**Julio Brau**

# Congruence conditions on supersingular primes

**Master's thesis, defended on June 22, 2009**

**Thesis advisor: Peter Stevenhagen**

**Mathematisch Instituut**
**Universiteit Leiden**

# Contents

**1 Introduction** **1**

1.1 Motivating problem . . . . . . . . . . . . . . . . . . . . . . . . . . . . 1

1.2 Elliptic Curves and Galois Representations . . . . . . . . . . . . . . . . 1

**2 The Galois representation of $Y^2 = (X+1)(X^2+4)$** **4**

2.1 Computation of $G_\ell$ for $\ell \geqslant 5$ . . . . . . . . . . . . . . . . . . . . . . . . 4

2.2 Computation of $G_\ell$ for $\ell = 2$ and $\ell = 3$ . . . . . . . . . . . . . . . . . . 7

2.3 Computation of a split and stable $m$ . . . . . . . . . . . . . . . . . . . . 15

**3 Congruence conditions on the supersingular primes** **19**

# 1 Introduction

## 1.1 Motivating problem

The origin of this thesis lies in an email by A. Berkovich dated June 26th 2007, which posed the following question: what are the primes $p$ such that $S(p) = 0$? Here

$$S(p) = \sum_{x=0}^{p-1} \left( \frac{(x+1)(x^2+4)}{p} \right).$$

We have that $S(p) = 0$ whenever $(x+1)(x^2+4)$ is a square mod $p$ not divisible by $p$ for exactly the same amount of residues $x$ for which it is a non-square. The first primes for which this happens are 2, 11, 131, 251, 491, 599, 1439, 3371, 5639, 5879, and 6971. It was also noted by Berkovich that for primes greater than 2, these are $-1$ or 11 mod 120. Does this always hold, and if so, why is this the case?

This is the motivating question behind this work, as this question which is posed in a simple manner can be rephrased in terms of elliptic curves. In answering it we will naturally be led to study Galois representations associated to elliptic curves. As we will see, finding the complete Galois representation of a certain elliptic curve will show something even stronger, and in particular answer the question posed at the start.

## 1.2 Elliptic Curves and Galois Representations

As we mentioned, we would like to rephrase the above problem in the language of elliptic curves and Galois representations. To do so, we will first recall some basic facts and definitions, as well as establishing the notation we will use throughout this paper.

Let $E$ be an elliptic curve over $\mathbb{Q}$ given by the equation $Y^2 = f(X)$ with $\in \mathbb{Z}[X]$ monic of degree 3. Recall that for primes of good reduction $p$, that is, primes such that $v_p(\Delta) = 0$ holds, we may reduce the curve mod $p$ so as to obtain an elliptic curve $\tilde{E}$ over $\mathbb{F}_p$. Hasse's theorem gives an estimate for the number of $\mathbb{F}_p$-rational points on $\tilde{E}$. More specifically, we have

$$|\#\tilde{E}(\mathbb{F}_p) - p - 1| \leqslant 2\sqrt{p}.$$

We can determine $\#\tilde{E}(\mathbb{F}_p)$ by checking for each $x \in \mathbb{F}_p$ whether $f(x)$ is a non-zero square, zero, or a non-square in $\mathbb{F}_p$, which will yield respectively two, one or zero $\mathbb{F}_p$-rational points on $\tilde{E}$. The Legendre symbol $\left(\frac{f(x)}{p}\right)$ will have the value 1, 0 or $-1$ respectively in each case, hence we may write

$$\#\tilde{E}(\mathbb{F}_p) = p + 1 + S(p)$$

where $S(p)$ is as in 1.1. Recall also that if we denote the Frobenius endomorphism of $\tilde{E}$ by $\sigma_p$, then it satisfies the quadratic equation

$$\sigma_p^2 - t_p\sigma_p + p = 0 \quad \text{in} \quad \mathrm{End}(\tilde{E}),$$

where the integer $t_p$ satisfies $\#\tilde{E}(\mathbb{F}_p) = p + 1 - t_p$ and is referred to as the *trace of Frobenius*. We see then that we have $S(p) = -t_p$.

With all this in mind, the problem posed in 1.1 can be rephrased by asking for the elliptic curve given by the equation $Y^2 = (X+1)(X^2+4)$, for which primes $p$ is the trace of Frobenius $t_p$ equal to zero, or equivalently, for which primes $p$ do we have $\#\tilde{E}(\mathbb{F}_p) = p + 1$? Primes $p$ with this property are called *supersingular primes* of $E$.

When $E$ does not have complex multiplication over $\bar{\mathbb{Q}}$, its set of supersingular primes is somewhat mysterious, and several open questions regarding this special set of primes still remain. Serre has shown that the set of supersingular primes for $E$ has density 0, but it is still not known what their asymptotic growth is. There is however a conjecture of Lang and Trotter which says that

$$\#\{p < x : p \text{ is supersingular}\} \sim c\frac{\sqrt{x}}{\log x}$$

as $x \to \infty$, where $c > 0$ is a constant depending on $E$. Even though supersingular primes for $E$ are quite rare, Elkies has shown that nonetheless there are infinitely many.

Looking back at the motivating question, it appears that for the specific curve given by $Y^2 = (X+1)(X^2+4)$, we have the somewhat surprising observation that odd supersingular primes seem to satisfy a congruence condition, namely they all seem to be in the residue class of $-1$ or $11 \bmod 120$. Since this curve has no complex multiplication, we immediately see that, by Dirichlet's Theorem on primes in arithmetic progressions, the converse to this observation cannot hold.

We are interested in studying the set of primes $p$ such that the trace of Frobenius $t_p$ is 0. As we will now see, this naturally leads us to study the Galois representation attached to $E$, since in this way we will be able to realize $t_p$ as the trace of a matrix of the Frobenius element.

Recall that if we denote by $E[m]$ the $m$-torsion subgroup of $E$, then each element of $G = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on $E[m]$. In particular $G$ acts on $E[\ell^n]$ for a prime $\ell$ and a positive integer $n$, hence it also acts on the *$\ell$-adic Tate module*

$$T_\ell(E) = \varprojlim_n E[\ell^n]$$

of $E$. For each prime $\ell$ denote by

$$\rho_\ell : G \longrightarrow \mathrm{Aut}(T_\ell(E)) \simeq \mathrm{GL}_2(\mathbb{Z}_\ell)$$

the representation given by the action of $G$ on $T_\ell(E)$, where the isomorphism on the right involves choosing a basis for $T_\ell(E)$. Taking the product $T(E) = \prod_\ell T_\ell(E)$ over all primes $\ell$ gives the *complete Galois representation* attached $E$, which we denote by

$$\rho : G \longrightarrow \mathrm{Aut}(T(E)) \simeq \prod_\ell \mathrm{GL}_2(\mathbb{Z}_\ell) = \mathrm{GL}_2(\hat{\mathbb{Z}}).$$

For each positive integer $m$ we may reduce $\mathrm{GL}_2(\hat{\mathbb{Z}})$ mod $m$, thereby obtaining a representation

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

for a certain choice of basis. Let $G(m)$ denote its image, so that $G(m) \subset \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. This representation is given by the action of $G$ on $E[m]$. The fixed field of $\mathrm{Ker}\rho_{(m)}$ is the $m$-torsion field of $\mathbb{Q}$, that is, the finite extension of $\mathbb{Q}$ obtained by adjoining the coordinates of all $m$-torsion points of $E$, which we shall denote by $\mathbb{Q}(E[m])$. We have then that $G(m) \simeq G/\,Ker\,\rho_{(m)} \simeq \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q})$.

Note that since $\mathbb{Q}(\zeta_m) \subset \mathbb{Q}(E[m])$, then $G(m)$ acts on $\zeta_m$. This action is via the determinant, that is, the element $\sigma \in G(m)$ acts on $\zeta_m$ by $\zeta_m \mapsto \zeta_m^{\det(\sigma)}$. From this it follows that the composite map

$$\rho : G \longrightarrow \mathrm{GL}_2(\hat{\mathbb{Z}}) \xrightarrow{\det} \hat{\mathbb{Z}}^*$$

is surjective: it is the cyclotomic character.

Also, let $G_m$ denote the projection of $\rho(G)$ into the finite product

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

Then we have $G_m = \mathrm{Gal}(K_m/\mathbb{Q})$, where $K_m$ is the $m$-power torsion field, that is, the infinite extension of $\mathbb{Q}$ obtained by adjoining the coordinates of all $m^n$-torsion points of $E$ for all $n$.

The main result in the theory of Galois representations of elliptic curves over the rationals without CM is the following theorem of Serre, proved in [6].

**Theorem 1.1** (Serre)**.** *Let $E$ be an elliptic curve over $\mathbb{Q}$ without CM. Then $\rho(G)$ is a subgroup of finite index of $\mathrm{GL}_2(\hat{\mathbb{Z}})$.*

This is equivalent to the following two conditions holding simultaneously:

(i) $G_\ell$ is of finite index in $\mathrm{GL}_2(\mathbb{Z}_\ell)$ for all $\ell$.

(ii) $G_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$ for almost all $\ell$.

It is also equivalent to saying that there is an integer $m$ such that the following holds:

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

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

$$\pi_m : \prod_{\ell | m} \mathrm{GL}_2(\mathbb{Z}_\ell) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$$

denotes the reduction map.

When (i) holds we say $m$ *splits* $\rho$, and when (ii) holds we say $m$ is *stable.* Note that $m$ splitting $\rho$ depends only on the primes dividing $\ell$ and not on the powers to which these primes occur, and $m$ being stable depends on the primes dividing $m$ and their respective powers. Given a split and stable $m$, the complete Galois representation of $E$ is completely determined at a finite level, that is, it suffices to know $G(m)$, since

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

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

Given a prime $p$ such that $p \nmid \ell\Delta$, we recall that $I_p$ acts trivially on $T_\ell(E)$, where $I_p$ denotes the inertia subgroup of $p$ in $G$. Then we say that $\rho_\ell$ is unramified at $p$ and its Frobenius element $\sigma_p$ is well defined (up to conjugation) in $\rho_\ell(G)$. The element $\rho_\ell(\sigma_p)$ has characteristic polynomial

$$\Phi_p(X) = X^2 - t_p X + p \in \mathbb{Z}[X],$$

which does not depend on the choice of basis. Here $t_p$ is the trace of the matrix $\rho_\ell(\sigma_p)$ and $p$ is the determinant. We see then how Frobenius elements of unramified primes allow us to realize $t_p$ as the trace of a matrix $\rho_\ell(\sigma_p)$ in $\mathrm{GL}_2(\mathbb{Z}_\ell)$.

In the following section we find a split and stable $m$ for the elliptic curve mentioned in the introduction. This gives us the complete Galois representation of our curve, and so helps us study the behaviour of its supersingular primes.

# 2 The Galois representation of $Y^2 = (X+1)(X^2+4)$

## 2.1 Computation of $G_\ell$ for $\ell \geqslant 5$

In this section we compute the complete Galois representation of the elliptic curve given by $Y^2 = (X+1)(X^2+4)$. Since it is more convenient to have the rational 2-torsion point be the origin, we make the substitution $x \mapsto x+1$, thus obtaining the curve given by $Y^2 = X(X^2 - 2X + 5)$. This will be the curve of interest for the rest of the paper.

Our first step is to compute $G(\ell)$ for all primes $\ell$. As we will see, for almost all primes this group will be the full $\mathrm{GL}_2(\mathbb{F}_\ell)$. Note first that our curve $E$ has discriminant $\Delta = -2^8 5^2$ and $j$-invariant $j = 2^8 11^3/5^2$, hence it does not have CM and it has bad reduction at 2 and 5. It has multiplicative (semi-stable) reduction at 5 and additive reduction at 2. It follows from [8], pg. 357, that $E$ is isomorphic to a Tate curve over an unramified quadratic extension of $\mathbb{Q}_5$. The following result of Serre tells us that such Tate curves give elements of order $\ell$ in $G(\ell)$. See [5], §IV-20, for the proof.

**Lemma 2.1.** *Suppose that an elliptic curve $E$ has multiplicative reduction at $p$, and let $\ell$ be a prime that does not divide $-v_p(j)$. Then $\rho_{(\ell)}(I_p) \subset G(\ell)$ contains an element of order $\ell$.*

Since for our curve we have that $v_5(j) = -2$, the lemma implies that $G(\ell)$ has en element of order $\ell$ for $\ell \geqslant 3$. This fact will be useful in conjunction with the following proposition, which tells us that if $G(\ell)$ has an element of order $\ell$, there are only two possibilities for $G(\ell)$. We say that a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ is *Borel* if it is upper triangular.

**Proposition 2.2.** *Let $H$ be a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ of order divisible by $\ell$. Then either $H$ contains $\mathrm{SL}_2(\mathbb{F}_\ell)$ or $H$ is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$.*

*Proof.* See [6], §2.4. □

Using Lemma 2.1 and Proposition 2.2 we see that for $\ell \geqslant 3$ either $G(\ell)$ is contained in a Borel subgroup or it contains $\mathrm{SL}_2(\mathbb{F}_\ell)$. The surjectivity of the determinant map thus implies that if $G(\ell)$ is not contained in a Borel subgroup, then it must equal $\mathrm{GL}_2(\mathbb{F}_\ell)$, so to show that $G(\ell) = \mathrm{GL}_2(\mathbb{F}_\ell)$ holds for almost all $\ell$, it suffices to see that for almost all $\ell$ we cannot have $G(\ell)$ contained in a Borel subgroup.

Let us see what happens if $G(\ell)$ is contained in a Borel subgroup, that is, the elements of $G(\ell)$ can be represented by upper triangular matrices. Note that the diagonal entries of these matrices are given by characters of $G$, which we denote by $\chi'$ and $\chi''$. Thus $G(\ell)$ can be represented by matrices of the form

$$\begin{pmatrix} \chi' & * \\ 0 & \chi'' \end{pmatrix},$$

where $\chi', \chi'' : G \to \mathbb{F}_\ell^*$ are characters of $G$ mapping to $\mathbb{F}_\ell^*$. Since $\mathbb{F}_\ell^*$ is abelian, by the Kronecker-Weber Theorem these characters factor through $\hat{\mathbb{Z}}^* = \mathrm{Gal}(\mathbb{Q}(\zeta_\infty)/\mathbb{Q})$. Further, since the image of these characters is finite, they factor through finite quotients of $\hat{\mathbb{Z}}^*$, and hence can be viewed as Dirichlet characters

$$\chi' : (\mathbb{Z}/f'\mathbb{Z})^* \longrightarrow \mathbb{F}_\ell^* \quad \text{and} \quad \chi'' : (\mathbb{Z}/f''\mathbb{Z})^* \longrightarrow \mathbb{F}_\ell^*$$

where $f'$ and $f''$ are the conductors of $\chi'$ and $\chi''$. Write

$$f' = \prod_p p^{n'(p)} \quad \text{and} \quad f'' = \prod_p p^{n''(p)}.$$

Then

$$(\mathbb{Z}/f'\mathbb{Z})^* \simeq \prod_p (\mathbb{Z}/p^{n'(p)}\mathbb{Z})^* \quad \text{and} \quad (\mathbb{Z}/f''\mathbb{Z})^* \simeq \prod_p (\mathbb{Z}/p^{n''(p)}\mathbb{Z})^*$$

Denote the restriction of $\chi'$ to its $p$-th factor $(\mathbb{Z}/p^{n'(p)}\mathbb{Z})^*$ by $\chi'_p$ and note that since $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})$ is unramified outside $p$, then $\chi'$ maps $I_p$ to

$$\mathbb{Z}_p^* \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$$

hence the diagram

$$\begin{tikzcd}
I_p \arrow[rr, "\chi'|_{I_p}"] \arrow[dr, "\chi'|_{I_p}"'] & & \mathbb{F}_\ell^* \\
& (\mathbb{Z}/p^{n'(p)}\mathbb{Z})^* \arrow[ur, "\chi'_p"'] &
\end{tikzcd}$$

is commutative. We define $\chi''_p$ in the same manner.

Let $p$ be a prime of potential good reduction of $E$, that is, one such that $v_p(j) \geqslant 0$ holds. Let $\mathbb{Q}_p^{nr}$ denote the maximal unramified extension of $\mathbb{Q}_p$, and let $L$ be the smallest extension of $\mathbb{Q}_p^{nr}$ over which $E$ acquires good reduction. Also let $v$ be the normalized valuation on $L$. Then for $\ell \neq p$ we have that $I_v$ acts trivially on $T_\ell(E)$, hence the action of $I_p$ on $T_\ell(E)$ factors through the finite quotient

$$I_p/I_v \simeq \mathrm{Gal}(L/\mathbb{Q}_p^{nr})$$

and this quotient is independent of $\ell$. The following proposition is proved by Serre in [6], §5.6.

**Proposition 2.3.** *Let $\ell \geqslant 5$ and let $p \neq \ell$ be a prime of bad reduction at which $E$ is not semi-stable. Then the images of $\chi'_p$ and $\chi''_p$ in $\mathbb{F}_p^*$ are isomorphic to the group* $\mathrm{Gal}(L/\mathbb{Q}_p^{nr})$.

We are now ready to prove the following

**Theorem 2.4.** *For our curve $E$ we have $G(\ell) = \mathrm{GL}_2(\mathbb{F}_\ell)$ for $\ell \geqslant 5$.*

*Proof.* As we have already seen, for $\ell \geqslant 3$ the image of the inertia group $I_5$ in $G(\ell)$ contains an element of order $\ell$, hence if $G(\ell) \neq \mathrm{GL}_2(\mathbb{F}_\ell)$ holds then $G(\ell)$ is contained in a Borel subgroup. Also, note that we have potential good reduction at 2 , hence $v(\Delta) \equiv 0 \pmod{12}$. Since $v_2(\Delta) = 8$, we must have that $3|\mathrm{Gal}(L/\mathbb{Q}_2^{nr})$. It follows by Proposition 2.3 that if $G(\ell)$ is contained in a Borel subgroup, and if $\ell \geqslant 5$ then $\chi'_2, \chi''_2$ have image in $\mathbb{F}_\ell^*$ of order divisible by 3, a contradiction, since no quotient of $\left(\mathbb{Z}/2^n\mathbb{Z}\right)^*$ has order divisible by 3. This shows that we have $G(\ell) = \mathrm{GL}_2(\mathbb{F}_\ell)$ for $\ell \geqslant 5$. □

**Lemma 2.5.** *Let $\ell \geqslant 5$ and $H$ be a closed subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ for which the reduction mod $\ell$ contains $\mathrm{SL}_2(\mathbb{F}_\ell)$. Then $H$ contains $\mathrm{SL}_2(\mathbb{Z}_\ell)$.*

*Proof.* See [2], Chapter 17, §4. □

**Corollary 2.6.** *For our curve $E$ we have $G_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$ for $\ell \geqslant 5$.*

*Proof.* By Theorem 2.4 we have $G(\ell) = \mathrm{GL}_2(\mathbb{F}_\ell)$, and so by Lemma 2.5 we have $\mathrm{SL}_2(\mathbb{Z}_\ell) \subset G_\ell$. But $\det : G_\ell \to \mathbb{F}_\ell^*$ is surjective, hence the result. □

## 2.2 Computation of $G_\ell$ for $\ell = 2$ and $\ell = 3$

Now we must deal with the exceptional cases $\ell = 2, 3$. In these cases we know that $G(\ell)$ will not be all of $\mathrm{GL}_2(\mathbb{F}_\ell)$, since $E$ has rational 2 and 3-torsion points that are fixed by $G$. The idea for determining $G_\ell$ will be to recover it as the inverse image under the reduction map of $G(\ell^n)$ for some $n$, that is, finding an $n$ such that $\ell^n$ is stable and computing $G(\ell^n)$ for that $n$.

For now we fix a prime $\ell$. By successively adjoining to $\mathbb{Q}$ the $\ell$-power torsion of $E$ we obtain a tower of field extensions $\mathbb{Q} \subset \mathbb{Q}(E[\ell]) \subset \mathbb{Q}(E[\ell^2]) \subset \cdots \subset \mathbb{Q}(E[\ell^\infty])$. Let us look more closely at the different Galois groups that arise in such a tower. Let $M = M_2(\mathbb{Z}_\ell)$ denote the set of all $2 \times 2$ matrices with coefficients in $\mathbb{Z}_\ell$, and let

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

where $\pi_{\ell^n}$ is the reduction map mod $\ell^n$. Also, let

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

Note that we have $G_\ell/U_n \simeq G(\ell^n) = \mathrm{Gal}(\mathbb{Q}(E[\ell^n])/\mathbb{Q})$. We obtain in this manner a filtration $G_\ell \supset U_1 \supset U_2 \supset \cdots \supset \{1\}$. Consider now the map

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

Since mod $\ell^{n+1}$ we have $(I + \ell^n X)(I + \ell^n Y) = I + \ell^n(X + Y)$ with $X, Y \in M_2(\mathbb{F}_\ell)$, this is seen to be a group isomorphism, and $M/\ell M \simeq M_2(\mathbb{F}_\ell)$ is a vector space of dimension 4. From this we see that working in $V_n/V_{n+1}$ is essentially doing linear algebra over a vector space of dimension 4. If we look at the extension $\mathbb{Q}(E[\ell^{n+1}])/\mathbb{Q}(E[\ell^n])$, its Galois group $U_n/U_{n+1}$ is naturally a subspace of $V_n/V_{n+1}$, hence it follows that $[\mathbb{Q}(E[\ell^{n+1}]) : \mathbb{Q}(E[\ell^n])]$ divides $\ell^4$. We will refer to $U_n/U_{n+1}$ as the *vector space associated* to $U_n$. It has dimension at most 4 over $\mathbb{F}_\ell$.

As was already remarked, Theorem 1.1 implies that $G_\ell = \mathrm{GL}_2(\mathbb{Z}_\ell)$ holds for almost all $\ell$. For all such $\ell$ we have $G(\ell^n) = \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ for all $n$, hence the associated vector space to $U_n$ has dimension 4 for all $n$. It could happen however that $G_\ell \subsetneq \mathrm{GL}_2(\mathbb{Z}_\ell)$, for example if $G(\ell) \subsetneq \mathrm{GL}_2(\mathbb{F}_\ell)$. In such cases the following lemma allows us to reduce the problem of determining $G_\ell$ to a finite computation, namely, that of determining the smallest $n$ such that $U_n/U_{n+1}$ has dimension 4. It is separated into two cases depending on whether $\ell$ is even or odd.

**Lemma 2.7.** *(i) Let $\ell \geqslant 3$. With the notation introduced above, suppose that for some $n \geqslant 1$ the vector space associated to $U_n$ has dimension 4. Then we have $U_n = V_n$.*

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

*Proof.* This is essentially the same as Lemma 2 in [4], §6. □

**Remark 2.8.** From $U_n = V_n$ it follows that $G_\ell = \pi_\ell^{-1}(G(\ell^n))$, in other words, $\ell^n$ is stable. Of course we want to find the smallest $n$ for which this holds in order to reduce computations as much as possible.

To use Lemma 2.7 we will need to show that for some $n$, the space $U_n/U_{n+1}$ has dimension 4. It will then suffice to produce four elements $Y_i \in G_\ell$ such that

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

for $1 \leqslant i \leqslant 4$, and such that the $X_i$ are linearly independent mod $\ell$. The way to do this is by means of Frobenius elements at unramified primes, since we know that their characteristic equation looks like

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

and we can compute $t_p$ by counting the $\mathbb{F}_p$-rational points of $\tilde{E}$. This can be done easily using machine computation, and in this manner we can explicitly write down matrices of elements in $G_\ell$, which we can then reduce mod a suitable $\ell^n$.

**Lemma 2.9.** *The group $G(3)$ is of order 6, given explicitly under a suitable basis, by*

$$\left\{ \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \mid a \in \mathbb{F}_3,\ b \in \mathbb{F}_3^* \right\}.$$

*It is isomorphic to $S_3$.*

*Proof.* Since $E$ has a rational 3-torsion point, there is a basis such that the elements of $G(3)$ are matrices of the form

$$\begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \quad a, b \in \mathbb{F}_3$$

so it suffices to determine which values $a$ and $b$ can take. Since $\det : G(3) \to \mathbb{F}_3^*$ is surjective, we know that $b$ must take both of the values $\pm 1$. The 3-division polynomial of $E$ factors over $\mathbb{Q}$ as

$$(x-1)(3x^3 - 5x^2 + 25x + 25)$$

and the splitting field of $3x^3 - 5x^2 + 25x + 25$ has degree 6 over $\mathbb{Q}$, hence $\#G(3) \geqslant 6$ so we conclude $\#G(3) = 6$, proving the Lemma. This last part could also be concluded from Lemma 2.1 since this gives that $G(3)$ has an element of order 3. □

**Theorem 2.10.** *The integer* 3 *is stable, in other words we have* $G_3 = \pi_3^{-1}(G(3))$.

*Proof.* By Lemma 2.7 it suffices to find four elements $Y_i$ in $G_3$ such that

$$Y_i \equiv I + 3X_i \pmod 9$$

for $1 \leqslant i \leqslant 4$, and such that the $X_i$ are linearly independent over $\mathbb{F}_3$. We exhibit these by means of Frobenius elements.

Take $p = 17$. Machine computation gives $\Phi_{17}(X) = X^2 + 6X + 17$. Since

$$\Phi_{17}(X) \equiv (X-7)(X-5) \pmod 9,$$

it follows by Hensel that we can lift these roots to $\mathbb{Z}_3$ and so we can diagonalize $\sigma_{17}$ over $\mathbb{Z}_3$, so for a suitable basis we have

$$\sigma_{17} \equiv \begin{pmatrix} 7 & 0 \\ 0 & 5 \end{pmatrix} \pmod 9.$$

We obtain

$$\sigma_{17}^2 \equiv I + 3\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \pmod 9,$$

which is our first $Y_i$.

Next, take $p = 11$, which has characteristic polynomial

$$\Phi_{11}(X) = X^2 + 11 \equiv (X-4)(X-5) \pmod 9$$

hence $\sigma_{11}$ is diagonalizable. Since

$$4^2 \equiv 5^2 \equiv 7 \pmod 9$$

we have

$$\sigma_{11}^2 \equiv 7I \equiv I + 3 \cdot 2I \pmod 9,$$

hence $\sigma_{11}^2$ is a scalar mod 9 over any basis, in particular the basis we used to diagonalize $\sigma_{17}$. It follows that these two elements are linearly independent in $U_1/U_2$, and they span the diagonal matrices.

For our third element pick $p = 79$. As the 3-division polynomial splits completely mod 79, Frobenius acts trivially on its splitting field, which is the 3-torsion field. It follows that

$$\sigma_{79} = I + 3Z, \qquad Z \in \mathrm{Mat}_2(\mathbb{Z}_3).$$

Plugging this into $\Phi_{79}(X)$, we see that $Z$ satisfies the characteristic equation

$$Z^2 + Z + 2 = 0$$

which is irreducible mod 3, hence $Z$ is not triangular with respect to any basis. Since $\sigma_{17}^2$ and $\sigma_{11}^2$ span the diagonal elements, we can obtain a third element $Y_3$ of the form

$$I + 3\begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix} \qquad x, y \neq 0 \pmod 3,$$

which is linearly independent of the first two. Finally, the space of matrices $Y \pmod 3$ such that $I + 3Y$ belongs to $G_3 \pmod 9$ is invariant under conjugation by $G_3$. Also, we have

$$\begin{pmatrix} 1 & 0 \\ 0 & u \end{pmatrix}\begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & u \end{pmatrix}^{-1} = \begin{pmatrix} 0 & u^{-1}x \\ uy & 0 \end{pmatrix}$$

and all $u \in (\mathbb{Z}/3\mathbb{Z})^*$ arise in elements of $G_3$, hence we can obtain a fourth linearly independent matrix, completing the proof. $\square$

The 2-torsion case is the most complicated, and computing $G_2$ requires considerably more work. The reason for this is that, as we will see, the smallest $n$ for which the vector space associated to $U_n$ has level 4 is $n = 3$, hence it is necessary to compute $G(8)$.

We know $E$ has a rational 2-torsion point, namely $(0, 0)$, hence if we choose a basis for $E[2]$ that includes $P_2 = (0, 0)$, then $G(2)$ can be represented by matrices of the form

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \quad a \in \mathbb{F}_2.$$

The $x$-coordinates of the other two non-zero points in $E[2]$ are given by roots of

$$X^2 - 2X + 5 = 0,$$

which does not have rational roots, hence $a$ can take both values of $\mathbb{F}_2$ and $G(2)$ is cyclic of order 2, namely

$$G(2) \simeq \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\rangle \simeq \{\pm 1\}.$$

The splitting field of $X^2 - 2X + 5$ is $\mathbb{Q}(i)$, hence $\mathbb{Q}(E[2]) = \mathbb{Q}(i)$.

In determining $G(4)$, recall that for every elliptic curve $E/\mathbb{Q}$ the fourth root of unity $i = \zeta_4$ is contained in $\mathbb{Q}(E[4])$, but for our curve $E$ it is already contained in $\mathbb{Q}(E[2])$. We have that the group $G(4)$ acts on $i$ via the determinant and also via its projection on $G(2)$. These actions must be compatible, hence this imposes a restriction on the elements in $G(4)$, which is the reason we don't get all 16 lifts to $G(4)$ of each element of $G(2)$. It follows that we have $[\mathbb{Q}(E[4]) : \mathbb{Q}(E[2])] \leqslant 8$. To see how many lifts there are for each element in $G(2)$, we determine explicitly the field $\mathbb{Q}(E[4])$ using 2-descent, as in [1]. To this end choose a basis for $E[2]$ to consist of

$P_2 = (0,0)$ and $Q_2 = (1+2i, 0)$. Let $E'$ be the curve given by $Y^2 = X(X^2+4X-16)$ and consider the 2-isogeny $\phi : E \to E'$ given by

$$\phi(x,y) = \left(\frac{y^2}{x^2}, y - \frac{5y}{x^2}\right)$$

and its dual isogeny $\hat{\phi} : E' \to E$ given by

$$\hat{\phi}(u,v) = \left(\frac{v^2}{4u^2}, \frac{1}{8}\left(v + \frac{16v}{u^2}\right)\right)$$

so that $\hat{\phi} \circ \phi$ is the multiplication by 2 map. We find points $P_4, Q_4 \in E[4]$ such that $2P_4 = P_2$ and $2Q_4 = Q_2$, hence which form a basis for $E[4]$. Starting with $P_2$, we see that the two points in $E'$ that map to $P_2$ are $(-2 \pm 2\sqrt{5}, 0)$ and the points in $E$ that map to these are $(\pm\sqrt{5}, \pm 2\sqrt{5\epsilon})$, where $\epsilon = (-1+\sqrt{5})/2$. These are the four points of order 4 that map to $P_2$ under multiplication by 2. Since we want to choose a basis for $E[4]$ we pick one of these four points to be our first basis element, so let $P_4 = (\sqrt{5}, 2\sqrt{5\epsilon})$. We do the same thing with $Q_2$. The points in $E'$ that map to $Q_2$ are $(4i, \pm 8i\sqrt{\pi})$ for $\pi = 1+2i$, and the points in $E$ that map to these are $(\pi \pm 2\zeta_8\sqrt{\pi}, 2\zeta_8(\pi \pm 2\zeta_8\sqrt{\pi}))$, where we choose one of these to be our second basis element. We then obtain a basis for $E[4]$ consisting of the two points

$$P_4 = (\sqrt{5}, 2\sqrt{5\epsilon}) \qquad Q_4 = (\pi + 2\zeta_8\sqrt{\pi}, 2\zeta_8(\pi + 2\zeta_8\sqrt{\pi})).$$

Now the 4-division polynomial of our curve $E$ is

$$\psi_4(X) = 2X^6 - 8X^5 + 50X^4 - 250X^2 + 200X - 250$$

which factors over $\mathbb{Q}$ as

$$\psi_4(X) = 2(X^2-5)(X^4 - 4X^3 + 30X^2 - 20X + 25).$$

The roots of the right hand factor are $\pi \pm 2\zeta_8\sqrt{\pi}$ and $\overline{\pi} \pm 2\zeta_8\sqrt{-\overline{\pi}}$. Note then that $\mathbb{Q}(\zeta_8\sqrt{\pi}, \zeta_8\sqrt{-\overline{\pi}})$ is the splitting field of $\psi_4(X)$. We also have that $\zeta_8 \in \mathbb{Q}(E[4])$ and the degree of $\mathbb{Q}(\zeta_8\sqrt{\pi}, \zeta_8\sqrt{-\overline{\pi}}, \zeta_8)$ over $\mathbb{Q}(i)$ is 8 hence we conclude that

$$\mathbb{Q}(E[4]) = \mathbb{Q}(\zeta_8\sqrt{\pi}, \zeta_8\sqrt{-\overline{\pi}}, \zeta_8) = \mathbb{Q}(i, \sqrt{\pi}, \sqrt{\overline{\pi}}, \zeta_8).$$

For general $m$ denote the splitting field of $\psi_m(X)$ by $\mathbb{Q}(E[m]_x)$. If $\mathbb{Q}(E[m]_x)$ contains the square roots of $f(\alpha_i)$, where $\alpha_i$ are the roots of $\psi_m(X)$ and $E$ is given by the equation $Y^2 = f(X)$, then it will equal the full $m$-torsion field $\mathbb{Q}(E[m])$. If this is not the case, then adjoining the square root of $f(\alpha)$ for one root $\alpha$ of $\psi_m(X)$ will give a quadratic extension of $\mathbb{Q}(E[m]_x)$ which will contain the square roots of $f(\alpha_i)$ for all roots $\alpha_i$ of $\psi_m(X)$, hence will be equal to $\mathbb{Q}(E[m])$. We have then that $\mathbb{Q}(E[m])$ is either equal to $\mathbb{Q}(E[m]_x)$ or a quadratic extension of it, and the Galois group $\mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}(E[m]_x))$ equals $G(m) \cap \{\pm I\}$. For our curve we have just seen that $\mathbb{Q}(E[4])$ has degree 2 over $\mathbb{Q}(E[4]_x)$ since $\zeta_8$ is in $\mathbb{Q}(E[4])$ but not in $\mathbb{Q}(E[4]_x)$.

The following figure shows the situation for the 4-torsion.

$$\begin{tikzcd}
 & \mathbb{Q}(E[4]) \arrow[d, dash, "2"'] & & \\
 & \mathbb{Q}(E[4]_x) \arrow[dl, dash, "2"'] \arrow[d, dash, "2"'] \arrow[dr, dash, "2"] & & \\
\mathbb{Q}(\zeta_8\sqrt{\pi}) \arrow[dr, dash, "2"'] & \mathbb{Q}(\zeta_8\sqrt{-\bar{\pi}}) \arrow[d, dash, "2"'] & \mathbb{Q}(i,\sqrt{5}) \arrow[dl, dash, "2"'] \arrow[d, dash, "2"'] \arrow[dr, dash, "2"] & \\
 & \mathbb{Q}(i) \arrow[dr, dash, "2"'] & \mathbb{Q}(\sqrt{-5}) \arrow[d, dash, "2"'] & \mathbb{Q}(\sqrt{5}) \arrow[dl, dash, "2"] \\
 & & \mathbb{Q} &
\end{tikzcd}$$

From the previous remarks on the compatibility of the action of $G(2)$ and $G(4)$ on $i$ we conclude that if we choose as basis $\{P_4, Q_4\}$ then $G(4)$ can be represented by those matrices $X \in \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ which satisfy the following two conditions:

(i) $X \equiv \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \pmod 2$ with $a \in \mathbb{F}_2$.

(ii) $\det X \equiv (-1)^a \pmod 4$.

Next we determine $G(8)$. Here we have a similar situation as with $G(4)$, since as we saw $\zeta_8$ is already contained in $\mathbb{Q}(E[4])$, so again we don't get all possible lifts from elements in $G(4)$, and the degree of $\mathbb{Q}(E[8])$ over $\mathbb{Q}(E[4])$ is at most 8. We have then that there exists a surjective map $\phi_8 : G(4) \twoheadrightarrow (\mathbb{Z}/8\mathbb{Z})^*$. We determine explicitly what this map is. If we denote the $x$ and $y$ coordinates of $Q$ by $x_Q$ and $y_Q$ respectively, then

$$\frac{y_Q}{2x_Q} = \zeta_8,$$

hence the action of en element of $G(4)$ on $\zeta_8$ depends only on its action on the second basis element $Q$. It suffices then to determine where $\phi$ maps matrices of the form

$$\begin{pmatrix} * & b \\ * & d \end{pmatrix}$$

where $b \in \mathbb{Z}/4\mathbb{Z}$ and $d \in (\mathbb{Z}/4\mathbb{Z})^*$.

Since $= \mathbb{Q}(i, \sqrt{\pi}, \sqrt{\bar{\pi}})/\mathbb{Q}$ is a $D_4$ extension and $\mathbb{Q}(i, \sqrt{\pi}, \sqrt{\bar{\pi}}, \zeta_8) = \mathbb{Q}(i, \sqrt{\pi}, \sqrt{\bar{\pi}}, \sqrt{2})$ it follows that

$$G(4) \simeq D_4 \times C_2.$$

Note that $G(4)' = [G(4), G(4)]$ has index 8 in $G(4)$ and

$$G(4)/G(4)' = G(4)^{\mathrm{ab}} = \mathrm{Gal}(\mathbb{Q}(i, \sqrt{2}, \sqrt{5})/\mathbb{Q})$$

is of exponent 2, hence we have $G(4)^2 = G(4)'$. It follows that $G(4)'$ consists of the of elements of $G(4)$ that fix everything that is abelian over $\mathbb{Q}$ and act non-trivially on elements of $\mathbb{Q}(E[4])$ that are not. Let $\sigma$ be the non-trivial element of $G(4)^2$. We see from the explicit coordinates of $P_4$ and $Q_4$ that $\sigma$ has to map $P_4$ to $-P_4$. Also, elements in $G(4)^2$ are of determinant 1 and different from $-I$ by the same argument so we conclude then

$$G(4)^2 = \left\langle \begin{pmatrix} -1 & 2 \\ 0 & -1 \end{pmatrix} \right\rangle.$$

This can also be verified by direct computation. It follows that the matrix

$$A = \begin{pmatrix} -1 & 2 \\ 0 & -1 \end{pmatrix}$$

is in the kernel of $\phi_8$. If $B$ is an element with $d = -1$ then $AB$ will have $d = 1$ and $\phi_8(AB) = \phi_8(A)$, hence $\phi_8$ is completely determined by its action on matrices of the form

$$\begin{pmatrix} * & b \\ * & 1 \end{pmatrix}.$$

Matrices with $b = 0$ fix $Q_4$ and hence map to the identity in $(\mathbb{Z}/8\mathbb{Z})^*$. Matrices with $b = 2$ reduce to the identity mod 2 hence fix $i = \zeta_8^2$ and so map to $5 \in (\mathbb{Z}/8\mathbb{Z})^*$. Matrices with the other two possibilities for $b$ map to the other two elements of $(\mathbb{Z}/8\mathbb{Z})^*$, that is, either $b = 1 \mapsto (\zeta_8 \mapsto \zeta_8^3)$ and $b = 3 \mapsto (\zeta_8 \mapsto \zeta_8^7)$ or $b = 1 \mapsto (\zeta_8 \mapsto \zeta_8^7)$ and $b = 3 \mapsto (\zeta_8 \mapsto \zeta_8^3)$. Which one of these occurs depends on the basis that we choose. Both can occur since one is obtained from the other by the change of basis transformation

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

Elements in $G(8)$ act on $\zeta_8$ via the determinant, and also via their reduction to $G(4)$ with the action we just described. Note that $-I \notin G(8)$ holds, since it has determinant 1 hence would act as the identity on $\zeta_8$. However via reduction mod 4 it would act as $\zeta_8 \mapsto \zeta_8^5$. This implies that $\mathbb{Q}(E[8]) = \mathbb{Q}(E[8]_x)$, so $\mathbb{Q}(E[8])$ is of degree at most 8 over $\mathbb{Q}(E[4])$. Finally, we want to show that $\mathbb{Q}(E[8])$ is of degree exactly 8 over $\mathbb{Q}(E[4])$. Using machine computation we see that $\psi_8(X)$ factors over $\mathbb{Q}$ as

$$\psi_8(X) = \psi_4(X) f_1(X) f_2(X)$$

where $f_1$ is of degree 8 and $f_2$ is of degree 16. Also, $f_2$ factors over $\mathbb{Q}(E[4]_x)$ as $f_2 = g_1 g_2 g_3 g_4$ where each $g_i$ is of degree 4. If $[\mathbb{Q}(E[8]) : \mathbb{Q}(E[4])] < 8$ holds then any root $\alpha$ of $g_i$ would generate $\mathbb{Q}(E[8])$ over $\mathbb{Q}(E[4])$. Using machine computation we see that the prime 89 splits completely in $\mathbb{Q}(E[4])$ and $g_1$ has exactly one root mod 89. This shows that $\mathbb{Q}(E[4])(\alpha)$ is not normal over $\mathbb{Q}$, where $\alpha$ is a root of $g_1$. In particular, it is not equal to $\mathbb{Q}(E[8])$. We conclude that $\mathbb{Q}(E[8])$ is of degree 8 over $\mathbb{Q}(E[4])$ and so $G(8)$ is the subgroup of elements $X$ in $\mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$ that satisfy

(i) $(X \bmod 4) \in G(4)$.

(ii) $\det X = \phi(X \bmod 4) \in (\mathbb{Z}/8\mathbb{Z})^*$

where $\phi$ is the map from $G(4)$ to $(\mathbb{Z}/8\mathbb{Z})^*$. The following theorem will tell us that one can recover the full group $G_2$ from its reduction mod 8.

**Theorem 2.11.** *The integer 8 is stable, that is, $G_2 = \pi_2^{-1}(G(8))$.*

*Proof.* We proceed exactly as we did in showing the stability of $\ell = 3$. Again using Lemma 2.7 we must exhibit four elements $Y_i$ in $G_2$ such that

$$Y_i \equiv I + 8X_i \pmod{16}$$

for $1 \leqslant i \leqslant 4$, and such that the $X_i$ are linearly independent over $\mathbb{F}_2$. For $p = 19$, the Frobenius element $\sigma_{19}$ has characteristic polynomial

$$\Phi_{19}(X) = X^2 + 4X + 19$$

which has distinct roots in $\mathbb{Z}_2$ since its discriminant is $4^2 - 4 \cdot 19 = 4(-15)$ and $-15 \equiv 1 \pmod 8$, hence the discriminant is a square in $\mathbb{Z}_2$. It follows that we can diagonalize $\sigma_{19}$ over $\mathbb{Z}_2$ and reducing mod 16 gives that for a certain choice of basis we have

$$\sigma_{19} \equiv \begin{pmatrix} 5 & 0 \\ 0 & 7 \end{pmatrix} \pmod{16}.$$

We then obtain

$$\sigma_{19}^2 \equiv \begin{pmatrix} 9 & 0 \\ 0 & 1 \end{pmatrix} \equiv I + 8\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \pmod{16}.$$

Next we take $p = 79$ with characteristic polynomial

$$\Phi_{79}(X) = X^2 - 8X + 79 \equiv (X-3)(X-5) \pmod{16}.$$

The discriminant of $\Phi_{79}(X)$ is $4(-63)$ so $\Phi_{79}$ is diagonalizable over $\mathbb{Z}_2$ and we obtain that

$$\sigma_{79} \equiv \begin{pmatrix} 3 & 0 \\ 0 & 5 \end{pmatrix} \pmod{16}$$

hence

$$\sigma_{79}^2 \equiv 9I \equiv I + 8I \pmod{16},$$

which is a scalar matrix with respect to any basis, hence we obtain an element linearly independent from the first one, and these two elements span the diagonal matrices.

Now take $p = 2441$. Since $\psi_8(X)$ splits completely mod 2441, we can write

$$\sigma_{2441} = I + 8Z \quad Z \in \mathrm{Mat}_2(\mathbb{Z}_2)$$

and plugging this into the characteristic equation gives

$$Z^2 + 7Z + 39 = 0$$

which is irreducible over $\mathbb{Z}_2$, hence $Z$ is not diagonalizable over any basis. This implies we obtain a third element of the form

$$I + 8\begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix} \qquad x, y \neq 0 \pmod 2.$$

Finally, we obtain the fourth linearly independent element by conjugating

$$\begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix} \quad \text{by} \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

and this completes the proof. □

## 2.3 Computation of a split and stable $m$

Now that we have computed $G_\ell$ for all $\ell$, we would like to split $\rho$ at some integer $m$, so as to reduce the problem to computing $G_m$. We would expect such an $m$ to be divisible by at least the primes 2, 3 and 5, since at $\ell \in \{2, 3\}$ we don't get all of $\mathrm{GL}_2(\mathbb{Z}_\ell)$, and the 5-power torsion field is not independent of the 2-power torsion field, as they both contain $\sqrt{5}$. We will see in what follows that these three primes already split $\rho$.

Let $M$ be an integer and $L$ the set of primes $\ell$ such that $\ell \nmid M$. Let $G_L$ denote the image of the representation

$$\rho_L : G \longrightarrow \prod_{\ell \in L} \mathrm{GL}_2(\mathbb{Z}_\ell).$$

Then by definition $\rho(G)$ is a subgroup of $G_M \times G_L$ whose projections on the two factors are surjective. The following lemma of Goursat will prove to be very useful in determining the image $\rho(G)$.

**Lemma 2.12** (Goursat's lemma). *Let $G_1$ and $G_2$ be groups and let $G$ be a subgroup of $G_1 \times G_2$ such that the two projections $p_1 : G \to G_1$ and $p_2 : G \to G_2$ are surjective. Let $N_1$ be the kernel of $p_2$ and $N_2$ be the kernel of $p_1$. We can identify $N_1$ as a normal subgroup of $G_1$ and $N_2$ as a normal subgroup of $G_2$. Then there is an isomorphism*

$$\varphi : G_1/N_1 \longrightarrow G_2/N_2$$

*such that*

$$G = \{(a, b) \in G_1 \times G_2 \mid \varphi(aN_1) = bN_2\}.$$

We refer to the normal subgroups $N_1$ and $N_2$ in the Goursat's Lemma as *Goursat subgroups*. It follows from Goursat's lemma that for a given integer $M$, determining $\rho(G) \leqslant G_M \times G_L$ can be achieved by determining the possible Goursat subgroups of $G_M$ and $G_L$, or what is equivalent, the possible isomorphisms from a quotient of $G_M$ with a quotient of $G_L$. Note that $G$ is the full product $G_1 \times G_2$ if and only if $N_1 = G_1$ and $N_2 = G_2$ hold. We see then that $M$ splits $\rho$ if $N_M = G_M$ and

$$G_L = \prod_{\ell \in L} \mathrm{GL}_2(\mathbb{Z}_\ell).$$

In determining possible isomorphisms of finite quotients of two groups we naturally encounter *Jordan-Hölder constituents*. We will say that a prime *occurs* in a group if it divides the order of some solvable Jordan-Hölder constituent.

**Theorem 2.13.** *Let $m$ be divisible by 2, 3 and all primes of bad reduction of an elliptic curve $E/\mathbb{Q}$. Suppose also that:*

*(i) $G(\ell) = \mathrm{GL}_2(\mathbb{F}_\ell)$ for all $\ell \nmid m$.*

*(ii) If $\ell \nmid m$ then $\ell$ does not occur in $G_m$.*

*Then $m$ splits $\rho$.*

*Proof.* See [4], §6. □

**Corollary 2.14.** *The integer 30 splits $\rho$, that is,*

$$\rho(G) = G_{30} \times \prod_{\ell \geqslant 5} \mathrm{GL}_2(\mathbb{Z}_\ell).$$

*Proof.* We certainly have that $G(\ell) = \mathrm{GL}_2(\mathbb{F}_\ell)$ for $\ell > 5$. Also, the only prime that occurs in $G_2$ is 2, the primes that occur in $G_3$ are 2 and 3, and the primes that occur in $G_5$ are 2 and 5, hence these are the only primes that occur in $G_{30}$ and the conclusion follows from Theorem 2.13. □

We are left then with determining $G_{30}$. To do this we proceed in two steps. The first step will be to determine $G_{10}$, which is the Galois group of the 10-power torsion field, that is $K_{10}$, which is the composite of the fields $K_2$ and $K_5$. By Goursat's lemma we have that

$$G_{10} = \{(\sigma, \tau) \mid \sigma|_{K_2 \cap K_5} = \tau|_{K_2 \cap K_5}\} \subset G_2 \times G_5$$

so determining $G_{10}$ amounts to determining $K_2 \cap K_5$.

Let $N_2$ and $N_5$ be the corresponding Goursat subgroups, so that

$$G_2/N_2 \simeq G_5/N_5.$$

Let $U = \mathrm{Gal}(K_5/\mathbb{Q}(E[5]))$ and map $U$ to $G_2/N_2$ via

$$U \longrightarrow G_5/N_5 \xrightarrow{\sim} G_2/N_2.$$

Since $G_2$ is a pro-2 group and $U$ is a pro-5 group it follows that $U$ must map to the identity in $G_2/N_2$ hence also in $G_5/N_5$, so we have $U \subset N_5$. This implies that $K_2 \cap K_5 \subset \mathbb{Q}(E[5])$, so it suffices to find the intersection of $K_2$ with $\mathbb{Q}(E[5])$.

**Lemma 2.15.** *$\mathbb{Q}(\zeta_5) \subset K_2 \cap K_5$.*

*Proof.* It suffices to show that $\zeta_5 \in \mathbb{Q}(E[8])$. We have the following field inclusions:

$$\begin{tikzcd}
 & \mathbb{Q}(\zeta_{20}) \arrow[dl, dash, "2"'] \arrow[d, dash, "2"'] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(i, \sqrt{5}) \arrow[dr, dash, "2"'] & \mathbb{Q}(\zeta_{20} + \zeta_{20}^{-1}) \arrow[d, dash, "2"'] & \mathbb{Q}(\zeta_5) \arrow[dl, dash, "2"] \\
 & \mathbb{Q}(\sqrt{5}) &
\end{tikzcd}$$

The minimal polynomial of $\zeta_{20} + \zeta_{20}^{-1}$ over $\mathbb{Q}$ is $X^4 - 5X^2 + 5$ which has roots

$$\pm\sqrt{\frac{5 \pm \sqrt{5}}{2}}$$

which all lie in $\mathbb{Q}(\zeta_{20} + \zeta_{20}^{-1})$ since it is Galois over $\mathbb{Q}$.

On the other hand, we have already seen using 2-descent that

$$P_4 = (\sqrt{5}, 2\sqrt{5\epsilon}) \in E[4]. \tag{1}$$

Both coordinates of $P_4$ lie in $\mathbb{Q}(E[4])$ hence in $\mathbb{Q}(E[8])$. Using 2-descent again, we find that $\sqrt[4]{5}$ lies in $\mathbb{Q}(E[8])$, hence so does

$$2\sqrt[4]{5}\sqrt{5\epsilon} = 2\sqrt{5}\sqrt{\frac{5 - \sqrt{5}}{2}}$$

Since $i \in \mathbb{Q}(E[8])$ we conclude that

$$\mathbb{Q}(\zeta_{20}) = \mathbb{Q}\left(i, \sqrt{\frac{5 - \sqrt{5}}{2}}\right) \subset \mathbb{Q}(E[8])$$

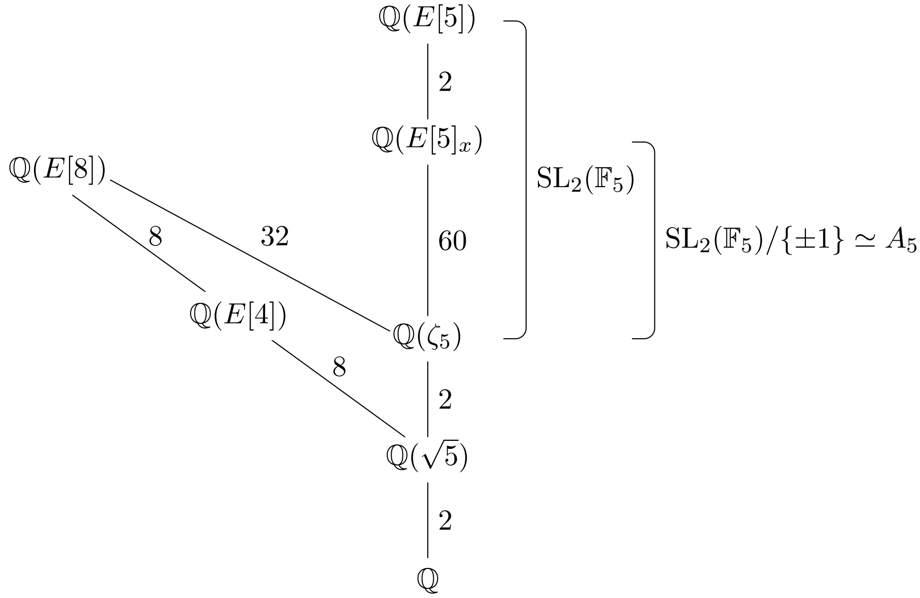
so $\zeta_5 \in \mathbb{Q}(E[8])$, as desired. $\square$

Using this lemma we are now ready to prove

**Theorem 2.16.** *$K_2 \cap K_5 = \mathbb{Q}(\zeta_5)$ and*

$$G_{10} = \{(\sigma, \tau) \mid \sigma(\zeta_5) = \tau(\zeta_5)\} \subset G_2 \times G_5.$$

*Proof.* By the previous lemma and the remarks preceding it we have the following lattice of subfields:




Let $L = K_2 \cap \mathbb{Q}(E[5])$ and suppose the inclusion $\mathbb{Q}(\zeta_5) \subset L$ is strict. Since $L$ is Galois over $\mathbb{Q}(\zeta_5)$, it follows that $L \not\subset \mathbb{Q}(E[5]_x)$, for if it were it would correspond to a non-trivial normal subgroup of

$$\mathrm{Gal}(\mathbb{Q}(E[5]_x)/\mathbb{Q}(\zeta_5) \simeq A_5$$

contradicting the simplicity of $A_5$. Since every finite subfield of $K_2$ is of degree a power of 2 and $L$ is not contained in $\mathbb{Q}(E[5]_x)$, it must be that $L$ is quadratic over $\mathbb{Q}(\zeta_5)$, and so

$$\mathrm{SL}_2(\mathbb{F}_5) \simeq \mathrm{Gal}(\mathbb{Q}(E[5])/\mathbb{Q}(\zeta_5)) \simeq A_5 \times \{\pm 1\}$$

which is not true. This contradiction shows that $L = \mathbb{Q}(\zeta_5)$. The fact that

$$G_{10} = \{(\sigma, \tau) \mid \sigma(\zeta_5) = \tau(\zeta_5)\} \subset G_2 \times G_5$$

is an immediate consequence, proving the theorem. $\square$

To find $G_{30}$ we again use Goursat, since $G_{30} \subset G_3 \times G_{10}$.

**Theorem 2.17.** *$K_3 \cap K_{10} = \mathbb{Q}$ and $G_{30} = G_3 \times G_{10}$.*

*Proof.* Again let $N_3$ and $N_{10}$ denote the corresponding Goursat subgroups. We know $K_3$ has a unique quadratic subfield, which is $\mathbb{Q}(\zeta_3)$. Note that this subfield is not contained in $K_3 \cap K_{10}$, since 3 ramifies in $\mathbb{Q}(\zeta_3)$ and $K_{10}$ is unramified outside 2 and 5. From this it follows that $G_3/N_3$ is a 3-group. Let $U = \mathrm{Gal}(K_{10}/\mathbb{Q}(E[5]))$, and map $U$ to $G_3/N_3$ via

$$U \longrightarrow G_{10}/N_{10} \xrightarrow{\sim} G_3/N_3.$$

Since $G_2$ is a pro-2 group and $\mathrm{Gal}(K_5/\mathbb{Q}(E[5]))$ is a pro-5 group, any finite quotient of $U$ has order of the form $2^\alpha 5^\beta$, hence $U$ must map to the identity in $G_3/N_3$, from which $U \subset N_{10}$ follows.

Let $L = K_3 \cap K_{10} = K_3 \cap \mathbb{Q}(E[5])$ and let $N$ be the normal subgroup of $\mathrm{GL}_2(\mathbb{F}_5)$ corresponding to $L$. As we previously saw, the field $L$ must be a 3-power extension of $\mathbb{Q}$, hence

$$\#\mathrm{GL}_2(\mathbb{F}_5)/N = 3^k,$$

The Jordan-Hölder constituents of $\mathrm{GL}_2(\mathbb{F}_5)$ are $C_2, C_2, A_5, C_2$, and $A_5$ is the only group from this list that has order divisible by 3, however it is simple and different from $C_3$, so it follows that no quotient of $\mathrm{GL}_2(\mathbb{F}_5)$ has order a power of 3, so we must have $N = \mathrm{GL}_2(\mathbb{F}_5)$ and the conclusion follows. $\square$

Now that we know $G_{30}$, we know the complete Galois representation of our curve $E$. We summarize the results of this section in the following theorem.

**Theorem 2.18.** *The integer $m = 120 = 2^3 \cdot 3 \cdot 5$ splits and stabilizes $\rho$, and we have*

$$\rho(G) = G_{30} \times \prod_{\ell \geqslant 5} \mathrm{GL}_2(\mathbb{Z}_\ell),$$

*where $G_{30} = G_{120} = \pi^{-1}(G(120))$ with*

$$G(120) = \{(\sigma_8, \sigma_3, \sigma_5) \in G(8) \times G(3) \times G(5) \mid \sigma_8(\zeta_5) = \sigma_5(\zeta_5)\}.$$

*The index of $\rho(G)$ in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ equals 384.*

# 3 Congruence conditions on the supersingular primes of $Y^2 = (X+1)(X^2+4)$

We conclude by using the now known complete Galois representation of our curve $E$ to determine congruence conditions on its supersingular primes. We will see that something even stronger holds, namely, we find congruence relations between the trace of Frobenius $t_p$ and $p$ modulo primes dividing $m$.

The complete Galois representation of $E$ tells us that for the primes 2, 3 and 5 there are certain restrictions on the matrices one can get. The 3-power torsion field is independent of the 10-power torsion field, however there are still restrictions since as we have seen we do not obtain all of $\mathrm{GL}_2(\mathbb{Z}_3)$. With the 2-power torsion field there are restrictions coming from the fact that we do not obtain all of $\mathrm{GL}_2(\mathbb{Z}_2)$, and additional restrictions coming from the intersection of the 2-power torsion field with the 5-tower torsion field. We will see how these restrictions imply congruence relations between $t_p$ and $p$ for unramified primes $p$, modulo 2, 3 and 5.

We start with the prime 3 as this gives the simplest relations.

**Proposition 3.1.** *Let $p > 5$ be a prime. Then we have $t_p \equiv 1 + p \pmod 3$.*

*Proof.* Let $\sigma_p$ be the Frobenius element at $p$. Then by Lemma 2.9 and theorem 2.10 we have that

$$\rho_3(\sigma_p) \equiv \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix} \pmod 3$$

hence

$$\begin{aligned} 1 + b &\equiv t_p \pmod 3 \\ b &\equiv p \pmod 3 \end{aligned}$$

from where $t_p \equiv 1 + p \pmod 3$ follows. □

**Remark 3.2.** The previous proposition is also immediate from the fact that $E$ has a rational 3-torsion point, hence we have

$$p + 1 - t_p \equiv \#\tilde{E}(\mathbb{F}_p) \equiv 0 \pmod 3.$$

The congruence conditions that we will now derive are however more subtle.

**Theorem 3.3.** *Let $p > 5$ be a prime. Then $t_p \equiv 0 \pmod 8$ implies $p \equiv -1$ or $11 \pmod{40}$.*

*Proof.* Let $\sigma_p$ be the Frobenius element at $p$ and suppose that $t_p \equiv 0 \pmod 8$. Then as we have seen we have

$$\rho_2(\sigma_p) \equiv \begin{pmatrix} a & b \\ c & d \end{pmatrix} \pmod 4$$

where

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \pmod 2$$

and $p \equiv ad - bc \equiv (-1)^x \pmod 4$. Since $t_p \equiv 0$ holds, we have $a + d \equiv 0 \pmod 4$ and so

$$-d^2 - bc \equiv p \pmod 4.$$

Suppose $x = 0$, that is, $p \equiv 1 \pmod 4$. Then $b \equiv 0$ or 2, hence $bc \equiv 0 \pmod 4$ and so

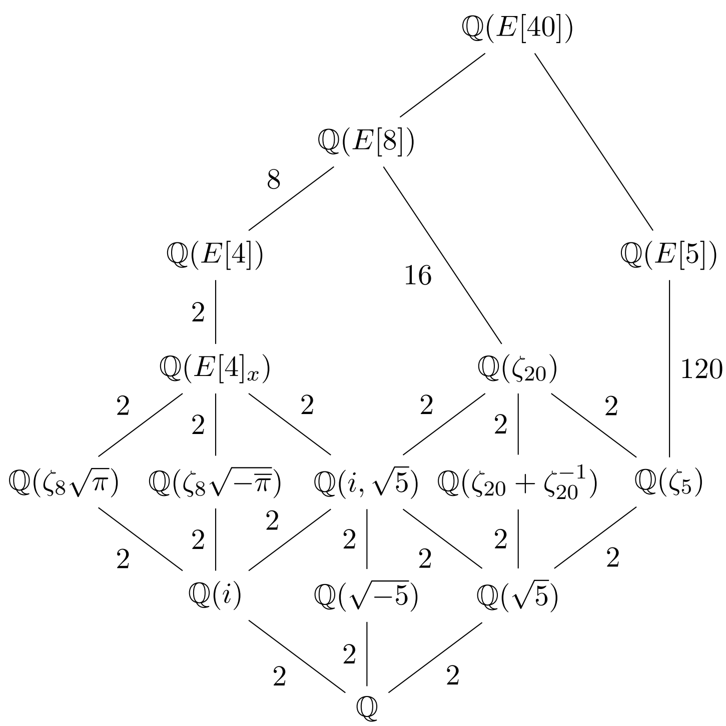
$$-d^2 \equiv 1 \pmod 4,$$

a contradiction, hence $p \equiv -1 \pmod 4$.

Since $p \equiv -1 \pmod 4$, it follows that $\rho_2(\sigma_p)$ does not act trivially on $\mathbb{Q}(i) = \mathbb{Q}(E[2])$, hence $\tilde{E}$ does not have full 2-torsion over $\mathbb{F}_p$, in fact $\tilde{E}(\mathbb{F}_p)[2^\infty]$ is cyclic, where $\tilde{E}(\mathbb{F}_p)[2^\infty]$ denotes the subgroup of all $\mathbb{F}_p$-rational points having order a power of 2. We do have however that

$$\#\tilde{E}(\mathbb{F}_p) = p + 1 - t_p \equiv 0 \pmod 4$$

so $\tilde{E}$ must have an point of order 4 over $\mathbb{F}_p$. Let's look at the lattice of subfields arising from the 2-power and 5-power torsion.




Let $\overline{P_0}$ be a point of order 4 over $\mathbb{F}_p$. Then there is a point $P_0$ of order 4 over an extension $K$ of $\mathbb{Q}$ such that $P_0$ maps to $\overline{P_0}$ under the reduction map $E \to \tilde{E} = (E \bmod \mathfrak{p})$, where $\mathfrak{p} \subset K$ is a prime of good reduction above $p$. It follows that $\overline{P_0}$ is defined over $\mathbb{F}_p$ precisely when the Frobenius element at $\mathfrak{p}$ acts trivially on $K$.

It follows that one of $\zeta_8\sqrt{-\pi}$, $\zeta_8\sqrt{\pi}$, $\sqrt{5}$ is defined over $\mathbb{F}_p$, hence $\rho_2(\sigma_p)$ acts trivially on one of $\mathbb{Q}(\zeta_8\sqrt{-\pi}), \mathbb{Q}(\zeta_8\sqrt{\pi}), \mathbb{Q}(\sqrt{5})$. Since $p \equiv -1 \pmod 4$ holds, $\rho_2(\sigma_p)(i) = -i$ follows and hence it must be $\sqrt{5}$ defined over $\mathbb{F}_p$ and it is the $x$-coordinate of the $\mathbb{F}_p$-rational point of order 4. It follows that $\sigma_p$ acts trivially on $\mathbb{Q}(\sqrt{5})$, and since $\rho_5(\sigma_p)$ acts on $\mathbb{Q}(\zeta_5)$ via its determinant, it follows that

$$p = \det \rho_5(\sigma_p) \equiv \pm 1 \pmod 5.$$

So far we have shown that $t_p \equiv 0 \pmod 8$ implies $p \equiv -1 \pmod 4$ and $p \equiv \pm 1 \pmod 5$. We now see what happens mod 8. Since $p$ is $-1$ mod 4 it is either 3 or $-1$ mod 8. We show that

$$p \equiv -1 \pmod 8 \Longrightarrow p \equiv -1 \pmod 5.$$

Suppose then that that $8|p+1$. Note then that $8|\#\tilde{E}(\mathbb{F}_p)$. Since $\tilde{E}(\mathbb{F}_p)[2^\infty]$ is cyclic, it follows that $\tilde{E}$ must also have an $\mathbb{F}_p$-rational point $\overline{P_8}$ of order 8. If we denote by $\overline{P_4}$ the torsion point of order 4 over $\mathbb{F}_p$, then $\overline{P_8}$ must satisfy that $2\overline{P_8} = \overline{P_4}$. By computing $P_8$ from $P_4$ using 2-descent, it follows from (1), §2.3, that we have $\mathbb{Q}(\zeta_{20} + \zeta_{20}^{-1}) = \mathbb{Q}(\beta)$, where $\beta$ is the $x$-coordinate of $P_8$.

We conclude then that $\rho_2(\sigma_p)$ acts trivially on $\mathbb{Q}(\zeta_{20} + \zeta_{20}^{-1})$, so it cannot act trivially on $\mathbb{Q}(\zeta_5)$, for if it did it would also act trivially on $\mathbb{Q}(i)$, which is not the case. Since $\rho_5(\sigma_p)$ acts on $\zeta_5$ via its determinant and it does not fix $\zeta_5$, we conclude $p \equiv -1 \pmod 5$.

Finally suppose $p \equiv 3 \pmod 8$. This implies that $\tilde{E}$ does not have a rational point of order 8, hence $\rho_2(\sigma_p)$ does not fix $\mathbb{Q}(\zeta_{20} + \zeta_{20}^{-1})$. We know it also does not fix $\mathbb{Q}(i, \sqrt{5})$, which means that $p$ does not split completely in either of these two fields. This tells us that $p$ is inert going from $\mathbb{Q}(\sqrt{5})$ to $\mathbb{Q}(i, \sqrt{5})$ and also going from $\mathbb{Q}(\sqrt{5})$ to $\mathbb{Q}(\zeta_{20} + \zeta_{20}^{-1})$. However, since $\mathbb{Q}(\zeta_{20})/\mathbb{Q}(\sqrt{5})$ is a $V_4$ extension and $p$ is unramified, this implies that $p$ splits in $\mathbb{Q}(\zeta_5)$, hence $p \equiv 1 \pmod 5$. This concludes the proof of the theorem. □

We are now ready to answer the question posed at the beginning of this thesis.

**Corollary 3.4.** *Let $p > 5$ be a supersingular prime of the curve*

$$E : Y^2 = X(X^2 - 2X + 5).$$

*Then $p \equiv -1$ or $11 \pmod{120}$.*

*Proof.* If $p$ is supersingular, then $t_p = 0$, hence $t_p$ is 0 mod 3 and mod 8. The result then follows by putting together the congruence conditions obtained in Proposition 3.1 and Theorem 3.3. □

## References


[1] J.W.S. Cassels. *Lectures on Elliptic Curves.* Cambridge University Press, 1991.

[2] S. Lang. *Elliptic Functions.* Springer, 1973.

[3] S. Lang. *Algebra.* Springer, 2002.

[4] S. Lang and H. Trotter. *Frobenius Distributions in* $\mathrm{GL}_2$*-Extensions.* Springer, 1974.

[5] J.-P Serre. *Abelian $\ell$-adic representations and elliptic curves.* Benjamin, 1968.

[6] J.-P Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Inventiones mathematicae*, 15:259–331, 1972.

[7] J.-P Serre and J. Tate. Good reduction of abelian varieties. *Annals of Mathematics*, 88:492–517, 1968.

[8] J. Silverman. *The Arithmetic of Elliptic Curves.* Springer, 1986.