Tame Galois realizations of $\mathrm{GL}_2(\mathbb{F}_\ell)$ over $\mathbb{Q}$[1]

Sara Arias-de-Reyna and Núria Vila [2]

Abstract

This paper concerns the tame inverse Galois problem. For each prime number ℓ we construct infinitely many semistable elliptic curves over $\mathbb{Q}$ with good supersingular reduction at ℓ. The Galois action on the ℓ-torsion points of these elliptic curves provides tame Galois realizations of $\mathrm{GL}_2(\mathbb{F}_\ell)$ over $\mathbb{Q}$.

Keywords: Tame ramification; Galois extension; Supersingular elliptic curve.

1 Introduction

Assume that a certain finite group G can be realized as a Galois group over $\mathbb{Q}$, say $G \simeq \mathrm{Gal}(K/\mathbb{Q})$ with $K/\mathbb{Q}$ a finite Galois extension, i.e. the inverse Galois problem over $\mathbb{Q}$ has an affirmative answer for the group G. One might wonder whether, in addition, there exist extensions $K/\mathbb{Q}$ with some prescribed ramification properties. In this regard, B. Birch [2] posed the following question, known as the tame inverse Galois problem:

Problem 1.1. Given a finite group G, is there a tamely ramified normal extension $K/\mathbb{Q}$ such that $\mathrm{Gal}(K/\mathbb{Q}) \simeq G$?

An affirmative answer to this problem is known for solvable groups, for all symmetric groups S_n, for all alternating groups A_n, and for the Mathieu groups M_{11} and M_{12}, as well as for their finite central extensions (cf. [7], [9], [10]).

Let ℓ be a prime number. It is a classical result that the linear groups $\mathrm{GL}_2(\mathbb{F}_\ell)$ can be realized as Galois groups over the field of rational numbers (cf. [17]). In this paper we address the tame inverse Galois problem when $G = \mathrm{GL}_2(\mathbb{F}_\ell)$.

We will approach this problem by means of the Galois representations attached to the ℓ-torsion points of elliptic curves. Under certain hypotheses, these representations will supply us with tame Galois realizations of $\mathrm{GL}_2(\mathbb{F}_\ell)$. More precisely, we shall need a surjective representation such that the image of the wild inertia subgroups for the different primes p is trivial.

[1] Preprint version. A final version is published in *Journal of Number Theory*, Volume **129**, Issue 5, 1056–1065 (2009).

[2] Dept. d'Àlgebra i Geometria, Universitat de Barcelona, Gran Via de les Corts, Catalanes, 585, 08007 Barcelona, Spain E-mail addresses: ariasdereyna@ub.edu (S. Arias-de-Reyna), nuriavila@ub.edu (N. Vila).

Our results are largely based on the study of the Galois representations attached to the ℓ-torsion points of elliptic curves carried out by J.-P. Serre in [13]. We will also make use of a result of B. Mazur to ensure the surjectivity of the representations (see [8]). When handling supersingular elliptic curves, we have found the paper [3] of J. Brillhart and P. Morton very enlightening.

Our main result provides an affirmative answer to Problem 1.1 when $G = \mathrm{GL}_2(\mathbb{F}_\ell)$.

Theorem 1.2. *For each prime number ℓ, there exist infinitely many finite Galois extensions $K/\mathbb{Q}$, tamely ramified, such that*

$$\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell).$$

Furthermore, we can explicitly produce elliptic curves E such that the extension of $\mathbb{Q}$ obtained by adjoining the coordinates of the ℓ-torsion points of E meets the requirements of Problem 1.1 when $G = \mathrm{GL}_2(\mathbb{F}_\ell)$.

The rest of the paper is organized as follows. In Section 2 we recall some basic aspects of the Galois representations attached to the ℓ-torsion points of a rational elliptic curve and we establish a result that ensures that the corresponding extension provides a tamely ramified realization of $\mathrm{GL}_2(\mathbb{F}_\ell)$ as a Galois group over $\mathbb{Q}$. Section 3 addresses the problem of constructing explicitly, for any prime number $\ell > 2$, an elliptic curve over $\mathbb{Q}$ with good supersingular reduction at ℓ. Section 4 is devoted to the construction of elliptic curves satisfying the conditions of the result in Section 2, using the construction carried out in Section 3. Finally, in Section 5 we present a few examples that illustrate the construction described in Section 4.

Acknowledgements: Research partially supported by MEC grant MTM2006-04895. The first author is also supported by a FPU predoctoral grant AP-20040601 of the MEC.

2 Galois representations attached to the ℓ-torsion points of an elliptic curve

Let ℓ be a prime number. Let $E/\mathbb{Q}$ be an elliptic curve defined over the rational numbers. The action of the absolute Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $E[\ell]$, the group of ℓ-torsion points of the elliptic curve, gives rise to a group homomorphism

$$\varphi_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[\ell]) \simeq \mathrm{GL}_2(\mathbb{F}_\ell).$$

This homomorphism is continuous when we consider the Krull topology on $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and the discrete topology on $\mathrm{GL}_2(\mathbb{F}_\ell)$. Denote by $\mathbb{Q}(E[\ell])$ the finite Galois extension obtained by adjoining to $\mathbb{Q}$ the coordinates of the ℓ-torsion points of E. Since $\mathrm{ker}\varphi_\ell = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(E[\ell]))$, the image of φ_ℓ can be realized as Galois group over $\mathbb{Q}$

$$\mathrm{Im}\varphi_\ell \simeq \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})/\mathrm{ker}\varphi_\ell \simeq \mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}).$$

If φ_ℓ is surjective, we obtain a realization of $\mathrm{Aut}(E[\ell]) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)$ as Galois group over $\mathbb{Q}$.

If $E/\mathbb{Q}$ is a semistable elliptic curve and $\ell \geq 11$, then by results of J.-P. Serre and B. Mazur we know that the Galois representation attached to the ℓ-torsion points of E is surjective. In the rest of the section, we shall only consider semistable elliptic curves. What remains to be done is to find suitable conditions that guarantee that the field extension $\mathbb{Q}(E[\ell])/\mathbb{Q}$ is tamely ramified.

For each prime number p, let us fix an immersion of the absolute Galois group of the field of p-adic numbers into $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Inside the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ we can consider the inertia subgroup $I_p = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_{p,\mathrm{unr}})$ and the wild inertia subgroup $I_{p,\mathrm{w}} = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_{p,\mathrm{t}})$, where $\mathbb{Q}_{p,\mathrm{unr}}$ and $\mathbb{Q}_{p,\mathrm{t}}$ denote the maximal unramified extension and the maximal tamely ramified extension of $\mathbb{Q}_p$, respectively.

A prime p is unramified (respectively tamely ramified) in $\mathbb{Q}(E[\ell])/\mathbb{Q}$ if and only if $\varphi_\ell(I_p) = 1$ (resp. $\varphi_\ell(I_{p,\mathrm{w}}) = 1$).

We are led to the following statement:

Theorem 2.1. *Let $\ell \geq 11$ be a prime number. Let $E/\mathbb{Q}$ be a semistable elliptic curve such that ℓ has good supersingular reduction. Then the extension $\mathbb{Q}(E[\ell])/\mathbb{Q}$ is tamely ramified with Galois group*

$$\mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell).$$

Proof. Since E is semistable and $\ell \geq 11$, the representation φ_ℓ is surjective (cf. Theorem 4 of [8]). It suffices to show that the extension $\mathbb{Q}(E[\ell])/\mathbb{Q}$ is tamely ramified. Let p be a prime number.

Assume first that $p \neq \ell$. If E has good reduction at p, the Néron–Ogg–Shafarevich criterion claims that $\varphi_\ell(I_p) = 1$, and therefore $\varphi_\ell(I_{p,\mathrm{w}})$ is also trivial. If E has multiplicative reduction at p, the result will be proven using Tate curves. Following the notation of [16], Appendix C, § 14, we know that there exists $q \in \mathbb{Q}_p^*$ with p-adic absolute value $|q|_p < 1$, such that E is isomorphic to the Tate curve E_q, either over $\mathbb{Q}_p$ or a unramified quadratic extension of $\mathbb{Q}_p$. In both cases, the action of the inertia group I_p on the ℓ-torsion points of E coincides with the action on the ℓ-torsion points of E_q. But the ℓ-torsion points of E_q satisfy the following short exact sequence of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-modules:

$$1 \to \mu_\ell \to E_q[\ell] \to \mathbb{Z}/\ell\mathbb{Z} \to 0,$$

where μ_ℓ denotes the group of the ℓth roots of unity in $\overline{\mathbb{Q}}_p^*$ and the action of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ on $\mathbb{Z}/\ell\mathbb{Z}$ is trivial (see Appendix A.1.2, p. IV-31 of [15]). Therefore, choosing a suitable basis of $E_q[\ell]$, the image of I_p by the representation φ_ℓ satisfies

$$\varphi_\ell(I_p) \subseteq \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}.$$

That is to say, it is contained in a cyclic group of order ℓ. But since $I_{p,\mathrm{w}}$ is a p-group, the elements of $\varphi_\ell(I_{p,\mathrm{w}})$ have order equal to a power of p. Therefore the image of $I_{p,\mathrm{w}}$ must be trivial.

Suppose now that $p = \ell$. J.-P. Serre has proven that, if E is an elliptic curve defined over the field of p-adic numbers which has good supersingular reduction, then the image of the wild inertia group $I_{p,\mathrm{w}}$ by the representation φ_p is trivial (cf. [13], Proposition 12). This concludes the proof. □

From now on, our aim shall be to find, for each prime $\ell \geq 11$, an elliptic curve satisfying the hypotheses of Theorem 2.1.

Remark 2.2. The most delicate point when we try to ensure that the extension $\mathbb{Q}(E[\ell])/\mathbb{Q}$ is tamely ramified is the control of the ramification at the prime $p = \ell$. In Theorem 2.1, this control is achieved by requiring that the reduction at the prime be good and supersingular.

Let us fix an elliptic curve $E/\mathbb{Q}$ without complex multiplication. J.-P. Serre has proven that the set of primes having good supersingular reduction has density zero (see [12], § 3.4, Corollary 1). However, according to N.D. Elkies [6], this set is infinite. In any case, it seems that, given an elliptic curve, in this way we can prove only for few primes that the realization of φ_ℓ obtained will be tamely ramified. Thus, a study of the ramification in the case of ordinary reduction might seem advisable. However, in a note to [13] (Note 1 to n° 94, p. 706 of [14]), Serre states that it might seem reasonable to think that the density of the set of primes of good ordinary reduction such that the wild inertia group acts trivially is also zero.

3 Supersingular elliptic curves

In this section we construct, for each prime number $\ell > 2$, an elliptic curve $E/\mathbb{Q}$ with good supersingular reduction at ℓ. We first recall some results on supersingular elliptic curves over a finite field, and then describe an explicit construction. Let us denote by $\overline{\mathbb{F}}_\ell$ an algebraic closure of $\mathbb{F}_\ell$.

We start by recalling a characterization of supersingular elliptic curves over a finite field of characteristic ℓ in terms of the Deuring polynomial, which is defined by the following expression:

$$H_\ell(x) = \sum_{k=0}^{\frac{\ell-1}{2}} \binom{\frac{\ell-1}{2}}{k} x^k.$$

Proposition 3.1. *Let ℓ be an odd prime number. Let $\lambda \in \overline{\mathbb{F}}_\ell$, $\lambda \neq 0, 1$, and let us consider the elliptic curve E defined over $\overline{\mathbb{F}}_\ell$ by the equation in Legendre form $y^2 = x(x-1)(x-\lambda)$. Then E is supersingular if and only if $H_\ell(\lambda) = 0$.*

Proof. See [16], Chapter V, Theorem 4.1. □

Let us bear in mind that we are looking for an elliptic curve E, defined over $\mathbb{Q}$, such that its reduction modulo ℓ is a supersingular elliptic curve. Therefore, the j-invariant of E must belong to $\mathbb{Q}$, and consequently the j-invariant of the reduction must lie in $\mathbb{F}_\ell$. Our problem is therefore to find a root λ of $H_\ell(x)$ such that the elliptic curve given by the equation $y^2 = x(x-1)(x-\lambda)$ has j-invariant in $\mathbb{F}_\ell$.

Remark 3.2. Assume that ℓ is a prime congruent to 3 modulo 4, so that $\frac{\ell-1}{2}$ is odd. Then $H_\ell(x)$ contains an even number of terms, namely $\frac{\ell-1}{2} + 1$. Besides, they can be paired in the following way:

$$\binom{\frac{\ell-1}{2}}{k}^2 x^k \text{ and } \binom{\frac{\ell-1}{2}}{\frac{\ell-1}{2} - k} x^{\frac{\ell-1}{2}-k}.$$

Since $\frac{\ell-1}{2}$ is odd, $(-1)^k$ and $(-1)^{\frac{\ell-1}{2}-k}$ have opposite signs, hence $H_\ell(-1)=0$. Therefore Proposition 3.1 implies that the elliptic curve defined over $\mathbb{F}_\ell$ by the equation $y^2 = x(x-1)(x+1)$ is a supersingular elliptic curve whenever ℓ is congruent to $3 \pmod 4$.

In the general case, however, things are less simple. To begin with, if $\ell \equiv 1 \pmod 4$, $H_\ell(x)$ has no linear factors over $\mathbb{F}_\ell$ (see [3], Theorem 1-(a)). We need some knowledge of the roots of the Deuring polynomial. Let us recall the following well-known facts (see for instance Theorem 4.1-(c) of Chapter V of [16] and Proposition 2.2 of [[1]):

Proposition 3.3. *Let ℓ be an odd prime number.*

- *The roots of $H_\ell(x)$ are simple.*
- *The roots of $H_\ell(x)$ lie in $\mathbb{F}_{\ell^2}$.*

Since the roots of $H_\ell(x)$ are at most in $\mathbb{F}_{\ell^2}$, $H_\ell(x)$ splits in linear and quadratic factors over $\mathbb{F}_\ell$. Proposition 6 of [3] gives us a characterization of the factors that will yield an elliptic curve with j-invariant in $\mathbb{F}_\ell$:

Proposition 3.4. . *Let $\ell > 3$ be a prime number. The j-invariant of the supersingular elliptic curve defined by the Legendre equation $y^2 = x(x-1)(x-\lambda)$ lies in $\mathbb{F}_\ell$ if and only if λ is an element of $\mathbb{F}_\ell$, or else it is quadratic over $\mathbb{F}_\ell$ satisfying that either its norm is equal to 1, or its trace is equal to 1, or its norm and trace are equal to each other.*

We will now focus on factors of the form $x^2 - x + a$, that is, factors with trace equal to 1 (as a matter of fact, if we find an irreducible quadratic factor of this form, we can easily produce quadratic factors of the other two types: see the proof of Theorem 1-(a, b) of [3]). In [4], L. Carlitz studies the divisibility of $H_\ell(x)$ by certain factors of this form (for instance, he proves that the factor $x^2 - x + 1$ divides $H_\ell(x)$ if $(-3/\ell) = -1$, see Theorem 16 of [4]). But we will not fix the value of a in the expression $x^2 - x + a$; for us it will suffice to know that there exists a factor of this form, which can be computed effectively. J. Brillhart and P. Morton have counted the number of factors of this form that divide $H_\ell(x)$ (see Theorem 1-(b) of [3]).

Theorem 3.5. . *Let $\ell > 3$ be a prime number. The number of monic irreducible quadratic factors of $H_\ell(x)$ having middle coefficient -1 is*

$$N_2 = \begin{cases} h(-\ell)/2 & \textit{if } \ell \equiv 1 \pmod 4, \\ (3h(-\ell)-1)/2 & \textit{if } \ell \equiv 3 \pmod 8, \\ (h(-\ell)-1)/2 & \textit{if } \ell \equiv 7 \pmod 8, \end{cases}$$

where $h(-\ell)$ denotes the class number of $\mathbb{Q}(\sqrt{-\ell})$.

Corollary 3.6. . *Let $\ell > 3$ be a prime. There exists $a \in \mathbb{F}_\ell$ such that $x^2 - x + a$ divides $H_\ell(x)$.*

Proof. Since $h(-\ell) \geq 1$, it is obvious from the previous theorem that whenever $\ell \equiv 1 \pmod 4$ or $\ell \equiv 3 \pmod 8$ the number of monic irreducible quadratic factors of $H_\ell(x)$ having middle coefficient -1 is strictly greater than 0. Trouble may arise when $\ell \equiv 7 \pmod 8$ and $h(-\ell) = 1$. But the only prime which satisfies these two conditions is $\ell = 7$. Yet $H_7(x) = (x+1)(x+3)(x+5)$, and the product of the two factors $(x+1)(x+5)$ yields $x^2 - x + 5$, which has the desired form. □

Provided we have a factor of $H_\ell(x)$ of the form $x^2 - x + a$, what we are trying to do is to give a Weierstrass equation such that, after a change of coordinates, we can write it in Legendre form $y^2 = x(x-1)(x-\lambda)$, where λ is a root of this factor of $H_\ell(x)$, that is,

$$\lambda = \frac{1}{2} \pm \frac{\sqrt{1-4a}}{2}.$$

Let us consider a Weierstrass equation of the form

$$y^2 = (x - e_1)(x - e_2)(x - e_3),$$

and let us try to determine e_1, e_2, e_3 so that this equation satisfies the condition above.

A change of coordinates yields a Weierstrass equation in Legendre form, with $\lambda = (e_3 - e_1)/(e_2 - e_1)$. Since we know that, in general, λ does not lie in $\mathbb{F}_\ell$, we cannot expect to find e_1, e_2, e_3 all in $\mathbb{F}_\ell$. Instead, we shall assume one of them lies in $\mathbb{F}_{\ell^2}$. Proposition 3.3 implies that one of the others is its conjugate, and that the remaining one does lie in $\mathbb{F}_\ell$.

Taking all this into account, we look for b, c, $d \in \mathbb{F}_\ell$, such that the equation

$$y^2 = (x-b)(x-(c+\theta))(x-(c-\theta)) \tag{3.1}$$

where $\theta \in \mathbb{F}_{\ell^2}$ satisfies $\theta^2 + d = 0$, defines an elliptic curve with $\lambda = \frac{1}{2} \pm \frac{\sqrt{1-4a}}{2}$.

Proposition 3.7. *Let $\ell > 3$ be a prime number, and let $a \in \mathbb{F}_\ell$ be such that the polynomial $x^2 - x + a$ divides the Deuring polynomial $H_\ell(x)$. If b, c, $d \in \mathbb{F}_\ell$ satisfy*

$$d = 4a - 1,$$
$$b = c + (4a - 1)$$

then the equation

$$y^2 = x^3 - (b+2c)x^2 + (2bc + c^2 + d)x - (bc^2 + bd) \tag{3.2}$$

defines a supersingular elliptic curve over $\mathbb{F}_\ell$.

Proof. Note that the discriminant of (3.2) is $\Delta = -64d((b-c)^2 + d)^2$, which is different from zero. Indeed, if $d = 0$, we would have that $4a - 1 = 0$, and therefore $x^2 - x + a = x^2 - x + 1/4 = (x - 1/2)^2$, which has a double root, in contradiction to Proposition 3.3. If $(b-c)^2 + d = 0$, then $4a(4a-1) = 0$, and hence either $a = 1/4$ (which cannot happen, as we have just seen) or $a = 0$. But then $x^2 - x$ would divide $H_\ell(x)$, and zero is never a root of the Deuring polynomial.

Finally, (3.2) can be written as (3.1). Hence we can express the curve defined by (3.2) in Legendre form with $\lambda = \frac{1}{2} + \frac{b-c}{2\theta} = \frac{1}{2} \pm \frac{\sqrt{1-4a}}{2}$. Therefore λ is a root of $x^2 - x + a$. Thus we conclude that $H_\ell(\lambda) = 0$, and Proposition 3.1 implies that the elliptic curve defined by (3.2) is a supersingular elliptic curve. □

Remark 3.8. . Given a prime $\ell > 3$, let b, c, $d \in \mathbb{F}_\ell$ be as above. Then, lifting these coefficients to $\mathbb{Z}$, we obtain a Weierstrass equation, defined over $\mathbb{Q}$, such that reducing modulo ℓ we obtain the supersingular elliptic curve given in Proposition 3.7.

4 Explicit construction

In this section we will construct, for each prime number ℓ, an elliptic curve such that the Galois representation attached to the group of ℓ-torsion points provides us with a tame realization of $\mathrm{GL}_2(\mathbb{F}_\ell)$ as Galois group over $\mathbb{Q}$. We will first assume that $\ell \geq 11$, so that we can apply Theorem 2.1. The primes 2, 3, 5, and 7 will be considered at the end of the section.

Let us fix a prime $\ell \geq 11$. We shall start by stating the problem we wish to solve, taking into account the contents of Theorem 2.1.

Problem 4.1. Find a_1, a_2, a_3, a_4, $a_6 \in \mathbb{Q}$ such that:

- The Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{4.3}$$

  has a nonzero discriminant, and therefore defines an elliptic curve.

- The elliptic curve defined by (4.3) is semistable.

- The elliptic curve defined by (4.3) has good supersingular reduction at the prime ℓ.

In what follows, we will replace the conditions that appear in Problem 4.1 by others which are more restrictive but also more convenient for us. First of all, we shall look for a_1, a_3, a_2, a_4, $a_6 \in \mathbb{Z}$. This will allow us to control the behavior of the different primes p by requiring the coefficients of the equation to satisfy certain congruences modulo p.

Section 3 dealt with the last condition, so let us now tackle the semistability condition. The kind of reduction modulo p of a curve defined by a Weierstrass equation over $\mathbb{Z}$, minimal with respect to the p-adic valuation, can easily be classified in terms of the quantities c_4 and Δ (their expressions can be found in [16], Chapter III, §1).

According to Section 3, it is clear that when $\ell \equiv 3 \pmod 4$ one can give a simpler construction, so we treat it first and then turn to the general case.

Assume therefore that $\ell \equiv 3 \pmod 4$. We will determine a value $\lambda \in \mathbb{Z}$ such that the equation

$$y^2 = x(x-1)(x-\lambda) \tag{4.4}$$

satisfies the conditions in Problem 4.1. From Remark 3.2 it follows that the last condition will be satisfied provided we require $\lambda \equiv -1 \pmod{\ell}$. Now, $if p \neq 2$, (4.4) is a minimal Weierstrass equation, and further the reduction of E at p is either good or multiplicative, since p cannot divide both Δ and c_4. Thus in order to ensure semistability we just have to control the prime $p = 2$. We must change coordinates to obtain a minimal Weierstrass equation with respect to the 2-adic valuation. Let us consider the following one:

$$\begin{cases} x = 2^2x' + r, \\ y = 2^3y' + 2^2sx' + t, \end{cases} \tag{4.5}$$

where $r,\ s,\ t \in \mathbb{Q}$. If we choose $r,\ s,\ t$ so that the new equation has coefficients in $\mathbb{Z}$, it will be a minimal Weierstrass equation, and moreover the reduction at $p = 2$ will either be good or multiplicative, since the quantity c_4 attached to the new equation will be odd. To ensure that the coefficients of the new equation are integers we just have to solve the following congruence system:

$$\begin{cases} t \equiv 0 \pmod{4}, \\ 1 + \lambda - 3r + s^2 \equiv 0 \pmod{4}, \\ -\lambda + 2r + 2\lambda r - 3r^2 + 2st \equiv 0 \pmod{16}, \\ -\lambda r + r^2 + \lambda r^2 - r^3 + t^2 \equiv 0 \pmod{64}. \end{cases}$$

Let us choose $r = s = 1, t = 0$. Then the system reduces to the single equation $\lambda \equiv 1 \pmod{16}$. We have thus solved Problem 4.1 whenever $\ell \equiv 3 \pmod{4}$:

Proposition 4.2. *Let $\ell \geq 11$ be a prime number such that $\ell \equiv 3 \pmod{4}$, and let $\lambda \in \mathbb{Z}$ be such that*

- $\lambda \equiv -1 \pmod{\ell}$*;*
- $\lambda \equiv 1 \pmod{16}$.

Then the equation $y^2 = x(x-1)(x-\lambda)$ satisfies the conditions of Problem 4.1.

Let us now consider any prime $\ell \geq 11$. In order to make it easier to deal with the supersingularity condition applying Proposition 3.7, we shall look for a Weierstrass equation of the shape

$$y^2 = (x-b)\left(x - (c + i\sqrt{d})\right)\left(x - (c - i\sqrt{d})\right) \tag{4.6}$$

where b, c, $d \in \mathbb{Z}$. Our aim is to find some conditions that assure us that it defines a semistable elliptic curve.

A direct calculation yields that $\Delta = -64d((b-c)^2 + d)^2$ and $c_4 = 16((b-c)^2 - 3d)$. The conditions on b, c, d that we will require in Theorem 4.4 to enable us to apply Proposition 3.7 shall in particular imply that Δ is different from zero.

If an odd prime p divides both Δ and c_4, then it would have to divide $b - c$ and d. So to guarantee that the curve is semistable at all odd primes p, we must require that the greatest common divisor of $b - c$ and d be a power of two.

Again, the strategy to deal with $p = 2$ is to find a suitable change of variables, so as to obtain an equation where one of the new quantities c_4 or Δ is odd. This assures us that it is minimal at 2, and that the elliptic curve it defines is semistable at 2. The idea to perform this is the following:

Remark 4.3. . Let us take any elliptic curve given by an equation of the form

$$y^2 = (x - b_0)\left(x - (c_0 + i\sqrt{d_0})\right)\left(x - (c_0 - i\sqrt{d_0})\right),$$

and satisfying that there exists a change of variables, preserving the Weierstrass form, that yields a new equation such that the quantity Δ' (or else c_4') attached to it is odd. Then if we require b, c, d to be congruent to b_0, c_0, d_0 modulo a high enough power of 2, the elliptic curve defined by (4.6) will be semistable at 2. The reason why this holds is simply that the same change of variables, applied to (4.6), will yield an equation such that the quantity Δ' (or else c_4') attached to it is odd.

Let us consider the curve 17A1 from Cremona Tables [5],

$$y^2 + xy + y = x^3 - x^2 - x - 14. \tag{4.7}$$

This curve is semistable, and has good reduction at every prime different from 17. The discriminant of this equation is $\Delta = -83521$, which is odd. Therefore, this is a minimal model for $p \neq 2$. Through a change of variables, we can transform this equation into

$$y^2 = x^3 - 3x^2 - 8x - 880 = (x - 11)\left(x^2 + 8x + 80\right) \tag{4.8}$$

which has the desired shape with $b_0 = 11$, $c_0 = -4$, $d_0 = 64$. The change of variables from (4.8) to (4.7) is the following:

$$\begin{cases} x = 4x', \\ y = 8y' + 4x' + 4. \end{cases}$$

If we apply this change of variables to (4.6), we see that we must require b, c, d to be congruent to b_0, c_0, d_0 modulo $2 \cdot 64 = 128$. In this way, we will be certain that all coefficients are integers, and moreover of the same parity than those of (4.7).

The previous reasoning, together with Corollary 3.6 and Proposition 3.7, enables us to solve Problem 4.1:

Theorem 4.4. . *Let $\ell \geq 11$ be a prime number. Assume $a \in \mathbb{Z}$ is such that, if $\overline{a}$ denotes its reduction modulo ℓ, the factor $x^2 - x + \overline{a}$ divides the Deuring polynomial $H_\ell(x)$ in $\mathbb{F}_\ell[x]$.*

Let us pick b, c, $d \in \mathbb{Z}$ satisfying:

- *$b - c$ and d are relatively prime,*
- *$b - c \equiv 4a - 1 \pmod{\ell}$, $d \equiv 4a - 1 \pmod{\ell}$,*
- *$b \equiv 11 \pmod{128}$, $c \equiv -4 \pmod{128}$, $d \equiv 64 \pmod{128}$.*

Then the equation

$$y^2 = x^3 - (b + 2c)x^2 + (2bc + c^2 + d)x - (bc^2 + bd) \tag{4.9}$$

defines a semistable elliptic curve with good supersingular reduction at ℓ.

Note that this theorem gives an explicit construction of infinitely many semistable elliptic curves with good supersingular reduction at the prime ℓ.

Remark 4.5. Theorem 4.4 allows us to obtain tame realizations of $\mathrm{GL}_2(\mathbb{F}_\ell)$ provided $\ell \geq 11$. To complete this result, we can take specific curves that yield tame realizations when $\ell = 2$, 3, 5 and 7.

- $\ell = 2$: The curve 19A3 of Cremona Tables [5] is semistable, has good supersingular reduction at 2, and the Galois representation attached to its group of 2-torsion points is surjective (cf. [11], Theorem 3.2).
- $\ell = 3$: The curve 17A1 of Cremona Tables [5] is semistable, has good supersingular reduction at 3, and the Galois representation attached to its group of 3-torsion points is surjective (cf. [11], Theorem 3.2).
- $\ell = 5$: The curve 14A1 of Cremona Tables [5] is semistable, has good supersingular reduction at 5, and the Galois representation attached to its group of 5-torsion points is surjective (cf. [11], Theorem 3.2).
- $\ell = 7$: The curve 15A1 of Cremona Tables [5] is semistable, has good supersingular reduction at 7, and the Galois representation attached to its group of 7-torsion points is surjective (cf. [11], Theorem 3.2).

Once we have these curves, it is not difficult to construct infinitely many semistable elliptic curves with good supersingular reduction at ℓ, whenever $\ell = 2$, 3, 5, 7, satisfying that the Galois representation attached to the ℓ-torsion points is surjective. Namely, by using Proposition 19 of [13] for $\ell = 5$ and $\ell = 7$, and Proposition 2.1 and Theorem 2.3(iii) of [11] for $\ell = 2$ and $\ell = 3$ respectively, one just has to consider an equation whose coefficients are integers congruent to the coefficients of the examples above modulo a suitable (finite) set of primes. Thus as a consequence of Theorems 2.1, 4.4 and Remark 4.5, we are able to state the following result.

Theorem 4.6. *For each prime number ℓ, there exist infinitely many elliptic curves $E/\mathbb{Q}$ such that the Galois extension $\mathbb{Q}(E[\ell])/\mathbb{Q}$ is tamely ramified with Galois group $\mathrm{GL}_2(\mathbb{F}_\ell)$.*

In this way we prove Theorem 1.2, which was stated in the introduction. Note that Theorem 4.4 and Remark 4.5 give us infinitely many tamely ramified Galois extensions $K/\mathbb{Q}$ with Galois group $\mathrm{GL}_2(\mathbb{F}_\ell)$.

5 Examples

The aim of this section is to display a few examples of elliptic curves, obtained by the method we have presented, that provide a tame realization of $\mathrm{GL}_2(\mathbb{F}_\ell)$ for several prime numbers ℓ.

Example 5.1. . Let us consider the prime $\ell = 11$. Since $11 = 4{\cdot}2{+}3$, we can make use of Proposition 4.2. That is to say, we must pick $\lambda \in \mathbb{Z}$ such that $\lambda \equiv -1 \pmod{11}$ and $\lambda \equiv 1 \pmod{16}$. The smallest positive integer satisfying these conditions is $\lambda = 65$. Hence the curve E defined by the equation

$$y^2 = x(x-1)(x-65) \tag{5.10}$$

is a semistable elliptic curve and has good supersingular reduction at $\ell = 11$. Indeed, this curve is the one labelled 130B2 in Cremona Tables [5]: thus, it is semistable (its conductor equals $2 \cdot 5 \cdot 13$) and we can easily check that the reduction at 11 is supersingular. Theorem 2.1 implies that the Galois extension $\mathbb{Q}(E[11])/\mathbb{Q}$ yields a tame realization of $\mathrm{GL}_2(\mathbb{F}_{11})$ as Galois group over $\mathbb{Q}$.

Example 5.2. . Let us consider the prime $\ell = 13$. According to Theorem 4.4, the first step is to find a. We compute the Deuring polynomial,

$$H_{13}(x) = (x^2+4x+9)(x^2+7x+1)(x^2+12x+3).$$

Since the factor $x^2+12x+3$ divides $H_{13}(x)$, we may take $a = 3$.

Therefore, we have to select b, c, $d \in \mathbb{Z}$ such that $\gcd(b-c, d) = 1$, $b \equiv 11 \pmod{128}$, $c \equiv -4 \pmod{128}$, $d \equiv 64 \pmod{128}$, $b \equiv c + 11 \pmod{13}$, $d \equiv 11 \pmod{13}$.

For instance, we may take $c = -4$, $b = 267$, $d = 960$, and the elliptic curve E we obtain is

$$y^2 = x^3 - 259x^2 - 1160x - 260592.$$

This is a semistable elliptic curve (its conductor is $N = 3 \cdot 5 \cdot 47 \cdot 1583$), and it has good supersingular reduction at 13. Now Theorem 2.1 enables us to claim that the Galois extension $\mathbb{Q}(E[13])/\mathbb{Q}$ gives rise to a tame realization of $\mathrm{GL}_2(\mathbb{F}_{13})$ as Galois group over $\mathbb{Q}$.

Example 5.3. . Let us consider the prime $\ell = 17$. First of all, we must find a value for a (cf. Theorem 4.4). Computing the Deuring polynomial, we obtain

$$H_{17}(x) = (x^2+x+16)(x^2+14x+1)(x^2+16x+1)(x^2+16x+16).$$

Both factors $x^2+16x+1$ and $x^2+16x+16$ divide $H_{17}(x)$, so we can take either $a = 1$ or $a = -1$. Let us pick $a = -1$.

Therefore, we have to select b, c, $d \in \mathbb{Z}$ such that $\gcd(b-c, d) = 1$, $b \equiv 11 \pmod{128}$, $c \equiv -4 \pmod{128}$, $d \equiv 64 \pmod{128}$, $b \equiv c - 5 \pmod{17}$, $d \equiv -5 \pmod{17}$. For example, let us choose $c = -4$, $b = 1419$, $d = 1984$. We obtain the elliptic curve E defined by

$$y^2 = x^3 - 1411x^2 - 9352x - 2838000.$$

This is a semistable elliptic curve (its conductor is $N = 7 \cdot 31 \cdot 289559$), and it has good supersingular reduction at 17. Applying Theorem 2.1, we conclude that the Galois extension $\mathbb{Q}(E[17])/\mathbb{Q}$ provides a tame realization of $\mathrm{GL}_2(\mathbb{F}_{17})$ as Galois group over $\mathbb{Q}$.

References

[1] R. Auer, J. Top, *Legendre elliptic curves over finite fields*, J. Number Theory **95** (2) (2002) 303–312.

[2] B. Birch, *Noncongruence subgroups, covers and drawings*, in: Leila Schneps (Ed.), *The Grothendieck Theory of Dessins d'Enfants*, Cambridge Univ. Press, 1994, pp. 25–46.

[3] J. Brillhart, P. Morton, *Class numbers of quadratic fields, Hasse invariants of elliptic curves, and the supersingular polynomial*, J. Number Theory **106** (1) (2004) 79–111.

[4] L. Carlitz, *Congruence properties of special elliptic functions*, Monatsh. Math. **58** (1954) 77–90.

[5] J.E. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge Univ. Press, 1992.

[6] N.D. Elkies, *The existence of infinitely many supersingular primes for every elliptic curve over* $\mathbb{Q}$, Invent. Math. **89** (3) (1987) 561–567.

[7] J. Klüners, G. Malle, *Counting nilpotent Galois extensions*, J. Reine Angew. Math. **572** (2004) 1–26.

[8] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978) 129–162.

[9] B. Plans, *Central embedding problems, the arithmetic lifting property, and tame extensions of* $\mathbb{Q}$, Int. Math. Res. Not. **23** (2003) 1249–1267.

[10] B. Plans, N. Vila, *Tame A_n-extensions of* $\mathbb{Q}$, J. Algebra **266** (1) (2003) 27–33.

[11] A. Reverter, N. Vila, *Images of mod p Galois representations associated to elliptic curves*, Canad. Math. Bull. **44** (3) (2001) 313–322.

[12] J.-P. Serre, *Groupes de Lie ℓ-Adiques Attachés aux Courbes Elliptiques*, in: Colloque de Clermont-Ferrand, IHES, 1964.

[13] J.-P. Serre, *Proprietes galoisiénnés des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972) 259–331.

[14] J.-P. Serre, *Oeuvres*, vol. III, 1972–1984, Springer-Verlag, Berlin, 1986.

[15] J.-P. Serre, *Abelian ℓ-Adic Representations and Elliptic Curves*, Addison–Wesley Publishing Company, 1989.

[16] J. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math., vol. **106**, Springer, 1986.

[17] H. Weber, *Lehrbuch der Algebra III*, Vieweg, Braunschweig, 1908.