbb{Q})\}$. Finally, in order to determine which of those points correspond to points in $C(\mathbb{Q})$ we only have to determine which points in $x(E_i^\delta(K)) \cap \mathbb{P}^1(\mathbb{Q})$ lift to $C(\mathbb{Q})$, for any of the two subcovers.

Let be $K = \mathbb{Q}(\alpha)$ where α is a root of the polynomial $g(x) = 4x^3 - 4x^2 + 3x - 2$ then we choose the following factorization of the polynomial $f(x)$:

$$f_1(x) = (x-2)(x-\alpha), \quad f_2(x) = (x^2+1)(4x^2+4(\alpha-1)x+(4\alpha^2-4\alpha+3)).$$

We could have chosen other factorizations over other number fields, but this one works for our purpose. Now, in order to compute the (finite) set \mathcal{T} of twists necessary to cover all the rational points we compute the Fake 2-Selmer group of C/\mathbb{Q} (see [11]). This can be done by the Magma function `TwoCoverDescent`. We check that all the possible twists come from the points in the set S_1 : let $\delta \in \mathcal{T}$, then $\delta = f_2(x_0) \in K^*/K^{*2}$ for x_0 the x -coordinate of an affine point in S_1 ; and $\delta = 1$. Note that $f_2(3/4) \in K^2$. Therefore we have obtained $\mathcal{T} = \{1\} \cup \{f_2(x_0) : x_0 \in \{0, 2\}\}$. For any $\delta \in \mathcal{T}$ we have that $\mathrm{rank}_{\mathbb{Z}}(E_2^\delta(K)) < 3$, then we can apply Elliptic Chabauty to the covering $x : E_2^\delta \rightarrow \mathbb{P}^1$, to obtain the set $C(\mathbb{Q})$. The following tables illustrates the data obtained

for each δ the corresponding point in $\mathbb{P}^1(\mathbb{Q})$:

δ	1	$\alpha^2 - \alpha + 3/4$	$5\alpha^2 + 5\alpha + 55/4$
$x(P) \in \mathbb{P}^1(\mathbb{Q}), P \in E_2^\delta(K)$	$[3/4 : 1], [1 : 0]$	$[0 : 1]$	$[2 : 1]$

Therefore we finish with $C(\mathbb{Q}) = S_1$.

• Genus > 2 : Similar to the case in section 4.1.1: the data can be found in Table 14. But in this case we have found some non-CM rational points:

- $j = 3^3 5^7 7^5 / 2^7$ in the modular curve of genus 3 asociated to $[8X5, 7Ns]$. But this j -invariant corresponds to $[8X5, 7Ns.3.1]$ (see Table 5).
- $j = -2^2 3^7 5^3 439^3$ in the modular genus 6 curve associated to the pair $[4X7, 9XE]$.

5. PROOF OF THE THEOREM 16 AND 18

We have discussed previously that our computations allow us to compute the genus of the modular curves obtained as the fiber product of modular curves arising from pairs of non-surjective (mod p or p -adic) Galois representations. In particular, those curves can have infinitely many non-CM points and non-cusps if and only if it has genus 0 with some rational point; or it is an elliptic curve with positive rank. Apart from the case with a single group (see Tables 1, 2, 4), we have obtained the following:

- Genus 0: For each curve of genus zero we check that it has a rational point. See Tables 6 and 7 for all those possible pairs.
- Genus 1: There are 40 modular curves of genus 1 associated to pairs of mod p and p -adic non-surjective representations. From them, the 9 elliptic curves of positive rank appear in Table 8. Note that the cases $[8X5, 3Nn]$ and $[3Nn, 5S4]$ do not appear at Theorems 16 and 18. In the following paragraphs we describe the reasons that we can discard those cases:

- ★ $[8X5, 3Nn]$: Let \mathcal{E} be the modular curve associated to $[8X5, 3Nn]$, then \mathcal{E}/\mathbb{Q} is the elliptic curve with Cremona label 576a3 and has j -map equal to $j(x) = 8x^3$ where $(x, y) \in \mathcal{E}(\mathbb{Q})$. Now let 8X17 be the group

$$\langle (\frac{1}{2} \frac{0}{1}), (\frac{1}{0} \frac{0}{7}), (\frac{1}{0} \frac{1}{5}) \rangle \subsetneq 8X5 \subsetneq GL_2(\mathbb{Z}/8\mathbb{Z}).$$

The modular curve associated to the (nonmaximal) exceptional pair $[8X17, 3Nn]$ is the elliptic curve \mathcal{E}'/\mathbb{Q} with Cremona label 576a1. The j -map \mathcal{E}' is equal to $j'(t) = 8 \left(\frac{x^3 + 32}{x^2} \right)^3$ where $(x, y) \in \mathcal{E}'(\mathbb{Q})$. As the Cremona labels indicate, there is an isogeny $\varphi : \mathcal{E}' \rightarrow \mathcal{E}$ defined by

$$\varphi(x, y) = \left(\frac{x^3 + 32}{x^2}, \frac{x^3 y - 64y}{x^3} \right),$$

of degree 3. A simple calculation shows that $j'(x, y) = j(\varphi(x, y))$ and thus $\text{Im}(j) = \text{Im}(j')$. Because of the relationship between these two groups and the j -maps of these modular curves, any elliptic curve that have potentially $G_E^\infty(2)$ conjugate to a subgroup of 8X5 and $G_E^\infty(3)$ conjugate to a subgroup of 3Nn must have (smaller) images: $G_E^\infty(2)$ conjugate to 8X17. Further, 8X17 is a subgroup of 2B and so the mod 2 Galois representation was already non-surjective. Thus, there are no elliptic curves of type $[8X5, 3Nn]$ despite the fact that $\mathcal{E}(\mathbb{Q})$ contains infinitely many points.

- ★ $[3Nn, 5S4]$: Similarly the type $[3Nn, 5S4]$ does not actually occur for any elliptic curves over \mathbb{Q} despite the fact that the modular curve corresponding to this type has infinitely many rational points. This is again because the modular curves for $[3Nn, 5S4]$ and $[3Nn, 5Ns]$ are isogenous elliptic curves and their j -maps are related in the same way as the curves above. The group 5Ns is a proper subgroup of 5S4 and thus every elliptic curve coming from a rational point on the modular curve for $[3Nn, 5S4]$ also comes from a point on the modular curve for the smaller type $[3Nn, 5Ns]$. In this case the modular curve associated to $[3Nn, 5S4]$ has Cremona label 225a2 and for $[3Nn, 5Ns]$ is 225a1. These elliptic curves both have rank 1 and are 3-isogenous to each other.

To summarize the above two cases, any elliptic cure of type $[8X5, 3Nn]$ (resp. $[3Nn, 5S4]$) must also be of smaller type $[8X17, 3Nn]$ (resp. $[3Nn, 5Ns]$). So there are no elliptic curves of exact adic type $[8X5, 3Nn]$ (resp. exact type $[3Nn, 5S4]$) as all the curves of these types much have strictly smaller exact (adic-)type.

Now, we know that for a given (adic-)type to occur for infinitely many $\overline{\mathbb{Q}}$ -isomorphism classes of elliptic curves it must be that the corresponding moduli space is genus 0 with a rational points or an elliptic curve with positive rank over \mathbb{Q} . Calculating all the possibilities gives the lists that appear in part (A) of Theorems 16 and 18 and

the proof of Corollary 17 shows that the list in Theorem 16 part (A) is in fact complete. Further, a similar analysis of the computations completes the proof of Theorem 18.

In fact, with a further computation, we can prove the following lemma as well.

Lemma 22. *There are no (adically-)exceptional types of length 3 such that there exist infinitely many non-isomorphic classes of non-CM elliptic curves over \mathbb{Q} .*

Proof. Let us suppose that there is a type of length 3 of the form $[G_1, G_2, G_3]$ such that there exist infinitely many non-isomorphic classes of non-CM elliptic curves over \mathbb{Q} with that type. In order for this to be the case it must be that all the subtypes of length 2, $[G_i, G_j]$, occur for infinitely many $\overline{\mathbb{Q}}$ -isomorphism classes of elliptic curves. Looking for all the possibilities in all the pairs at (A) in Theorems 16 and 18 we have that the unique possibility is $[3Nn, 5B, 2B]$. The modular curve associated to $[3Nn, 5B, 2B]$ is equivalent to the fiber product of X_{3Nn} and $X_{10B} = X_0(10)$. This modular curve² has genus 2 and an hyperelliptic model is $C : y^2 = x^6 - 18x^3 + 1$. Since its jacobian has rank 0 we can apply Chabauty to obtain all the rational points. We have obtained that all the rational points, correspond to cusps. Therefore there not exist any triples $[G_1, G_2, G_3]$ of exceptional types or adically-exceptional types such that there exist infinitely many non-isomorphic classes of non-CM elliptic curves over \mathbb{Q} of that type. \square

In order to complete the proof of Theorem 10 we still need to justify that there are infinitely many distinct $\overline{\mathbb{Q}}$ -isomorphism classes of elliptic curves defined over \mathbb{Q} with Serre's constant corresponding to the levels of all the modular curves associated to the types that appear in Tables 6, 7 and 9. We have justified already that all the other's appears, but there is a subtlety that still needs to be sorted out with 104. While we have seen that there are infinitely many $\overline{\mathbb{Q}}$ -isomorphism classes of elliptic curve of type $[8X4, 13B]$ since the modular curve corresponding to $[8X4, 13B]$ is genus 1 of positive rank, but it is possible that for all but finitely many of these $\overline{\mathbb{Q}}$ -isomorphism classes the mod 2 or mod 4 image is not actually surjective while still being contained inside $8X4$. Therefore, all but finitely many of these curve might have smaller Serre's constant (either 26 or 52). We start by showing that if E/\mathbb{Q} has type $[8X4, 13B]$, then the mod 2 Galois representation associated to E must be surjective. Since having mod 8 image contained in the group associated to $8X4$ corresponds to having $\Delta(E) = -2t^2$ for some $t \in \mathbb{Q}$ we know that the only way that E could have non-surjective mod 2 image would be for E to have a rational point of order 2. This, of course, is impossible for an elliptic curve of type $[8X4, 13B]$ since any such curve already has a 13-isogeny and there are no elliptic curves over \mathbb{Q} with a 26-isogeny. Lastly, using the database in [35] we see that in order for an elliptic curve to have surjective image mod 2, be of type $[8X4, 13B]$, and to not have surjective image mod 4 if for the mod 4 image to be contained in the group associated to $4X7$. This would mean that E also has type $[4X7, 13B]$, but our computations show that the modular curve corresponding to $[4X7, 13B]$ is genus 3 and so there can be at most finitely many such $\overline{\mathbb{Q}}$ -isomorphism classes. Thus, there must be infinitely many curves with Serre's constant 104 and we have completed the proof of Theorem 10. That is, \mathcal{A}_∞ is the set consisting of the levels of all the modular curves associated to the types that appear in Tables 6, 7 and 9.

To finish our project we still need to complete the classification of possible (adic-)types and Serre's constant. To do this we fix our attention to the associated modular curves with finitely many rational points. That is, genus 1 and rank 0, or genus >1 :

- Genus 1 and rank 0: There are 28 elliptic curves of rank 0. Only 8 have points that correspond to non-CM elliptic curves. All the data appears in Tables 11 and 12. The case $[4X7, 3B]$ does not appear in that table:

- ★ The modular curve associated to the type $[4X7, 3B]$ is the elliptic curve \mathcal{E}/\mathbb{Q} with Cremona label 48a6 and with Mordell-Weil group $\mathcal{E}(\mathbb{Q}) \simeq \mathbb{Z}/8\mathbb{Z}$. These points give the non-CM j -invariants $j_1 = -3^3 \cdot 11^3/2^2$ and $j_2 = 3^2 \cdot 23^3/2^6$. Now, let $j(t)$ be the j -map (see Table 6) of the genus 0 modular curve associated to the type $[4X3, 3B]$. Therefore $j(-1/2) = j_1$ and $j(-1) = j_2$. Therefore there are no elliptic curves with type $[4X7, 3B]$ as any curve with this combination of images actually has smaller images $[4X20, 3B]$. Here $4X7$ refers to the level 4 group X_{20} in the notation of [35].

- Genus = 2: We have computed all the rational points of all the modular curves of genus 2. In all the cases we have not obtained non-CM elliptic curves, except in the case $[4X7, 7B]$:

- ★ The associated modular curve to the type $[4X7, 7B]$ has genus 2 and we have computed all its rational points. In this cases the non-CM non-singular j -invariants are $j_1 = 3^3 \cdot 13/2^2$ and $j_2 = -3^3 \cdot 13 \cdot 479^3/2^{14}$

²A remarkable fact is that this genus 2 curve is new modular of level 90 and its jacobian is \mathbb{Q} -isogenous to the product of two elliptic curves (see [2]).

(see Table 13). That corresponds to evaluate the j -map of the genus 0 modular curve associated to the type [4X3, 7B] at the values $7/2$ and 2 respectively. Therefore any elliptic curve E with those j -invariants satisfies that $G_E^\infty(2)$ is conjugate to a subgroup of 4X3 and 4X7, and $G_E^\infty(7)$ is conjugate to a subgroup of 7B.

- Genus > 2 : We did a point search to find all easily visible points of bounded height. We have found only non-CM, non-cusps in the modular curve associated to the types [8X5, 7Ns] and [4X7, 9XE]. But the case [8X5, 7Ns] does not appear at the statement:

- ★ The corresponding modular curve to the type [8X5, 7Ns] has genus 3 and searching for points of height less than or equal to 10^6 yields only one non-CM non-singular j -invariant, $j = 3^3 \cdot 5 \cdot 7^5 / 2^7$ (see Table 14) that corresponds to the unique j -invariant for the case $G_E(7)$ labeled as 7Ns.3.1 (see Table 1).

The above proves (B) of Theorems 16 and 18.

Example 23. Let E be the elliptic curve given by Weierstrass equation $y^2 + xy + y = x^3 - 126x - 552$. This curve has Cremona reference 50a1, it does not have CM and according to LMFDB [30], $G_E(3) = 3B.1.2$, $G_E(5) = 5B.1.3$, and $G_E(p) = \text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ for every other prime p . Checking the 2-adic representation in [30] (which uses the data collected in [35]) we see that the image of $\rho_{E,2^\infty}$ is the pullback of the group 8X4 under the standard reduction map $\pi : \text{GL}_2(\mathbb{Z}_2) \rightarrow \text{GL}_2(\mathbb{Z}/8\mathbb{Z})$. So the 2-adic representation associated to E is not surjective and $A(E) = 120$. Here we point out that if we let $\pi_k : \text{GL}_2(\mathbb{Z}/8\mathbb{Z}) \rightarrow \text{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$ be the standard componentwise reduction map for $k = 1$, and 2 , then $\pi_1(H) = \text{GL}_2(\mathbb{Z}/2\mathbb{Z})$ and $\pi_2(H) = \text{GL}_2(\mathbb{Z}/4\mathbb{Z})$ where $H = G_E^\infty(2)$. Therefore, $\rho_{E,2}$ and $\rho_{E,4}$ are both surjective. The modular curve whose points correspond to elliptic curves with these mod 3, 5, and 8 images is genus greater than 1, so there are only finitely many \mathbb{Q} -isomorphism classes of elliptic curves with this particular combination of images. Moreover, since we have obtained all the rational points at the modular curve associated to [3B, 5B] we are done.

Remark 24. In fact we can check that for the four j -invariants coming from the modular curve [3B, 5B] have that the image of $\rho_{E,2^\infty}$ is the pullback of the group 8X4. Similarly with [3B, 7B] and 8X4; and [3B, 5S4] with 8X3. In particular this complete the computation of all the points at the modular curves associated to [4X3, 3B, 5S4], [8X4, 3B, 5B] and [8X4, 3B, 7B].

Therefore we have obtained all the possible j -invariants for the item (B) at Theorems 16 and 18, except (maybe) the type [4X7, 9XE]. The modular curve associated to the former case has genus 6. In this article we have not tried to compute all the rational points of such a curves. This will be done in an ongoing project [17].

APPENDIX: TABLES

In this section, we give tables of data that summarize the results that we used in our computations as well as the data that we collected. Tables 1, 2, and 3 are taken from the results in [41] where Zywinia does a search for all possible images of the mod p representations associated to non-CM elliptic curves over \mathbb{Q} and then computes the moduli spaces for the ones that actually occur. Throughout [41] Zywinia is careful to distinguish between subgroup of $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ that do and do not contain $-I$. This is because if E and E' are quadratic twists of each other then we do not necessarily know that $G_E(p) = G_{E'}(p)$. In this case all that can be said is that $\langle G_E(p), -I \rangle = \langle G_{E'}(p), -I \rangle$. Therefore, if $G \subseteq \text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ contains $-I$, then $G_E(p) \subseteq G$ if and only if $G_{E'}(p) \subseteq G$, while if $-I \notin G$ then it is possible that $G_E(p) \subseteq G$ and $G_{E'}(p) \not\subseteq G$. Combining this with the fact that two non-CM elliptic curves E/\mathbb{Q} and E'/\mathbb{Q} are \mathbb{Q} -isomorphic if and only if they are quadratic twists of each other, we have that the moduli spaces associated to groups containing $-I$ are completely determined by a j -map and are coarse moduli spaces (See Tables 1). On the other hand, the moduli spaces associated to groups that do not contain $-I$ are called fine moduli spaces and are given by elliptic surfaces such that each nonsingular specialization is a representative of a \mathbb{Q} -isomorphism class with the given type (See Table 3). We have included these three tables for the sake of completeness.

There are places in the tables where the polynomials that need to be written are too complicated to fit in the space provided. In those cases we simplify the entry by defining some notation for factors of the polynomials. The extra data is then presented at the end of the Appendix organized by table number.

Below we give a description of each of the tables:

- Table 1: For each possible groups $G_E(p) \neq \text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ with $-I \in G_E(p)$ we give Sutherland's and Zywinia's labels, the level, generators, the (possibly constant) j -maps, and the Cremona label of an elliptic curve with minimal conductor with mod p image equal to the given group.

- Table 2: For each possible groups $G_E(p) \neq \text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ with $-I \notin G_E(p)$ we give Sutherland's and Zywin's labels, the level, generators, and the Cremona label of an elliptic curve with minimal conductor with mod p image equal to the given group.
- Table 3: For each possible groups $G_E(p) \neq \text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ with $-I \notin G_E(p)$ we give an elliptic curve model for the fine moduli.
- Table 4: For each group $G_E(p^k)$ with $k \geq 2$ that surjects onto $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ we give the level, generators j -map, and the Cremona label of an elliptic curve with minimal conductor with mod p image equal to the given group.
- Table 5: For each group in Table 1 that only has finitely many $\overline{\mathbb{Q}}$ -isomorphism classes, we check if the corresponding j -invariants are in the image of the j -map of other modular curves. The results of this checking are compiled in this table.
- Table 6: For each exceptional type $[G_E(p), G_E(q)]$ such that $G_E(p)$ and $G_E(q)$ containing $-I$ and the corresponding modular curve has genus 0 we give the j -map associated to the curve and the Cremona label of an elliptic curve with minimal conductor and that type. We do the same thing for maximal adically exceptional types.
- Table 7: For each exceptional type $[G_E(p), G_E(q)]$ such that $G_E(p)$ and $G_E(q)$ with $-I$ not in one of the groups such that the corresponding modular curve has genus 0 we give the parametrization to obtain a fine moduli associated to the curve and the Cremona label of an elliptic curve with minimal conductor and that type.
- Table 8: For each exceptional type such that the corresponding modular curve is genus 1 we give the the Cremona reference of the modular curve as well as the structure of the Mordell-Weil group of the modular curve in the case of the curve is elliptic, otherwise we show a reason why does not have rational points. We do the same thing for maximal adically-exceptional types.
- Table 9: For each modular curve in Table 8 with positive rank, except $[8X5, 3Nn]$ and $[3Nn, 5S4]$ (see §5), we give the j -map, Cremona reference of the modular curve, and the Cremona reference of an elliptic curve with minimal conductor (if this is less than 400.000) and that (adic-)type.
- Table 10: For each modular curve in Table 9 with positive rank such that the examples of minimal conductor are greater than 400000 and thus does not have a page in the LMFDB, we give a minimal model of the an elliptic curve with that (adic-)type and its conductor.
- Table 11: For each modular curve in Table 8 with rank 0 and $-I$ in both group we give a complete list of the j -invariants that correspond to all the $\overline{\mathbb{Q}}$ -isomorphic classes with that (adic-)type, and the Cremona labels of examples of elliptic curves with that combination of representations of minimal conductor.
- Table 12: For each modular curve in Table 8 with rank 0 and $-I$ not in both groups we give a complete list of the Cremona labels of all elliptic curves with that (adic-)type.
- Table 13: For each possible (adic-)type whose curve has genus 2 we give a complete list of non-cusps and rational points and their corresponding elliptic curves j -invariants.
- Table 14: We give a list of the modular curves that one would classify all the non-cusps and rational points in order to prove Conjecture 12. For each type we add a subscript indicating the genus of the corresponding modular curve, a superscript of cm when the only points we have found correspond to elliptic curves with CM or a superscript of \emptyset in the case that we have not found any rational point.
- Table 15: We give examples of elliptic curves with a given (adic-)type whose modular curves have genus greater than one and whose points correspond to elliptic curves that do not appear in the LMFDB.

Remark 25. All the `Magma` [10] code to compute the tables in this appendix is available in the online supplement [16]. Some of the code for this paper was taken from [18].

Sutherland	Zywin	Model	Example
3B.1.1	$H_{3,1}$	$\mathcal{E}_{3,3}$	19a3
3B.1.2	$H_{3,2}$	$\mathcal{E}_{3,3}^{-3}$	19a2
3Cs.1.1	$H_{1,1}$	$\mathcal{E}_{3,1}$ or $\mathcal{E}_{3,1}^{-3}$	19a1
5B.1.1	$H_{6,1}$	$\mathcal{E}_{5,6}$	11a3
5B.1.2	$H_{5,1}$	$\mathcal{E}_{5,5}$	11a2
5B.1.3	$H_{5,2}$	$\mathcal{E}_{5,5}^5$	75a1
5B.1.4	$H_{6,2}$	$\mathcal{E}_{5,6}^5$	75a2
5Cs.1.1	$H_{1,1}$	$\mathcal{E}_{5,1}$	11a1
5Cs.1.3	$H_{1,2}$	$\mathcal{E}_{5,1}^5$	275b2

Sutherland	Zywin	Model	Example
7B.1.1	$H_{3,1}$	$\mathcal{E}_{7,3}$	26b1
7B.1.2	$H_{5,2}$	$\mathcal{E}_{7,5}^{-7}$	637a1
7B.1.3	$H_{4,1}$	$\mathcal{E}_{7,4}$	26b2
7B.1.4	$H_{4,2}$	$\mathcal{E}_{7,4}^{-7}$	294a1
7B.1.5	$H_{5,1}$	$\mathcal{E}_{7,5}$	637a2
7B.1.6	$H_{3,2}$	$\mathcal{E}_{7,3}^{-7}$	294a2
7B.2.1	$H_{7,2}$	$\mathcal{E}_{7,7}^{-7}$	338b1
7B.2.3	$H_{7,1}$	$\mathcal{E}_{7,7}$	338b2
7Ns.2.1	$H_{1,1}$	$\mathcal{E}_{7,1}$ or $\mathcal{E}_{7,1}^{-7}$	2450ba1

Sutherland	Zywin	Model	Example
11B.1.4	$H_{1,1}$	$\mathcal{E}_{11,1}$	121a2
11B.1.5	$H_{2,1}$	$\mathcal{E}_{11,2}$	121a1
11B.1.6	$H_{2,2}$	$\mathcal{E}_{11,2}^{-11}$	121c2
11B.1.7	$H_{1,2}$	$\mathcal{E}_{11,1}^{-11}$	121c1
13B.3.1	$H_{5,1}$	$\mathcal{E}_{13,5}$	147b1
13B.3.2	$H_{4,1}$	$\mathcal{E}_{13,4}$	147b2
13B.3.4	$H_{5,2}$	$\mathcal{E}_{13,5}^{13}$	24843o1
13B.3.7	$H_{4,2}$	$\mathcal{E}_{13,4}^{13}$	24843o2

Sutherland	Zywina	Level	Generators	j-map	Example
2Cs	G_1	2		$256 \frac{(t^2+t+1)^3}{t^2(t+1)^2}$	15a1
2B	G_2	2	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$256 \frac{(t+1)^3}{t}$	15a4
2Cn	G_3	2	$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$	$t^2 + 1728$	392b1
3Cs	G_1	3	$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$	$27 \frac{(t+1)^3(t+3)^3(t^2+3)^3}{t^3(t^2+3t+3)^3}$	175b2
3Ns	G_2	3	$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$	$27 \frac{(t+1)^3(t-3)^3}{t^3}$	1210d1
3B	G_3	3	$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$27 \frac{(t+1)(t+9)^3}{t^3}$	175b1
3Nn	G_4	3	$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 2 & 2 \end{pmatrix}$	t^3	245a1
5Cs.4.1	G_1	5	$\begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$	$\frac{(t^{20}+228t^{15}+494t^{10}-228t^5+1)^3}{t^5(t^{10}-11t^5-1)^5}$	99d2
5Cs	G_2	5	$\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$	$\frac{(t^2+5t+5)^3(t^4+5t^2+25)^3(t^4+5t^3+20t^2+25t+25)^3}{t^5(t^4+5t^3+15t^2+25t+25)^5}$	18176b2
5Ns.2.1	G_3	5	$\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix}$	$\frac{5^4 t^3 (t^2+5t+10)^3 (2t^2+5t+5)^3 (4t^4+30t^3+95t^2+150t+100)^3}{(t^2+5t+5)^5 (t^4+5t^3+15t^2+25t+25)^5}$	6975a1
5Ns	G_4	5	$\begin{pmatrix} 0 & 4 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$	$\frac{(t+5)^3(t^2-5)^3(t^2+5t+10)^3}{(t^2+5t+5)^5}$	608b1
5B.4.2	G_5	5	$\begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\frac{(t^4+228t^3+494t^2-228t+1)^3}{t(t^2-11t-1)^5}$	99d3
5B.4.1	G_6	5	$\begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\frac{(t^4-12t^3+14t^2+12t+1)^3}{t^5(t^2-11t-1)}$	99d1
5Nn	G_7	5	$\begin{pmatrix} 1 & 0 \\ 0 & 4 \end{pmatrix}, \begin{pmatrix} 2 & 3 \\ 4 & 2 \end{pmatrix}$	$\frac{5^3(t+1)(2t+1)^3(2t^2-3t+3)^3}{(t^2+t-1)^5}$	675b1
5B	G_8	5	$\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\frac{5^2(t^2+10t+5)^3}{t^5}$	867c1
5S4	G_9	5	$\begin{pmatrix} 0 & 3 \\ 3 & 4 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 4 & 4 \end{pmatrix}$	$t^3(t^2+5t+40)$	648a1
7Ns.3.1	G_1	7	$\begin{pmatrix} 3 & 0 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 4 & 0 \end{pmatrix}$	$3^3 \cdot 5 \cdot 7^5 / 2^7$	2450a1
7Ns	G_2	7	$\begin{pmatrix} 0 & 6 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}$	$\frac{t(t+1)^3(t^2-5t+1)^3(t^2-5t+8)^3(t^4-5t^3+8t^2-7t+7)^3}{(t^3-4t^2+3t+1)^7}$	9225a1
7B.6.1	G_3	7	$\begin{pmatrix} 6 & 0 \\ 0 & 6 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\frac{(t^2-t+1)^3(t^6-11t^5+30t^4-15t^3-10t^2+5t+1)^3}{(t-1)^7 t^7 (t^3-8t^2+5t+1)}$	208d1
7B.6.3	G_4	7	$\begin{pmatrix} 6 & 0 \\ 0 & 6 \end{pmatrix}, \begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\frac{(t^2-t+1)^3(t^6+229t^5+270t^4-1695t^3+1430t^2-235t+1)^3}{(t-1)t(t^3-8t^2+5t+1)^7}$	208d2
7B.6.2	G_5	7	$\begin{pmatrix} 6 & 0 \\ 0 & 6 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$-\frac{(t^2-3t-3)^3(t^2-t+1)^3(3t^2-9t+5)^3(5t^2-t-1)^3}{(t^3-2t^2-t+1)(t^3-t^2-2t+1)^7}$	5733d1
7Nn	G_6	7	$\begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}, \begin{pmatrix} 2 & 5 \\ 4 & 2 \end{pmatrix}$	$\frac{64t^3(t^2+7)^3(t^2-7t+14)^3(5t^2-14t-7)^3}{(t^3-7t^2+7t+7)^7}$	15341a1
7B	G_7	7	$\begin{pmatrix} 3 & 0 \\ 0 & 5 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\frac{(t^2+245t+2401)^3(t^2+13t+49)}{t^7}$	338a1
11B.10.4	G_1	11	$\begin{pmatrix} 10 & 0 \\ 0 & 10 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 6 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	-11^2	1089f2
11B.10.5	G_2	11	$\begin{pmatrix} 10 & 0 \\ 0 & 10 \end{pmatrix}, \begin{pmatrix} 5 & 0 \\ 0 & 7 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$-11 \cdot 131^3$	1089f1
11Nn	G_3	11	$\begin{pmatrix} 1 & 0 \\ 0 & 10 \end{pmatrix}, \begin{pmatrix} 3 & 5 \\ 8 & 3 \end{pmatrix}$	$\frac{P_{11}(x,y)^3}{(11y+(2x^2+17x-34))^2((x-4)y-(5x-9))^{11}}, \quad y^2+y=x^3-x^2-7x+10$	232544f1
13B.5.2	G_1	13	$\begin{pmatrix} 5 & 0 \\ 0 & 8 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\frac{(t^2-t+1)^3 P_{13}(t)^3}{(t-1)t(t^3-4t^2+t+1)^{13}}$	2890d2
13B.5.1	G_2	13	$\begin{pmatrix} 5 & 0 \\ 0 & 8 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\frac{(t^2-t+1)^3(t^{12}-9t^{11}+29t^{10}-40t^9+22t^8-16t^7+40t^6-22t^5-23t^4+25t^3-4t^2-3t+1)^3}{(t-1)^{13} t^{13} (t^3-4t^2+t+1)}$	2890d1
13B.5.4	G_3	13	$\begin{pmatrix} 5 & 0 \\ 0 & 8 \end{pmatrix}, \begin{pmatrix} 4 & 0 \\ 0 & 7 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$-\frac{13^4(t^2-t+1)^3(t^4-t^3+2t^2-9t+3)^3(3t^4-3t^3-7t^2+12t-4)^3(4t^4-4t^3-5t^2+3t-1)^3}{(t^3-4t^2+t+1)^{13} (5t^3-7t^2-8t+5)}$	216320i1
13B.4.2	G_4	13	$\begin{pmatrix} 4 & 0 \\ 0 & 10 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\frac{(t^4-t^3+5t^2+t+1)(t^8+235t^7+1207t^6+955t^5+3840t^4-955t^3+1207t^2-235t+1)^3}{t(t^2-3t-1)^{13}}$	147c2
13B.4.1	G_5	13	$\begin{pmatrix} 4 & 0 \\ 0 & 10 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\frac{(t^4-t^3+5t^2+t+1)(t^8-5t^7+7t^6-5t^5+5t^3+7t^2+5t+1)^3}{t^{13}(t^2-3t-1)}$	147c1
13B	G_6	13	$\begin{pmatrix} 2 & 0 \\ 0 & 7 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$\frac{(t^2+5t+13)(t^4+7t^3+20t^2+19t+1)^3}{t}$	2450bb1
13S4	G_7	13	$\begin{pmatrix} 3 & 0 \\ 12 & 9 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 9 & 5 \\ 0 & 6 \end{pmatrix}$	$\frac{2^4 \cdot 5 \cdot 13^4 \cdot 17^3}{3^{13}}, -\frac{2^{12} \cdot 5^3 \cdot 11 \cdot 13^4}{3^{13}} \text{ or } \frac{2^{18} \cdot 3^3 \cdot 13^4 \cdot 127^3 \cdot 139^3 \cdot 157^3 \cdot 283^3 \cdot 929}{5^{13} \cdot 61^{13}}$	5070011
17B.4.2	G_1	17	$\begin{pmatrix} 4 & 0 \\ 0 & 13 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 10 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$-17 \cdot 373^3 / 2^{17}$	14450bk1
17B.4.6	G_2	17	$\begin{pmatrix} 4 & 0 \\ 0 & 13 \end{pmatrix}, \begin{pmatrix} 6 & 0 \\ 0 & 9 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$-17^2 \cdot 101^3 / 2$	14450bk2
37B.8.1	G_1	37	$\begin{pmatrix} 8 & 0 \\ 0 & 14 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$-7 \cdot 11^3$	1225e1
37B.8.2	G_2	37	$\begin{pmatrix} 8 & 0 \\ 0 & 14 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$	$-7 \cdot 137^3 \cdot 2083^3$	1225e2

 TABLE 1. Groups $G_E(p)$ containing $-I$, for non-CM elliptic curves E/\mathbb{Q}

TABLE 2. Groups $G_E(p)$ not containing $-I$, for non-CM elliptic curves E/\mathbb{Q}

$\mathcal{E}_{3,1} : y^2$	$= x^3 - 3(t+1)(t+3)(t^2+3)x - 2(t^2-3)(t^4+6t^3+18t^2+18t+9)$
$\mathcal{E}_{3,3} : y^2$	$= x^3 - 3(t+1)^3(t+9)x - 2(t+1)^4(t^2-18t-27)$
$\mathcal{E}_{5,1} : y^2$	$= x^3 - 27(t^{20} + 228t^{15} + 494t^{10} - 228t^5 + 1)x + 54(t^{30} - 522t^{25} - 10005t^{20} - 10005t^{10} + 522t^5 + 1)$
$\mathcal{E}_{5,5} : y^2$	$= x^3 - 27(t^4 + 228t^3 + 494t^2 - 228t + 1)x + 54(t^6 - 522t^5 - 10005t^4 - 10005t^2 + 522t + 1)$
$\mathcal{E}_{5,6} : y^2$	$= x^3 - 27(t^4 - 12t^3 + 14t^2 + 12t + 1)x + 54(t^6 - 18t^5 + 75t^4 + 75t^2 + 18t + 1)$
$\mathcal{E}_{7,1} : y^2$	$= x^3 - 5^3 7^3 x - 5^4 7^2 106$
$\mathcal{E}_{7,3} : y^2$	$= x^3 - 27(t^2 - t + 1)(t^6 - 11t^5 + 30t^4 - 15t^3 - 10t^2 + 5t + 1)x + 54Q_{7,3}(t)$
$\mathcal{E}_{7,4} : y^2$	$= x^3 - 27(t^2 - t + 1)(t^6 + 229t^5 + 270t^4 - 1695t^3 + 1430t^2 - 235t + 1)x + 54Q_{7,4}(t)$
$\mathcal{E}_{7,5} : y^2$	$= x^3 - 27 \cdot 7(t^2 - 3t - 3)(t^2 - t + 1)(3t^2 - 9t + 5)(5t^2 - t - 1)x - 54 \cdot 7^2 Q_{7,5}(t)$
$\mathcal{E}_{7,7} : y^2$	$= x^3 - 27(t^2 + 13t + 49)^3(t^2 + 245t + 2401)x + 54(t^2 + 13t + 49)^4(t^4 - 490t^3 - 21609t^2 - 235298t - 823543)$
$\mathcal{E}_{11,1} : y^2$	$= x^3 - 27 \cdot 11^4 x + 54 \cdot 11^5 \cdot 43$
$\mathcal{E}_{11,2} : y^2$	$= x^3 - 27 \cdot 11^3 \cdot 131x + 54 \cdot 11^4 \cdot 4973$
$\mathcal{E}_{13,4} : y^2$	$= x^3 - 27(t^4 - t^3 + 5t^2 + t + 1)^3 P_{13,4}(t)x + 54(t^2 + 1)(t^4 - t^3 + 5t^2 + t + 1)^4 Q_{13,4}(t)$
$\mathcal{E}_{13,5} : y^2$	$= x^3 - 27(t^4 - t^3 + 5t^2 + t + 1)^3 P_{13,5}(t)x + 54(t^2 + 1)(t^4 - t^3 + 5t^2 + t + 1)^4 Q_{13,5}(t)$

TABLE 3. Elliptic curve model for the fine moduli

Type	level	generators	j-map	Example
4X3	4	$\begin{pmatrix} 3 & 3 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 3 & 1 \end{pmatrix}$	$-t^2 + 1728$	567a1
4X7	4	$\begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$	$-4t^3(t+8)$	216a1
8X4	8	$\begin{pmatrix} 7 & 7 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 5 & 0 \\ 1 & 1 \end{pmatrix}$	$-2t^2 + 1728$	216a1
8X5	8	$\begin{pmatrix} 5 & 5 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$	$2t^2 + 1728$	1682b1
9XE	9	$\begin{pmatrix} 4 & 5 \\ 4 & 4 \end{pmatrix}, \begin{pmatrix} 4 & 8 \\ 8 & 6 \end{pmatrix}$	$\frac{3^7(t^2-1)^3(t^6+3t^5+6t^4+t^3-3t^2+12t+16)^3(2t^3+3t^2-3t-5)}{(t^3-3t-1)^9}$	1944c1

TABLE 4. Maximal groups $G_E^\infty(p)$, for non-CM elliptic curves E/\mathbb{Q} and $p = 2, 3$

Type	j-invariants	Examples
[4X3, 11B.10.4]	-11^2	1089h1
[4X3, 11B.10.5]	$-11 \cdot 131^3$	1089h2
[8X5, 7Ns.3.1]	$3^3 \cdot 5 \cdot 7^5 / 2^7$	2450a1

TABLE 5. Modular curves: isolated point

Type	j -maps	Example
[2B, 3B]	$\frac{(11t-8)^3(1259t^3-2856t^2+2112t-512)^3}{2(t-1)t^6(3t-2)^3(25t-16)^2}$	80b1
[2B, 3Cs]	$-\frac{(54t^3-1)^3(54t^3-54t^2-1)^3(2916t^6+2916t^5+2916t^4-108t^3-54t^2+1)^3}{729t^6(3t+1)^6(6t-1)^3(9t^2-3t+1)^6(36t^2+6t+1)^3}$	98a3
[2B, 3Nn]	$\frac{(t^3+16)^3}{t^3}$	1568d1
[2B, 3Ns]	$\frac{(1024t^3+1920t^2+768t+115)^3(1024t^3+1920t^2+1200t+223)^3}{46656(t+1)^3(4t+1)^3(16t+7)^6}$	726a1
[2B, 5B]	$-\frac{(5t^6-2080t^5+81920t^4-1310720t^3+10485760t^2-41943040t+67108864)^3}{8(t-8)^5t^{10}(5t-32)^2}$	768b1
[2B, 5B.4.1]	$\frac{P_1(t)^3}{590490000000000t^{10}(3788t+1)^5(3818t+1)^{10}(3848t+1)^5(14118064t^2+7516t+1)(14690764t^2+7666t+1)^2}$	198e1
[2B, 5B.4.2]	$-\frac{P_2(t)^3}{4t^2(2t-1)^2(4t-1)(4t^2+2t-1)^{10}(16t^2-12t+1)^5}$	198e3
[2Cn, 3B]	$\frac{9(t^2+3)(t^2+27)^3}{t^6}$	196a1
[2Cn, 5S4]	$\frac{(3t^2+1)^3(64t^4+11t^2+1)}{t^{10}}$	1444a1
[2Cn, 7B]	$\frac{(7t^2-t+1)(7t^2+t+1)(2401t^4+245t^2+1)^3}{t^2}$	1922e1
[2Cs, 3B]	$\frac{(7t^2+6t+3)^3(127t^6+738t^5+1605t^4+1260t^3+345t^2+18t+3)^3}{4(t-1)^6t^2(t+1)^6(t+3)^2(3t+1)^6(5t+3)^2}$	150c2
[3Nn, 5B]	$\frac{(3125t^6+250t^3+1)^3}{t^3}$	1369e1
[4X3, 3B]	$-\frac{9(t^2-2t-26)^3(t^2-2t-2)}{(t-1)^6}$	242a1
[4X3, 5S4]	$\frac{(3t^2-1)^3(64t^4-11t^2+1)}{t^{10}}$	324b1
[4X3, 7B]	$-\frac{(t^4-245t^2+2401)^3(t^4-13t^2+49)}{t^{14}}$	1369c2
[4X7, 3Nn]	$-\frac{(32t^3+1)^3}{64t^{12}}$	80802b1
[8X4, 3B]	$-\frac{9(t^2-2t-53)^3(t^2-2t-5)}{2(t-1)^6}$	1296k2
[8X4, 5S4]	$\frac{2(3t^2-2)^3(32t^4-11t^2+2)}{t^{10}}$	4232d1
[8X4, 7B]	$-\frac{(49t^4-26t^2+4)(2401t^4-490t^2+4)^3}{128t^2}$	162c3
[8X5, 3B]	$\frac{9(t^2+6)(t^2+54)^3}{2t^6}$	7938d1
[8X5, 5S4]	$\frac{2(3t^2+2)^3(32t^4+11t^2+2)}{t^{10}}$	16200e1
[8X5, 7B]	$\frac{(49t^4+26t^2+4)(2401t^4+490t^2+4)^3}{128t^2}$	12482f2

TABLE 6. Modular curves of genus 0

Type	Model	Parametrization	Example
[2B, 3B.1.1]	$\mathcal{E}_{3,3}$	$\frac{512(t-1)(3t-2)^3}{t^3(25t-16)}$	14a4
[2B, 3B.1.2]	$\mathcal{E}_{3,3}^{-3}$		14a3
[2B, 3Cs.1.1]	$\mathcal{E}_{3,1}$ or $\mathcal{E}_{3,1}^{-3}$	$-\frac{(6t-1)^3(36t^2+6t+1)^3}{432t^3(3t+1)^3(9t^2-3t+1)^3}$	14a1
[2B, 5B.1.1]	$\mathcal{E}_{5,6}$	$\frac{(3788t+1)^5(3848t+1)^5(14118064t^2+7516t+1)}{388800000t^5(3818t+1)^5(14690764t^2+7666t+1)}$	66c1
[2B, 5B.1.4]	$\mathcal{E}_{5,6}^5$		150b3
[2B, 5B.1.2]	$\mathcal{E}_{5,5}$	$-\frac{(4t-1)(16t^2-12t+1)^5}{32t(2t-1)(4t^2+2t-1)^5}$	66c3
[2B, 5B.1.3]	$\mathcal{E}_{5,5}^5$		150b1
[2Cn, 3B.1.1]	$\mathcal{E}_{3,3}$	$\frac{3(t^4-54t^2-243)}{t^3}$	196b1
[2Cn, 3B.1.2]	$\mathcal{E}_{3,3}^{-3}$		196b2
[2Cn, 7B.2.1]	$\mathcal{E}_{7,7}^{-7}$	$-\frac{823543t^8+235298t^6+21609t^4+490t^2-1}{t}$	1922c1
[2Cn, 7B.2.3]	$\mathcal{E}_{7,7}$		1922c2
[2Cs, 3B.1.1]	$\mathcal{E}_{3,3}$	$-\frac{(t+3)(3t+1)^3}{32t(t+1)^3}$	30a2
[2Cs, 3B.1.2]	$\mathcal{E}_{3,3}^{-3}$		30a6

TABLE 7. Modular curves of genus 0: Fine Moduli Spaces

Type	\mathcal{E}/\mathbb{Q}	$\mathcal{E}(\mathbb{Q})$
[2B, 5Nn]	50b1	$\mathbb{Z}/5\mathbb{Z}$
[2B, 5Ns]	50b1	$\mathbb{Z}/5\mathbb{Z}$
[2B, 5S4]	50b2	$\mathbb{Z}/5\mathbb{Z}$
[2Cn, 13B]	52a1	$\mathbb{Z}/2\mathbb{Z}$
[2Cn, 13B.4.1]	52a2	$\mathbb{Z}/2\mathbb{Z}$
[2Cn, 13B.4.2]	52a2	$\mathbb{Z}/2\mathbb{Z}$
[2Cn, 3Cs]	36a3	$\mathbb{Z}/2\mathbb{Z}$
[2Cn, 3Nn]	36a3	$\mathbb{Z}/2\mathbb{Z}$
[2Cn, 3Ns]	36a4	$\mathbb{Z}/2\mathbb{Z}$
[2Cn, 5B]	20a3	$\mathbb{Z}/2\mathbb{Z}$
[2Cn, 5B.4.1]	20a4	$\mathbb{Z}/2\mathbb{Z}$
[2Cn, 5B.4.2]	20a4	$\mathbb{Z}/2\mathbb{Z}$
[2Cn, 5Nn]	Non Elliptic: $\mathcal{E}(\mathbb{Q}_5) = \emptyset$	

Type	\mathcal{E}/\mathbb{Q}	$\mathcal{E}(\mathbb{Q})$
[2Cs, 3Nn]	36a1	$\mathbb{Z}/6\mathbb{Z}$
[2Cs, 3Ns]	36a1	$\mathbb{Z}/6\mathbb{Z}$
[3B, 5B]	15a1	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$
[3B, 5B.4.1]	15a3	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$
[3B, 5B.4.2]	15a3	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$
[3B, 5S4]	75c1	$\mathbb{Z}/5\mathbb{Z}$
[3B, 7B]	21a1	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$
[3Nn, 5Nn]	225a1	\mathbb{Z}
[3Nn, 5Ns]	225a1	\mathbb{Z}
[3Nn, 5S4]	225a2	\mathbb{Z}
[3Nn, 7Nn]	441b1	$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}$
[3Ns, 5B]	15a3	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$

Type	\mathcal{E}/\mathbb{Q}	$\mathcal{E}(\mathbb{Q})$
[4X3, 3Nn]	144a3	$\mathbb{Z}/2\mathbb{Z}$
[4X3, 13B]	208c1	$\mathbb{Z}/2\mathbb{Z}$
[4X3, 5B]	80b3	$\mathbb{Z}/2\mathbb{Z}$
[4X3, 5Nn]	Non Elliptic: $\mathcal{E}(\mathbb{Q}_5) = \emptyset$	
[4X7, 3B]	48a6	$\mathbb{Z}/8\mathbb{Z}$
[4X7, 5B]	80a4	$\mathbb{Z}/4\mathbb{Z}$
[4X7, 5S4]	400h1	\mathbb{Z}
[8X4, 3Nn]	576e3	$\mathbb{Z}/2\mathbb{Z}$
[8X4, 5B]	320f4	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$
[8X4, 5Nn]	Non Elliptic: $\mathcal{E}(\mathbb{Q}_2) = \emptyset$	
[8X4, 13B]	832h2	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$
[8X5, 3Nn]	576a3	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$
[8X5, 5B]	320c4	$\mathbb{Z}/2\mathbb{Z}$
[8X5, 5Nn]	1600g2	$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$
[8X5, 13B]	832d2	$\mathbb{Z}/2\mathbb{Z}$

TABLE 8. Modular curves of genus 1

Type	j -maps	\mathcal{E}/\mathbb{Q}	Example
[3Nn, 5Nn]	$\frac{125(xy+4x-y^2+4)(xy-12x+2y^2-8y-12)^3 F_1(x,y)^3}{F_2(x,y)^5}$	225a1	Table 10
[3Nn, 5Ns]	$-\frac{(y-2)^3(y^2+y+4)^3(y^2+6y+4)^3}{(y^2+y-1)^5}$	225a1	Table 10
[3Nn, 7Nn]	$\frac{(7xy+28x-2y^2-30y+59)^3 F_3(x,y)^3 F_4(x,y)^3 F_5(x,y)^3}{F_6(x,y)^7}$	441b1	Table 10
[4X7, 5S4]	$\frac{G_1(x,y)}{1024}$	400h1	12996c1
[8X4, 5B]	$-\frac{(x^2-470x+5225)^3}{2(x+15)^5}$	320f4	6400b1
[8X4, 13B]	$-\frac{(x^2-2x+28)(x^4-478x^3+7688x^2-38328x+149808)^3}{2(x+4)^{13}}$	832h2	20736c1
[8X5, 5Nn]	$\frac{8000G_2(x,y)}{(x^2-86x-151)^{10}}$	1600g2	313600bz1

TABLE 9. Modular elliptic curve with positive rank

Type	Example	$\mathcal{N}_{\mathbb{Q}}(E)$
[3Nn, 5Nn]	$y^2 = x^3 + x^2 + 1218089157x + 10584902461321$	50840066816
[3Nn, 5Ns]	$y^2 = x^3 - 1419330328x + 20580980954064$	1774432
[3Nn, 7Nn]	$y^2 = x^3 - x^2 - 439163751869x + 112018153929262517$	1541679392

TABLE 10. Examples out of LMFDB: Genus $X_G = 1$

Type	j -invariants		Examples
[3B, 5B]	[3B, 5B.4.1]	$\{-5 \cdot 29^3/2^5, 5 \cdot 211^3/2^{15}\}$	400c3, 400c4
	[3B, 5B.4.2]	$\{-5^2/2, -5^2 \cdot 241^3/2^3\}$	400c1, 400c2
[3B, 5S4]	$\{-2^4 \cdot 3^2 \cdot 13^3, 2^4 \cdot 3^3\}$		1296i1, 1296i2
[3B, 7B]	$\{-3^2 \cdot 5^3 \cdot 101^3/2^{21}, -3^3 \cdot 5^3 \cdot 383^3/2^7, 3^3 \cdot 5^3/2, -3^2 \cdot 5^6/2^3\}$		1296k4, 1296k3, 1296k1, 1296k2
[3Ns, 5B]	$\{11^3/2^3, -29^3 \cdot 41^3/2^{15}\}$		338e1, 338e2
[4X7, 5B]	$\{-5^2 \cdot 41^3/2^2, 5 \cdot 59^3/2^{10}\}$		14450bj1, 14450d1

TABLE 11. Modular elliptic curves with rank 0: Coarse moduli

Type	All curves	Type	All curves
[3B, 5B.1.1]	50b1, 50b2	[3B.1.1, 5B.1.3]	50a1
[3B, 5B.1.2]	50b3, 50b4	[3B.1.1, 5B.1.4]	50a3
[3B, 7B.2.1]	7938u3, 7938u4	[3B.1.1, 5B.4.1]	450b4
[3B, 7B.2.3]	7938u1, 7938u2	[3B.1.1, 5B.4.2]	450b2
		[3B.1.1, 5S4]	324b1, 324d1
		[3B.1.1, 7B]	162c1, 162c3
		[3B.1.1, 7B.2.1]	162b1
		[3B.1.1, 7B.2.3]	162b3
		[3B.1.2, 5B.1.3]	50a2
		[3B.1.2, 5B.1.4]	50a4
		[3B.1.2, 5B.4.1]	450b3
		[3B.1.2, 5B.4.2]	450b1
		[3B.1.2, 5S4]	324b2, 324d2
		[3B.1.2, 7B]	162c2, 162c4
		[3B.1.2, 7B.2.1]	162b2
		[3B.1.2, 7B.2.3]	162b4

TABLE 12. Modular elliptic curves with rank 0: Fine moduli

Type	Rank	Non-cuspidal points	j -invariants
[2B, 5Ns. 2. 1]	0	\emptyset	—
[2B, 7Nn]	0	$(-4, 3), (1/2, 3)$ $(-1, 0)$ $(32, -1)$	$2^6 3^3$ 0 $2^3 3^3 11^3$
[2Cn, 5Ns]	0	$(0, -2)$	$2^6 3^3$
[2Cn, 7B. 6. 1]	0	\emptyset	—
[2Cn, 7B. 6. 2]	0	\emptyset	—
[2Cn, 7B. 6. 3]	0	\emptyset	—
[2Cs, 5S4]	0	$(1, 3), (-2, 3), (-1/2, 3)$	$2^6 3^3$
[3B, 5Nn]	0	$(1, 1)$ $(-1/9, 1/2)$ $(-9, -1/2), (-9, -1)$ $(-1, -1/2), (-1, -1)$	$2^4 3^3 5^3$ $-2^{15} 3^3 5^3$ 0
[3Nn, 13B]	0	\emptyset	—
[3Nn, 5B. 4. 1]	0	\emptyset	—
[3Nn, 5B. 4. 2]	0	\emptyset	—
[3Nn, 7B]	0	$(255, 7)$ $(-15, -7)$	$3^3 5^3 17^3$ $-3^3 5^3$
[3Ns, 5S4]	1	$(1/3, -8), (-9, -8)$ $(-1, 0), (3, 0)$	-2^{15} 0
[5S4, 7B]	0	\emptyset	—
[2Cn, 9XE]	0	\emptyset	—
[4X3, 9XE]	0	\emptyset	—
[4X7, 5Nn]	2	$(40, 1/2)$ $(-440, 3/5)$ $(120, -3/2)$ $(-16008, -21/13)$ $(0, -1), (0, -1/2)$ $(-8, -1/2), (-8, -1)$	$-2^{15} 3^3 5^3$ $-2^{15} 3^3 5^3 11^3$ $-2^{18} 3^3 5^3$ $-2^{18} 3^3 5^3 23^3 29^3$ 0
[4X7, 7B]	1	$(-3/2, -49/4)$ $(-479/16, -4)$	$3^3 13/2^2$ $-3^3 13 479^3/2^{14}$
[8X4, 9XE]	0	\emptyset	—
[8X5, 9XE]	2	$C(\mathbb{Q}_3) = \emptyset$	—

TABLE 13. Modular curves of genus 2

[2B, 7Ns] ₃ ^{cm}	[2Cn, 7Nn] ₃ ^{cm}	[2Cn, 7Ns] ₃ ⁰	[3Nn, 7Ns] ₃ ^{cm}	[3Ns, 5Nn] ₃ ^{cm}	[4X3, 7Nn] ₃ ^{cm}	[4X3, 7Ns] ₃ ⁰
[4X7, 13B] ₃ ⁰	[8X4, 7Nn] ₃ ^{cm}	[8X4, 7Ns] ₃ ⁰	[8X5, 7Nn] ₃ ^{cm}	[8X5, 7Ns] ₃	[3Nn, 5Cs] ₄ ⁰	[3Nn, 5Ns. 2. 1] ₄ ^{cm}
[5S4, 13B] ₄ ⁰	[4X7, 7Nn] ₄ ^{cm}	[9XE, 2B] ₄ ^{cm}	[3B, 7Nn] ₅ ^{cm}	[5Nn, 7B] ₅ ^{cm}	[3B, 7Ns] ₆ ^{cm}	[3Ns, 7Nn] ₆ ^{cm}
[5B, 7Nn] ₆ ⁰	[4X7, 7Ns] ₆ ^{cm}	[4X7, 9XE] ₆	[2Cn, 11Nn] ₇ ^{cm}	[3Nn, 11Nn] ₇ ^{cm}	[5S4, 7Nn] ₇ ^{cm}	[4X3, 11Nn] ₇ ^{cm}
[8X4, 11Nn] ₇ ^{cm}	[8X5, 11Nn] ₇ ^{cm}	[2B, 11Nn] ₈ ^{cm}	[9XE, 5S4] ₈ ^{cm}	[5B, 7Ns] ₉ ⁰	[5Nn, 13B] ₉ ⁰	[5S4, 7Ns] ₉ ^{cm}
[9XE, 5B] ₁₀ ⁰	[5Nn, 7Nn] ₁₃ ^{cm}	[4X7, 11Nn] ₁₃ ^{cm}	[3B, 11Nn] ₁₄ ^{cm}	[9XE, 7B] ₁₄ ⁰	[5Nn, 7Ns] ₁₈ ^{cm}	[9XE, 5Nn] ₁₈ ^{cm}
[5S4, 11Nn] ₁₉ ^{cm}	[5B, 11Nn] ₂₀ ⁰	[7Nn, 13B] ₂₀ ⁰	[9XE, 13B] ₂₆ ⁰	[7Ns, 13B] ₂₇ ⁰	[7B, 11Nn] ₃₂ ⁰	[5Nn, 11Nn] ₃₈ ^{cm}
[9XE, 7Nn] ₄₀ ^{cm}	[9XE, 7Ns] ₅₄ ^{cm}	[11Nn, 13B] ₅₆ ⁰	[7Nn, 11Nn] ₈₁ ^{cm}	[9XE, 11Nn] ₁₁₁ ^{cm}	[7Ns, 11Nn] ₁₁₂ ^{cm}	

TABLE 14. Remaining maximal modular curves of genus > 2

Type	j -invariant	Example	Conductor
[4X7,9XE]	$-2^2 3^7 5^3 439^3$	$y^2 = x^3 - 1126035x + 459913278$	701784
13S4	$-\frac{2^{12} \cdot 5^3 \cdot 11 \cdot 13^4}{3^{13}}$	$y^2 + y = x^3 + x^2 - 7653878762768x + 8080142566037338385$	374369283576145574257827
	$\frac{2^{18} \cdot 3^3 \cdot 13^4 \cdot 127^3 \cdot 139^3 \cdot 157^3 \cdot 283^3 \cdot 929}{5^{13} \cdot 61^{13}}$	$y^2 + y = x^3 - 53690013976669148x + 4788368560731534924873003$	528531611786945

TABLE 15. Examples out of LMFDB: Genus $X_G > 1$ **Extra information: Polynomials for some of the tables:**

• Table 1:

$$\begin{aligned}
P_{11}(x, y) &= (x^2 + 3x - 6)(11(x^2 - 5)y + (2x^4 + 23x^3 - 72x^2 - 28x + 127))(6y + 11x - 19)(22(x - 2)y + (5x^3 + 17x^2 - 112x + 120)) \\
P_{13}(t) &= t^{12} + 231t^{11} + 269t^{10} - 3160t^9 + 6022t^8 - 9616t^7 + 21880t^6 - 34102t^5 + 28297t^4 - 12455t^3 + 2876t^2 - 243t + 1
\end{aligned}$$

• Table 3:

$$\begin{aligned}
Q_{7,3}(t) &= t^{12} - 18t^{11} + 117t^{10} - 354t^9 + 570t^8 - 486t^7 + 273t^6 - 222t^5 + 174t^4 - 46t^3 - 15t^2 + 6t + 1 \\
Q_{7,4}(t) &= t^{12} - 522t^{11} - 8955t^{10} + 37950t^9 - 70998t^8 + 131562t^7 - 253239t^6 + 316290t^5 - 218058t^4 + 80090t^3 - 14631t^2 + 510t + 1 \\
Q_{7,5}(t) &= (t^4 - 6t^3 + 17t^2 - 24t + 9)(3t^4 - 4t^3 - 5t^2 - 2t - 1)(9t^4 - 12t^3 - t^2 + 8t - 3) \\
P_{13,4}(t) &= t^8 + 235t^7 + 1207t^6 + 955t^5 + 3840t^4 - 955t^3 + 1207t^2 - 235t + 1 \\
P_{13,5}(t) &= t^8 - 5t^7 + 7t^6 - 5t^5 + 5t^3 + 7t^2 + 5t + 1 \\
Q_{13,4}(t) &= t^{12} - 512t^{11} - 13079t^{10} - 32300t^9 - 104792t^8 - 111870t^7 - 419368t^6 + 111870t^5 - 104792t^4 + 32300t^3 - 13079t^2 + 512t + 1 \\
Q_{13,5}(t) &= t^{12} - 8t^{11} + 25t^{10} - 44t^9 + 40t^8 + 18t^7 - 40t^6 - 18t^5 + 40t^4 + 44t^3 + 25t^2 + 8t + 1
\end{aligned}$$

• Table 6:

$$\begin{aligned}
P_1(t) &= 9289670605927434230887788667927350765223936t^{12} + 29278270369999901950955093380872504213504t^{11} \\
&\quad + 42292791583476109342488555094120464384t^{10} + 37025228725171770917082043542364160t^9 \\
&\quad + 21878993767277277183859380817920t^8 + 9193668584402084086752989184t^7 + 2816901155195900104390656t^6 \\
&\quad + 634096368731743520256t^5 + 104078307564875520t^4 + 12147786424640t^3 + 957045024t^2 + 45696t + 1 \\
P_2(t) &= 65536t^{12} - 4063232t^{11} + 16777216t^{10} - 28958720t^9 + 27832320t^8 - 16576512t^7 \\
&\quad + 6385664t^6 - 1608192t^5 + 261120t^4 - 25920t^3 + 1376t^2 - 32t + 1
\end{aligned}$$

• Table 9:

$$\begin{aligned}
F_1(x, y) &= 53x^2y^2 - 232x^2y + 272x^2 + 17xy^3 - 372xy^2 + 504xy + 544x + 2y^4 - 56y^3 + 468y^2 + 736y + 272 \\
F_2(x, y) &= 11x^2y^2 - 24x^2y - 16x^2 - xy^3 - 44xy^2 + 8xy - 32x - y^4 + 8y^3 + 76y^2 + 32y - 16 \\
F_3(x, y) &= 28x^2y^2 - 266x^2y - 1169x^2 + 14xy^3 - 126xy^2 + 378xy - 5180x - 5y^4 - 52y^3 + 1032y^2 + 2612y - 5711 \\
F_4(x, y) &= 28x^2y^2 + 77x^2y + 203x^2 - 7xy^3 - 280xy^2 - 189xy + 875x + y^4 + 30y^3 + 509y^2 - 542y + 956 \\
F_5(x, y) &= 14x^2y^2 - 133x^2y + 616x^2 + 7xy^3 - 210xy^2 + 385xy + 2947x + 2y^4 - 38y^3 + 185y^2 + 1758y + 3529 \\
F_6(x, y) &= 7x^3y^3 + 329x^3y^2 - 448x^3y - 4207x^3 - 21x^2y^4 - 42x^2y^3 - 1575x^2y^2 - 1554x^2y - 28749x^2 + 147xy^4 + \\
&\quad 294xy^3 + 3822xy^2 + 3675xy - 65268x + y^6 - 4y^5 - 565y^4 - 260y^3 + 20710y^2 + 11170y - 49223 \\
G_1(x, y) &= -x^{10} - 210x^9 - 20x^8y - 7085x^8 - 1440x^7y - 72280x^7 - 25904x^6y - 262770x^6 - 150880x^5y - 650220x^5 - 323320x^4y \\
&\quad - 2073650x^4 - 703840x^3y - 3299800x^3 - 1393200x^2y - 4157325x^2 - 1015200xy - 4799250x - 580500y - 1454625 \\
G_2(x, y) &= x^{20} + 1260x^{19} - 56x^{18}y + 42870x^{18} - 13456x^{17}y + 403100x^{17} + 440168x^{16}y + 1335852085x^{16} \\
&\quad - 121312128x^{15}y - 61881358352x^{15} - 1307723360x^{14}y + 6615621682760x^{14} + 89306042944x^{13}y \\
&\quad - 160467247908880x^{13} - 47113584888416x^{12}y + 4865894105161650x^{12} + 2738042048551808x^{11}y \\
&\quad + 387841608615974760x^{11} - 171889581774911248x^{10}y - 31426480449116277436x^{10} + \\
&\quad 6725955511078796960x^9y + 1497426397985497774920x^9 - 223160321487761337552x^8y - \\
&\quad 47343303309980334099710x^8 + 4384140813703797518208x^7y + 1177623302292232438580400x^7 + \\
&\quad 23859921698214377667616x^6y - 18020700523192267143943480x^6 - 3625628171475452791902656x^5y - \\
&\quad 91886854155885171733697488x^5 + 78452198711443613319043360x^4y + \\
&\quad 5946599171665206805434677005x^4 - 1229423961196759128856211328x^3y - \\
&\quad 57315101050144284752075165940x^3 + 3544228211661585891755479432x^2y + \\
&\quad 2147304967678389238737065757750x^2 + 693493926872718537524755967344xy + \\
&\quad 51452457690608652712058018333180x + 4183073553838029267128981247656y + \\
&\quad 223823753822802307667379753623561
\end{aligned}$$

REFERENCES

- [1] C. Adelmann, *The decomposition of primes in torsion point fields*. Lecture Notes in Mathematics, 1761. Springer-Verlag, Berlin, 2001. vi+142 pp. 7
- [2] M. Baker, E. González-Jiménez, J. González, and B. Poonen. *Finiteness results for modular curves of genus at least 2*. Amer. J. Math. **127** (2005), 1325–1387. 12
- [3] J. S. Balakrishnan, N. Dogra, J. S. Müller, J. Tuitman, and J. Vonk. *Explicit Chabauty-Kim for the Split Cartan Modular Curve of Level 13*. To appear in Ann. of Math. arXiv:1711.05846. 2, 7
- [4] B. Baran. *Normalizers of non-split cartan subgroups, modular curves, and the class number one problem*. J. Number Theory **130** (2010), 2753–2772. 7
- [5] B. Baran. *An exceptional isomorphism between modular curves of level 13*. J. Number Theory **145** (2014), 273–300. 2, 7
- [6] B. S. Banwait and J. E. Cremona. *Tetrahedral elliptic curves and the local-global principle for isogenies*. Algebra Number Theory **8** (2014), no. 5, 1201–1229. 7
- [7] Y. Bilu and P. Parent, *Serre’s uniformity problem in the split Cartan case*, Ann. Math. (2), **173** (2011), 569–584. 2
- [8] Y. Bilu, P. Parent and M. Rebolledo, *Rational points on $X_0^+(p^r)(\mathbb{Q})$* , Ann. Inst. Fourier (Grenoble) **63** (2013), 957–984. 2
- [9] B.J. Birch, and W. Kuyk (eds.), *Modular Functions of One Variable IV*. Lecture Notes in Mathematics **476**. Springer (1975). 3
- [10] W. Bosma, J. Cannon, C. Fieker, and A. Steel (eds.). *Handbook of Magma functions, Edition 2.23*. <http://magma.maths.usyd.edu.au/magma>, 2018. 14
- [11] N. Bruin and M. Stoll, *Two-cover descent on hyperelliptic curves*. Math. Comp. **78** (2009), 2347–2370. 10
- [12] C. Camacho-Navarro, W. Li, J. Morrow, J. Petok, and David Zureick-Brown. *Modular curves of low composite level and genus zero subgroups*. In preparation. 4
- [13] A.C. Cojocaru, *On the surjectivity of the Galois representations associated to non-CM elliptic curves* (with an appendix by Ernst Kani). Can. Math. Bull. **48** (2005), 16–31. 2
- [14] J.E. Cremona, *Elliptic curve data for conductors up to 400.000*. Available on <http://www.warwick.ac.uk/~masgaj/ftp/data>, 2016. 3
- [15] H.B. Daniels, *An infinite family of Serre curves*. J. Number Theory **155** (2015), 226–247. 3
- [16] H.B. Daniels, E. González-Jiménez. Magma scripts and electronic transcript of computations for the paper “Serre’s constant of elliptic curves over the rationals”. <http://matematicas.uam.es/~enrique.gonzalez.jimenez> 14
- [17] H.B. Daniels, E. González-Jiménez. *Serre’s constant of elliptic curves over the rationals II*. In preparation. 3, 8, 13
- [18] H.B. Daniels, Á. Lozano-Robledo, F. Najman, and A.V. Sutherland, *Torsion subgroups of rational elliptic curves over the compositum of all cubic fields*. Math. Comp. **87** (2018), 425–458. 14
- [19] F. Diamond and J. Shurman, *A first course in modular forms*. Graduate Texts in Mathematics, 228. Springer-Verlag, New York, 2005. xvi+436 pp. 9
- [20] T. Dokchitser and V. Dokchitser, *Surjectivity of mod 2^n representations of elliptic curves*. Math. Z. **272** (2012), no. 3–4, 961–964. 2
- [21] W. D. Duke, *Elliptic curves with no exceptional primes*. C. R. Math. Acad. Sci. Paris Sér. I **325** (1997), 813–818. 1, 4
- [22] N.D. Elkies, *Elliptic curves with 3-adic Galois representation surjective mod 3 but not mod 9*. arXiv:math/0612734. 2
- [23] N. Jones, *Almost all elliptic curves are Serre curves*. Trans. Amer. Math. Soc. **362** (3), (2010), 1547–1570. 3
- [24] M. A. Kenku, *The modular curve $X_0(39)$ and rational isogeny*. Math. Proc. Cambridge Philos. Soc. **85** (1979), 21–23. 8
- [25] M. A. Kenku, *The modular curves $X_0(65)$ and $X_0(91)$ and rational isogeny*. Math. Proc. Cambridge Philos. Soc. **87** (1980), 15–20. 8
- [26] M. A. Kenku, *The modular curve $X_0(169)$ and rational isogeny*. J. London Math. Soc. (2) **22** (1980), 239–244. 8
- [27] M. A. Kenku, *The modular curve $X_0(125)$, $X_1(25)$ and $X_1(49)$* . J. London Math. Soc. (2) **23** (1981), 415–427. 8
- [28] P. Lemos, *Serre’s uniformity conjecture for elliptic curves with rational cyclic isogenies*. Trans. Amer. Math. Soc. **371** (2019), no. 1, 137–146. 2
- [29] P. Lemos, *Some cases of Serre’s uniformity problem*. To appear in Math. Z. 2
- [30] LMFDB Collaboration, *The L-functions and modular forms database*. Available at <http://www.lmfdb.org>. 3, 13
- [31] L. Mavrides, *Modular curves and surjectivity of Galois representations attached to elliptic curves over \mathbb{Q}* . Master Thesis (University of Warwick) 2011. 2
- [32] B. Mazur, *Modular curves and the Eisenstein ideal*. Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186. 8
- [33] B. Mazur, *Rational isogenies of prime degree*. Invent. Math. **44** (1978), 129–162. 2, 8
- [34] J. S. Morrow, *Composite images of Galois for elliptic curves over \mathbb{Q} & Entanglement fields*. To appear in Math. Comp. 4
- [35] J. Rouse, D. Zureick-Brown, *Elliptic curves over \mathbb{Q} and 2-adic images of Galois*. Research in Number Theory **1** (2015), 34 pages. (data files and subgroup descriptions available at <http://users.wfu.edu/rouseja/2adic/>). 2, 12, 13
- [36] J.-P. Serre, *Propriétés galoisiennes des points d’ordre fini des courbes elliptiques*. Invent. Math. **15** (1972), no. 4, 259–331. 1, 2
- [37] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*. Inst. Hautes Études Sci. Publ. Math. **54** (1981), 323–401. 1
- [38] J.-P. Serre, *Abelian l -adic representations and elliptic curves*. Research Notes in Mathematics, vol. 7, A K Peters, Ltd., Wellesley, MA, 1998. 2
- [39] A.V. Sutherland, *Computing images of Galois representations attached to elliptic curves*. Forum Math. Sigma **4** (2016), e4, 79 pp. 3
- [40] A.V. Sutherland and D. Zywinia, *Modular curves of prime power-level with infinitely many rational points*. Algebra Number Theory **11** (2017), 1199–1229. 8, 9
- [41] D. Zywinia, *On the possible images of the mod ℓ representations associated to elliptic curves over \mathbb{Q}* . arXiv:1508.07660. 2, 3, 5, 7, 9, 13
- [42] D. Zywinia, *On the surjectivity of mod ℓ representations associated to elliptic curves*. arXiv:1508.07661. 8

DEPARTMENT OF MATHEMATICS AND STATISTICS, AMHERST COLLEGE, MA 01002, USA

E-mail address: `hdaniels@amherst.edu`

URL: `http://hdaniels.people.amherst.edu`

UNIVERSIDAD AUTÓNOMA DE MADRID, DEPARTAMENTO DE MATEMÁTICAS, MADRID, SPAIN

E-mail address: `enrique.gonzalez.jimenez@uam.es`

URL: `http://matematicas.uam.es/~enrique.gonzalez.jimenez`