JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Harris B. DANIELS et Jeremy ROUSE

Minimal Subgroups of $\mathbf{GL_2}(\mathbb{Z}_S)$

Tome 37, nº 2 (2025), p. 579-597.

https://doi.org/10.5802/jtnb.1333

Le Journal de Théorie des Nombres de Bordeaux *est membre du Centre Mersenne pour l'édition scientifique ouverte*
http://www.centre-mersenne.org/
e-ISSN : 2118-8572

Journal de Théorie des Nombres
de Bordeaux **37** (2025), 579–597

Minimal Subgroups of $\mathbf{GL_2}(\mathbb{Z}_S)$

par Harris B. DANIELS et Jeremy ROUSE

Résumé. Soient L un corps de nombres, E une courbe elliptique sur L, S un ensemble de nombres premiers, et $\rho_{E,S} : \mathrm{Gal}(\overline{L}/L) \to \mathrm{GL}_2(\mathbb{Z}_S)$ la représentation galoisienne S-adique. Si $L \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$ pour chaque entier n dont tous les facteurs premiers sont dans S, alors $\det \rho_{E,S} : \mathrm{Gal}(\overline{L}/L) \to \mathrm{GL}_2(\mathbb{Z}_S)$ est surjectif. Disons qu'un sous-groupe H de $\mathrm{GL}_2(\mathbb{Z}_S)$ d'indice fini est *minimal* si $\det : H \to \mathbb{Z}_S^\times$ est surjectif, mais $\det : K \to \mathbb{Z}_S^\times$ n'est pas surjectif pour chaque sous-groupe K de H propre et fermé. Nous montrons que $\mathrm{GL}_2(\mathbb{Z}_S)$ n'admet un sous-groupe minimal que si $S = \{2\}$, et que dans $\mathrm{GL}_2(\mathbb{Z}_2)$ il y en a plein. Nous donnons un modèle pour toute courbe modulaire de genre 0 associée à un sous-groupe minimal, et construisons une famille infinie de courbes elliptiques sur des corps quadratiques imaginaires ayant mauvaise réduction seulement en 2 et une image 2-adique minimale.

Abstract. Let E be an elliptic curve over a number field L and for a finite set S of primes, let $\rho_{E,S} : \mathrm{Gal}(\overline{L}/L) \to \mathrm{GL}_2(\mathbb{Z}_S)$ be the S-adic Galois representation. If $L \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$ for all positive integers n whose prime factors are in S, then $\det \rho_{E,S} : \mathrm{Gal}(\overline{L}/L) \to \mathbb{Z}_S^\times$ is surjective. We say that a finite index subgroup $H \subseteq \mathrm{GL}_2(\mathbb{Z}_S)$ is *minimal* if $\det : H \to \mathbb{Z}_S^\times$ is surjective, but $\det : K \to \mathbb{Z}_S^\times$ is not surjective for any proper closed subgroup K of H. We show that there are no minimal subgroups of $\mathrm{GL}_2(\mathbb{Z}_S)$ unless $S = \{2\}$, while minimal subgroups of $\mathrm{GL}_2(\mathbb{Z}_2)$ are plentiful. We give models for all the genus 0 modular curves associated to minimal subgroups of $\mathrm{GL}_2(\mathbb{Z}_2)$, and construct an infinite family of elliptic curves over imaginary quadratic fields with bad reduction only at 2 and with minimal 2-adic image.

1. Introduction

Given an elliptic curve $E/\mathbb{Q}$, a prime p, and a fixed algebraic closure of $\overline{\mathbb{Q}}$, one can construct the p-adic Galois representation associated to E,

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

Recently there has been great interest in studying the groups of the form $G_{E,p} = \mathrm{Im}(\rho_{E,p^\infty})$. A few classical results about $G_{E,p}$ include that $\det(G_{E,p}) = \mathbb{Z}_p^\times$ and if E does not have complex multiplication, then $[\mathrm{GL}_2(\mathbb{Z}_p) : G_{E,p}]$ is finite (see Chapter IV of [18]).

Manuscrit reçu le 19 mars 2024, révisé le 9 septembre 2024, accepté le 17 janvier 2025.
2020 *Mathematics Subject Classification.* 11G05, 11F80, 14H52, 22E50.
Mots-clefs. Elliptic Curves, Galois Representations, Profinite Groups.

Given these two things, a natural question to ask is if there is an elliptic curve $E/\mathbb{Q}$ and prime p such that $G_{E,p}$ has the property that if $H \subsetneq G_{E,p}$, then $\det(H) \subsetneq \mathbb{Z}_p^\times$? Before answering this question, we phrase it more broadly.

Let S be a finite set of primes. We also let

$$\mathbb{Z}_S = \varprojlim \mathbb{Z}/n\mathbb{Z}$$

with respect to divisibility, but restricting n to be divisible only by primes in S. In this case we have that

$$\mathrm{GL}_2(\mathbb{Z}_S) = \prod_{p \in S} \mathrm{GL}_2(\mathbb{Z}_p).$$

Definition 1.1. *A group $H \subseteq \mathrm{GL}_2(\mathbb{Z}_S)$ of finite index is called* minimal *if $\det(H) = \mathbb{Z}_S^\times$, but for every maximal closed subgroup $M \subsetneq H$ we have that $\det(M) \subsetneq \mathbb{Z}_S^\times$.*

So a more general question would be if there is an elliptic curve $E/\mathbb{Q}$ and a set of primes $S \subseteq \mathbb{Z}$ such that the image of the S-adic Galois representation $\operatorname{Im} \rho_{E,S} = G_{E,S} \subseteq \prod_{p \in S} G_{E,p} \subseteq \mathrm{GL}_2(\mathbb{Z}_S)$ is minimal and if so, can we classify all of, or maybe almost all of, such curves?

In order to start examining this question, we start by looking for examples.

1.1. First Examples. We claim that if $E/\mathbb{Q}$ is an elliptic curve that does not have complex multiplication and E only has bad reduction at 2, then $G_{E,2}$ is a minimal group.

Suppose that $E/\mathbb{Q}$ is an elliptic curve without complex multiplication that only has bad reduction at 2. From the criterion of Néron–Ogg–Shafarevich [19] we know that the extension $\mathbb{Q}(E[2^\infty])/\mathbb{Q}$ is only ramified at 2. From the main theorem of [22] we know that there are no such cubic extensions of $\mathbb{Q}$. This, together with the fact that $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \simeq S_3$ would force E to have a point of order 2 defined over $\mathbb{Q}$. Besides being able to conclude that E has to have a rational point of order 2, this allows us to conclude that $G_{E,2}$ is in fact a pro 2-group. This is because once we know that E has a rational point of order 2, we know that $[\mathbb{Q}(E[2]) : \mathbb{Q}] = 1$ or 2 and $[\mathbb{Q}(E[2^{n+1}]) : \mathbb{Q}(E[2^n])]$ is always a power of 2. Now that we know that $G_{E,2}$ is a pro 2-group, we can use a classical result in group theory that says that any proper maximal subgroup of a pro p-group is normal and has index p. (Here and elsewhere, we require a maximal subgroup of a profinite group to be closed.)

Thus, in our case, the maximal proper subgroups of $G_{E,2}$ all have index 2 and are normal. But the Galois correspondence says that these maximal subgroups correspond to quadratic subfields of $\mathbb{Q}(E[2^\infty])$. Again, from the main theorem of [22] the only possible quadratic subfields of $\mathbb{Q}(E[2^\infty])$

are subfields of $\mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2})$. From this we know that every maximal subgroup of $G_{E,2}$ fixes one of these fields. Lastly, using the Weil pairing we see that none of the maximal subgroups of $G_{E,2}$ can have surjective determinant.

Searching [10] we find that there are 8 elliptic curves defined over $\mathbb{Q}$ without complex multiplication that only have bad reduction at 2. These elliptic curves have labels

`128.a1`, `128.a2`, `128.a3`, `128.a4`, `128.b1`, `128.b2`, `128.b3` and `128.b4`.

Remark 1.2. We know that these are in fact all of the elliptic curves over $\mathbb{Q}$ with bad reduction only at 2. This is because any elliptic curve with only bad reduction at two has conductor equal to a power of 2, but there is a bound on the exponent that can appear on 2 from [20, Theorem 10.2]. Thus any elliptic curve over $\mathbb{Q}$ with bad reduction only at 2 has conductor bounded by 256. So the completeness of the data in [10] allows us to conclude that these are all of them.

Examining these curves further in the LMFDB, we see that they all have different 2-adic images and the modular curves associated to each of these 8 different subgroups of $\mathrm{GL}_2(\mathbb{Z}_2)$ are genus 0. Using the labels conventions established in [16], these groups are

`32.96.0.1`, `32.96.0.3`, `32.96.0.25`, `32.96.0.27`, `32.96.0.102`, `32.96.0.104`, `32.96.0.106`, and `32.96.0.108`.

The models associated to each of the corresponding modular curves have been computed in [17][1]. So, our pure thought argument that had initially led to 8 examples has in fact led us to 8 separate infinite families of elliptic curves whose 2-adic images are minimal. Thus it seems that this phenomenon might be quite common.

With these examples in hand, we move on to trying to better understand this phenomenon abstractly.

1.2. Statement of results and outline. Our first main result is that minimal groups are a 2-adic phenomena.

Theorem 1.3. *Let S be a finite nonempty set of primes and $H \subseteq \mathrm{GL}_2(\mathbb{Z}_S)$ a minimal group of finite level. Then $S = \{2\}$.*

This, together with the complete classification of possible 2-adic images available in [17] completes the classification of elliptic curves defined over $\mathbb{Q}$ with minimal image.

On the other hand, minimal subgroups of $\mathrm{GL}_2(\mathbb{Z}_2)$ are plentiful.

Theorem 1.4. *Let $H \leq \mathrm{GL}_2(\mathbb{Z}_2)$ be any finite-index subgroup with $\det(H) = \mathbb{Z}_2^\times$. Then there is a minimal subgroup $M \leq H$ with $|H : M| < \infty$.*

[1] In this paper the curves are labeled `X238a-d` and `X239a-d`

Our approach for proving the above result is the following. If A and B are randomly chosen elements of H, let $\langle A, B\rangle$ be the smallest closed subgroup containing A and B. We show that if $\det(\langle A, B\rangle) = \mathbb{Z}_2^\times$, then $\langle A, B\rangle$ is a minimal subgroup of H with probability 1.

Finally, while there are only 8 non-CM elliptic curves $E/\mathbb{Q}$ with bad reduction only at 2, we can give an infinite family of elliptic curves E defined over quadratic extensions of $\mathbb{Q}$ with bad reduction only at 2 that have minimal 2-adic image.

Proposition 1.5. *Suppose that n is a positive integer and let $a = \sqrt{-(2^n+1)}$. Let*

$$E : y^2 = x^3 + 2ax^2 + (a^2+1)x.$$

Then E has bad reduction only at prime ideals above 2 in $\mathbb{Q}(a)$. If n is odd and $n \neq 3$, then $\rho_{E,2^\infty}(G_{\mathbb{Q}(a)})$ is minimal and has RSZB label `8.24.0.86`. If $n = 2$, then $\rho_{E,2^\infty}(G_{\mathbb{Q}(a)})$ is minimal and has RSZB label `16.384.9.895`. If $n = 10$, then $\rho_{E,2^\infty}(G_{\mathbb{Q}(a)})$ is minimal and has RSZB label `16.384.9.894`.

An outline of the paper is as follows. In Section 3 we prove Theorem 1.3 and discuss a generalization to principally polarized abelian varieties. In Section 4 we prove Theorem 1.4 using ideas from p-adic Lie theory. In Section 5 we describe a search to find all the genus 0 minimal groups and then compute models for the corresponding modular curves. The models for these curves were computed using [1], the techniques in [14], and guided by the information available in [10]. All the code for these computations is available at [7]. Lastly, we prove Proposition 1.5 in Section 6.

1.3. Acknowledgements. We would first like to thank the anonymous referee for their thoughtful comments on a previous version of this paper. The second author is thankful to Amherst College for hospitality during a visit in September 2022.

2. Background

The goal of this section is to establish notation and remind the reader of the basic facts necessary for the results in this paper. For more detail about elliptic curves, readers should see [20, 21]. For more information about modular curves the reader should see [11]. Lastly, for more information about p-adic Lie theory see [8].

2.1. Elliptic Curves. Elliptic curves are defined as smooth projective genus 1 curves with a specified point. They are ubiquitous in mathematics and can be found in the center of many of the open problems in modern number theory.

One of the most interesting aspects of elliptic curves is that given an elliptic curve E defined over a number field K, the set of K-rational points

on E can be given the structure of a finitely generated abelian group. That is to say, that $E(K) \simeq \mathbb{Z}^r \oplus T$, for some $r \in \mathbb{Z}_{\geq 0}$ and finite abelian group T.

We call r the *rank* of E over K, and T the torsion subgroup of $E(K)$, often denoted $E(K)_{\mathrm{tors}}$. A classical result in the study of elliptic curves is that if we fix an algebraic closure of K, denoted $\overline{K}$, then

$$E[n] = \{P \in E(\overline{K}) : nP = \mathcal{O}\} \simeq (\mathbb{Z}/n\mathbb{Z})^2.$$

Further, there is a natural componentwise action of $\mathrm{Gal}(\overline{K}/K)$ on $E[n]$ that induces a representation

$$\bar{\rho}_{E,n} \colon \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

We call $\bar{\rho}_{E,n}$ the *mod n representations associated with E*. Using the mod n representations associated to E and the appropriate inverse limits, we can define the p-adic and adelic Galois representations attached to E. We denote these representations

$$\rho_{E,p^\infty} \colon \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{GL}_2(\mathbb{Z}_p),$$
$$\text{and} \qquad \rho_E \colon \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{GL}_2(\widehat{\mathbb{Z}}) \simeq \prod_p \mathrm{GL}_2(\mathbb{Z}_p).$$

Here we note these representations all depend on which points we pick as a basis for the n-torsion of $E(K)$, and changing the basis replaces the image with a conjugate subgroup. It is not hard to see that if $H \subseteq \mathrm{GL}_2(\mathbb{Z}_S)$ is minimal, then every conjugate of H in $\mathrm{GL}_2(\mathbb{Z}_S)$ is also minimal.

Given an elliptic curve E/K, we denote by $j(E)$ the usual j-invariant of E. If E^D is the quadratic twist of E by D (i.e. if $E : y^2 = x^3 + ax^2 + bx + c$, then $E^D : y^2 = x^3 + Dax^2 + D^2bx^3 + D^3c$), then $j(E) = j(E^D)$. Conversely, if E_1 and E_2 are two elliptic curves defined over K with $j(E_1) = j(E_2) \notin \{0, 1728\}$, then E_2 is a quadratic twist of E_1.

2.2. Modular Curves. Modular curves are an important tool for studying elliptic curves and their Galois representations. The points on these curves correspond to elliptic curves whose mod n Galois representations are contained inside of a particular subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ up to conjugation. The goal of this subsection is to give the basic definitions and theorems needed for this paper. The interested reader is encouraged to see [11]. For the remainder of the section n will be an integer greater than 1.

Associated to each group $G \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ such that $\det(G) = (\mathbb{Z}/n\mathbb{Z})^\times$, and $-I \in G$ is a modular curve X_G. The curve X_G is a smooth, projective, and geometrically integral curve defined over $\mathbb{Q}$. We say that G has genus g if X_G is a curve with genus g.

Again, assuming that the group G contains $-I$, the curve X_G comes with a natural map

$$\pi_G : X_G \longrightarrow \mathbb{P}^1_{\mathbb{Q}}$$

called the j-map associate to G, such that if E/K is an elliptic curve with $j(E) \notin \{0, 1728\}$, then $\operatorname{Im} \bar{\rho}_{E,n}$ is conjugate to a subgroup of G if and only if there is a $P \in X_G(K)$ such that $j(E) = \pi_G(P)$.

In the case that $-I \notin G$, X_G is an algebraic stack and its course space is the same as $X_{\tilde{G}}$, where $\tilde{G} = \langle G, -I \rangle$. In this case the moduli interpretation is different; if $-I \notin G$, if the image of $\bar{\rho}_{E,n} \subseteq G$, this does not imply the same for the quadratic twist E_D. In this situation, if U is the complement in $X_{\tilde{G}}$ of the cusps and preimages of $j = 0$ and 1728, there is a universal elliptic curve $\mathcal{E} \to U$ so that E has image contained in G if and only if there is some (not necessarily unique) t so that $E \cong \mathcal{E}_t$ over K. For more detail see [17, Section 2 and 5].

Remark 2.1. A careful reading of the moduli interpretation, one notices that an elliptic curve $E/\mathbb{Q}$ having a corresponding point on $X_G(\mathbb{Q})$ does not ensure that $\operatorname{Im} \bar{\rho}_{E,n}$ is conjugate to G. It only ensures that $\operatorname{Im} \bar{\rho}_{E,n}$ is conjugate to a subgroup of G. That said, if G is a minimal group containing all matrices $\equiv I \pmod{n}$, since $\det \circ \bar{\rho}_{E,n}$ is surjective, it must be that $\operatorname{Im} \bar{\rho}_{E,n} = G$.

There has been an immense amount of progress on computing modular curves X_G, their j-maps π_G, and their rational points. The work here relies directly or indirectly on the previous work and so we mention some of that work here. In particular, [16, 17, 23] all make major contributions to our understanding the modular curves associates to subgroups of $\mathrm{GL}_2(\mathbb{Z}/\ell^k\mathbb{Z})$ for a prime ℓ and integer $k \geq 1$. Work has now started on understanding how these images can occur simultaneously and how they fit together [4, 5, 6, 24].

3. Minimality is a 2-adic phenomena

Notice that if H is a minimal subgroup of $\mathrm{GL}_2(\mathbb{Z}_S)$, then every maximal open subgroup of H can be obtained as the inverse image of a subgroup of $\mathbb{Z}_S^\times$ under the map $\det : H \to \mathbb{Z}_S^\times$. This is because if M_1 and M_2 were maximal subgroups of H such that $\det(M_1) = \det(M_2) \subsetneq \mathbb{Z}_S^\times$, then $\det^{-1}(\det(M_1)) = \det^{-1}(\det(M_2))$ would be a proper subgroup of H that contains both M_1 and M_2. The maximality of M_1 and M_2 then forces $M_1 = M_2$. So if H is minimal, then every maximal subgroup of H is normal in H. Further, if we let $p \in S$, $k \in \mathbb{Z}_+$ and $\pi_{p^k} : H \to \mathrm{GL}_2(\mathbb{Z}/p^k\mathbb{Z})$ be the standard component-wise reduction map on H, the $\pi_{p^k}(H)$ also has the property that all of its maximal subgroups are normal.

Without giving too much background, we recall the definition of a nilpotent group.

Definition 3.1. *Let G be a group. We say that G is* nilpotent *if G has a finite central series.*

The following result demonstrates the relevance of this concept to $\pi_{p^k}(H)$.

Theorem 3.2 ([9, Chapter 6, Theorem 3 & Corollary 4])**.** *Let G be a finite group. The following are equivalent;*

(1) *The group G is nilpotent.*
(2) *Every Sylow subgroup of G is normal.*
(3) *The group G is the direct product of its Sylow subgroups.*
(4) *Every maximal subgroup of G is normal in G.*

From this we immediately get the following proposition

Proposition 3.3. *If H is a minimal subgroup of $\mathrm{GL}_2(\mathbb{Z}_S)$, then for every $p \in S$ and $k \in \mathbb{Z}_+$, we have that $\pi_{p^k}(H)$ is nilpotent.*

Before we prove the main result of this section, we need one more definition.

Definition 3.4. *Let $G \subseteq \mathrm{GL}_2(\mathbb{Z}_S)$ be an open subgroup and given any $n \in \mathbb{Z}_+$ only divisible by primes in S, define $\rho_n : \mathrm{GL}_2(\mathbb{Z}_S) \to \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ to be the standard component-wise reduction map. Suppose there is an $n \in \mathbb{Z}_+$ such that $G = \rho_n^{-1}(\rho_n(G))$. In this case we say that G has* finite level *and we define the* level *of G is the smallest $N \in \mathbb{Z}_+$ such that $G = \rho_N^{-1}(\rho_N(G))$. If no such $n \in \mathbb{Z}_+$ exists, we say that G has infinite level.*

Remark 3.5. The assumption that H has finite level is not crucial. It is known by work of Nikolov and Segal [13] that every topologically finitely generated profinite group has the property that every finite index subgroup is open.

We are now ready to provide a proof of Theorem 1.3.

Proof of Theorem 1.3. We prove this theorem by contradiction. Suppose that S is a nonempty set of primes, p is an odd prime such that $p \in S$, and H is a minimal subgroup of $\mathrm{GL}_2(\mathbb{Z}_S)$ of finite level.

Since H has finite level we know that there is a $k \in \mathbb{Z}_+$ such that p^{k-1} divides the level of H, while p^k does not. From this, it follows that $M \in \rho_{p^k}(H)$ if and only if $M \in \rho_{p^{k-1}}(H)$. In particular, $H_{p^k} = \rho_{p^k}(H)$ contains all matrices equivalent to the identity mod p^{k-1}.

As we noted before, we know that H_{p^k} is a finite nilpotent group. From Theorem 3.2 we have that H_{p^k} must be the direct product of its p-Sylow subgroups. That is, if we let $P = \mathrm{Syl}_p(H_{p^k})$ and $Q = \prod_{q \neq p} \mathrm{Syl}_q(H_{p^k})$, then $H_{p^k} \simeq P \times Q$. So given any $B \in H_{p^k}$ we can find $X \in Q$ and $Y \in P$ such that $B = XY$. We also know that X and Y commute with each other in $H_{p^k} \simeq P \times Q$ since we have $X \in Q$ and $Y \in P$. Since $Y \in \mathrm{Syl}_p(H_{p^k})$, we know that the order of Y is a power of p and thus for some j $\det(Y)^{p^j} = \det(Y^{p^j}) = \det(I) \equiv 1 \bmod p$. Fermat's little theorem says $\det(Y)^{p^j} \equiv 1 \bmod p$ forces $\det(Y) \equiv 1 \bmod p$.

Next, notice that for any $Z \in M_2(\mathbb{Z}/p^k\mathbb{Z})$ we have that $I + p^{k-1}Z \in H_{p^k}$ since $I + p^{k-1}Z \equiv I \bmod p^{k-1}$. Now, a simple computation shows that $I + p^{k-1}Z$, has order dividing p and so it must be that $(I + p^{k-1}Z) \in P$. Since everything in P commutes with the elements of Q we have that

$$X(I + p^{k-1}Z) = (I + p^{k-1}Z)X.$$

An immediate consequence of this is that

$$XZ \equiv ZX \bmod p.$$

Since Z was an arbitrary element of $M_2(\mathbb{Z}/p^k\mathbb{Z})$, we can see that $X \bmod p$ commutes with everything in $M_2(\mathbb{Z}/p\mathbb{Z})$. An elementary computation shows that it must be that

$$X \equiv \begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} \bmod p$$

for some $\alpha \in \mathbb{Z}/p\mathbb{Z}$ and so $\det(X) \equiv \alpha^2 \bmod p$. Bringing it all together we get that

$$\det(B) = \det(XY) = \det(X)\det(Y) \equiv \alpha^2 \bmod p.$$

Thus for every $B \in H$, $\det(B)$ is a quadratic residue in $\mathbb{Z}/p\mathbb{Z}$. Since p is an odd prime, not every element of $\mathbb{Z}/p\mathbb{Z}$ is a quadratic residue. This contradicts the assumption that $\det(H) = \mathbb{Z}_S^\times$. □

Remark 3.6. One way to make sense of what is happening here is that we are requiring our minimal groups to have surjective determinant. Looking at $\mathbb{Z}_p^\times$, we see that there is structural difference depending on if $p = 2$ or if p is odd. When $p = 2$, the group $\mathbb{Z}_2^\times$ is a 2-group, but when p is odd, $\mathbb{Z}_p^\times$ is not a p-group. This is because $(\mathbb{Z}/p\mathbb{Z})^\times$ has size $p - 1$. This factor of $p - 1$ is what prevents $\mathbb{Z}_p^\times$ from being a p-group when p is odd, but there is no problem here when $p = 2$.

3.1. A diversion into higher dimensional abelian varieties. Elliptic curves are 1-dimensional abelian varieties, and much of what is true for elliptic curves is also true for abelian varieties being careful to adjust the details where necessary. Given the aim of this paper, we will not be able to provide all of the background information here, but the interested reader is encouraged to see [12].

To start, we let A be a principally polarized g-dimensional abelian variety defined over a number field K disjoint from $\mathbb{Q}(\zeta_n)$. Then because the Weil-pairing is a non-degenerate, alternating, Galois invariant bilinear form on $A[n]$, it follows that the mod n Galois representations associated to A,

$$\bar{\rho}_{A,n} : \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{Aut}(A[n]) \simeq \mathrm{GL}_{2g}(\mathbb{Z}/n\mathbb{Z})$$

actually has its image (up to conjugation) contained inside of $\mathrm{GSp}_{2g}(\mathbb{Z}/n\mathbb{Z})$. To define this group, let Ω be the $2g \times 2g$ block matrix of the form

$$\Omega = \begin{bmatrix} 0 & -I_g \\ I_g & 0 \end{bmatrix},$$

where I_g is the $g \times g$ identity matrix. For a ring R, the group $\mathrm{GSp}_{2g}(R)$ can be defined as the set of $2g \times 2g$ matrices M, with entries in R such that

$$M^T \Omega M = \lambda \Omega$$

for some $\lambda \in R^\times$. With this, we can define a map

$$\mathrm{Mult}\colon\ \mathrm{GSp}_{2g}(R) \longrightarrow R^\times$$

given by $\mathrm{Mult}(M) = \lambda$, where $M^T \Omega M = \lambda \Omega$. It turns out that in the case that A is a principally polarized g-dimensional abelian variety defined over a number field K disjoint from $\mathbb{Q}(\zeta_n)$, properties of the Weil pairing imply that

$$\mathrm{Mult} \circ \bar{\rho}_{A,n} : \mathrm{Gal}(\overline{K}/K) \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$$

is surjective.

With this in hand, we can see that the argument in the proof of Theorem 1.3 generalizes to $\mathrm{GSp}_{2g}(\mathbb{Z}_S)$. In particular, if we assume that A/K is an abelian variety of dimension g, p is a prime, and the image of the mod p^k Galois representation attached to A is nilpotent and contains all matrices in $\mathrm{GSp}_{2g}(\mathbb{Z}/p^k\mathbb{Z})$ that are congruent to the identity modulo p^{k-1}, then any X in the image of $\bar{\rho}_{A,p^k}$ with order coprime to p must commute with matrices $I + p^{k-1}Z \in \mathrm{GSp}_{2g}(\mathbb{Z}/p^k\mathbb{Z})$. Writing

$$X = \begin{bmatrix} X_1 & X_2 \\ X_3 & X_4 \end{bmatrix}$$

and taking

$$Z = \begin{bmatrix} A & 0 \\ 0 & -A^T \end{bmatrix}$$

for an arbitrary $A \in \mathrm{GL}_g(\mathbb{Z}/p\mathbb{Z})$ shows that $X_1 \equiv \lambda_1 I_g \bmod p$ and $X_4 \equiv \lambda_2 I_g \bmod p$.

Taking

$$Z = \begin{bmatrix} I_g & I_g \\ 0 & -I_g \end{bmatrix}$$

shows that $X_3 \equiv 0 \bmod p$ and taking

$$Z = \begin{bmatrix} I_g & 0 \\ I_g & -I_g \end{bmatrix}$$

shows that $X_2 \equiv 0 \bmod p$ and that $X_1 \equiv X_4 \bmod p$. It follows that

$$X \equiv \begin{bmatrix} \lambda I_g & 0 \\ 0 & \lambda I_g \end{bmatrix} \bmod p.$$

which shows that $\mathrm{Mult}(X) \equiv \lambda^2 \bmod p$.

Any element in the image of $\bar{\rho}_{A,p^k}$ must have the form XY for some Y with order a power of p. This implies that $\mathrm{Mult}(Y) \equiv 1 \bmod p$, and so $\mathrm{Mult}(XY) = \mathrm{Mult}(X)\,\mathrm{Mult}(Y) \equiv \lambda^2 \bmod p$. If $p > 2$, this contradicts that $\mathrm{Mult} \circ \bar{\rho}_{A,p}$ is surjective, and this is a contradiction.

3.2. A diversion into CM elliptic curves. In the definition of minimal, we assumed that $H \subseteq \mathrm{GL}_2(\mathbb{Z}_S)$ was a finite index subgroup and $\det : H \to \mathbb{Z}_S^\times$ is surjective. This will be true if H is the S-adic image of Galois for a non-CM elliptic curve E defined over some number field K with the property that $K \cap \mathbb{Q}(\zeta_n) = K$ for any positive integer n all of whose prime factors are in S (as proven in [18]). What about the CM case?

First, at no point in the argument in Subsection 1.1 do we need to exclude CM elliptic curves. Thus the argument applies also to the CM case and shows that if $E/\mathbb{Q}$ is a CM elliptic curve with bad reduction only at 2, then $\mathrm{Im}\,\rho_{E,2^\infty} \subseteq \mathrm{GL}_2(\mathbb{Z}_2)$ is a subgroup for which $\det(\mathrm{Im}\,\rho_{E,2^\infty}) = \mathbb{Z}_2^\times$ and for which every proper closed subgroup comes from the determinant.

However, the argument in the proof of Theorem 1.3 used in a crucial way that the image of the S-adic Galois representation had finite level, and this will not be true for CM curves. This raises the following open question.

Question 3.7. Is there a finite set of primes S containing at least one odd prime, a number field K with the property that $K \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$ for all positive integers n all of whose prime factors are in S, and a CM elliptic curve E/K for which every maximal closed subgroup of the S-adic image of Galois comes from $\mathbb{Z}_S^\times$?

4. Minimal groups are plentiful

The goal of this section is to show that the minimal groups are plentiful inside of $\mathrm{GL}_2(\mathbb{Z}_2)$. We start with a lemma about how minimal groups are generated.

Lemma 4.1. *If $G \subseteq \mathrm{GL}_2(\mathbb{Z}_2)$ is a minimal group, then G must be (topologically) generated by 2 elements of $\mathrm{GL}_2(\mathbb{Z}_2)$.*

Proof. Suppose $G \subseteq \mathrm{GL}_2(\mathbb{Z}_2)$ is a minimal group. Then G must have precisely three maximal closed subgroups, each of which is the preimage under $\det : G \to \mathbb{Z}_2^\times$ of one of the three maximal closed subgroups of $\mathbb{Z}_2^\times$. □

Our goal is to show that a "randomly" chosen two generator subgroup of $\mathrm{GL}_2(\mathbb{Z}_2)$ with surjective determinant is minimal. To quantify this, recall that $\mathrm{GL}_2(\mathbb{Z}_2)$ has a Haar measure which (because $\mathrm{GL}_2(\mathbb{Z}_2)$ is compact) is both left and right invariant. The main question we must answer is the following.

Question 4.2. If we randomly pick $A, B \in \mathrm{GL}_2(\mathbb{Z}_2)$, what is the probability that the topological closure of $\langle A, B\rangle$ is a minimal group?

For a finite set $S \subseteq \mathrm{GL}_2(\mathbb{Z}_2)$, we write $\langle S\rangle$ for the closure of the subgroup generated by S.

Theorem 4.3. *The set of pairs* $(A, B) \in \mathrm{GL}_2(\mathbb{Z}_2)^2$ *for which* $\langle A, B\rangle$ *has infinite index in* $\mathrm{GL}_2(\mathbb{Z}_2)$ *has measure zero.*

Lemma 4.4. *Suppose that*

$$f(x_1, x_2, \ldots, x_n) = \sum_{\mathbf{s}\in\mathbb{Z}^n_{\geq 0}} a_{\mathbf{s}} x^{\mathbf{s}}$$

is a multivariable power series that converges on an open subset $D \subseteq \mathbb{Z}_2^n$ *with the property that not all* $a_{\mathbf{s}}$ *are equal to zero. Then the measure of*

$$\{(x_1, x_2, \ldots, x_n) \in D : f(x_1, x_2, \ldots, x_n) = 0\}$$

is zero with respect to natural p-adic Haar measure.

Proof. [2] We prove this by induction on n. Let μ_n denote the usual measure on $\mathbb{Z}_2^n$.

For $n = 1$, the power series $f(x_1)$ is a p-adic analytic function on D, and it is well-known (see for example [15, Section 6.2]) that the zeros of an analytic function are isolated. From this it follows that $f(x_1)$ has finitely many zeros in $\mathbb{Z}_2$ and a finite set has measure zero.[3]

Now assume that the result is true for power series in $n-1$ variables and write

$$f(x_1, x_2, \ldots, x_n) = \sum_{j=0}^{\infty} a_j(x_1, \ldots, x_{n-1}) x_n^j.$$

Let E be the zero set of f and let χ_E be the characteristic function of E. By the Fubini theorem, we have

$$\mu_n(E) = \int_{\mathbb{Z}_2^{n-1}} \int_{\mathbb{Z}_2} \chi_E(\vec{x}, x_n)\, \mathrm{d}x_n\, \mathrm{d}\vec{x}.$$

If we assume that $\mu_n(E) > 0$, the integrand must be positive on a set of positive measure. In particular, there is some $F \subseteq \mathbb{Z}_2^{n-1}$ so that $\mu_{n-1}(F) > 0$ and for all $\vec{x} \in F$,

$$\mu_1(\{x_n : (\vec{x}, x_n) \in E\}) > 0.$$

[2] The proof of this lemma follows the argument in the MSE post here, which proves the result in $\mathbb{C}^n$.

[3] Strassmann's theorem gives a more explicit upper bound on the number of zeros of a p-adic power series.

So if $\vec{x} \in F$, there is a positive measure set of x_n for which

$$\sum_{j=0}^{\infty} a_j(\vec{x}) x_n^j$$

vanishes. By the one-variable case, it follows that the one-variable power series $\sum a_j(\vec{x}) x_n^j$ vanishes, and therefore $a_j(\vec{x}) = 0$. This shows that each a_j vanishes on a set of positive measure and the $n-1$ variable case shows that $a_j = 0$ for all j. This shows that all the coefficients of f are equal to zero and so $f = 0$. □

Next, we need to apply ideas from p-adic Lie theory. For an introduction to this material, see [8]. Let $\Gamma_2 = \{M \in \mathrm{GL}_2(\mathbb{Z}_2) : M \equiv I \pmod 4\}$. Suppose that $A, B \in \Gamma_2$ and $G = \langle A, B \rangle$. Because Γ_2 is a uniform 2-group, the group Γ_2 can be given the structure of a $\mathbb{Z}_2$-Lie algebra via the operations

$$x + y = \lim_{n \to \infty} (x^{p^n} y^{p^n})^{p^{-n}}$$

and the Lie bracket

$$(x, y) = \lim_{n \to \infty} [x^{p^n}, y^{p^n}]^{p^{-2n}}$$

(where $[a, b] = aba^{-1}b^{-1}$).

Let $\mathfrak{gl}_2(R)$ denote the usual Lie algebra of 2×2 matrices with entries in R, where the Lie bracket is given via $[X, Y] = XY - YX$. Theorem 7.13 of [8] shows that the logarithm map sending $G \to \log(G) \subseteq \mathfrak{gl}_2(4\mathbb{Z}_2)$ is a Lie algebra isomorphism.

If $\log(G)$ has rank 4 as a $\mathbb{Z}_2$-module, then there is a positive integer $k \geq 2$ so that $\log(G)$ contains any matrix $\equiv 0 \pmod{2^k}$. If $X \equiv 0 \pmod{2^k}$, then $\log(I + X) \equiv 0 \pmod{2^k}$. Hence $\log(I + X) \in \log(G)$ and thus $I + X = \exp(\log(I + X)) \in G$. This shows that G has finite index.

Proof of Theorem 4.3. Fix two matrices $\overline{A}$ and $\overline{B}$ in $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ and let

$$A = \overline{A} + \begin{bmatrix} 4a_1 & 4a_2 \\ 4a_3 & 4a_4 \end{bmatrix}$$

$$B = \overline{B} + \begin{bmatrix} 4b_1 & 4b_2 \\ 4b_3 & 4b_4 \end{bmatrix}.$$

Because the exponent of $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ is 12, we have that $\overline{A}^{12} \equiv \overline{B}^{12} \equiv I \pmod 4$.

Let M be the 4×4 matrix whose columns consist of the entries of

$$\log(A^{12}), \log(B^{12}), [\log(A^{12}), \log(B^{12})], [[\log(A^{12}), \log(B^{12})], \log(A^{12})],$$

and let $d = \det(M)$. By the discussion above, if $d \neq 0$, then the four matrices above, which are all in $\log(\langle A^{12}, B^{12} \rangle)$, are linearly independent over $\mathbb{Z}_2$ which implies that $\log(\langle A^{12}, B^{12} \rangle)$ is a free $\mathbb{Z}_2$-module of rank 4,

and this implies that $\langle A^{12}, B^{12}\rangle$ has finite index in $\mathrm{GL}_2(\mathbb{Z}_2)$ (which implies that $\langle A, B\rangle$ also has finite index).

This d is a power series in the 8 variables $a_1, a_2, a_3, a_4, b_1, b_2, b_3, b_4$ which only depends on $\overline{A}$ and $\overline{B}$. Moreover, because $A^{12} \equiv I \pmod 4$ and $B^{12} \equiv I \pmod 4$, $A^{12} - I$ is a polynomial in $4a_1$, $4a_2$, $4a_3$ and $4a_4$ and the formula for the logarithm implies that $\log(A^{12})$ and $\log(B^{12})$ are power series in $\{4a_1, 4a_2, 4a_3, 4a_4\}$ and $\{4b_1, 4b_2, 4b_3, 4b_4\}$ respectively. This ensures that d converges on all of $\mathbb{Z}_2^8$.

The result will follow if we can show that for each pair $(\overline{A}, \overline{B}) \in \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})^2$, the power series d is nonzero. It suffices to show that this power series d has at least one nonzero specialization. We check this computationally by randomly choosing the $a_1, \ldots, b_4 \in \{1, 2, 3\}$ and computing d and checking if it is nonzero. In all 96^2 cases, we find a case where $d \not\equiv 0 \pmod{2^{50}}$. This completes the proof. □

Proof of Theorem 1.4. Suppose that $H \subseteq \mathrm{GL}_2(\mathbb{Z}_2)$ is a given subgroup with $\det(H) = \mathbb{Z}_2^\times$. If $A \in \mathrm{GL}_2(\mathbb{Z}_2)$ is a randomly chosen matrix with $\det(A) \equiv 3 \pmod 8$ and $B \in \mathrm{GL}_2(\mathbb{Z}_2)$ is a randomly chosen matrix with $\det(B) \equiv 5 \pmod 8$, let $M = \langle A, B\rangle$. This is a subgroup of $\mathrm{GL}_2(\mathbb{Z}_2)$ with $\det(M) = \mathbb{Z}_2^\times$ and precisely three maximal closed subgroups. With probability 1, M has finite-index in $\mathbb{Z}_2^\times$, and with probability $\frac{1}{|\mathrm{GL}_2(\mathbb{Z}_2):H|^2}$, we have $M \leq H$. So there is a positive probability that M is a minimal subgroup of H, and therefore minimal subgroups of H exist. □

5. Genus 0 Examples

5.1. The search for genus 0 groups. We now turn our attention to finding all of the genus 0 minimal subgroups of $\mathrm{GL}_2(\mathbb{Z}_2)$ up to conjugacy. We focus on genus zero curves because they supply infinitely many examples of elliptic curves whose 2-adic representations are minimal. Our first challenge is to find a finite box that contains all of the genus 0 minimal groups. According to [2, 3], the largest index of a subgroup of $\mathrm{PSL}_2(\mathbb{Z}_2)$ with genus 0 is 48. If $G \subseteq \mathrm{GL}_2(\mathbb{Z}_2)$ is a minimal group with $|\mathrm{GL}_2(\mathbb{Z}_2) : G| = d$, then surjectivity of the determinant gives that $|\mathrm{SL}_2(\mathbb{Z}_2) : G \cap \mathrm{SL}_2(\mathbb{Z}_2)| = d$ and this implies that the image of $G \cap \mathrm{SL}_2(\mathbb{Z}_2)$ in $\mathrm{PSL}_2(\mathbb{Z}_2)$ has index d or $d/2$. It follows that $d \leq 96$.

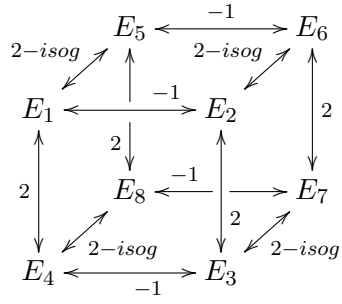
Next, if P is a Sylow 2-subgroup of $\mathrm{GL}_2(\mathbb{Z}_2)$, then $|\mathrm{GL}_2(\mathbb{Z}_2) : P| = 3$. Each maximal closed subgroup of P has level at most 8 and index 6. If $H \subseteq \mathrm{GL}_2(\mathbb{Z}_2)$ has level 2^k with $k \geq 2$, then every maximal subgroup of H has level dividing 2^{k+1} by Lemma 3.3 of [17]. Hence $|\mathrm{GL}_2(\mathbb{Z}_2) : G| \leq 96$ implies that the level of G is at most 128.

Searching for subgroups of $\mathrm{GL}_2(\mathbb{Z}/128\mathbb{Z})$ yields 7652 minimal groups, of which 28 have genus 0. Eight of these were already listed in Section 1. For the other 20 minimal groups G, the modular curve X_G is a conic without

rational points. None of these 28 genus 0 minimal groups contain $-I$. In fact, none of the minimal groups of level ≤ 128 contain $-I$. We conjecture that it is impossible for a minimal subgroup of $\mathrm{GL}_2(\mathbb{Z}_2)$ to contain $-I$.

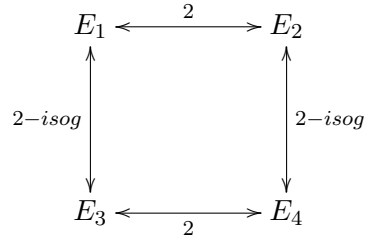
5.2. Models for the corresponding modular curves. The models for the 28 genus 0 modular curves corresponding to elliptic curves with minimal 2-adic image were computed using a combination of techniques. The 8 modular curves that were found using pure thought were computed in [17] and we simplified the models. The remaining 20 models were computed by using the techniques in [14] to compute covering models for modular curves associated to supergroups of these groups that contain $-I$. We then use this information together with information from [17] and compute models for these curves as fiber products of known modular curves.

Returning to the 8 minimal groups G that we found using pure thought in Section 1, if E_1 is the universal elliptic curve over X_G, then 3 other universal elliptic curves can be obtained by taking of twists of E_1 by -1, 2, and -2. We remark here that we are guaranteed that if E is an elliptic curve whose 2-adic image is minimal, then the twists of E by -1, 2 and -2 will also have minimal image because $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$ are the quadratic subfields of $\mathbb{Q}(\zeta_{2^\infty}) \subseteq \mathbb{Q}(E[2^\infty])$. The other 4 examples are 2-isogenous to the curves obtained this way. It turns out that this relationship persists for most of the other genus 0 minimal groups without points defined over $\mathbb{Q}$. That relationship is made explicit below. The vertical maps are twists by 2, the horizontal maps are twists by -1, and the maps from front to back are 2-isogenies.



E_1	16.48.0.25	32.96.0.2	32.96.0.1
E_2	16.48.0.26	32.96.0.4	32.96.0.3
E_3	16.48.0.82	32.96.0.26	32.96.0.25
E_4	16.48.0.83	32.96.0.28	32.96.0.27
E_5	16.48.0.238	32.96.0.105	32.96.0.108
E_6	16.48.0.239	32.96.0.107	32.96.0.106
E_7	16.48.0.234	32.96.0.101	32.96.0.104
E_8	16.48.0.235	32.96.0.103	32.96.0.102

The remaining 4 cases have RSZB label `8.24.0.44`, `8.24.0.86`, `8.24.0.123`, and `8.24.0.125`. If X_G is one of these modular curves, there is a universal elliptic curve E_1 parametrizing elliptic curves with 2-adic image contained in G. These elliptic curves are defined over $F = \mathbb{Q}(X_G)$, the function field of a pointless conic, and there is an automorphism $\varphi : F \to F$ with the property that $\varphi(E) \simeq E^{-1}$, where E^{-1} is the quadratic twist of E by -1. The existence of this automorphism collapses the cube above down to a square. The data can be summarized as follows:



E_1	`8.24.0.44`
E_2	`8.24.0.86`
E_3	`8.24.0.125`
E_4	`8.24.0.123`

For each of the families of elliptic curves we provide simplified models for E_1. The interested user can then take twists and isogenies to recover the remaining models. See Remark 5.2 for more details. For each curve we give a model for, we will define the base field as well as provide an A and B from the base field such that a generic elliptic curve with the corresponding image has the form

$$y^2 = x^3 + Ax^2 + Bx.$$

For three of the four families of curves, the base field they are defined over is the field of fractions of $\mathbb{Q}[a, b]/(a^2 + b^2 + 1)$ while the remaining curve is defined over $\mathbb{Q}(t)$.

Remark 5.1. We pause of a moment and give a quick summary of what is happening here. What we know is that every elliptic curve (up to isomorphism) over a number field K in which -1 is the sum of two squares and image in `16.48.0.25`, `39.96.0.2`, or `8.24.0.44` can be obtained by choosing a and b in K with $a^2 + b^2 = -1$ and plugging those a and b into our formulas. For `32.96.0.1`, every curve (up to isomorphism) defined over $\mathbb{Q}$ with this image can be obtained by choosing a $t \in \mathbb{Q}$ and plugging it into our formulas.

16.48.0.25	A	$2^2(b^2-2b-1)(b^2+2b-1)$
	B	$2^3(b^2+1)^2(b^2+2b-1)^2$
32.96.0.2	A	$2^6(b^2-3)(b^4-22b^2-7)(b^8+116b^6+1462b^4+4372b^2+3281)a$ $-2^2(b^8-108b^6+790b^4+116b^2-527)$ $\times(b^8+116b^6+1462b^4+4372b^2+3281)$
	B	$-2^7(b^2-3)^4(3b^{10}-101b^8-850b^6+5126b^4+5983b^2-913)$ $\times(b^{12}-210b^{10}+455b^8+27236b^6+2879b^4-62834b^2-35047)a$ $+2^3(b^2-3)^5(b^{22}-993b^{20}+80239b^{18}-183591b^{16}-25060758b^{14}$ $-46958090b^{12}+1283004574b^{10}+35562780 98b^8$ $+21550793 65b^6-1522506117b^4$ $-1813927741b^2-391647931)$
8.24.0.44	A	$2(b^2+1)(64b^4-16b^3+144b^2-16b+79)(8b^2+7)$
	B	$2^4(b^2+1)^3(32768b^{10}-20480b^9+245760b^8-92160b^7$ $+660480b^6-153216b^5+833280b^4-111840b^3$ $+504360b^2-30305b+118568)$
32.96.0.1	A	$-2^2(t^{16}-120t^{14}+1820t^{12}-8008t^{10}$ $+12870t^8-8008t^6+1820t^4-120t^2+1)$
	B	$2^3(t^2+1)^8(t^8-8t^7-28t^6+56t^5+70t^4-56t^3-28t^2+8t+1)^2$

Remark 5.2. Each of the elliptic curves above has a unique rational 2-isogeny. The kernel of this isogeny is exactly $\{\mathcal{O},(0,0)\}$. A classical result tells us that if E is an elliptic curve of the form

$$y^2=x^3+Ax^2+Bx,$$

and $\varphi\colon E\to E'$ is the 2-isogeny with kernel $\{\mathcal{O},(0,0)\}$, then E' is given by

$$y^2=x^3-2Ax^2+(A^2-4B)x.$$

Using this and [21, Proposition 5.4], we can easily compute the models for the other elliptic curves in each family.

6. Elliptic curves over imaginary quadratic fields with minimal image

In this final section, we give a family of elliptic curves defined over imaginary quadratic fields with minimal 2-adic image and bad reduction only at 2.

Proposition 6.1. *Suppose that n is a positive integer and let $a=\sqrt{-(2^n+1)}$. Let*

$$E: y^2=x^3+2ax^2+(a^2+1)x.$$

Then E has bad reduction only at prime ideals above 2 in $\mathbb{Q}(a)$. If n is odd and $n\neq 3$, then $\rho_{E,2^\infty}(G_{\mathbb{Q}(a)})$ is minimal and has RSZB label `8.24.0.86`. *If $n=2$, then $\rho_{E,2^\infty}(G_{\mathbb{Q}(a)})$ is minimal and has RSZB label* `16.384.9.895`. *If $n=10$, then $\rho_{E,2^\infty}(G_{\mathbb{Q}(a)})$ is minimal and has RSZB label* `16.384.9.894`.

Proof. The discriminant $\Delta(E) = -64(a^2+1)^2 = -64(-2^n)^2 = -2^{2n+6}$ is a power of 2, and therefore the only primes at which E could have bad reduction are primes above 2. This proves the first claim.

A computation with models of 2-adic modular curves in [17] shows that $y^2 = x^3 + 2tx^2 + (t^2+1)x$ is the universal elliptic curve with 2-adic image `4.12.0.12`. It follows that for any $n \geq 1$, the 2-adic image is contained in `4.12.0.12`. Note that this level 4 subgroup does not contain $-I$ and hence $-I \notin \rho_{E,2^\infty}(\mathbb{Q}(a))$ for any n.

Suppose that n is odd. Note that $2^n + 1$ cannot be twice a square. Moreover, $2^n + 1$ is a square if and only if $n = 3$. This ensures that $\mathbb{Q}(a) \notin \{\mathbb{Q}(i), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{2})\}$.

There are four maximal subgroups of `4.12.0.12` with surjective determinant, and they are `4.24.0.9`, `4.24.0.10`, `8.24.0.85`, and `8.24.0.86`. Using a model for `8.12.0.40` (generated by `8.24.0.86` and $-I$) we see that the 2-adic image $y^2 = x^3+2tx^2+(t^2+1)x$ is contained in `8.24.0.86` if and only if $t^2 + 1 = -2u^2$. This certainly occurs if $t = a = \sqrt{-(2^n+1)}$ with n odd. Moreover, `8.24.0.86` is a minimal group, and so if $\rho_{E,2^\infty}(G_{\mathbb{Q}(a)})$ is contained in it and has surjective determinant, it must equal it.

Suppose now that $n = 2$. Let $E' : y^2 = x^3 + 2a^2x^2 + a^2(a^2+1)x$. Then $E' : y^2 = x^3 - 10x^2 + 20x$ is a quadratic twist of E (by an element of $\mathbb{Q}(a)$). We know from the LMFDB that $\rho_{E',2^\infty}(G_{\mathbb{Q}})$ is `16.96.3.338`. This group and all of its index 2 subgroups contain $-I$. This implies that $\rho_{E',2^\infty}(G_{\mathbb{Q}(a)})$ contains $-I$, but we know that $\rho_{E,2^\infty}(G_{\mathbb{Q}(a)})$ does not. This implies that $\rho_{E,2^\infty}(G_{\mathbb{Q}(a)})$ is an index 2 subgroup of $\rho_{E',2^\infty}(G_{\mathbb{Q}(a)})$, which in turn implies that $\rho_{E',2^\infty}(G_{\mathbb{Q}(a)})$ must be a proper subgroup of $\rho_{E',2^\infty}(G_{\mathbb{Q}})$. There are four index two subgroups with surjective determinant up to conjugacy, and only one of these is contained in `4.6.0.5` (the subgroup generated by `4.12.0.12` and $-I$). This subgroup is `16.192.9.211` and so this must be $\rho_{E',2^\infty}(G_{\mathbb{Q}(a)})$. The group `16.192.9.211` has several index 2 subgroups that do not contain $-I$ and only one of these is contained in `4.12.0.12`. This subgroup has label `16.384.9.895`, and is minimal.

We apply the same process with $n = 10$. Let $E' : y^2 = x^3 + 2a^2x^2 + a^2(a^2+1)x$. Then $E' : y^2 = x^3 - 2050x^2 + 1049600x$ is a quadratic twist of E (by an element of $\mathbb{Q}(a)$). Since $j(E') = 257^3/2^8$, one of the exceptional j-invariants from the 2-adic classification, it follows that $\rho_{E',2^\infty}(G_{\mathbb{Q}})$ is `16.96.3.335`. Once again, this subgroup has no index 2 subgroups that do not contain $-I$, and therefore $\rho_{E',2}(G_{\mathbb{Q}(a)})$ must. However, $\rho_{E,2^\infty}(G_{\mathbb{Q}(a)})$ does not, and this implies that $\rho_{E,2^\infty}(G_{\mathbb{Q}(a)})$ is an index two subgroup of $\rho_{E',2^\infty}(G_{\mathbb{Q}(a)})$. There are four index two subgroups of `16.96.3.335` with surjective determinant up to conjugacy, and only one of these is contained in `4.6.0.5`. This subgroup is `16.192.9.208` and so this must be

$\rho_{E',2^\infty}(G_{\mathbb{Q}(a)})$. The group `16.192.9.208` has two index 2 subgroups without $-I$ up to conjugacy and the only one which is contained in `4.12.0.12` is the minimal `16.384.9.894`, which must equal $\rho_{E,2^\infty}(G_{\mathbb{Q}(a)})$. □

References

[1] W. Bosma, J. Cannon & C. Playoust, "The Magma algebra system. I. The user language", *J. Symb. Comput.* **24** (1997), no. 3-4, p. 235-265.

[2] C. J. Cummins & S. Pauli, "Data associate to Congruence subgroups of PSL(2, ℤ) of genus less than or equal to 24", `https://mathstats.uncg.edu/sites/pauli/congruence/`, accessed 2024-01-01.

[3] ———, "Congruence subgroups of PSL(2, ℤ) of genus less than or equal to 24", *Exp. Math.* **12** (2003), no. 2, p. 243-255.

[4] H. B. Daniels & E. González-Jiménez, "Serre's constant of elliptic curves over the rationals", *Exp. Math.* **31** (2022), no. 2, p. 518-536.

[5] H. B. Daniels, Á. Lozano-Robledo & J. S. Morrow, "Towards a classification of entanglements of Galois representations attached to elliptic curves", *Rev. Mat. Iberoam.* **39** (2023), no. 3, p. 803-844.

[6] H. B. Daniels & J. S. Morrow, "A group theoretic perspective on entanglements of division fields", *Trans. Amer. Math. Soc., Ser. B* **9** (2022), p. 827-858.

[7] H. B. Daniels & J. Rouse, "Code for Minimal Subgroups of $\mathrm{GL}_2(\mathbb{Z}_S)$", `https://github.com/HDaniels432/Minimal-Groups`, 2024, accessed 2024-03-06.

[8] J. D. Dixon, M. P. F. du Sautoy, A. Mann & D. Segal, *Analytic pro-p groups*, second ed., Cambridge Studies in Advanced Mathematics, vol. 61, Cambridge University Press, 1999, xviii+368 pages.

[9] D. S. Dummit & R. M. Foote, *Abstract algebra*, third ed., John Wiley & Sons, 2004, xii+932 pages.

[10] The LMFDB Collaboration, "The L-functions and modular forms database", `https://www.lmfdb.org`, 2023, accessed 2023-08-02.

[11] Á. Lozano-Robledo, *Elliptic curves, modular forms, and their L-functions*, Student Mathematical Library, vol. 58, American Mathematical Society, 2011, xiv+195 pages.

[12] J. S. Milne, "Abelian varieties", in *Arithmetic geometry (Storrs, Conn., 1984)*, Springer, 1986, p. 103-150.

[13] N. Nikolov & D. Segal, "Finite index subgroups in profinite groups", *C. R. Math.* **337** (2003), no. 5, p. 303-308.

[14] Rakvi, "A classification of genus 0 modular curves with rational points", *Math. Comput.* **93** (2024), no. 348, p. 1859-1902.

[15] A. M. Robert, *A course in p-adic analysis*, Graduate Texts in Mathematics, vol. 198, Springer, 2000, xvi+437 pages.

[16] J. Rouse, A. V. Sutherland & D. Zureick-Brown, "ℓ-adic images of Galois for elliptic curves over ℚ (and an appendix with John Voight)", *Forum Math. Sigma* **10** (2022), article no. e62 (63 pages), with an appendix with John Voight.

[17] J. Rouse & D. Zureick-Brown, "Elliptic curves over ℚ and 2-adic images of Galois", *Res. Number Theory* **1** (2015), article no. 12 (34 pages).

[18] J.-P. Serre, *Abelian l-adic representations and elliptic curves*, W. A. Benjamin, Inc., 1968, McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute, xvi+177 pages.

[19] J.-P. Serre & J. Tate, "Good reduction of abelian varieties", *Ann. Math. (2)* **88** (1968), p. 492-517.

[20] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer, 1994, xiv+525 pages.

[21] ———, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, 2009, xx+513 pages.

[22] J. Tate, "The non-existence of certain Galois extensions of **Q** unramified outside 2", in *Arithmetic geometry (Tempe, AZ, 1993)*, Contemporary Mathematics, vol. 174, American Mathematical Society, 1994, p. 153-156.

[23] D. Zywina, "On the possible images of the mod ell representations associated to elliptic curves over $\mathbb{Q}$", 2015, https://arxiv.org/abs/1508.07660.

[24] ———, "Explicit open images for elliptic curves over $\mathbb{Q}$", 2022, https://arxiv.org/abs/2206.14959.

Harris B. Daniels
Department of Mathematics and Statistics
Amherst College
Amherst, MA 01002, USA
E-mail: hdaniels@amherst.edu
URL: https://hdaniels.people.amherst.edu/

Jeremy Rouse
Department of Mathematics
Wake Forest University
Winston-Salem, NC 27109, USA
E-mail: rouseja@wfu.edu
URL: https://users.wfu.edu/rouseja/