THE DENSITY OF ODD ORDER REDUCTIONS FOR ELLIPTIC CURVES WITH A RATIONAL POINT OF ORDER 2

KE LIANG AND JEREMY ROUSE

Abstract. Suppose that $E/Q$ is an elliptic curve with a rational point $T$ of order 2 and $\alpha \in E(Q)$ is a point of infinite order. We consider the problem of determining the density of primes $p$ for which $\alpha \in E(F_p)$ has odd order. This density is determined by the image of the arboreal Galois representation $\tau_{E,2^k} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to AGL_2(\mathbb{Z}/2^k\mathbb{Z})$. Assuming that $\alpha$ is primitive (that is, neither $\alpha$ nor $\alpha + T$ is twice a point over $\mathbb{Q}$) and that the image of the ordinary mod $2^k$ Galois representation is as large as possible (subject to $E$ having a rational point of order 2), we determine that there are 63 possibilities for the image of $\tau_{E,2^k}$. As a consequence, the density of primes $p$ for which the order of $\alpha$ is odd is between $1/14$ and $89/168$.

1. Introduction and Statement of Results

Let $E/Q$ be an elliptic curve and $\alpha \in E(Q)$ be a point of infinite order. For each prime $p$ for which $E/F_p$ has good reduction, the reduced point $\alpha \in E(F_p)$ has finite order, say $M_p$. What can one say about the sequence of numbers $M_p$ as $p$ varies?

We are particularly interested in how often the number $M_p$ is odd. More precisely, let $S$ denote the set of primes $p$ for which $p \nmid N(E)$ and for which $M_p$ is odd. We are interested in the relative density of $S$ within the set of primes, namely $\lim_{x \to \infty} \frac{\pi_S(x)}{\pi(x)}$. Naively, one would expect this to occur 50 percent of the time, but this is often not the case. For example, in [5], the authors show that if $E : y^2 + y = x^3 - x$ and $\alpha = (0,0)$, then

$$\lim_{x \to \infty} \frac{\pi_S(x)}{\pi(x)} = \frac{11}{21} \approx 0.52381.$$ 

Moreover, for each positive integer $k$, there is a Galois representation (depending both on $E$ and the point $\alpha$) $\tau_{E,2^k} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to (\mathbb{Z}/2^k\mathbb{Z})^2 \rtimes \text{GL}_2(\mathbb{Z}/2^k\mathbb{Z}) := AGL_2(\mathbb{Z}/2^k\mathbb{Z})$, and Theorem 3.2 of [5] implies that the relative density of the set $S$ only depends on the image of $\tau_{E,2^k}$ (for all $k$).

Variations of this problem have been studied by several authors. (See for example [9], [8], [6], and [3].) In [4], the authors study the problem of determining the image of $\tau$ subject to the constraints that (i) the usual mod $2^k$ Galois representation $\rho_{E,2^k} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_2(\mathbb{Z}/2^k\mathbb{Z})$ is surjective for all $k$, and (ii) $\alpha \in E(\mathbb{Q})$ is not equal to $2\gamma$ for any $\gamma \in E(\mathbb{Q})$. They show that under these hypotheses, there are two possibilities for the image of $\tau$: $AGL_2(\mathbb{Z}/2^k\mathbb{Z})$, and an index 4 subgroup thereof. In the latter case, the density is $179/336$. 
The goal of the present paper is to study the situation when the image of $\rho_{E,2^k}$ is
\[
\Gamma_0(2) := \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{GL}_2(\mathbb{Z}/2^k\mathbb{Z}) : c \equiv 0 \pmod{2} \right\}.
\]
In this situation, $E$ has a rational point of order 2, which we refer to as $T$. We wish to impose the “primitivity condition” that neither $\alpha$ nor $\alpha + T$ is equal to $2\gamma$ for some $\gamma \in E(\mathbb{Q})$. This condition is automatically satisfied if we choose $\alpha$ to be a generator of the group $E(\mathbb{Q})$. This assumption means that there are only finitely many possibilities for the image of $\tau_{E,2^k}$.

**Theorem 1.** Let $E/\mathbb{Q}$ be an elliptic curve with the image of $\rho_{E,2^k}$ equal to $\Gamma_0(2)$ for all $k$. Let $T$ denote the unique rational point of order 2 in $E(\mathbb{Q})$, and suppose that $\alpha \in E(\mathbb{Q})$ has the property that neither $\alpha$ nor $\alpha + T$ is of the form $2\gamma$ for $\gamma \in E(\mathbb{Q})$. Then, there are precisely 63 possibilities for the image of $\tau_{E,2^k}$ (up to conjugacy in $\text{AGL}_2(\mathbb{Z}/2^k\mathbb{Z})$), and there are 21 possibilities for the relative density of the set of primes for which $\alpha$ has odd order modulo $p$, ranging from $1/14 \approx 0.0714$ to $89/168 \approx 0.5298$.

We can translate all of the hypotheses in the theorem into purely group theoretic statements. In Section 3 we solve the problem of determining which possible subgroups of $\text{AGL}_2(\mathbb{Z}/2^k\mathbb{Z})$ could be the image of $\tau$ by computing with Magma. In all, we find that there are 63 candidates as shown in the graph below.

In Section 4 we give concrete conditions that describe when the image of $\tau_{E,2^k}$ lies in each of the subgroups above, and we exhibit a pair $(E, \alpha)$ of an elliptic curve and a point $\alpha$ with
each of the 63 possible images. Finally, in Section 5 we give a method suited to computer computation for computing the relative density of the set of primes where $\alpha$ has odd order, given the image of $\tau_{E,2^k}$.

Acknowledgements. The authors used Magma [2] (version 2.23-11) for computations. A part of this work constitutes the first author’s thesis at Wake Forest University.

2. Background

Let $E/\mathbb{Q}$ be an elliptic curve. For a positive integer $m$, define $E[m] = \{ Q : mQ = 0 \}$, where 0 denotes the identity of the group law. We have that $E[m](\mathbb{C}) \cong (\mathbb{Z}/m\mathbb{Z})^2$. We say that $E$ has good reduction at $p$ if $E/\mathbb{F}_p$ is non-singular, and we say that $E$ has bad reduction otherwise. If we choose a basis $\langle E \rangle$, we get the usual mod $m$ Galois representation $\rho_{E,m} : \text{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}) \to \text{GL}_2(\mathbb{Z}/m\mathbb{Z})$ given by $\rho_{E,m}(\sigma) = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, where

$$\sigma(A) = aA + bB \text{ and } \sigma(B) = cA + dB.$$ 

If $E/\mathbb{Q}$ is an elliptic curve and $\text{im } \rho_{E,2^k} = \Gamma_0(2)$, then $E$ has a rational point of order 2. By translating this rational point to the origin, we can assume that $E : y^2 = x^3 + ax^2 + bx$ for some $a,b \in \mathbb{Z}$ and that $T = (0,0)$ is the unique point of order 2. The subgroup $\{(0 : 1 : 0), T\}$ is the kernel of an isogeny $\phi : E \rightarrow E'$ where $E' : y^2 = x^3 + (-2a)x^2 + (a^2 - 4b)x$, and

$$\phi(x, y) = \left( \frac{y^2}{x^2}, \frac{y(x^2 - b)}{x^2} \right).$$

The dual isogeny $\psi : E' \to E$ has a similar formula (see [12] page 79). We have $\psi \circ \phi(P) = 2P$ for all $P \in E(\mathbb{Q})$ and $\phi \circ \psi(Q) = 2Q$ for all $Q \in E'(\mathbb{Q})$.

Let $\alpha \in E(\mathbb{Q})$ be a point of infinite order. For a positive integer $m$, let $[m^{-1}]\alpha = \{ P \in E(\mathbb{C}) : mP = \alpha \}$ be the preimage of $\alpha$ under the multiplication by $m$ map. For a positive integer $k$, there are $4^k$ points $\delta \in [(2^k)^{-1}]\alpha$. The coordinates of these points are algebraic numbers and we define $K_k$ to be the field obtained by adjoining to $\mathbb{Q}$ these coordinates. The extension $K_k/\mathbb{Q}$ is Galois. For each positive integer $k$, we choose one point $\beta_k$ so that $2^k \beta_k = \alpha$ and we choose these in such a way that $2 \beta_k = \beta_{k-1}$. If $\sigma \in \text{Gal}(K_k/\mathbb{Q})$, $\sigma(\beta_k)$ is also in $[(2^k)^{-1}]\alpha$ and hence we can write

$$\sigma(\beta_k) = \beta_k + cA + fB,$$

where $\langle A,B \rangle = E[2^k]$. The map $\tau_{E,2^k} : \text{Gal}(K_k/\mathbb{Q}) \to \text{AGL}_2(\mathbb{Z}/2^k\mathbb{Z})$ given by

$$\tau_{E,2^k}(\sigma) = \left( \begin{bmatrix} e & f \\ \end{bmatrix}, \rho_{E,2^k}(\sigma) \right)$$

is the arboreal Galois representation. Here $\rho_{E,2^k}$ is as given above. We think of $\begin{bmatrix} e & f \end{bmatrix} \in (\mathbb{Z}/2^k\mathbb{Z})^2$ as being a row vector. The group operation on $\text{AGL}_2(\mathbb{Z}/2^k\mathbb{Z})$ is given by $(\vec{v}_1, M_1) * (\vec{v}_2, M_2) = (\vec{v}_2 + \vec{v}_1M_1, M_1M_2)$. This makes it so that the action of $\sigma \in \text{Gal}(K_k/\mathbb{Q})$ on $[(2^k)^{-1}]\alpha$ is equivalent to the action of the function $\vec{v} + \vec{x}M$ on row vectors $\vec{x} \in (\mathbb{Z}/2^k\mathbb{Z})^2$. 


(where \((\vec{v}, M) = \tau_{E,2^k}(\sigma)\)). Moreover, the map
\[
\begin{bmatrix} c & f \\ a & b \end{bmatrix} \mapsto \begin{bmatrix} a & b & 0 \\ c & d & 0 \\ e & f & 1 \end{bmatrix}
\]
from \(\text{AGL}_2(\mathbb{Z}/2^k\mathbb{Z})\) to \(\text{GL}_3(\mathbb{Z}/2^k\mathbb{Z})\) is a homomorphism, and it is convenient to think of \(\text{AGL}_2(\mathbb{Z}/2^k\mathbb{Z})\) as a subgroup of \(\text{GL}_3(\mathbb{Z}/2^k\mathbb{Z})\) for computational purposes. Note that \(\text{AGL}_2(\mathbb{Z}/2^k\mathbb{Z})\) consists of pairs of vectors in \((\mathbb{Z}/2^k\mathbb{Z})^2\) and matrices \(M \in \text{GL}_2(\mathbb{Z}/2^k\mathbb{Z})\) and so \(|\text{AGL}_2(\mathbb{Z}/2^k\mathbb{Z})| = 2^{2k} \cdot |\text{GL}_2(\mathbb{Z}/2^k\mathbb{Z})| = 3 \cdot 2^{6k-3} \).

We wish to give a brief accounting of the connection between the image of \(\tau_{E,2^k}\) and the relative density of primes \(p\) for which \(\alpha \in E(\mathbb{F}_p)\) has odd order. For a more detailed explanation, see Theorem 5.1 of [1].

Let \(p\) be an odd prime with \(p \nmid N(E)\). Then it is straightforward to see that \(\alpha \in E(\mathbb{F}_p)\) has odd order if and only if for all \(k \geq 1\), there is some point \(\beta_k \in [(2^k)^{-1}]\alpha \cap E(\mathbb{F}_p)\). This corresponds to some element of \([(2^k)^{-1}]\alpha \) “having coordinates in \(\mathbb{F}_p\).” More precisely, if \(O_{K_k}\) is the ring of algebraic integers in \(K_k\), and \(p\) is a prime ideal above \(p\) and \(\sigma_p \in \text{Gal}(K_k/\mathbb{Q})\) is the corresponding Frobenius automorphism at \(p\), saying that some element of \([(2^k)^{-1}]\alpha \) “has coordinates in \(\mathbb{F}_p\)” is asking for \(\sigma_p\) to fix some element of \([(2^k)^{-1}]\alpha \). Since the action of \(\sigma_p\) on \([(2^k)^{-1}]\alpha \) is equivalent to the action of the function \(f(x) = \vec{v} + xM\) on \((\mathbb{Z}/2^k\mathbb{Z})^2\), where \((\vec{v}, M) = \tau_{E,2^k}(\sigma_p)\), this is the same as asking for \(f(x)\) to have a fixed point. Equivalently, \(\vec{v} \in \text{Row}(M - I)\). In the case that \(\det(M - I) \equiv 0 \pmod{2^k}\), \(\vec{v} \in \text{Row}(M - I)\) implies that \([(2^k)^{-1}]\alpha \cap E(\mathbb{F}_p)\) is nonempty for all \(k\) and so \(\alpha \in E(\mathbb{F}_p)\) has odd order. The relative density of \(p\) for which \(\det(\rho_{E,2^k}(\sigma_p) - I) \equiv 0 \pmod{2^k}\) tends to zero as \(k \to \infty\). Thus, the Chebotarev Density theorem implies that
\[
\lim_{x \to \infty} \frac{\pi_S(x)}{\pi(x)} = \lim_{k \to \infty} \frac{\#\{(\vec{v}, M) \in \text{im} \tau_{E,2^k} : \vec{v} \in \text{Row}(M - I)\}}{|\text{im} \tau_{E,2^k}|}.
\]

### 3. Group Theory

We study the possibilities for the image of \(\tau\), assuming \(\text{im} \rho\) is as large as possible subject to \(E\) having a rational point of order 2. Specifically, we will deal with the case when the image of \(\rho_{E,2^k}\) is \(\Gamma_0(2)\). In essence, we have a homomorphism \(\tau : \text{Gal}(K_k)/\mathbb{Q} \to G\), where \(G\) is some finite group, and we are interested in understanding when \(\tau\) is surjective.

**Definition.** Let \(\Gamma_0^\oplus(2)\) be the subgroup of \(\text{AGL}_2(\mathbb{Z}/2^k\mathbb{Z})\) consisting the matrices
\[
\begin{bmatrix} a & b & 0 \\ c & d & 0 \\ e & f & 1 \end{bmatrix}
\]
with \(e, f\) any entries in \(\mathbb{Z}/2^k\mathbb{Z}\) and \(\begin{bmatrix} a & b \\ c & d \end{bmatrix} \) is in \(\Gamma_0(2)\).

We have \(|\text{AGL}_2(\mathbb{Z}/2^k\mathbb{Z}) : \Gamma_0^\oplus(2)| = 3\), so \(|\Gamma_0^\oplus(2)| = 2^{6k-3}\).
Recall that if $G$ is a finite group, the Frattini subgroup $\Phi(G)$ is the intersection of all maximal subgroups of $G$. Here are two facts about the Frattini subgroup.

**Theorem 2** (Theorem 5.2.13 of [10] p. 135). If $G$ is a finite group and $N$ is a normal subgroup of $G$, then $\Phi(N) \trianglelefteq \Phi(G)$.

**Theorem 3** (Theorem 5.3.1 of [10] p. 139). Let $G$ be a group whose order is a power of 2. If $M \subseteq G$ is a maximal subgroup, then $|G : M| = 2$. As a consequence, if $x \in G$, then $x^2 \in \Phi(G)$.

The next result gives us a method for finding all maximal subgroups of a subgroup $M \subseteq \Gamma_0^\square(2)$ that contains the kernel of reduction mod 8.

**Theorem 4.** For any $k \geq 3$, if $M \subseteq \Gamma_0^\square(2)$ and $M$ contains $\{(\vec{v}, M) : \vec{v} \equiv 0 \pmod{8}, M \equiv I \pmod{8}\}$, then $\Phi(M) \supseteq \{(\vec{v}, M) : \vec{v} \equiv 0 \pmod{16}, M \equiv I \pmod{16}\}$.

**Proof.** If $N = \{(\vec{v}, M) : \vec{v} \equiv 0 \pmod{8}, M \equiv I \pmod{8}\}$, then $N$ is the kernel of the map $\phi : G \to AGL_2(\mathbb{Z}/8\mathbb{Z})$ with $\phi((\vec{v}, M)) = (\vec{v} \pmod{8}, M \pmod{8})$, so $N$ is a normal subgroup of $G$. Since $|N| = 2^{6k-20}$ so that $N$ is a power of 2, we have that if $x \in N$, then $x^2 \in \Phi(N)$ by Theorem 3. If $\vec{v} \equiv 0 \pmod{16}$, then $\vec{v} = 2\vec{w}$ with $x = (\vec{w}, I) \in N$. So, we have $x^2 = (2\vec{w}, I) = (\vec{w}, I) \in \Phi(N)$.

We claim that every element $(\vec{0}, I + 2^l g)$ is in $\Phi(N)$ for $4 \leq l \leq k$, where $g$ is any $2 \times 2$ matrix with entries in $\mathbb{Z}/2^{k-l}\mathbb{Z}$.

We prove this by backwards induction on $l$. The case that $l = k$ is the base case and is trivial. Assume that for all $l > r$, every element $(\vec{0}, I + 2^l g)$ is in $\Phi(N)$. We prove the same for $l = r$. We have $x = (\vec{0}, I + 2^{r-1} g) \in N$ and so $x^2 = (\vec{0}, (I + 2^{r-1} g)^2) = (\vec{0}, I + 2^r g + 2^{2r-2} g^2) \in \Phi(N)$. So we have $I + 2^r g + 2^{2r-2} g^2 \equiv I + 2^r g \pmod{2^{2r-2}}$.

Since $r \geq 4$, we have that $2r - 4 \geq r$ and by the induction hypothesis, every matrix $h$ congruent to the identity mod $2^{2r-2}$ has $(\vec{0}, h) \in \Phi(N)$. This completes the induction.

It follows that $\Phi(N)$ contains all the elements of the form $(0, I + 2^l g)$ and all elements of the form $(\vec{v}, I)$ where $\vec{v} \equiv 0 \pmod{16}$. Thus, it contains all elements of the form $(0, I + 2^4 g) \ast (\vec{v}, I) = (\vec{v} + \vec{0}, I + 2^4 g) = (\vec{v}, I + 2^4 g)$.

This shows that $\Phi(N)$ contains all of these elements and by Theorem 2, $\Phi(N) \subseteq \Phi(M)$. □

Here are our computation steps in Magma, from which we can know there are only 63 possible candidates:

1. We start with $\Gamma_0^\square(2)$ and compute its maximal subgroups. We say a subgroup $M$ is _happy_ if the image of $M$ inside $GL_2(\mathbb{Z}/2^k\mathbb{Z})$ is $\Gamma_0(2)$, $M \not\subseteq \left\{ \begin{bmatrix} a & b & 0 \\ c & d & 0 \\ e & f & 1 \end{bmatrix} : e \equiv f \equiv 0 \pmod{2} \right\}$. 


\((\alpha \not\in 2E(\mathbb{Q}))\) and \(M \not\subseteq \left\{ \begin{bmatrix} a & b & 0 \\ c & d & 0 \\ e & f & 1 \end{bmatrix} : e \equiv c/2 \pmod{2}, f \equiv (d-1)/2 \pmod{2} \right\}\)

\((\alpha + T \not\in 2E(\mathbb{Q}))\).

(2) We make a list of all happy subgroups \(\subseteq \text{AGL}_2(\mathbb{Z}/8\mathbb{Z})\) and we get 63 subgroups (up to conjugacy).

(3) We make a list of all happy subgroups \(\subseteq \text{AGL}_2(\mathbb{Z}/16\mathbb{Z})\) and we get 63 subgroups (up to conjugacy).

If \(M\) is one of these 63 happy subgroups of \(\text{AGL}_2(\mathbb{Z}/8\mathbb{Z})\) and \(K \subseteq M\) is any happy subgroup of it, then \(K \subseteq L\) for some maximal subgroup \(L\) of \(M\). Then, \(\Phi(M) \subseteq L\) and \(\{(\bar{v}, M) : \bar{v} \equiv 0 \pmod{16}, M \equiv I \pmod{16}\} \subseteq \Phi(M)\) so that \(L\) will show up in our list in step 3. In other words, \(H\) is one of our 63 subgroups if and only if

\[
H \supseteq \left\{ \begin{bmatrix} a & b & 0 \\ c & d & 0 \\ e & f & 1 \end{bmatrix} : a \equiv d \equiv 1 \pmod{8}, b \equiv c \equiv e \equiv f \equiv 0 \pmod{8} \right\}.
\]

For use in the next section, it will be helpful to define certain subgroups and discuss the corresponding subfields.

**Definition.** Let \(G\) be a finite group and suppose that \(N_1\) and \(N_2\) are subgroups of \(G\) with \(|G : N_1| = |G : N_2| = 2\). It follows that \(N_1\) and \(N_2\) are both normal subgroups. Define \(N_1 \ast N_2 = \{g \in G : \text{either } g \in N_1 \text{ and } g \in N_2 \text{ or } g \not\in N_1 \text{ and } g \not\in N_2\}\).

**Claim 5.** \(N_1 \ast N_2\) is a subgroup of \(G\) and \(|G : N_1 \ast N_2| = 2\).

**Proof.** Let \(\phi : G \to (G/N_1) \times (G/N_2)\) be given by \(\phi(x) = (xN_1, xN_2)\). Then, \(G/N_1 \cong \mathbb{Z}/2\mathbb{Z}\) and \(G/N_2 \cong \mathbb{Z}/2\mathbb{Z}\). Then, \(N_1 \ast N_2 = \{g \in G : \phi(g) = (0, 0) \text{ or } \phi(g) = (1, 1)\}\) is clearly a subgroup of \(G\) of index 2. 

Suppose \(M \subseteq \Gamma_0(2)\) is the pre-image under \(\Gamma_0(2) \to \Gamma_0(2)\) of a maximal subgroup of \(\Gamma_0(2)\). For each \(H \subseteq \Gamma_0(2)\) that is happy, with \(\text{im } \rho = \Gamma_0(2)\), \(M \ast H\) is a happy subgroup of \(\Gamma_0(2)\) with \(\text{im } \rho = \Gamma_0(2)\).

If \(G = \text{Gal}(K/\mathbb{Q})\) and \(N_1\) and \(N_2\) are subgroups of \(G\), they correspond to subfields \(K_1/\mathbb{Q}\) and \(K_2/\mathbb{Q}\). Since \(|G : N_1| = 2\) and \(|G : N_2| = 2\), \(|K_1 : \mathbb{Q}| = |K_2 : \mathbb{Q}| = 2\). Thus, \(K_1 = \mathbb{Q}(\sqrt{d_1})\) and \(K_2 = \mathbb{Q}(\sqrt{d_2})\), where \(N_1 = \text{Gal}(K/K_1)\) and \(N_2 = \text{Gal}(K/K_2)\). In this case, \(N_1 \ast N_2\) corresponds to \(\mathbb{Q}(\sqrt{d_1d_2})\). This is because we have \(\sigma(\sqrt{d_1}) = \sqrt{d_1}\) if and only if \(\sigma \in N_1\); otherwise \(\sigma(\sqrt{d_1}) = -\sqrt{d_1}\) and \(\sigma(\sqrt{d_1}) = \sqrt{d_2}\) if and only if \(\sigma \in N_2\).

Then, we have that \(\sigma(\sqrt{d_1d_2}) = \sqrt{d_1d_2}\) if and only if

\[
\frac{\sigma(\sqrt{d_1})}{\sqrt{d_1}} = \frac{\sigma(\sqrt{d_2})}{\sqrt{d_2}},
\]

and so \(\sigma(\sqrt{d_1d_2}) = \sqrt{d_1d_2}\) if and only if \(\sigma \in N_1 \ast N_2\).
4. Interpretation of the images of $\tau$

In this section, we describe the interpretation of the 63 possible different images of $\tau_{E,2^k}$, up to conjugacy. We will describe the methods we used to find an interpretation for each of the possible images of $\tau_{E,2^k}$, and end this section by giving a table of images, interpretations, densities, and elliptic curves that yield each image.

The lattice of the happy subgroups of $\Gamma_0(2)$ is the following.

![Figure 1. Possible images of $\tau_{E,2^k}$](image)

The subgroup 1 corresponds to $\Gamma_0^\oplus(2)$. The sixteen orange boxes on the second level represent index 2 subgroups of $\Gamma_0^\oplus(2)$, while those boxes on the third and fourth level represent index 4 and index 8 subgroups, respectively.

Suppose that $E/\mathbb{Q}$ is an elliptic curve with a rational point of order 2 and $\alpha \in E(\mathbb{Q})$ is a point of infinite order. Assume that that $E : y^2 = x^3 + ax^2 + bx$. We denote $\alpha = (c,ck)$, which forces $b = ck^2 - ac - c^2$. We will specify curves in this family by the parameters $a$, $c$ and $k$. The group $\Gamma_0^\oplus(2)$ has 31 maximal subgroups of index 2. These subgroups can be
generated (using the * operation of Section 3) from five subgroups. One of these is
\[ M = \left\{ \begin{bmatrix} a & b & 0 \\ c & d & 0 \\ e & f & 1 \end{bmatrix} : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(2) \text{ and } e \equiv 0 \pmod{2} \right\}. \]

The other four are maximal subgroups of the form
\[ \left\{ \begin{bmatrix} a & b & 0 \\ c & d & 0 \\ e & f & 1 \end{bmatrix} : \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in K \right\} \]
where \( K \subseteq \Gamma_0(2) \) is a maximal subgroup. We define \( M_{-1} \) to be the maximal subgroup of this form corresponding to \( K = \{ g \in \Gamma_0(2) : \det(g) \equiv 1 \pmod{4} \} \), \( M_2 \) to be the maximal subgroup of this form corresponding to \( K = \{ g \in \Gamma_0(2) : \det(g) \equiv \pm 1 \pmod{8} \} \), \( M_b \) to correspond to \( K = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(2) : c \equiv 0 \pmod{4} \right\} \) and \( M_{a^2-4b} \) to correspond to \( K = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(2) : b \equiv 0 \pmod{2} \right\} \). For \( d \in \{-1,2,b,a^2-4b\} \) the fixed field of \( \tau_{E,2^k}^{-1}(M_d) \) is \( \mathbb{Q}(\sqrt{d}) \).

Let \( H_i \) denote the \( i \)th subgroup in the chart above. (For a Magma file that contains generators of each subgroup, as well as other scripts and log files related to the computations in this section, see the page [http://users.wfu.edu/rouseja/liang-rouse/](http://users.wfu.edu/rouseja/liang-rouse/).

The subgroup \( H_2 \) equals the subgroup \( M \) defined above. We have that \( \text{im} \tau \subseteq H_2 \) if and only if for all \( \sigma \in \text{Gal}(K_k/\mathbb{Q}) \), \( \sigma(\beta_1) = \beta_1 \) or \( \beta_1 + T \). This implies that \( \alpha' = \phi(\beta_1) = \phi(\beta_1 + T) \) in \( E'(\mathbb{Q}) \) is rational. Since \( \psi(\alpha') = \alpha \), this implies that the \( x \)-coordinate of \( \alpha, c, \) is a perfect square. Hence, \( \text{im} \tau \subseteq H_2 \) if and only if \( c \) is a perfect square. This gives the interpretation for subgroup 2. It follows from this that \( \text{im} \tau = \Gamma_0(2) \) if and only if \( \langle -1,2,b,a^2-4b \rangle \subseteq (\mathbb{Q}^\times)/(\mathbb{Q}^\times)^2 \) has order 32 (which is equivalent to there being no multiplicative relations, mod squares, involving \(-1,2,b,a^2-4b \) and \( c \)).

Given a number \( d \in \{-1,2,b,a^2-4b\} \), we let \( M_d \subseteq \Gamma_0(2) \) denote the maximal subgroup with the property that \( g \in M_d \) if and only if when \( \tau_{E,2^k}(\sigma) = g \), we have that \( \sigma \) fixes \( \sqrt{d} \). That is, \( M_d \) is the subgroup of \( \Gamma_0(2) \) corresponding to \( \mathbb{Q}(\sqrt{d}) \). It is not hard to see that \( \text{im} \tau_{E,2^k} \subseteq H_2 \ast M_d \) if and only if \( cd \) is a perfect square, and this furnishes the interpretations for subgroups 3 through 17. We will use this trick for other batches of subgroups (18-24, 25-32, 33-39, 40-47, 48-55, and 56-63). In particular, we will compute the interpretation for one such subgroup, and then use this group-theoretic method to find the interpretation for all other subgroups in that batch.

It follows from the interpretations above that maximal subgroups of subgroups 2 and 10 arise because either the point \( \alpha \) or \( \alpha + T \) is the image of a rational point under the isogeny \( \psi : E' \to E \). The situation where subgroups 7 and 15 is a bit more mysterious, and we will take a moment to explain where those maximal subgroups come from. First, the discriminant of the curve \( E \) is \( \Delta(E) = 16b^2(a^2-4b) \), and an examination of the classification of 2-adic
images of elliptic curves over $\mathbb{Q}$ by the second author and David Zureick-Brown (see [11])
shows that for any curve $E/\mathbb{Q}$, $\sqrt{\Delta(E)} \in \mathbb{Q}(E[4])$. (In fact, the modular curve $X_{2a}$ of $\mathbb{I}$
parametrizes elliptic curves whose discriminant is a fourth power.) Now, the image of $\tau$ is
contained in subgroup 15 if and only if $\frac{-(a^2 - 4b)}{c(2cd + 4kc)}$ is a square in $\mathbb{Q}$, and in this case the
field $\mathbb{Q}(\beta_1)$ obtained by adjoining a preimage of $\alpha$ under multiplication by 2 is also a radical
extension: we have $\mathbb{Q}(\beta_1) = \mathbb{Q}(\sqrt{c\sqrt{2cd + 4kc}})$. This implies that the quantity
\[
\frac{-(a^2 - 4b)}{c(2cd + 4kc)^2}
\]
is a square in $\mathbb{Q}$, but is a fourth power in $\mathbb{Q}(\beta_1, E[8])$, and this means that
\[
\mathbb{Q}\left(\sqrt[4]{\frac{-(a^2 - 4b)}{c(2cd + 4kc)^2}}\right)/\mathbb{Q}
\]
gives rise to a quadratic extension which examples show can be independent of the other 15
quadratic subextensions coming from square roots of products of $\{-1, 2, b, a^2 - 4b\}$. This
explains the presence of the maximal subgroups of subgroup 15. (For the maximal subgroups
of group 7, one can consider instead the field obtained by taking a preimage of $\alpha + T$.)

To compute the interpretation for one subgroup in each of our batches, we will use a technique
from [4] (see the proof of the Lemma on page 962) and [11] (see the proof of Lemma 9.1). Given a subgroup $H \subseteq \text{AGL}_2(\mathbb{Z}/2^k\mathbb{Z})$ and an elliptic curve $E$ (depending on the parameters
$a$, $c$ and $k$), we wish to compute a polynomial $f_{a,c,k}(x) \in \mathbb{Z}[a,c,k][x]$ so that $f_{a,c,k}(x)$ has a
rational root if and only if the image of $\tau_{E,2^k}$ is contained in $H$. Let $\beta_k$ denote a point so
that $2^k\beta_k = \alpha$, and let $A$ and $B$ be points which generate $E[2^k] \cong (\mathbb{Z}/2^k\mathbb{Z})^2$. For each right
coset $C$ of $H$ in $\text{AGL}_2(\mathbb{Z}/2^k\mathbb{Z})$, let
\[
\zeta_C = \sum_{\sigma \in C} \sigma(x(\beta_2 + A))\sigma(x(\beta_2 + B))\sigma(x(\beta_2 + A + B))^2.
\]
Then, let $f_{a,c,k}(x) = \prod_C(x - \zeta_C)$. A straightforward computation shows that the $x$-coordinates
of the points $\beta_k + r_1A + r_2B$, $0 \leq r_1, r_2 < 2^k$ are integral over $\mathbb{Z}[a,c,k]$ and it follows that
$f_{a,c,k}(x) \in \mathbb{Z}[a,c,k][x]$. Moreover, the change of variables $(x, y) \mapsto (t^2x, t^3y)$ sends $a \mapsto t^2a$, $c \mapsto t^2c$ and $k \mapsto tk$. For this reason, we say that $a$ and $c$ have weight 2 and $k$ has weight 1.
The map $(x, y) \mapsto (t^2x, t^3y)$ sends $\zeta_C$ to $t^8\zeta_C$, and it follows from this that the weight of the
coefficient of $x^i$ in $f_{a,c,k}$ is $8\deg(f_{a,c,k}) - 8i$. To find the polynomial $f_{a,c,k}$ one then simply
computes $f_{a,c,k}$ for several triples $(a, c, k)$ (by numerically computing the $x$-coordinates of the
$\beta_k + r_1A + r_2B$ using the fact that $E(C) \cong C/\Lambda$ for some lattice $\Lambda$), and uses linear algebra
to determine the coefficients of each monomial of the correct weight in the coefficient of $x^i$.
This method produces the polynomial $f_{a,c,k}(x) \in \mathbb{Z}[a,c,k][x]$.

Next, we present tables describing the various images. The table below gives for each sub-
group an element with the property that $\text{im} \tau_{E,2^k}$ is contained in that subgroup if and only
if that element is a square in $\mathbb{Q}$, a curve (specified by $[a,c,k]$) whose image is that subgroup,
the density of odd order reductions associated with that image of $\tau_{E,2^k}$ (for more detail about
how these were computed, see Section 5), and the value of $\pi_S(x)/\pi(x)$ for the curve specified
with $x = 10^7$. 

Subgroup 18 – 24 arise as images when $c = s^2$ is a perfect square. In this case, there are two points $\alpha' \in E'(\mathbb{Q})$ so that $\psi(\alpha') = \alpha$. We have

$$\alpha' = (a + 2s^2 + 2sk, 2s(a + 2s^2 + 2sk))$$

and the two choices of $\alpha'$ correspond to the choice of the sign of $s$. In the table below, we specify the square class of $x(\alpha')$ and this means that the image of $\tau$ is contained in the corresponding subgroup when either choice of $\alpha'$ results in $x(\alpha')$ being in the correct square class.

| Subgroup | Element | Curve     | Density     | $\pi_S(10^7)/\pi(10^7)$ |
|----------|---------|-----------|-------------|--------------------------|
| 18       | $-2bx(\alpha')$ | $[7, 16, 3]$ | $5123/10752 \approx 0.476470$ | 0.477010 |
| 19       | $2bx(\alpha')$ | $[-3, 1, 2]$ | $5123/10752 \approx 0.476470$ | 0.476296 |
| 20       | $-bx(\alpha')$ | $[28, 36, 1]$ | $83/168 \approx 0.494048$ | 0.494378 |
| 21       | $bx(\alpha')$ | $[-5, 1, 4]$ | $19/42 \approx 0.452381$ | 0.452681 |
| 22       | $-2x(\alpha')$ | $[2, 1, 3]$ | $5123/10752 \approx 0.476470$ | 0.476195 |
| 23       | $2x(\alpha')$ | $[-4, 1, 2]$ | $5123/10752 \approx 0.476470$ | 0.476213 |
| 24       | $-x(\alpha')$ | $[3, 1, 3]$ | $83/168 \approx 0.494048$ | 0.493984 |

Now we consider the batch of subgroups 25 – 32 which are subgroups of group 7. The image of $\tau$ is contained in group 7 if and only if $-bc(a^2 - 4b)$ is a square, which is equivalent to $-(a^2 - 4b)x(\alpha + T)$ being a square. We have $x(\alpha + T) = -a - c + k^2$ and so we let $-(a^2 - 4b)(-a - c + k^2) = d^2$. As above, there are two choices of $d$. Note that the quantities listed in the Element table can sometimes equal zero, and in this case, the table below does not determine the image of $\tau$. 

Now we consider the batch of subgroups 33-39, which are subgroups of group 10. This implies that $bc$ is a square, which implies that $x(\alpha + T)$ is a square and hence there are two points $\alpha' \in E'(\mathbb{Q})$ with $\psi(\alpha') = \alpha + T$. The table is the following.

| Subgroup | Element | Curve | Density | $\pi_s(10^7)/\pi(10^7)$ |
|----------|---------|-------|---------|-------------------------|
| 33       | $-2bx(\alpha')$ | $[-7, -14, 2]$ | $513/3584 \approx 0.143136$ | 0.143191 |
| 34       | $2bx(\alpha')$ | $[-3, 6, 2]$ | $513/3584 \approx 0.143136$ | 0.143121 |
| 35       | $-bx(\alpha')$ | $[-40, 45, 3]$ | $5/42 \approx 0.119048$ | 0.119048 |
| 36       | $bx(\alpha')$ | $[10, 10, 6]$ | $5/42 \approx 0.119048$ | 0.118733 |
| 37       | $-2\alpha(\alpha')$ | $[2, 3, 3]$ | $513/3584 \approx 0.143136$ | 0.143154 |
| 38       | $2\alpha(\alpha')$ | $[-2, 7, 3]$ | $513/3584 \approx 0.143136$ | 0.143036 |
| 39       | $-\alpha(\alpha')$ | $[2, 5, 4]$ | $5/42 \approx 0.119048$ | 0.118566 |

We consider the batch of subgroups 40-47, which are subgroups of group 15. We write $-c(a^2 - 4b) = d^2$, and there are two choices for $d$. As before, if either of these choices for $d$ makes the quantity listed in the Element column of the table a non-zero square, the image of $\tau$ is contained in the corresponding subgroup.

| Subgroup | Element | Curve | Density | $\pi_s(10^7)/\pi(10^7)$ |
|----------|---------|-------|---------|-------------------------|
| 40       | $2bcd(d + 2ck)$ | $[-45, 60, 5]$ | $2659/10752 \approx 0.247303$ | 0.247000 |
| 41       | $bcd(d + 2ck)$ | $[-210, -21, 12]$ | $89/336 \approx 0.264881$ | 0.265084 |
| 42       | $-2bcd(d + 2ck)$ | $[15, 15, 6]$ | $2659/10752 \approx 0.247303$ | 0.247006 |
| 43       | $-bcd(d + 2ck)$ | $[-55, 11, -9]$ | $89/336 \approx 0.264881$ | 0.264981 |
| 44       | $2cd(d + 2ck)$ | $[10, 5, 6]$ | $2659/10752 \approx 0.247303$ | 0.247056 |
| 45       | $cd(d + 2ck)$ | $[6, 3, 4]$ | $25/112 \approx 0.223214$ | 0.223415 |
| 46       | $-2cd(d + 2ck)$ | $[-6, -3, 2]$ | $2659/10752 \approx 0.247303$ | 0.247212 |
| 47       | $-cd(d + 2ck)$ | $[-14, -7, 6]$ | $25/112 \approx 0.223214$ | 0.223007 |

For the batch of subgroups 48-55, we have the same sort of phenomenon happening as with the maximal subgroups of groups 7 and 10, except this time on $E'$ instead of $E$. The image of $\tau$ is contained in group 20 if $-bx(\alpha')$ is a square, which is the same as saying that $-(b/c)(a + 2s^2 - 2sk)$ is a square (where again $c = s^2$). Write $-(b/c)(a + 2s^2 - 2sk) = d^2$ and recall now that there are two choices for $s$ and two choices for $d$ (per $s$ with $-b(a + 2s^2 - 2sk)$ a square). If any of these choices make it so the quantity in the Element column is a square, then the image of $\tau$ is contained in the corresponding subgroup.
\[ \begin{array}{|c|c|c|c|c|} \hline \text{Subgroup} & \text{Element} & \text{Curve} & \text{Density} & \pi_{S}(10^7)/\pi(10^7) \\ \hline 48 & 2(a^2 - 4b)(d + x(\alpha + T)) & [60, 36, 9] & 2659/5376 \approx 0.494606 & 0.494232 \\ 49 & b(a^2 - 4b)(d + x(\alpha + T)) & [30, 121, 1] & 89/168 \approx 0.529762 & 0.529399 \\ 50 & -2(a^2 - 4b)(d + x(\alpha + T)) & [90, 16, 16] & 2659/5376 \approx 0.494606 & 0.494423 \\ 51 & -2b(a^2 - 4b)(d + x(\alpha + T)) & [210, 81, 21] & 41/84 \approx 0.488095 & 0.487864 \\ 52 & -2b(d + x(\alpha + T)) & [15, 9, 2] & 2659/5376 \approx 0.494606 & 0.494824 \\ 53 & -(d + x(\alpha + T)) & [-12, 16, 1] & 41/84 \approx 0.488095 & 0.488500 \\ 54 & 2b(d + x(\alpha + T)) & [3, 1, 4] & 2659/5376 \approx 0.494606 & 0.494469 \\ 55 & d + x(\alpha + T) & [-7, 16, 11] & 25/56 \approx 0.446429 & 0.446331 \\ \hline \end{array} \]

The last batch of subgroups is 56-63, which are subgroups of group 35. For these groups, \( x(\alpha + T) = -a - c + k^2 \) is a square, so write \( -a - c + k^2 = s^2 \). The image of \( \tau \) is contained in group 35 if and only if \( -bx(\alpha') \) is a square, which means \((a + s^2 - k^2)(a + 2s^2 - 2sk) = d^2\). (Again, there are two choices for \( s \), and for a valid choice of \( s \), two choices for \( d \).) The table for this batch is the following.

In this section, we give a convenient way to compute the limit on the right hand side of \( [1] \), and in this section we allow \( \ell \) to be any prime number and \( G \subseteq AGL_2(\mathbb{Z}/\ell^m\mathbb{Z}) \) to be a subgroup of index \( m \). The right hand side of \( [1] \) is

\[
\mathcal{F}(G) = \lim_{k \to \infty} \frac{\#\{(\bar{v}, g) \in AGL_2(\mathbb{Z}/\ell^k\mathbb{Z}) : (\bar{v} \mod \ell^r, g \mod \ell^r) \in G \text{ and } \bar{v} \in \text{Row}(g - I)\}}{\#\{(\bar{v}, g) \in AGL_2(\mathbb{Z}/\ell^k\mathbb{Z}) : (\bar{v} \mod \ell^r, g \mod \ell^r) \in G\}}.
\]

By Theorem 3.2 of \( [5] \) if \( E/\mathbb{Q} \) is an elliptic curve without complex multiplication, \( \alpha \in E(\mathbb{Q}) \), and the image of \( \tau_{E, \ell^k} \) is the full preimage in \( AGL_2(\mathbb{Z}/\ell^k\mathbb{Z}) \) of \( G \) for all \( k \), the density of primes \( p \) for which \( \alpha \in E(\mathbb{F}_p) \) has order coprime to \( \ell \) is equal to \( \mathcal{F}(G) \).

A general procedure for computing \( \mathcal{F}(G) \) with a finite amount of computation has already been given by Lombardo and Perucca (see \([6]\) and \([7]\)). They also handle the cases that arise for elliptic curves with complex multiplication. We wish to give a few simple rules that allow for easy computer computation of \( \mathcal{F}(G) \). Given that our results essentially follow from the work of Lombardo and Perucca, we will not give full details in the proofs.

5. Calculating the density
For $\vec{v} \in (\mathbb{Z}/\ell^r\mathbb{Z})^2$ and $M \in M_2(\mathbb{Z}/\ell^r\mathbb{Z})$, we define

$$
\mu_r(\vec{v}, M) = \lim_{k \to \infty} \frac{\#\{(\vec{v}, \tilde{M}) \in (\mathbb{Z}/\ell^k\mathbb{Z})^2 \times M_2(\mathbb{Z}/\ell^k\mathbb{Z}) : (\vec{v}, \tilde{M}) \equiv (\vec{v}, M) \pmod{\ell^r}, \vec{v} \in \text{Row}(\tilde{M} - I)\}}{\#\text{AGL}_2(\mathbb{Z}/\ell^k\mathbb{Z})/m}. \ell^{6(k-r)}
$$

The quantity $\mu_r(\vec{v}, M)$ is the contribution to the density of all lifts of $(\vec{v}, M) \in G$ and so $\mathcal{F}(G) = \sum_{(\vec{v}, M) \in G} \mu_r(\vec{v}, g)$.

**Lemma 6.** If $\vec{v} \not\in \text{Row}(M - I)$, then $\mu_r(\vec{v}, M) = 0$.

**Proof.** It is easy to see that no lifts $(\vec{v}, \tilde{M})$ of $(\vec{v}, M)$ have $\vec{v} \in \text{Row}(\tilde{M} - I)$ either. \hfill \Box

**Lemma 7.** If $\vec{v} \equiv 0 \pmod{\ell}$ and $M - I \equiv 0 \pmod{\ell}$, then

$$
\mu_r(\vec{v}, M) = \frac{1}{\ell^6} \mu_r^{-1}\left(\frac{\vec{v}}{\ell^r}\left(\frac{M - I}{\ell}\right) + I\right).
$$

**Proof.** This follows easily from the fact that a solution to $\vec{v} \equiv \tilde{x}(M - I) \pmod{\ell^k}$ is equivalent to a solution to $\frac{\vec{v}}{\ell^r} \equiv \tilde{x}\frac{M - I}{\ell}$ (mod $\ell^{k-1}$). \hfill \Box

**Lemma 8.** If $\det(M - I) \not\equiv 0 \pmod{\ell^r}$ and $\vec{v} \in \text{Row}(M - I)$, then

$$
\mu_r(\vec{v}, M) = \frac{m}{\#\text{AGL}_2(\mathbb{Z}/\ell^r\mathbb{Z})}.
$$

**Proof.** This lemma is equivalent to the statement that every vector $\vec{v} \equiv \vec{v} \pmod{\ell^r}$ is in $\text{Row}(\tilde{M} - I)$ for any matrix $\tilde{M} \equiv M \pmod{\ell^r}$. If $y$ is an integer so that $y\det(\tilde{M} - I) \equiv \ell^{r-1} \pmod{\ell^r}$, this follows from the formula $y\text{adj}(\tilde{M} - I)(\tilde{M} - I) \equiv \ell^{r-1}I \pmod{\ell^r}$. Here $\text{adj}(M - I)$ is the adjoint of $\tilde{M} - I$. \hfill \Box

**Lemma 9.** Suppose that $\det(M - I) \equiv 0 \pmod{\ell^r}$, $\vec{v} \in \text{Row}(M - I)$, but not all entries in $M - I$ are $\equiv 0 \pmod{\ell}$. Then

$$
\mu_r(\vec{v}, M) = \frac{m}{\ell^{6r-4}(\ell - 1)^2(\ell + 1)^2}.
$$

**Proof.** We let $\vec{v} = [\epsilon \quad \zeta]$ and $M = I + \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$. We consider lifts $(\vec{v}, \tilde{M}) \pmod{\ell^{r+1}}$ with $\tilde{v} = [\epsilon + e\ell^r \quad \zeta + f\ell^r]$, $\tilde{M} = M + \ell^r\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ where $a, b, c, d, e, f \in \mathbb{Z}/\ell\mathbb{Z}$.

One can see that $\det(\tilde{M} - I) \equiv \det(M) + (\alpha\delta - b\gamma - c\beta + do)\ell^r \pmod{\ell^{r+1}}$ and the assumption that $M \not\equiv I \pmod{\ell}$ guarantees that there are $\ell^{r-\ell} \ell^r$ lifts $(\vec{v}, \tilde{M})$ of $(\vec{v}, M)$ with $\det(\tilde{M} - I) \not\equiv 0 \pmod{\ell^{r+1}}$. It then suffices to compute the number of lifts $(\vec{v}, \tilde{M})$ with $\det(\tilde{M} - I) \equiv 0 \pmod{\ell^{r+1}}$ and $\vec{v} \in \text{Row}(\tilde{M} - I)$. Cramer’s rule shows that this occurs if and only if the
choice of \((a, b, c, d, e, f)\) satisfies

\[
\begin{align*}
    a\delta - \gamma b - \beta c + ad &\equiv -\frac{\alpha\delta - \beta\gamma}{\ell^r} \quad \text{(mod } \ell) \\
    -c\zeta + de + e\delta - f\gamma &\equiv -\frac{\delta\epsilon - \gamma\zeta}{\ell^r} \quad \text{(mod } \ell) \\
    a\zeta - be - \beta e + \alpha f &\equiv -\frac{\alpha\zeta - \beta\epsilon}{\ell^r} \quad \text{(mod } \ell).
\end{align*}
\]

If we assume that \(\alpha \not\equiv 0 \pmod{\ell}\), one can choose arbitrary values for \(a, b, c\) and \(e\) and then solve the first and third congruences for \(d\) and \(f\). With these values for \(d\) and \(f\), one can prove the second congruence is also true. (So the second congruence follows from the first and the third, assuming that \(\alpha \not\equiv 0 \pmod{\ell}\).) This implies that there are \(\ell^4\) lifts \((\tilde{v}, \tilde{M})\) with \(\tilde{v} \in \text{Row}(\tilde{M} - I)\). (Similarly arguments apply if \(\beta, \gamma\) or \(\delta\) is \(\not\equiv 0 \pmod{\ell}\).) This implies that

\[
\mu_r(\tilde{v}, M) = \frac{m(1 - \frac{1}{\ell})}{\#\text{AGL}_2(\mathbb{Z}/\ell^r \mathbb{Z})} + \sum_{(\tilde{v}, \tilde{M})} \mu_{r+1}(\tilde{v}, \tilde{M}),
\]

where the sum is over the pairs \((\tilde{v}, \tilde{M})\) with \(\tilde{v} \in \text{Row}(M - I)\) and \(\det(\tilde{M}) \equiv 0 \pmod{\ell^{r+1}}\).

We apply the above equation repeatedly and obtain that

\[
\mu_r(\tilde{v}, M) = \frac{m}{\#\text{AGL}_2(\mathbb{Z}/\ell^r \mathbb{Z})} \cdot \left[1 + \frac{1}{\ell^2} + \frac{1}{\ell^4} + \cdots\right] = \frac{m}{(\ell - 1)^2(\ell + 1)^2\ell^{6r-4}}.
\]

Lemma 10. We have \(\mu_r(\bar{0}, I) = \frac{(\ell - 1)^{r+1}m}{\ell r^{4r-5}(\ell^6 - 1)}\).

Proof. By using Lemma 7 it suffices to handle the case that \(r = 1\). Lemma 7 also gives that

\[
\mu_1(\bar{0}, I) = \frac{1}{\ell^6} \mu_0(\bar{0}, I) = \frac{1}{\ell^6} \sum_{\tilde{v} \in (\mathbb{Z}/\ell \mathbb{Z})^2} \mu_1(\tilde{v}, M).
\]

There are \(\ell^2 \cdot \#\text{GL}_2(\mathbb{Z}/\ell \mathbb{Z})\) pairs \((\tilde{v}, M)\) for which \(M - I\) is invertible. The contribution of these pairs is \(\frac{m}{\ell^r}\) by Lemma 8.

If \(\det(M - I) \equiv 0 \pmod{\ell}\) but \(M - I\) is not the zero matrix, then \(\#\text{Row}(M - I) = \ell\) and there are \(\ell^3 + \ell^2 - \ell - 1\) matrices that fall into this case. By Lemma 9 the contribution of these cases is

\[
\frac{1}{\ell^6} \cdot \left(\frac{m}{(\ell - 1)^2\ell^2(\ell + 1)^2}\right) \cdot \ell(\ell^3 + \ell^2 - \ell - 1) = \frac{m}{(\ell - 1)^3\ell^7}.
\]
Finally, we have the case that $\vec{v} = \vec{0}$ and $M = I$ and we get

$$\mu_1(\vec{0}, I) = \frac{m}{\ell^6} + \frac{m}{(\ell - 1)\ell^7} + \frac{1}{\ell^6} \mu_1(\vec{0}, I).$$

Solving for $\mu_1(\vec{0}, I)$ gives the desired result. \qed

References

[1] Alexi Block Gorman, Tyler Genao, Heesu Hwang, Noam Kantor, Sarah Parsons, and Jeremy Rouse. The density of primes dividing a particular non-linear recurrence sequence. *Acta Arith.*, 175(1):71–100, 2016.

[2] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[3] Bryant Davis, Rebecca Kotsonis, and Jeremy Rouse. The density of primes dividing a term in the Somos-5 sequence. *Proc. Amer. Math. Soc. Ser. B*, 4:5–20, 2017.

[4] Tim Dokchitser and Vladimir Dokchitser. Surjectivity of mod $2^n$ representations of elliptic curves. *Math. Z.*, 272(3-4):961–964, 2012.

[5] Rafe Jones and Jeremy Rouse. Galois theory of iterated endomorphisms. *Proc. Lond. Math. Soc. (3)*, 100(3):763–794, 2010. Appendix A by Jeffrey D. Achter.

[6] Davide Lombardo and Antonella Perucca. Reductions of points on algebraic groups. Preprint.

[7] Davide Lombardo and Antonella Perucca. The 1-eigenspace for matrices in $\text{GL}_2(\mathbb{Z}_\ell)$. *New York J. Math.*, 23:897–925, 2017.

[8] Antonella Perucca. On the reduction of points on abelian varieties and tori. *Int. Math. Res. Not. IMRN*, (2):293–308, 2011.

[9] Richard Pink. On the order of the reduction of a point on an abelian variety. *Math. Ann.*, 330(2):275–291, 2004.

[10] Derek J. S. Robinson. *A course in the theory of groups*, volume 80 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1996.

[11] Jeremy Rouse and David Zureick-Brown. Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois. *Res. Number Theory*, 1:Art. 12, 34, 2015.

[12] Joseph H. Silverman and John Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.