Mathematical Research Letters **6**, 735–754 (1999)

PAIRS OF MOD 3 AND MOD 5 REPRESENTATIONS ARISING FROM ELLIPTIC CURVES

J. Manoharmayum*

Abstract. For an elliptic curve E_0 over $\mathbb{Q}$, we study the mod 3 representations, restricted to a decomposition group at 3, of elliptic curves over $\mathbb{Q}$ whose mod 5 representations are equivalent to the mod 5 representation given by E_0. Complete lists are obtained describing the mod 3 representations up to equivalence and twist by the quadratic unramified character of $\mathbb{Q}_3$.

1. Introduction

Let E_0 be an elliptic curve over $\mathbb{Q}$ and let $\overline{\rho}_{E_0,5} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(E_0[5]) \simeq GL_2(\mathbb{F}_5)$ be the representation obtained from the 5-division points. We want to describe representations $\overline{\rho}_{E,3}$ restricted to a decomposition group at 3, up to equivalence, that can arise as we vary over elliptic curves E, defined over $\mathbb{Q}$, with the property that $\overline{\rho}_{E_0,5} \sim \overline{\rho}_{E,5}$.

We first show that the problem is purely local (see Theorem A in section 2). More precisely, suppose we are given an elliptic curve E' over $\mathbb{Q}_3$ such that $\overline{\rho}_{E_0,5}|_{D_3} \sim \overline{\rho}_{E',5}$, where D_3 is a decomposition group at the prime 3. We then show that there is an elliptic curve E over $\mathbb{Q}$ such that $\overline{\rho}_{E_0,5} \sim \overline{\rho}_{E,5}$ and $\overline{\rho}_{E,3}|_{D_3} \sim \overline{\rho}_{E',3}$.

We can thus reduce our problem to looking at elliptic curves over $\mathbb{Q}_3$ with equivalent mod 5 representations and then describing the possible mod 3 representations of $\mathrm{Gal}(\overline{\mathbb{Q}}_3/\mathbb{Q}_3)$ that can arise, up to equivalence. Furthermore, if ρ_1 and ρ_2 are two $GL_2(\mathbb{F}_3)$ representations of $\mathrm{Gal}(\overline{\mathbb{Q}}_3/\mathbb{Q}_3)$ with determinant cyclotomic and whose restrictions to inertia are equivalent, then they are equivalent up to twist by the unique quadratic unramified character (see section 3). Hence for the purpose of describing the representations we seek, up to twist by the quadratic unramified character of $\mathbb{Q}_3$, we need only describe restrictions to the inertia subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}_3/\mathbb{Q}_3)$ — which, computationally, is easier to handle. These — the complete lists of mod 3 representations that occur — are worked out explicitly in section 5.

The motivation behind these calculations is the Shimura-Taniyama-Weil conjecture, and the work of C. Breuil, B. Conrad, F. Diamond and R. Taylor on the conjecture (as yet unpublished). To describe this a bit further, recall that

Received December 14, 1998. Revised November 23, 1999.
*Supported by an IGS, Trinity College, Cambridge.

one can show the modularity of an elliptic curve E, defined over $\mathbb{Q}$, by showing that the ℓ-adic representation $\rho_{E,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_2(\mathbb{Z}_\ell)$ is modular for some prime ℓ. The basic idea, due to Wiles, is that the modularity of $\rho_{E,\ell}$, under certain conditions, can be deduced from the modularity of $\overline{\rho}_{E,\ell}$. One then takes ℓ to be 3, since it is known that $\overline{\rho}_{E,3}$ is modular. The work of Wiles ([Wi], completed in [T-W]) shows the modularity of elliptic curves with semi-stable reduction. The results in [Wi] and [T-W] were further extended in [Dia], showing the Shimura-Taniyama-Weil conjecture for elliptic curves with semi-stable reduction at 3 and 5. In [CDT], the conjecture is established for elliptic curves with 3^3 not dividing the conductor. Further, it is shown in [CDT] that if E is a modular elliptic curve, then any elliptic curve over $\mathbb{Q}$ whose mod 5 representation is equivalent to $\overline{\rho}_{E,5}$ is modular. We can thus hope to establish modularity of a given elliptic curve by choosing an elliptic curve with equivalent mod 5 representation and which has a 'reasonably nice' mod 3 representation. It thus becomes important to understand the mod 3 representation restricted to a decomposition group at 3.

The principal results in this article are then the descriptions of the mod 3 representations for the cases when the mod 5 representation has wild ramification at the prime 3 (see the last two subsections in section 5). Although not stated explicitly, we list elliptic curves over $\mathbb{Q}_3$ with prescribed mod 3 and mod 5 representations, up to twist by the quadratic unramified character of $\mathbb{Q}_3$ — which is quite useful when studying deformations of certain $GL_2(\mathbb{F}_3)$ Galois representations.

I would like to thank R. Taylor for suggesting the problem; B. Conrad and F. Diamond for their comments. Also thanks to the referee for his detailed comments and corrections.

2. Reduction to the local case

Fix embeddings of $\overline{\mathbb{Q}}$ in $\mathbb{C}$ and in $\overline{\mathbb{Q}}_p$ for each prime p, and corresponding identifications of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ with D_p — a decomposition group at p. We can now write down precisely what we mean by reduction to the local case.

Theorem A. *Let M, N be positive coprime integers with $M = 3$ or 5. Suppose E_0 is a given elliptic curve over $\mathbb{Q}$. Let Σ be a finite set of (finite) primes, and assume that for each $p \in \Sigma$, we are given an elliptic curve $E_{(p)}$ over $\mathbb{Q}_p$ such that $\overline{\rho}_{E_{(p)},M} \sim \overline{\rho}_{E_0,M}|_{D_p}$. Further, assume that $\overline{\rho}_{E_0,M}|_{D_p}$ is reducible and decomposable for all but at most one prime in Σ.*

Then there are infinitely many elliptic curves E over $\mathbb{Q}$ satisfying

a) $\overline{\rho}_{E,M} \sim \overline{\rho}_{E_0,M}$,
b) $\overline{\rho}_{E,N}|_{D_p} \sim \overline{\rho}_{E_{(p)},N}$ for any $p \in \Sigma$, and
c) $\overline{\rho}_{E,N} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_2(\mathbb{Z}/N\mathbb{Z})$ is surjective.

We prove the above result at the end of this section. The case we are interested in is a direct consequence of Theorem A, and is stated below:

Corollary. Let E_0 be an elliptic curve over $\mathbb{Q}$, and let E' be an elliptic curve over $\mathbb{Q}_3$ such that $\overline{\rho}_{E_0,5}|_{D_3} \sim \overline{\rho}_{E',5}$. Then there are infinitely many elliptic curves E, defined over $\mathbb{Q}$, such that

- $\overline{\rho}_{E,5} \sim \overline{\rho}_{E_0,5}$,
- $\overline{\rho}_{E,3}|_{D_3} \sim \overline{\rho}_{E',3}$, and
- $\overline{\rho}_{E,3} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_2(\mathbb{F}_3)$ is surjective.

2.1. Tate curves. We begin by recalling some properties of potentially multiplicative elliptic curves over a p-adic local field. All of these and more can be found in [Se1], [Sil2]. We fix K a finite extension of $\mathbb{Q}_p$, and write v for the normalised discrete valuation of K (that is, a uniformizer has valuation 1).

Let $q \in K,\ v(q) > 0$. There is then an elliptic curve E_q, called the Tate curve, defined over K, such that $E_q(\overline{K}) \cong \overline{K}^{\times}/q^{\mathbb{Z}}$. The isomorphism is compatible with the action of $\mathrm{Gal}(\overline{K}/K)$. For a Tate curve $E_q,\ v(q) > 0$, the mod N representation then has the following description:

$$\overline{\rho}_{E_q,N} \sim \begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix},$$

where χ is the cyclotomic character modulo N. The representation $\overline{\rho}_{E_q,N}$ splits if and only if q is a perfect N-th power in K.

Suppose now that E is an elliptic curve over K. Then E has potentially multiplicative reduction if and only if $v(j(E)) < 0$. Given such an E there is then a unique $q \in K,\ v(q) > 0$, such that E is isomorphic to the Tate curve E_q over $\overline{K}$. In fact the isomorphism can be realized over at most a quadratic extension of K. If E has multiplicative reduction, then E is isomorphic to E_q over at most the quadratic unramified extension of K. Further, in this case, E is isomorphic to E_q over K if and only if E has split multiplicative reduction.

If E does not have multiplicative reduction over K, then the isomorphism has to be over a quadratic ramified extension of K. Thus $\overline{\rho}_{E,N}$ is then a twist by a ramified quadratic character of $\overline{\rho}_{E_q,N}$.

2.2. Twists of modular curves. We assume throughout that all our schemes are defined over $\mathbb{Q}$.

Let n be an integer greater than or equal to 3, and let $\mathcal{V}$ be a free $\mathbb{Z}/n\mathbb{Z}$-module scheme of rank 2 together with a non-degenerate, alternating pairing $\mathcal{V} \times \mathcal{V} \longrightarrow \boldsymbol{\mu}_n$.

Let us define an *elliptic curve with level $\mathcal{V}$ structure* to be a pair $(E_{/S}, \alpha)$ where $E_{/S}$ is an elliptic curve and $\alpha : \mathcal{V} \longrightarrow E[n]$ is an isomorphism of symplectic spaces. It is well-known that such a pair has no non-trivial automorphism and so the fine moduli space classifying elliptic curves with level $\mathcal{V}$ structure exists. In particular, there is a universal elliptic curve with level $\mathcal{V}$ structure. We denote the fine moduli space by $Y(\mathcal{V})$. The completion of $Y(\mathcal{V})$, denoted by $X(\mathcal{V})$, is a geometrically irreducible (a consequence of the pairing on $\mathcal{V}$ being fixed), smooth, projective curve. The genus of $X(\mathcal{V})$ is zero if and only if $n = 3\ ,4$ or 5 (see [Shi]).

We write $\mathcal{V}(i)$ for $\mathcal{V}$ with the pairing given by the composite $\mathcal{V}\times\mathcal{V} \longrightarrow \boldsymbol{\mu}_n \longrightarrow \boldsymbol{\mu}_n$, where the latter map is $x \longrightarrow x^i$ with $i \in (\mathbb{Z}/n\mathbb{Z})^\times$. By the standard pairing on $\boldsymbol{\mu}_n \times \mathbb{Z}/n\mathbb{Z}$, we mean the pairing given by

$$(\zeta_1,\ a_1)\ \times\ (\zeta_2,\ a_2)\ \longrightarrow\ \frac{\zeta_1^{a_2}}{\zeta_2^{a_1}}.$$

The moduli space and its completion for this standard pairing are denoted by $Y(n)$ and $X(n)$ respectively.

Suppose now that E is an elliptic curve over $\mathbb{Q}$ such that the mod n representation $\overline{\rho}_{E,n}$ is equivalent to the mod n representation induced by $\mathcal{V}$. It is not necessarily true that E corresponds to a point on $Y(\mathcal{V})$ since the Weil pairing on $E[n]$ might not coincide with the pairing on $\mathcal{V}$.

Assume now that the representation given by $\mathcal{V}$ is reducible and decomposable. That is $\mathcal{V} = \mathcal{V}_1 \oplus \mathcal{V}_2$ where $\mathcal{V}_1,\ \mathcal{V}_2$ are free of rank one as $\mathbb{Z}/n\mathbb{Z}$-modules. Then given a pair (E, α) lying on $Y(\mathcal{V})$ we can change the embedding α (for example by multiplication on the second factor $\mathcal{V}_2$) so that E gives rise to a point on $Y(\mathcal{V}(j))$ for any $j \in (\mathbb{Z}/n\mathbb{Z})^\times$.

We restrict to the case $n = 3$ or 5. We then have the following result which is essentially proved in [SB-T].

Proposition 2.2.1. *Let $\mathcal{V}$ be an $\mathbb{F}_p$-vector space scheme of dimension two over $\mathbb{Q}$ together with an alternating, non-degenerate pairing into $\boldsymbol{\mu}_p$. Assume p is either 3 or 5. Then $X(\mathcal{V})$ is isomorphic, over $\mathbb{Q}$, to $\mathbb{P}^1$.*

Proof. Let i be such that $\boldsymbol{\mu}_p \times \mathbb{F}_p(i)$ is isomorphic, as a symplectic space over $\overline{\mathbb{Q}}$, to $\mathcal{V}$. Since $\boldsymbol{\mu}_p \times \mathbb{F}_p(i)$ is reducible and decomposable, and $X(p)$ is $\mathbb{P}^1$, the same argument in [SB-T] applies. (See Lemma 1.1 for the case $p = 5$ and the paragraph after Theorem 1.2 for the case $p = 3$ in [SB-T].) □

Remark. Since $\mathbb{P}^1 - \{\text{non-zero finite number of points}\}$ has trivial Picard group, it follows (chapter II of [Ka-Ma]) that we can write the universal elliptic curve with level structure in Weierstrass form (as an elliptic curve over $\mathbb{P}^1 - \{\text{non-zero finite number of points}\}$).

For explicit formulas, see the articles by [R-S] and [Si].

2.3. Subgroups of general linear groups. We now state some results which will guarantee the surjectivity part of **Theorem A**. Fix a positive integer $N > 1$, and let $N = p_1^{n_1} \dots p_k^{n_k}$, where the p_i's are distinct primes, and $n_i \geq 1$, $i = 1, \dots, k$. We then have canonical isomorphisms

$$GL_2(\mathbb{Z}/N\mathbb{Z}) \simeq \prod_{i=1}^{k} GL_2(\mathbb{Z}/p_i^{n_i}\mathbb{Z})$$

and $SL_2(\mathbb{Z}/N\mathbb{Z}) \simeq \prod_{i=1}^{k} SL_2(\mathbb{Z}/p_i^{n_i}\mathbb{Z})$ (coming from the natural surjections $\mathbb{Z}/N\mathbb{Z} \longrightarrow \mathbb{Z}/p_i^{n_i}\mathbb{Z}$). We shall freely use the identifications given by these isomorphisms.

Proposition 2.3.1. *Let $N = p_1^{n_1} \dots p_k^{n_k}$ be a positive integer greater than 1, the p_i's, n_i's being as above. Denote by π_i the projection on to the i-th factor from $SL_2(\mathbb{Z}/N\mathbb{Z})$ to $SL_2(\mathbb{Z}/p_i^{n_i}\mathbb{Z})$, i.e., reduction mod $p_i^{n_i}$. Let H be a subgroup of $SL_2(\mathbb{Z}/N\mathbb{Z})$ such that $\pi_i(H) = SL_2(\mathbb{Z}/p_i^{n_i}\mathbb{Z})$, $i = 1, \dots k$. Assume further that there are $A_1, \dots A_k \in GL_2(\mathbb{Z}/N\mathbb{Z})$ such that each $A_i H A_i^{-1}$ contains an element x_i satisfying*

$$\pi_j(x_i) \quad = \quad \begin{cases} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & j \neq i, \\ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} & j = i. \end{cases}$$

Then $H = SL_2(\mathbb{Z}/N\mathbb{Z})$.

Proof. We have to show that H contains

$$\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \dots, SL_2(\mathbb{Z}/p_i^{n_i}\mathbb{Z}), \dots, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right).$$

We do it for $i = 1$, and observe that we might as well assume H contains x_1. Let $K = \bigcap_{i \neq 1} \ker(\pi_i)$, and note $x_1 \in K$. Then $\pi_1(K)$ is a normal subgroup of $\pi_1(H) = SL_2(\mathbb{Z}/p_1^{n_1}\mathbb{Z})$, and contains $\pi_1(x_1) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. We now have to show that $\pi_1(K) = SL_2(\mathbb{Z}/p_1^{n_1}\mathbb{Z})$.

We have $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$. So $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ is in $\pi_1(K)$. One then checks that $\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. But $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ generate $SL_2(\mathbb{Z})$ (see [Se2]), and so we get $\pi_1(K) = SL_2(\mathbb{Z}/p_1^{n_1}\mathbb{Z})$. □

Proposition 2.3.2. *Let E be an elliptic curve over $\mathbb{Q}$ such that some conjugate of the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ in $GL_2(\mathbb{Z}_l)$ under $\rho_l : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_2(\mathbb{Z}_l)$ contains the element $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Also, further assume that $\overline{\rho}_l : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_2(\mathbb{F}_l)$ is surjective. Then ρ_l is surjective.*

Proof. We show by induction that $\overline{\rho}_{l^n} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(E[l^n])$ is surjective.

Suppose true for n. The image of $\overline{\rho}_{l^{n+1}}$, without loss of generality, contains $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. It also must contain an element of the form

$$B = \begin{pmatrix} l^n u_1 & -1 + l^n u_2 \\ 1 + l^n u_3 & l^n u_4 \end{pmatrix},$$

which reduces modulo l^n to $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. One then checks that $CAC^{-1} = \begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix}$ with u a unit in $\mathbb{Z}/l^{n+1}\mathbb{Z}$, where $C = A^{-l^n u_1} B$. As in the previous proposition,

we deduce that the image contatins $SL_2(\mathbb{Z}/l^{n+1}\mathbb{Z})$, and since the determinant is the cyclotomic character, we get surjectivity. □

The following proposition, in some form, is in [Se3].

Proposition 2.3.3. *Let E be an elliptic curve over $\mathbb{Q}$, l an odd prime. Suppose the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ under $\overline{\rho}_l : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_2(\mathbb{F}_l)$ has order divisible by l, and suppose $\exists g \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that $tr(\overline{\rho}_l(g))^2 - 4\det(\overline{\rho}_l(g))$ is not a square in $\mathbb{F}_l$. Then $\overline{\rho}_l$ is surjective.*

Proof. Using proposition 15 of [Se3], all we need to show is that image of $\overline{\rho}_l$ is not contained in a Borel subgroup of $GL_2(\mathbb{F}_l)$. Suppose the contrary. Then $\overline{\rho}_l \sim \begin{pmatrix} \chi\epsilon & * \\ 0 & \epsilon^{-1} \end{pmatrix}$ where χ is the cyclotomic character, and ϵ is some character. Then $tr(\overline{\rho}_l(g)) = \chi(g)\epsilon(g) + \epsilon^{-1}(g)$, and hence $tr(\overline{\rho}_l(g))^2 - 4\chi(g) = tr(\overline{\rho}_l(g))^2 - 4\det(\overline{\rho}_l(g))$ has to be a square — a contradiction. □

2.4. Proof of Theorem A. We first show the existence of an elliptic curve satisfying (a) and (b) of the Theorem. We shall be using the following lemma which is a direct application of the main theorem of [Kis1] (see also [Kis2]).

Lemma. Let $E : y^2 = x^3 + 3ax + 2b$ be an elliptic curve over a complete discrete valuation field k of characterisitic zero and residue characteristic positive. Let n be a fixed positive integer.

Then there exists an $\epsilon > 0$ such that for any elliptic curve $E_1 : y^2 = x^3 + 3a_1x + 2b_1$ over k with $\max\{|a - a_1|, |b - b_1|\} \leq \epsilon$, the mod n representations $\overline{\rho}_{E,n}$ and $\overline{\rho}_{E_1,n}$ are equivalent. □

Let p be a prime in Σ such that $\overline{\rho}_{E_0,M}|_{D_p}$ is reducible and decomposable. We can then realize $E_{(p)}$, after choosing a suitable isomorphism $E_{(p)}[M] \xrightarrow{\alpha} E_0[M] \times \mathbb{Q}_p$, as a $\mathbb{Q}_p$-point on any of the curves $Y(E_0[M](i))/\mathbb{Q}_p$ (see proposition 2.2.1 and the discussion before that). Hence we may assume that, after suitable choices of isomorphisms on M-torsion points, all the elliptic curves $E_{(p)}$ lie on the same curve. Since $Y(E_0[M](i))/\mathbb{Q}$ is the projective line minus a non-zero finite number of points, it has trivial Picard group and so we can write the universal elliptic curve as $\mathcal{E}(t) : y^2 = x^3 + A(t)x + B(t)$, where $A(t),\ B(t) \in \mathbb{Q}(t)$.

We know that there is a $t_p \in \mathbb{Q}_p$ such that the fibre at t_p gives the elliptic curve $E_{(p)}$. By the weak approximation theorem, we can find a $t_0 \in \mathbb{Q}$ where t_0 and t_p are close enough so that, for each p in Σ, the elliptic curve $\mathcal{E}(t_0)$ satisfies the hypotheses of the lemma above for $E_{(p)}$ with $n = MN$. Hence $\mathcal{E}(t_0)/\mathbb{Q}$ satisfies the conditions (a) and (b) of the theorem.

Let c denote complex conjugation in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Note that $\overline{\rho}_{E_0,M}(c)$ has trace 0 , determinant -1. As in section 2.3, let $p_1^{n_1} \dots p_k^{n_k}$ be the prime factorisation of N. By the Chebotarev Density Theorem, we can find infinitely many primes l such that $l \equiv -1 (\mathrm{mod}\ MN)$, $\overline{\rho}_{E_0,M}$ is unramified at l, and $\mathrm{trace}(\overline{\rho}_{E_0,M}(\mathbf{Frob}_l)) = 0$. This follows, for example, by considering $\overline{\rho}_{E_0,M} \times \chi_N$:

$\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_2(\mathbb{Z}/M\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})^\times$. Fix k such primes $l_1, \ldots, l_k$ not in Σ. Let $a_i = MN/p_i^{n_i}$, and take, for each l_i, the Tate curve E_{q_i} over $\mathbb{Q}_{l_i}$ with $q_i = l_i^{a_i}$.

Further, by the Chinese Remainder Theorem, we can find a positive integer a satisfying

- $a \equiv 0 (\mathrm{mod}\ M)$,
- $a^2 + 4$ is not a square mod p_i, for all odd p_i, and
- $a \equiv 1 (\mathrm{mod}\ 2)$ if N is even.

We can then find a prime $l \equiv -1 (\mathrm{mod}\ MN)$ such that $MN < l$, $\overline{\rho}_{E_0,M}$ is unramified at l, trace of $\mathbf{Frob}_l$ is equal to 0, $l \notin \Sigma \cup \{l_1, \ldots l_k\}$ and $a < 2\sqrt{l}$. By Honda-Tate Theory (see [Hon], [Ta]), there is an elliptic curve E_l defined over $\mathbb{Q}_l$ with good reduction such that $l + 1 - |\bar{E}_l(\mathbb{F}_l)| = a$. Here, $\bar{E}_l$ is the reduction mod l of E_l.

We now take $\Sigma' = \Sigma \cup \{l_1, \ldots l_k\} \cup \{l\}$ with elliptic curves $E_{(p)}$ if $p \in \Sigma$, E_{q_i} over $\mathbb{Q}_{l_i}$ for l_i and E_l over $\mathbb{Q}_l$ for l. These then satisfy the hypotheses of the theorem (the extra elliptic curves we have introduced all have reducible and decomposable mod M representations). Hence we can find an elliptic curve E over $\mathbb{Q}$ satisfying (a) and (b) for Σ'. Each $\overline{\rho}_{E,p_i}$ is then surjective by 2.3.3, whenever p_i is odd. In the case p_i is even, $\overline{\rho}_{E,p_i}$ is again surjective because the image contains an element of order 2 (from E_{q_i}), and an element of order 3 (from E_l). Further, by 2.3.2, each $\overline{\rho}_{E,p_i^{n_i}}$ is surjective. Finally, by our construction of Σ', we note that the image of $\overline{\rho}_{E,N}$ in $GL_2(\mathbb{Z}/N\mathbb{Z})$ contains the elements x_i of proposition 2.3.1, possibly after conjugations (this follows, for example, by looking at the image of a generator of the tame inertia of $\mathrm{Gal}(\overline{\mathbb{Q}}_{l_i}/\mathbb{Q}_{l_i})$ under the mod N representation given by the Tate curve E_{q_i}). Hence, by 2.3.1, the image contains $SL_2(\mathbb{Z}/N\mathbb{Z})$. But the determinant of $\overline{\rho}_{E,N}$ is cyclotomic — hence $\overline{\rho}_{E,N}$ is surjective.

We know that there are infinitely many primes l' such that E_0 is unramified at l', $\mathrm{trace}(\overline{\rho}_{E_0,M}(\mathbf{Frob}_{l'}) = 0$ and $l' \equiv -1 (\mathrm{mod}\ M)$. Fix any such l' not in Σ', and take a Tate curve E_q over $\mathbb{Q}_{l'}$ where q is an M-th power. We then have $\overline{\rho}_{E_q,M} \sim \overline{\rho}_{E_0,M}|_{D_{l'}}$. Note that $\overline{\rho}_{E_q,N}$ will be ramified if N does not divide $v_l(q)$ — and we can make such a choice since $(M, N) = 1$. Having done so, replace Σ' by $\Sigma' \cup \{l'\}$ and continue the process, thus getting infinitely many elliptic curves satisfying (a), (b) and (c). □

3. $GL_2(\mathbb{F}_3)$ representations

Proposition 3.1. *Let $\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}_3}/\mathbb{Q}_3) \longrightarrow GL_2(\mathbb{F}_3)$ be a representation of the absolute Galois group of $\mathbb{Q}_3$ such that $\det(\overline{\rho}) = \chi$, the (mod 3) cyclotomic character. Let K be the splitting field of $\overline{\rho}$ (i.e., the extension of $\mathbb{Q}_3$ fixed by the kernel of $\overline{\rho}$). Then K determines $\overline{\rho}$ up to twist by a quadratic character.*

Proof. Set $G = \mathrm{Gal}(K/\mathbb{Q}_3)$, I the inertia subgroup of G. We denote by ζ a fixed primitive third root of unity. Note the order of $GL_2(\mathbb{F}_3)$ is 48.

Suppose that $\overline{\rho}$ is wildly ramified. We may then assume that the image of the wild part of inertia under $\overline{\rho}$ contains the subgroup generated by $\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$. Since the image of the wild part of inertia has to be a normal subgroup of the image of $\overline{\rho}$, we can conclude the image of $\overline{\rho}$ is contained in the subgroup of upper triangular matrices. We deduce that the representation is equivalent to $\chi^i\epsilon^j\begin{pmatrix}\chi & \sigma\\ 0 & 1\end{pmatrix}$, where i, j are either 0 or 1, $\sigma \in H^1(\mathrm{Gal}(\overline{\mathbb{Q}}_3/\mathbb{Q}_3), \mathbb{F}_3(1))$ is a non-trivial 1-cocycle and ϵ is the quadratic unramified character of $\mathbb{Q}_3$. The splitting field for $\begin{pmatrix}\chi & \sigma\\ 0 & 1\end{pmatrix}$ is determined by the cocycle σ, and this can then be calculated by using Kummer Theory. We get four splitting fields, and eight possible representations, up to twist by the quadratic unramified character. The splitting fields are given by $\mathbb{Q}_3(\zeta, \sqrt[3]{2})$, $\mathbb{Q}_3(\zeta, \sqrt[3]{3})$, $\mathbb{Q}_3(\zeta, \sqrt[3]{3.2})$ and $\mathbb{Q}_3(\zeta, \sqrt[3]{3.4})$. The representations then look like $\begin{pmatrix}1 & *\\ 0 & \chi\end{pmatrix}$ or $\begin{pmatrix}\chi & *\\ 0 & 1\end{pmatrix}$, up to twisting by the quadratic unramified character. The representation is reducible and indecomposable.

Suppose now that $\overline{\rho}$ is not wildly ramified. Since every element of order 4 in $GL_2(\mathbb{F}_3)$ has determinant 1, the order of I is either 2 or 8. If the order of image of inertia is 2, we easily obtain $\overline{\rho} \sim \epsilon^i \otimes \begin{pmatrix}\chi & 0\\ 0 & 1\end{pmatrix}$, where i is 0 or 1 and ϵ is the quadratic unramified character. The representation is reducible, and decomposable.

Finally suppose that the order of image of inertia is 8. Since the representation is tamely ramified, the image is cyclic and a lift of Frobenius acts on inertia by raising an element of inertia to its third power. It follows that the image of $\overline{\rho}$ is a Sylow 2-subgroup of $GL_2(\mathbb{F}_3)$. The result in this case is a consequence of the following description of the Sylow 2-subgroup of $GL_2(\mathbb{F}_3)$ and its automorphism group modulo inner automorphisms.

Let us write G for the Sylow 2-subgroup of $GL_2(\mathbb{F}_3)$ (which is unique up to conjugation). We have the following presentation of G in terms of generators and relations:

$$\langle \alpha, \beta | \alpha^2 = \beta^8 = e,\ \alpha\beta\alpha = \beta^3 \rangle.$$

The elements of order 8 are β, β^3, β^5, and β^7; those of order 2 are β^4, α, $\alpha\beta^2$, $\alpha\beta^4$, and $\alpha\beta^6$. We also have $\beta\alpha\beta^{-1} = \alpha\beta^2$.

It follows that, modulo inner automorphisms, any automorphism of G is either the identity, or is the automorphism of which sends β to β^5 and α to α. The latter has the following description: it sends an element g to $\mu(g)g$ where $\mu(\alpha^i\beta^j) = e$ if j is even, and $\mu(\alpha^i\beta^j) = \beta^4$ if j is odd. (In other words, μ is the composite of the natural surjection $G \longrightarrow G/\langle \alpha, \beta^2 \rangle$ and the isomorphism between $G/\langle \alpha, \beta^2 \rangle$ and $\langle \alpha, \beta^4 \rangle$.) □

As a consequence of the proof of 3.1, we get the following :

Corollary 3.2. *Let $\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}_3/\mathbb{Q}_3) \longrightarrow GL_2(\mathbb{F}_3)$ be a representation of the absolute Galois group of $\mathbb{Q}_3$ such that $\det(\overline{\rho}) = \chi$, the cyclotomic character. Let I_3 be the inertia subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}_3/\mathbb{Q}_3)$. Then $\overline{\rho}$, up to twist by the quadratic unramified character, is uniquely determined (up to conjugacy) by $\overline{\rho}|_{I_3}$.* □

Collecting together we make the following definitions:

Definition 3.3. *Let $\overline{\rho}$ be as above. We call $\overline{\rho}$:*

a) **H** *if it is absolutely irreducible,*
b) **D** *if it is reducible and decomposable, and*
c) **W** *if it is reducible and indecomposable.*

We make the following sub-division in (c). Up to twisting by the quadratic unramified character, we call $\overline{\rho}$

d) **WP** *if the splitting field contains $\mathbb{Q}_3(\zeta, \sqrt[3]{2})$,*
e) **WT**(1) *if the splitting field contains $\mathbb{Q}_3(\zeta, \sqrt[3]{3})$,*
f) **WT**(2) *if the splitting field contains $\mathbb{Q}_3(\zeta, \sqrt[3]{3.2})$, and*
g) **WT**(4) *if the splitting field contains $\mathbb{Q}_3(\zeta, \sqrt[3]{3.4})$.*

We also say $\overline{\rho}$, up to quadratic unramified twist, is of type $\mathbf{WP^{nr}}$ or $\mathbf{WP^{r}}$ according as whether $\overline{\rho} \sim \begin{pmatrix} 1 & * \\ 0 & \chi \end{pmatrix}$ or $\begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix}$. Similarly for $\mathbf{WT^{nr}}$ and $\mathbf{WT^{r}}$.

Remark. As a motivation for the symbols in the above definition, note representations of type **H** are "essentially harmless", those of type **D** are decomposable, and those of type **W** are wildly ramified. The symbol **WP** signifies peu-ramifié; and **WT**(i) signifies tres-ramifié, with the index i signifying the corresponding field conained in the splitting field.

Definition 3.4. *Let $\overline{\rho}$ be a $GL_2(\mathbb{F}_3)$ representation of the absolute Galois group of $\mathbb{Q}_3$ with determinant cyclotomic. Suppose $\overline{\rho}$ is of type* **H**. *We then call $\overline{\rho}$ of type*

- $\mathbf{H_s}$ *if there is an elliptic curve E over $\mathbb{Q}_3$ with supersingular reduction such that $\overline{\rho}$, or its quadratic unramified twist, is equivalent to $\overline{\rho}_{E,3}$*
- $\mathbf{H_s(1)}$ *otherwise.*

Remark. Suppose $\overline{\rho} = \overline{\rho}_{E,3}$ is of type **W**, where E is an elliptic curve over $\mathbb{Q}_3$. Up to quadratic unramified twist, $\overline{\rho} \sim \begin{pmatrix} 1 & * \\ 0 & \chi \end{pmatrix}$ or $\begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix}$ according as whether $E(\mathbb{Q}_3^{\mathrm{nr}})$ contains a non-trivial point of order 3 or not.

The following proposition summarises some facts about splitting fields for 3-torsion.

Proposition 3.5. *Let E be an elliptic curve over F, a field of characteristic 0, and suppose E has Weierstrass equation $y^2 = x^3 + 3ax + 2b$. Let $(x, y) \in E[3]$. Then x satisfies $x^4 + 6ax^2 + 8bx - 3a^2 = 0$. The splitting field for this polynomial is*

$$F\left(\sqrt{-a + \sqrt[3]{a^3 + b^2}}, \sqrt{-a + \zeta\sqrt[3]{a^3 + b^2}}, \sqrt{-a + \zeta^2\sqrt[3]{a^3 + b^2}}\right),$$

where ζ is a primitive third root of unity.

Proof. The statement about the quartic follows from the duplication formula in [Sil1]. The quartic has cubic resolvent (see [v-Wa]) $z^3 - 12az^2 + 48a^2z + 64b^2$, from which we get the statement about the splitting field. □

From the above proposition, we can easily read off the type of mod 3 representation for an elliptic curve over $\mathbb{Q}_3$, and we put this down in the next proposition.

Proposition 3.6. *Let E be an elliptic curve over $\mathbb{Q}_3$, with j-invariant j which is non-zero. Set $J = j/1728$, $\overline{\rho} = \overline{\rho}_{E,3}$. Then $\overline{\rho}$ is of type*

- **H** *if $J \equiv 1 (\mathrm{mod}\ 9)$,*
- **D** *if either $v(J) \neq 0$ and J is a cube, or $J \equiv -1 (\mathrm{mod}\ 9)$,*
- **WP**, **WT**(1), **WT**(2), or **WT**(4) *according as J or $J^{-1} \equiv 2,\ 3,\ 3.2$ or $3.4\ (\mathrm{mod}\ \mathbb{Q}_3^{\times 3})$ respectively.*

Proof. Since $J \neq 0$, we can write E as $y^2 = x^3 + 3ax + 2b$ where $a, b \in \mathbb{Q}_3$ and $a \neq 0$. We then get $J = a^3/(a^3 + b^2)$. Observe that, by proposition 3.4, we can not have $\overline{\rho}$ of type **H** or **D** if J is not a cube. In fact, the last bulleted item in the propositon is almost a tautology if J is not a cube.

So now assume that J is a cube. Then $\overline{\rho}$ will be of type **D** if and only if $\overline{\rho}$ becomes trivial when we go up to $\mathbb{Q}_3^{\mathrm{nr}}(\sqrt{-3})$. An elementary calculation then gives the remaining two cases. □

4. Elliptic curves over $\mathbb{Q}_3$ with potentially good reduction

From this section onwards, all elliptic curves will be over $\mathbb{Q}_3$. *Further, all elliptic curves in this section are assumed to have potentially good reduction (equivalently, they have integral j-invariants).* By the discriminant $\Delta(E)$ of an elliptic curve E over $\mathbb{Q}_3$, we shall always mean its minimal discriminant. By $\mathbf{f}(E)$, we mean the exponent (at 3) of the conductor of E. Given an elliptic curve E over $\mathbb{Q}_3$, we denote by $\mathbf{e}(E)$ the cardinality of the image of inertia under $\overline{\rho}_{E,5}$. We shall frequently abbreviate these to **e** and **f** when the context is clear.

In this section, we write down explicit Weierstrass equations for elliptic curves with potential good reduction as a first step to computing the mod 3 representations given by elliptic curves with prescribed mod 5 representation. Note, since our elliptic curves have potentially good reduction, the possible values of **e** are 1, 2, 3, 4, 6 and 12.

4.1. $\mathbf{e}(E) = 1$. Every elliptic curve over $\mathbb{F}_3$ can be put in the Weierstrass form $y^2 = x^3 + ax^2 + bx + c$ with $ab = 0$. Also, note that an elliptic curve with potentially good reduction will have good reduction if and only if the value of **e** is equal to 1. Thus every elliptic curve over $\mathbb{Q}_3$ with good reduction can be written as $y^2 = x^3 + ax^2 + bx + c$, where $a, b, c \in \mathbb{Z}_3$ and $ab \equiv 0 (\mathrm{mod}\ 3)$. For an elliptic curve E with good reduction, we shall write $\mathbf{a_3}$ for the trace of Frobenius

acting on $T_l(E)$ with $l \neq 3$ — i.e., $\mathbf{a_3} = 4 - |\bar{E}(\mathbb{F}_3)|$ where $\bar{E}$ is the reduction mod 3 of E.

The following proposition is then easily verified.

Proposition 4.1.1. *Let E be an elliptic curve over $\mathbb{Q}_3$ with good reduction. Then E can be written in one of the following ways:*

a) $\mathbf{a_3} \equiv 0 (\text{mod } 5)$
$y^2 = x^3 + x + b,$
$y^2 = x^3 - x + 3b,\ b \in \mathbb{Z}_3$.

b) $\mathbf{a_3} \equiv \pm 1 (\text{mod } 5)$
$y^2 = x^3 + x^2 + 3ax + 3b - 1,$
$y^2 = x^3 - x^2 + 3ax + 3b + 1,\ a, b \in \mathbb{Z}_3$.

c) $\mathbf{a_3} \equiv \pm 2 (\text{mod } 5)$
$y^2 = x^3 + x^2 + 3ax + 3b + 1,$
$y^2 = x^3 - x + 3b - 1$,
$y^2 = x^3 - x + 3b + 1,$
$y^2 = x^3 - x^2 + 3ax + 3b - 1,\ a, b \in \mathbb{Z}_3.$ □

4.2. $\mathbf{e = 2, 3}$ or 6.

Lemma 4.2.1. *Let E be an elliptic curve over $\mathbb{Q}_3$ with $\mathbf{e}(E) \neq 1$, and $j(E)$ integral. Then E can be put in the Weierstrass form $y^2 = x^3 + 3ax + 2b$, with $a, b \in \mathbb{Z}_3$, which has minimal discriminant.*

Proof. We follow the notation in [Sil1]. We may assume that E has Weierstrass equation $y^2 = x^3 + a_2x^2 + a_4x + a_6,\ a_i \in \mathbb{Z}_3$, with minimal discriminant. We then get $b_2 = 4a_2,\ \ b_4 = 2a_4,\ \ b_6 = 4a_6,\ \ c_4 = b_2^2 - 24b_4$ and $j(E) = c_4^3/\Delta(E)$.

Since $v(\Delta) > 0$ and j is integral, it follows that $v(a_2) > 0$, and hence we may assume $a_2 = 0$. Then $\Delta(E) = -8b_4^3 - 27b_6^2$ gives $v(a_4) > 0$. □

We start by analysing elliptic curves with potentially good reduction whose (minimal) discriminants have non-zero, even valuation. Note that if $\mathbf{e}(E)$ is 2, 3 or 6, then $v(\Delta(E))$ is even and positive (we are, of course, assuming that E has potentially good reduction).

Conversely, let E be an elliptic curve over $\mathbb{Q}_3$ having Weierstrass equation $y^2 = x^3 + 3ax + 2b,\ a, b$ integral with minimal discriminant. Note that $\Delta = -2^6 3^3 (a^3 + b^2),\ j = 2^6 3^3 a^3/(a^3 + b^2)$. Since $v(\Delta)$ is even, we must have $v(a^3 + b^2)$ odd. Thus a is a unit if and only if b is a unit.

Suppose a is a unit. Then we must have $a \equiv -1 (\text{mod } 3)$, and hence we can assume, after a change of variables, that $a = -1$. By the conditions on j and Δ, we must have $v(b^2 - 1) = 1$ or 3. We thus get the following equations:

- $y^2 = x^3 - 3x + 2b,\ v(b^2 - 1) = 1,$
- $y^2 = x^3 - 3x + 2b,\ v(b^2 - 1) = 3$.

Suppose now that a is not a unit. We cannot have $v(b^2) < v(a^3)$, for then $v(a^3 + b^2)$ would be even. If $v(a^3) < v(b^2)$, then $v(a)$ must be odd and is either 1 or 3. This is because $v(a) \geq 5$ implies $v(b) \geq 8$ which contradicts the minimality of Δ

(make the change of Weierstrass coordinates $x \mapsto 3^2x,\ y \mapsto 3^3y$). If $v(a) = 3$, then $v(b) \geq 5$, and again by the minimality of Δ, we see that $v(b) = 5$. The possible equations are then

- $y^2 = x^3 \pm 3^2x + 2.3^2c,\ c \in \mathbb{Z}_3$,
- $y^2 = x^3 \pm 3^4x + 2.3^5c,\ c \in \mathbb{Z}_3^\times$.

Claim. *The elliptic curves $y^2 = x^3 \pm 3^4x + 3^5c$ with c a unit in $\mathbb{Z}_3$ are minimal.*

Proof of claim. Suppose there is a change of variables $\{x = u^2x' + r,\ \ y = u^3y' + u^2sx' + t\}$ reducing the discriminant. From the table on page 49 of [Sil1], we get $u^2b_2' = 12r$, $u^4b_4' = b_4 + 6r^2$ and $u^6b_6' = b_6 + 2rb_4 + 4r^3$. As $v(\Delta) = 12,\ v(u) = 1$. The first two of the above relations then give $v(r) \geq 2$, contradicting the third one. □

The curves $y^2 = x^3 \pm 3^2x + 2.3^2c$ with $v(c) \geq 1$ have $v(\Delta) = 6$, and these curves have $\mathbf{e} = 2$ (making the transformation $x \mapsto 3x',\ \ y \mapsto 3\sqrt{3}y'$ reduces the discriminant). The curve $y^2 = x^3 \pm 3^2x + 2.3^2c$ with $v(c) = 0$ is a quadratic twist of the curve $y^2 = x^3 \pm 3^4x + 2.3^5c$, and so is minimal.

Finally suppose $v(a^3) = v(b^2)$ with a, b non-units. Again the minimality condition forces $v(a) \leq 3$, and thus we must have $v(a) = 2,\ v(b) = 3$. Replacing a by $3^2a'$, b by $3^3b'$ with a', b' units, we get $\Delta = -2^6 3^9(a'^3 + b'^2),\ j = 2^6 3^3 a'^3/(a'^3 + b'^2)$ with $v(a'^3 + b'^2) = 1$ or 3 (and $v(\Delta) = 10$ or 12 respectively). Hence in this case, we can take our curve to be $y^2 = x^3 - 3^3x + 2.3^3d$ with $v(d^2 - 1) = 1$ or 3.

Claim. *The elliptic curve $y^2 = x^3 - 3^3x + 2.3^3d$ with $v(d^2 - 1) = 3$ is not minimal.*

Proof of claim. Making the transformation $x \mapsto 3^2x + 3r\ ,\ y \mapsto 3^3y$, we get

$$y^2 = x^3 + rx^2 + 3^{-1}(r^2 - 1)x + 3^{-3}(r^3 - 3r + 2b).$$

Take $r = 1$ if $b \equiv 1 (\text{mod } 3^3),\ r = -1$ if $b \equiv -1 (\text{mod } 3^3)$. □

We summarise all these in the following proposition.

Proposition 4.2.2. *The elliptic curves over $\mathbb{Q}_3$ with integral j-invariant and valuation of minimal discriminant even, non-zero are :*

a) $y^2 = x^3 - 3x + 2b,\ v(b^2 - 1) = 1$
b) $y^2 = x^3 \pm 3^4x + 2.3^5b,\ b \in \mathbb{Z}_3^\times$
c) $y^2 = x^3 - 3^3x + 2.3^3b,\ v(b^2 - 1) = 1$
d) $y^2 = x^3 \pm 3^2x + 2.3^2b,\ b \in \mathbb{Z}_3^\times$
e) $y^2 = x^3 - 3x + 2b,\ v(b^2 - 1) = 3$
f) $y^2 = x^3 \pm 3^2x + 2.3^3b,\ b \in \mathbb{Z}_3$.

The curves in (a) and (b) achieve good reduction over a ramified degree 3 extension (i.e., have $\mathbf{e} = 3$). The curves in (c), (d) are the twists by a quadratic ramified character of the curves in (a) and (b) respectively, and they have $\mathbf{e} = 6$. The curves in (e), (f) acquire good reduction over a quadratic ramified extension i.e., they have $\mathbf{e} = 2$.

Proof. Only the statement about good reduction over a degree 3 extension for the curves in (a) and (b) needs to be checked.

(a) Suppose $b = 1 + 3u$, u a unit. Take $K = \mathbb{Q}_3(\pi)$ where π is a root of $(1+x)^3 - 3(1+x) + 2(1+3u) \equiv x^3 + 3x^2 + 2.3u$. This polynomial is irreducible over $\mathbb{Q}_3$ and as $3 = -\pi^3/(2u+\pi^2)$, π is a uniformizer for $\mathcal{O}_K$. By making the transformation $y \mapsto \pi^3 y$, $x \mapsto \pi^2 x + (1+\pi)$, we get

$$y^2 = x^3 - x^2\pi(1+\pi)/(2u+\pi^2) \ - x(2+\pi)/(2u+\pi^2) \ .$$

If $b = -1 + 3u$, u a unit, we take π to be a root of $(-1+x)^3 - 3(-1+x) - 2 + 2.3u \equiv x^3 - 3x^2 + 3.2u$ and then transform the curve by $y \mapsto \pi^3 y$, $x \mapsto \pi^2 x + (-1+\pi)$ to get

$$y^2 = x^3 + x^2\pi(-1+\pi)/(\pi^2 - 2u) + x(\pi - 2)/(\pi^2 - 2u) \ .$$

(b) In this case, $x^3 \pm 3^4 x + 2.3^5 b$, b a unit, is irreducible over $\mathbb{Q}_3$. Take a root α of this polynomial, and set $K = \mathbb{Q}_3(\alpha)$. Then $\pi = \alpha/3$ is a root of $z^3 \pm 3^2 z + 2.3^2 b$, and this gives $v_K(\pi) = 2$. Making the substitution $x \mapsto 3^2 x + \alpha$, $y \mapsto 3^3 y$ gives the curve

$$y^2 = x^3 + 3^{-1}\alpha x^2 + 3^{-3}\alpha^2 x \pm x.$$

□

Corollary 4.2.3. *Let E be an elliptic curve over $\mathbb{Q}_3$ with integral j-invariant. Then $\mathbf{e}(E) = 1,\ 2,\ 3$ or 6 if and only if the valuation of the minimal discriminant of E is even.* □

4.3. e = 4 or 12. From corollary 4.2.3, we know that the valuation of the minimal discriminant is odd. As before, we start with $E : y^2 = x^3 + 3ax + 2b$, where $a, b \in \mathbb{Z}_3$. Recall that this has discriminant $\Delta = -2^6 3^3 (a^3 + b^2)$ and $j = 2^6 3^3 a^3/(a^3 + b^2)$.

The case $j = 0$ is easy. In this case, we get $y^2 = x^3 + 3^n i$ with $n = 0, 1, 2, 3, 4$ or 5 and $i = \pm 1, \pm 4$ or ± 7.

When $j = 1728$, we have $b = 0$. We then get $y^2 = x^3 \pm 3^n x$, where $n = 1$ or 3 . It is easy to see that they have $\mathbf{e} = 4$.

So assume $j \neq 0,\ 1728$. Thus $ab \neq 0$. We first consider the case $v(a) = 0$. The possible curves are easily worked out to be:

- $y^2 = x^3 + 3x + 2b,\ b \in \mathbb{Z}_3 - \{0\}$
- $y^2 = x^3 - 3x + 2b,\ v(b^2 - 1) = 2$
- $y^2 = x^3 - 3x + 2.3b,\ b \in \mathbb{Z}_3 - \{0\}$.

So now assume $0 < v(a) < \infty$. If $v(b) > 5$, we must have $v(a) < 3$, and hence we must have $v(a) = 2$. Working out the remaining cases, for the other possible values of $v(b)$, we get the following possible curves :

- $y^2 = x^3 \pm 3^3 x + 2.3^6 b,\ b \in \mathbb{Z}_3 - \{0\}$
- $y^2 = x^3 \pm 3^{n+1} x + 2b,\ b \in \mathbb{Z}_3^{\times}, n \geq 1$
- $y^2 = x^3 \pm 3^{n+1} x + 2.3b,\ v(b) = 0,\ n \geq 1$
- $y^2 = x^3 \pm 3^{n+2} x + 2.3^2 b, v(b) = 0,\ n \geq 1$
- $y^2 = x^3 \pm 3^{n+3} x + 2.3^3 b,\ v(b) = 0,\ n \geq 1$

- $y^2 = x^3 - 3^3x + 2.3^3b,\ v(b^2-1) = 2$
- $y^2 = x^3 + 3^3x + 2.3^3b,\ v(b) = 0$
- $y^2 = x^3 \pm 3^{n+2}x + 2.3^4b,\ v(b) = 0$ *and* $n \geq 1$
- $y^2 = x^3 \pm 3^3x + 2.3^5b,\ v(b) = 0$
- $y^2 = x^3 \pm 3^{n+4}x + 2.3^5b,\ v(b) = 0$ *and* $n \geq 1$.

When $j \neq 0$ or 1728, we can use the table in Diamond-Kramer [D-K] to classify the curves we have listed by conductor and **e**. This immediately yields the following proposition :

Proposition 4.3.1. *Let E be an elliptic curve over $\mathbb{Q}_3$ with* $\mathbf{e} = 4$ or 12. *Then E can be put in one of the following Weierstrass forms, up to quadratic (possibly ramified) twist :*

1) $\mathbf{e} = 4$
   - $y^2 = x^3 + 3x + 2b,\ b \equiv \pm 2 (\text{mod } 9)$
   - $y^2 = x^3 \pm 3x + 2.3^2b,\ b \in \mathbb{Z}_3,\ b \neq 0$
   - $y^2 = x^3 \pm 3^{n+1}x + 2b,\ b \equiv \pm 4 (\text{mod } 9),\ n \geq 1,$

   plus the following curves with $j = 0$ or 1728*:*
   - $y^2 = x^3 \pm 3x$, $y^2 = x^3 \pm 3^3x$, $y^2 = x^3 \pm 1$ *and* $y^2 = x^3 \pm 3^3$.
2) $\mathbf{e} = 12,\ \mathbf{f} = 3$
   - $y^2 = x^3 + 3x + 2b,\ b \equiv \pm 1, \pm 4 (\text{mod } 9)$
   - $y^2 = x^3 \pm 3x + 2.3b,\ v(b) = 0$
   - $y^2 = x^3 - 3x + 2b,\ v(b^2-1) = 2$
   - $y^2 = x^3 \pm 3^{n+1}x + 2b,\ b \equiv \pm 1, \pm 2 (\text{mod } 9),\ n \geq 1$

   and the following curves with $j = 0$:
   - $y^2 = x^3 \pm 2b$, $y^2 = x^3 \pm 2.3^3b,\ b \equiv \pm 1, \pm 2 (\text{mod } 9)$
3) $\mathbf{e} = 12,\ \mathbf{f} = 5$
   - $y^2 = x^3 \pm 3^{n+1}x + 2.3b,\ v(b) = 0\ n \geq 1$
   - $y^2 = x^3 \pm 3^{n+2}x + 2.3^2b,\ v(b) = 0,\ n \geq 1$

   and the following curves with $j = 0$:
   - $y^2 = x^3 + 2.3^nb,\ n = 1, 2, 4$ or $5,\ v(b) = 0.$ □

Remark. The elliptic curves in 4.3.1 have minimal discriminant. To see this, note that since they have potentially good reduction and valuation of discriminant odd, by 4.2.1 we can assume any change of co-ordinates reducing the discriminant is of the form $x \to u^2x,\ y \to u^3y$. It is then easy to see that they have minimal discriminant.

5. Mod 3 Representations in a given class

Definition. Let E be an elliptic curve over $\mathbb{Q}_3$. Denote by $\mathcal{F}(E)$ the set of isomorphism classes of elliptic curves over $\mathbb{Q}_3$ whose mod 5 representation is equivalent to either $\overline{\rho}_{E,5}$ or the quadratic unramified twist of $\overline{\rho}_{E,5}$. We then define $\mathcal{G}(E)$ to be the set of of equivalence classes of representations $\overline{\rho}_{E',3}$: $\text{Gal}(\overline{\mathbb{Q}}_3/\mathbb{Q}_3) \longrightarrow GL_2(\mathbb{F}_3)$, up to twist by the quadratic unramified character, where E' is an elliptic curve in $\mathcal{F}(E)$. We identify — by 3.2 — $\mathcal{G}(E)$ with the

set of equivalence classes of representations $\overline{\rho}_{E',3}|_{I_3}$ where E' is an elliptic curve in $\mathcal{F}(E)$.

We now describe the set $\mathcal{G}$ for a given mod 5 representation, up to twist by the quadratic unramified character. In order to do this, we need to classify elliptic curves over $\mathbb{Q}_3$ with a prescribed mod 5 representation up to twist by the quadratic unramified character. The classification is easy when the mod 5 representation is either unramified, or tamely ramified. In the case of wild ramification, it turns out (see lemmas 5.3.1 and 5.4.1) the splitting field (for the mod 5 representation) determines the mod 5 representation, up to twist by the quadratic unramified character. The splitting field (for the mod 5 representation) is computed by looking at the 2-division points (see the discussions following lemmas 5.3.1 and 5.4.1).

5.1. Unramified mod 5 Representations. The unramified mod 5 representations are completely determined by the trace of the Frobenius. If the given elliptic curve has good reduction, then we can calculate the type of mod 3 representation by using proposition 3.6 . But there is still the possibility of the mod 5 representation having come from a curve with potentially multiplicative reduction.

Note that $\mathcal{F}(E)$ contains curves with multiplicative reduction which are isomorphic to a Tate curve either over $\mathbb{Q}_3$ or the quadratic unramified extension of $\mathbb{Q}_3$ if and only if $tr(\overline{\rho}_{E,5}(\mathbf{Frob})) \equiv \pm 1 (\mathrm{mod}\ 5)$. Using propositions 3.6 and 4.1.1 we get the following:

Theorem 5.1.1. *Let E be an elliptic curve over $\mathbb{Q}_3$ such that $\overline{\rho}_{E,5}$ is unramified. Then*

a) $\mathcal{G}(E) = \{\mathbf{H_s}\}$ *if* $tr(\overline{\rho}_{E,5}(\mathbf{Frob})) \equiv 0 (\mathrm{mod}\ 5)$
b) $\mathcal{G}(E) = \{\mathbf{H_s}, \mathbf{D}, \mathbf{WP^r}\}$ *if* $tr(\overline{\rho}_{E,5}(\mathbf{Frob})) \equiv \pm 2 (\mathrm{mod}\ 5)$
c) $\mathcal{G}(E) = \{\mathbf{D}, \mathbf{WP^r}, \mathbf{WT}(1)^{\mathbf{r}}, \mathbf{WT}(2)^{\mathbf{r}}, \mathbf{WT}(4)^{\mathbf{r}}\}$
if $tr(\overline{\rho}_{E,5}(\mathbf{Frob})) \equiv \pm 1 (\mathrm{mod}\ 5)$. □

5.2. Tamely Ramified Representations. Let E be an elliptic curve over $\mathbb{Q}_3$ such that $\overline{\rho}_{E,5}$ is tamely ramified. Then the image of inertia has order 2, 4, 5 or 10. When $\mathbf{e} = 5$ or 10, E necessarily has potentially multiplicative reduction, and the mod 3 representations can be easily read off from Tate curves. When $\mathbf{e} = 4$, the mod 5 representation splits over $\mathbb{Q}_3^{\mathrm{nr}}(\sqrt[4]{3})$, and it is easy to check that there is only one possible mod 5 representation up to twist by the quadratic unramified character. When $\mathbf{e} = 2$ we can again twist by a quadratic ramified character to get back to the situation in 5.1. Using 3.6 and 4.2.2, we get

Proposition 5.2.1. *Suppose E has mod 5 representation tamely ramified. Then*

- $\mathbf{e = 2}$. *Here $\mathcal{G}(E)$ is one of the following sets :*

$\{\mathbf{H_s(1)}\}$ *or* $\{\mathbf{H_s(1)}, \mathbf{D}, \mathbf{WP^{nr}}\}$ *or* $\{\mathbf{D}, \mathbf{WP^{nr}}, \mathbf{WT}(1)^{\mathbf{nr}}, \mathbf{WT}(2)^{\mathbf{nr}}, \mathbf{WT}(4)^{\mathbf{nr}}\}$.

Which of the sets occurs can be read off by twisting E by a quadratic ramified character.

- $\mathbf{e = 4}$. $\mathcal{G}(E) = \{\mathbf{H_s},\ \mathbf{H_s(1)},\ \mathbf{WP^r},\ \mathbf{WP^{nr}}\}$
- $\mathbf{e = 5}$. $\mathcal{G}(E) = \{\mathbf{D}, \mathbf{WP^r}, \mathbf{WT}(1)^{\mathbf{r}}, \mathbf{WT}(2)^{\mathbf{r}}, \mathbf{WT}(4)^{\mathbf{r}}\}$
- $\mathbf{e = 10}$. $\mathcal{G}(E) = \{\mathbf{D}, \mathbf{WP^{nr}}, \mathbf{WT}(1)^{\mathbf{nr}}, \mathbf{WT}(2)^{\mathbf{nr}}, \mathbf{WT}(4)^{\mathbf{nr}}\}$. □

5.3. e = 3 or 6.

Lemma 5.3.1. *Suppose E_1, E_2 are elliptic curves over $\mathbb{Q}_3$ such that $\overline{\rho}_{E_1,5}$ and $\overline{\rho}_{E_2,5}$ have the same splitting field K, and $\mathbf{e}(E_1) = \mathbf{e}(E_2) = 3$. Then $\overline{\rho}_{E_1,5}$ is, up to twist by the quadratic unramified character, equivalent to $\overline{\rho}_{E_2,5}$. Further, if K is a non-abelian extension of $\mathbb{Q}_3$, then the two representations are equivalent over $\mathbb{Q}_3$.*

Proof. We may assume that the image of inertia in $GL_2(\mathbb{F}_5)$ is

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

The normalizer of a Sylow 3-subgroup of $GL_2(\mathbb{F}_5)$ has order 48, and since a lift of Frobenius has determinant 3, we deduce that the splitting field for the representation is a degree 24 extension of $\mathbb{Q}_3$. There are then two cases to consider, depending on whether the representation is abelian or not.

(a) Abelian case : Fix generators of $\mathrm{Gal}(K/\mathbb{Q}_3)$ say σ, τ satisfying $\sigma^8 = \tau^3 = e$, $\sigma\tau = \tau\sigma$, where we take σ to be a lift of Frobenius. We may assume that the image of τ is $\begin{pmatrix}-1 & 1\\ -1 & 0\end{pmatrix}$. The image of σ is then a matrix of the form $\begin{pmatrix}x & y\\ -y & x+y\end{pmatrix}$ with $x^2 + xy + y^2 = 3$ and $2x + y = 0$ (as $\sigma^8 = e$), which gives $(x, y) = (-1, 2)$ or $(1, -2)$. Hence the representations vary by at most a quadratic unramified character.

(b) Non-abelian case : We can assume that

$$\mathrm{Gal}(K/\mathbb{Q}_3) = \langle \sigma, \tau | \sigma^8 = \tau^3 = e, \sigma\tau = \tau^2\sigma \rangle,$$

where σ is a lift of the Frobenius and τ goes to $\begin{pmatrix}-1 & 1\\ -1 & 0\end{pmatrix}$. The image of σ is then $\begin{pmatrix}a & b\\ a+b & -a\end{pmatrix}$ with $a^2 + ab + b^2 = 2$. If $a = 1$, then $b = 2$. If $a \neq 1$ the matrix $\begin{pmatrix}a+b+2 & -(a-1)\\ a-1 & b+3\end{pmatrix}$ is non-singular, fixes $\begin{pmatrix}-1 & 1\\ -1 & 0\end{pmatrix}$, and conjugates $\begin{pmatrix}a & b\\ a+b & -a\end{pmatrix}$ to $\begin{pmatrix}1 & 2\\ 3 & -1\end{pmatrix}$. □

Suppose $E : y^2 = x^3 + 3ax + 2b$ over $\mathbb{Q}_3$ has $\mathbf{e} = 3$. We follow the notation of the lemma above. Let F be the subfield fixed by σ (so $[F : \mathbb{Q}_3] = 3$). This is Galois when the mod 5 representation is abelian. Since the curve has good reduction over this extension, we deduce by considering the mod 2 representation that the mod 5 representation is abelian precisely when the discriminant of the elliptic curve E is a square in $\mathbb{Q}_3$. More precisely, one shows that if K is a

cubic extension of $\mathbb{Q}_3^{\mathrm{nr}}$ such that $K/\mathbb{Q}_3$ is Galois with non-abelian Galois group, then any two totally ramified cubic extensions of $\mathbb{Q}_3$ inside K are conjugate. As $\mathbb{Q}_3^{\mathrm{nr}}(E[2]) = \mathbb{Q}_3^{\mathrm{nr}}(E[5])$ in our case, we get the claim.

When $\overline{\rho}_{E,5}$ is non-abelian, there is only one possible splitting field, and hence one possible representation (up to equivalence). But in the abelian case, there are three possible splitting fields. These follow from local class field theory. (For the non-abelian case, we have to look at norm subgroups of $\mathbb{Q}_3(\sqrt{-1})^\times$ with an appropriate action of $\mathrm{Gal}(\mathbb{Q}_3(\sqrt{-1})/\mathbb{Q}_3)$.)

In the abelian case, we can determine the extension F as follows : it is the splitting field for 2-torsion. To see this, let $\mathbf{Frob}_F$ be the Frobenius for F. From the lemma, by using the Hasse bound, we see that $tr(\rho_{E,5}(\mathbf{Frob}_F)) = 0$. If F does not contain a root of the cubic $x^3 + 3ax + 2b$, $\overline{\rho}_{E,2}$ has to have order 3 as $E : y^2 = x^3 + 3ax + 2b$ has good reduction over F. Thus in particular the trace of $\mathbf{Frob}_F$ has to be odd — a contradiction.

We can now distinguish the possible splitting fields by looking at the norm subgroups for different F's. Here is the list of possible curves with inequivalent mod 5 representations with $\mathbf{e} = 3$:

a) Non-abelian :
   a1) $y^2 = x^3 - 3x + 2b,\ b^2 - 1 = 3u$ with $u \equiv 1 (\mathrm{mod}\ 3)$
   a2) $y^2 = x^3 + 3^4x + 2.3^5b,\ b$ a unit .

b) Abelian :
   (b1) $y^2 = x^3 - 3^4x + 2.3^5b,\ b \equiv \pm 2 (\mathrm{mod}\ 9)$ and $y^2 = x^3 - 3x + 2b,\ b \equiv \pm 4 (\mathrm{mod}\ 27)$ with norm subgroup $3.2\mathbb{Q}_3^{\times 3}$,
   (b2) $y^2 = x^3 - 3^4x + 2.3^5b,\ b \equiv \pm 4 (\mathrm{mod}\ 9)$ and $y^2 = x^3 - 3x + 2b,\ b \equiv \pm 13 (\mathrm{mod}\ 27)$ with norm subgroup $3\mathbb{Q}_3^{\times 3}$,
   (b3) $y^2 = x^3 - 3^4x + 2.3^5b,\ b \equiv \pm 1 (\mathrm{mod}\ 9)$ and $y^2 = x^3 - 3x + 2b,\ b \equiv \pm 22 (\mathrm{mod}\ 27)$ with norm subgroup $3.4\mathbb{Q}_3^{\times 3}$.

A direct calculation then gives the following result :

Theorem 5.3.2. *Let E be an elliptic curve over $\mathbb{Q}_3$ with $\mathbf{e}(E) = 3$. Then we have:*

- $\mathcal{G}(E) = \{\mathbf{WP^r}, \mathbf{WT}(1)^{\mathbf{nr}}, \mathbf{WT}(2)^{\mathbf{nr}}, \mathbf{WT}(4)^{\mathbf{nr}}\}$ *if $\overline{\rho}_{E,5}$ is non-abelian.*
- $\mathcal{G}(E)$ is $\{\mathbf{WP^r}, \mathbf{WT}(4)^{\mathbf{nr}}\}$ or $\{\mathbf{WP^r}, \mathbf{WT}(2)^{\mathbf{nr}}\}$ or $\{\mathbf{WP^r}, \mathbf{WT}(1)^{\mathbf{nr}}\}$ *if $\overline{\rho}_{E,5}$ is abelian. These correspond to the cases (b1), (b2), (b3) respectively.* □

Remark. Since the curves with $\mathbf{e} = 6$ are just twists over $\mathbb{Q}_3(\zeta)$ of the curves we have considered above, the description of $\mathcal{G}(E)$ is the same as above with a quadratic ramified twist.

5.4. e = 12.

Lemma 5.4.1. *Let E_1, E_2 be two elliptic curves over $\mathbb{Q}_3$ with $\mathbf{e}(E_1) = \mathbf{e}(E_2) = 12$. If the mod 5 representations have the same splitting field K, then they differ by at most the quadratic unramified character.*

Proof. The images of $\overline{\rho}_{E_1,5}$ and $\overline{\rho}_{E_2,5}$ have to be the full normaliser of a Sylow-3 subgroup of $GL_2(\mathbb{F}_5)$. The image of inertia is then the semi direct product of $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$ (see [D-K]). We can take a set of generators and relations for $\mathrm{Gal}(K/\mathbb{Q}_3)$ to be

$$\langle \sigma, \tau | \sigma^{12} = \tau^2,\ \sigma^{24} = \tau^4 = e,\ \tau\sigma\tau^{-1} = \sigma^5 \rangle$$

where σ is a lift of Frobenius. (See [D-K]. It also follows from the structure of the image as a subgroup of $GL_2(\mathbf{F}_5)$.) The inertia subgroup is generated by τ, σ^8.

One checks that the image of σ, possibly after twisting by the quadratic unramified character, can be taken to be $\begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix}$. The image of τ then has to be a matrix of the form $\begin{pmatrix} a & b \\ a+b & -a \end{pmatrix}$ with $a^2 + ab + b^2 = -1$, which we denote by A. If $(a,b) \neq (0,3)$, the matrix $C = \begin{pmatrix} a+b+2 & -a \\ a & b+2 \end{pmatrix}$ is non-singular and we have $C\begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix}C^{-1} = \begin{pmatrix} 2 & -1 \\ 1 & 1 \end{pmatrix}$, $CAC^{-1} = \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}$. If A is equal to $\begin{pmatrix} 0 & 3 \\ 3 & 0 \end{pmatrix}$, we take C to be $\begin{pmatrix} 3 & -1 \\ 1 & 2 \end{pmatrix}$. The lemma then follows. □

We keep the notation of the above lemma. Suppose E has $\mathbf{e}(E) = 12$. Let F be the subfield of K fixed by σ. By analysing the two division points, it follows that $F = \mathbb{Q}_3(\sqrt{\Delta(E)})$. To see this, let E be given by $y^2 = x^3 + 3ax + 2b$. Since $\mathbf{e} = 12$, $x^3 + 3ax + 2b$ is irreducible over $\mathbb{Q}_3$. Let L be the subfield of K fixed by σ^3. Then $L/\mathbb{Q}_3$ is a totally ramified, non-abelian Galois extension of degree 6.

If L contains a root of the cubic, then L has to be $\mathbb{Q}_3(E[2])$, and so $F = \mathbb{Q}_3(\sqrt{\Delta(E)})$. So suppose that L does not contain $\sqrt{\Delta(E)}$ and $x^3 + 3ax + 2b$ is irreducible over L. Then the image of $\overline{\rho}_{E,2}$ restricted to $\mathrm{Gal}(\overline{L}/L)$ will be the full group $GL_2(\mathbb{F}_2)$, and hence the image of inertia I_L will be of order 6 or 3 – neither of which is possible as $\overline{\rho}_{E,5}|_{I_L}$ has image order 2.

Let us identify the Galois group $\mathrm{Gal}(K/\mathbb{Q}_3)$ with the subgroup of $GL_2(\mathbb{F}_5)$ that we constructed in the lemma. We then see that $\mathrm{Gal}(F/\mathbb{Q}_3)$ acts on $\mathrm{Gal}(K/F)$ by raising every element to its fifth power. Under these conditions, we find by local class field theory that there is exactly one such extension when $F = \mathbb{Q}_3(\sqrt{3})$, and four when $F = \mathbb{Q}_3(\sqrt{-3})$. In the latter case, we find that only one corresponds to the case $\mathbf{f} = 3$, while the other three correspond to $\mathbf{f} = 5$. We can then distinguish the different ones by looking at 2-division points over $\mathbb{Q}_3^{\mathrm{nr}}$, after adjoining a third root of unity. The following lists elliptic curves with conductor exponent 3 or 5, by their mod 5 representations, up to twist by a quadratic unramified character.

$\mathbf{f} = 3, F = \mathbb{Q}_3(\sqrt{3})$:

- $y^2 = x^3 + 3x + 2b,\ b \equiv \pm 1, \pm 4 (\mathrm{mod}\ 9)$,
- $y^2 = x^3 - 3x + 2.3b,\ v(b) = 0$,

- $y^2 = x^3 - 3x + 2b$, $y^2 = x^3 - 3^3x + 2.3^3b$ where $b^2 - 1 = 9u$, $u \equiv -1 (\mathrm{mod}\ 3)$,
- $y^2 = x^3 + 3^3x + 2.3^3b$, $b \equiv \pm 1, \pm 4 (\mathrm{mod}\ 9)$,
- $y^2 = x^3 - 3^3x + 2.3^4b$ $v(b) = 0$.

$\mathbf{f} = 3, F = \mathbb{Q}_3(\sqrt{-3})$:

- $y^2 = x^3 + 3x + 2.3b$ $v(b) = 0$,
- $y^2 = x^3 - 3x + 2b$ with $b^2 - 1 = 9u$, $u \equiv 1 (\mathrm{mod}\ 3)$,
- $y^2 = x^3 \pm 3^{n+1}x + 2b$ and $y^2 = x^3 \pm 3^{n+3}x + 2.3^3b$, both with $b \equiv \pm 1, \pm 2 (\mathrm{mod}\ 9)$ and $n \geq 1$,
- $y^2 = x^3 - 3^3x + 2.3^3b$, $b^2 - 1 = 9u$, $u \equiv 1 (\mathrm{mod}\ 3)$,
- $y^2 = x^3 + 3^3x + 2.3^4b$ with $v(b) = 0$

  and finally the following curves with $j = 0$
- $y^2 = x^3 + 2b$, $y^2 = x^3 + 3^3b$ both with $b \equiv \pm 1, \pm 2 (\mathrm{mod}\ 9)$.

We ignore curves with $j = 0$ in what follows (but note that they are limiting cases of $n \to \infty$).

$\mathbf{f} = 5, \mathbb{Q}_3^{\mathrm{nr}}(\zeta, \sqrt[3]{3}) \subset K^{\mathrm{nr}}$:

- $y^2 = x^3 \pm 3^{n+2}x + 2.3b$, $b \equiv \pm 4 (\mathrm{mod}\ 9)$, $n \geq 1$
- $y^2 = x^3 + 3^2x + 2.3b$, $b \equiv \pm 1 (\mathrm{mod}\ 9)$
- $y^2 = x^3 - 3^2x + 2.3b$, $b \equiv \pm 2 (\mathrm{mod}\ 9)$
- $y^2 = x^3 \pm 3^{n+2}x + 2.3^2b$, $b \equiv \pm 4 (\mathrm{mod}\ 9)$ $n \geq 1$

And also the same congruences with the curves twisted by $\sqrt{3}$.

$\mathbf{f} = 5, \mathbb{Q}_3^{\mathrm{nr}}(\zeta, \sqrt[3]{3.2}) \subset K^{\mathrm{nr}}$: The same as above but with congruences ± 1, ± 2, ± 4, ± 2 respectively.

$\mathbf{f} = 5, \mathbb{Q}_3^{\mathrm{nr}}(\zeta, \sqrt[3]{3.4}) \subset K^{\mathrm{nr}}$: The same with congruences ± 2, ± 4, ± 1, ± 1 respectively.

Calculating the splitting fields for mod 3 representations, we get the following:

Theorem 5.4.2. *Let E be an elliptic curve over $\mathbb{Q}_3$ with $\mathbf{e}(E) = 12$. Then $\mathcal{G}(E)$ is*

a) $\left\{ \begin{matrix} \mathbf{D}, & \mathbf{H_s}, & \mathbf{H_s(1)}, & \mathbf{WP^r}, & \mathbf{WP^{nr}}, & \mathbf{WT}(1)^{\mathbf{r}}, \\ & \mathbf{WT}(1)^{\mathbf{nr}}, & \mathbf{WT}(2)^{\mathbf{r}}, & \mathbf{WT}(2)^{\mathbf{nr}}, & \mathbf{WT}(4)^{\mathbf{r}}, & \mathbf{WT}(4)^{\mathbf{nr}} \end{matrix} \right\}$
if the conductor has exponent 3,

b) $\{\mathbf{WT}(1)^{\mathbf{r}}, \mathbf{WT}(1)^{\mathbf{nr}}, \mathbf{WT}(2)^{\mathbf{r}}, \mathbf{WT}(2)^{\mathbf{nr}}, \mathbf{WT}(4)^{\mathbf{r}}, \mathbf{WT}(4)^{\mathbf{nr}}\}$ *if the conductor has exponent 5.* □

References

[CDT] B. Conrad, F. Diamond, and R. Taylor, *Modularity of certain potentially Barsotti-Tate Galois representations*. J. Amer. Math. Soc. **12** (1999), 521–567.

[Dia] F. Diamond, *On deformation rings and Hecke rings*, Ann. of Math. (2) **144** (1996), 137–166.

[D-K] F. Diamond and K. Kramer, *Classification of $\bar{\rho}_{E,l}$ by j invariant of E*, In *Modular forms and Fermat's last theorem* (Boston, MA, 1995), pp. 491–498, Springer-Verlag, New York, 1997.

[Hon] T. Honda, *Isogeny classes of abelian varieties over finite fields*, J. Math. Soc. Japan **20** (1968), 83–95.

[Ka-Ma] N.M. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies 108, Princeton University Press, Princeton, 1985.

[Kis1] M. Kisin, *Local constancy in p-adic families of Galois representations*, preprint.

[Kis2] ———, *Local constancy in p-adic families of Galois representations*, Princeton University Ph.D. thesis.

[R-S] K. Rubin and A. Silverberg, *Families of elliptic curves with constant mod p representations*, in *Elliptic Curves, Modular Forms, & Fermat's Last Theorem* (Hong Kong, 1993), pp. 148–161, Ser. Number Theory, I, Internat. Press, Cambridge, MA, 1995.

[SB-T] N.I. Shepherd-Barron and R. Taylor, *Mod 2 and mod 5 icosahedral representations*, J. Amer. Math. Soc. **10** (1997), 283–298.

[Se1] J.-P. Serre, *Abelian l-adic representations and elliptic curves*, W.A. Benjamin, Inc., New York, 1968.

[Se2] ———, *A course in arithmetic*, Graduate Texts in Mathematics, No. 7. Springer-Verlag, New York, 1973.

[Se3] ———, *Propriétés Galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.

[Shi] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Princeton Univ. Press, Princeton, N.J., 1971.

[Si] A. Silverberg, *Explicit families of elliptic curves with prescribed mod N representations*, in *Modular forms and Fermat's last theorem*, (Boston, MA, 1995), pp. 447–461, Springer-Verlag, New York, 1997.

[Sil1] J. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, 106. Springer-Verlag, New York, 1986.

[Sil2] ———, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, 151. Springer-Verlag, New York, 1994.

[Ta] J. Tate, *Classes d'isogénie des variétes abéliennes sur un corps fini (d'après T. Honda)*, Seminaire Bourbaki **352** (1968).

[T-W] R. Taylor and A. Wiles, *Ring theoretic properties of certain Hecke algebras*, Ann. of Math (3) **141** (1995), 553–572.

[v-Wa] B.L. van der Waerden, *Algebra*, Volume 1, Springer-Verlag, New York, 1991.

[Wi] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Annals of Math (3) **141** (1995), 443–551.

Department of Pure Mathematics and Mathematical Statistics, 16, Mill Lane, Cambridge CB2 1SB, U.K.

E-mail address: J.Manoharmayum@dpmms.cam.ac.uk