Proceedings of the London Mathematical Society Advance Access published March 24, 2011

doi:10.1112/plms/pdr001

One-parameter families of elliptic curves over $\mathbb{Q}$ with maximal Galois representations

Alina-Carmen Cojocaru, David Grant and Nathan Jones

Abstract

Let E be an elliptic curve over $\mathbb{Q}$ and let $\mathbb{Q}(E[n])$ be its nth division field. In 1972, Serre showed that if E is without complex multiplication, then the Galois group of $\mathbb{Q}(E[n])/\mathbb{Q}$ is as large as possible, that is, $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, for all integers n coprime to a constant integer $m(E,\mathbb{Q})$ depending (at most) on $E/\mathbb{Q}$. Serre also showed that the best one can hope for is to have $|\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) : \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})| \leqslant 2$ for all positive integers n. We study the frequency of this optimal situation in a one-parameter family of elliptic curves over $\mathbb{Q}$, and show that in essence, for almost all one-parameter families, almost all elliptic curves have this optimal behavior.

Contents

1. *Introduction*

Let E be an elliptic curve defined over $\mathbb{Q}$, without complex multiplication (that is, no complex multiplication over an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$). For an integer $n \geqslant 1$, let $E[n]$ denote the nth division group of E over $\overline{\mathbb{Q}}$ and let $\mathbb{Q}(E[n])$ denote the nth division field of E. The Galois group $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $E[n]$ and, after a choice of a $\mathbb{Z}/n\mathbb{Z}$-basis for $E[n]$, gives rise to an embedding $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \hookrightarrow \mathrm{Aut}(E[n]) \simeq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$.

Serre's Open Image Theorem [**29**] states that there exists a positive constant $c(E,\mathbb{Q})$, depending on $E/\mathbb{Q}$, such that $|\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}) : \mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q})| = 1$ for all primes $\ell \geqslant c(E,\mathbb{Q})$. Consequently, there exists a constant $m(E,\mathbb{Q})$ such that $|\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) : \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})| = 1$ for all integers n coprime to $m(E,\mathbb{Q})$ (see [**6**, Appendix] and the references therein, as well as [**13**]).[†]

Received 5 June 2010; revised 25 October 2010.

2000 *Mathematics Subject Classification* 11G05, 11F80, 11G30.

Alina-Carmen Cojocaru's work on this material was partially supported by the National Science Foundation under agreements No. DMS-0747724 and No. DMS-0635607. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

[†] Note that the integer $m(E,\mathbb{Q})$ may be defined in several ways. For instance, in [**6**], Cojocaru and Kani consider the integer $A(E/\mathbb{Q}) := 2 \times 3 \times 5 \times \prod_{\substack{\ell \text{ exceptional} \\ \ell < c(E,\mathbb{Q})}} \ell$, which they call 'Serre's constant associated to $E/\mathbb{Q}$', and which has the property that $|\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) : \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})| = 1$ for all integers n coprime to $A(E/\mathbb{Q})$. In [**13**], Jones considers the smallest integer $m = m_{E/\mathbb{Q}}$ such that, for every $n \geqslant 1$, $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) = \pi^{-1}(\mathrm{Gal}(\mathbb{Q}(E[\gcd(n,m)])/\mathbb{Q}))$, where $\pi : \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/\gcd(n,m)\mathbb{Z})$ is the canonical projection. The integer $m_{E/\mathbb{Q}}$, which Jones calls the 'torsion conductor of $E/\mathbb{Q}$', also has the property that $|\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) : \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})| = 1$ for all integers n coprime to $m_{E/\mathbb{Q}}$, and is always at least the square-free part of the

Serre's theorem suggests the following definition (already introduced by Lang and Trotter in [20]).

DEFINITION 1. For an elliptic curve $E/\mathbb{Q}$, we say that a positive integer n is *exceptional* if

$$|\operatorname{GL}_2(\mathbb{Z}/n\mathbb{Z}) : \operatorname{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})| > 1.$$

Serre showed that there is no $E/\mathbb{Q}$ such that $|\operatorname{GL}_2(\mathbb{Z}/n\mathbb{Z}) : \operatorname{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})| = 1$ for all $n \geqslant 1$. Indeed, as detailed in [31, pp. 310–311] (see also [15, Section 5]), the best one can hope for is $|\operatorname{GL}_2(\mathbb{Z}/n\mathbb{Z}) : \operatorname{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})| \leqslant 2$ for all $n \geqslant 1$. This prompts the following definition.

DEFINITION 2. An elliptic curve $E/\mathbb{Q}$ is called a *Serre curve* if

$$|\operatorname{GL}_2(\mathbb{Z}/n\mathbb{Z}) : \operatorname{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})| \leqslant 2,$$

for all $n \geqslant 1$.

Note that a Serre curve has no exceptional *primes*. In Corollary 8 of Section 3, we give a characterization of a Serre curve in terms of its exceptional numbers.

A few examples of Serre curves may be found in [29, 20]; for instance, $y^2 + y = x^3 - x$ and $y^2 + y = x^3 + x^2$ are Serre curves. In fact, Serre curves exist in abundance and they are the most common kind that one encounters. As such, they are particularly significant when studying conjectures about elliptic curves over $\mathbb{Q}$, as was done recently in [14]. The purpose of our paper is to show that, *when viewed in one-parameter families, Serre curves form an overwhelming majority* (see Main Theorem). In essence, for almost all one-parameter families, almost all elliptic curves are Serre curves. Before stating our main result, let us discuss prior related work.

An important question related to Serre's Open Image Theorem mentioned earlier, posed already by Serre in [29, 30], is as follows.

SERRE'S UNIFORMITY QUESTION. *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. Can the constant $c(E, \mathbb{Q})$ be made uniform in E?*

An affirmative answer to Serre's Uniformity Question has important applications to solving Fermat-type equations, as illustrated, for example, in [26]. It also immediately implies the uniform boundedness of the torsion group $E(\mathbb{Q})_{\text{tors}}$. Moreover, the question itself is an important and difficult arithmetic problem and is directly related to the study of $\mathbb{Q}$-rational points on various modular curves (see, again, [26] for a brief overview). In this direction, major achievements have been obtained in [1, 22, 24, 28, 29]; the work of [4] points out the main difficulty in completely answering Serre's Uniformity Question. In addition, a weaker version of Serre's Uniformity Question, that of bounding $c(E, \mathbb{Q})$ in terms of invariants of $E/\mathbb{Q}$, has been treated in [6, 18, 21, 30].

The least prime number candidate for $c(\mathbb{Q}) = c(E, \mathbb{Q})$, if it exists, is 41, as Mazur and Swinnerton-Dyer [25] showed that the curve $y^2 + xy + y = x^3 + x^2 - 8x + 6$ is without complex multiplication and has a subgroup of order 37 stabilized by $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Unfortunately, the recent work of [1] does not provide any explicit candidate for $c(\mathbb{Q})$.

---

absolute value of the minimal discriminant of $E/\mathbb{Q}$. While $A(E/\mathbb{Q})$ may be smaller and even uniform in E, $m_{E/\mathbb{Q}}$ varies with $E/\mathbb{Q}$ and encodes more information about the torsion of the curve. For more explanations, see [13, Remark 4].

Let us also remark that an affirmative answer to Serre's Uniformity Question would imply a relatively easy criterion for detecting Serre curves: it would suffice to find $\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})$ for $n = 36$ (see Proposition 4 in Section 3) and for n a prime up to $c(\mathbb{Q})$.

In [9], Duke studied an *average* version of Serre's Uniformity Question and showed that it has an affirmative answer with $c(E, \mathbb{Q}) = 2$ for most elliptic curves $E/\mathbb{Q}$ in a *two-parameter family*. To be precise, let $X > 0$ be a parameter and let

$$\begin{aligned}\mathcal{F}(X) := \{(a,b) \in \mathbb{Z}^2 : \gcd\{a^3, b^2\} \text{ is 12th power free,}\\ y^2 = x^3 + ax + b \text{ an elliptic curve over } \mathbb{Q},\ |a| \leqslant X^2, |b| \leqslant X^3\},\end{aligned}$$

that is, we consider the family of elliptic curves $E_{a,b}/\mathbb{Q} : y^2 = x^3 + ax + b$ with naive height $H(E_{a,b}) := \max\{|a|^3, |b|^2\} \leqslant X^6$. As shown in [3],

$$\#\mathcal{F}(X) \asymp X^5.$$

Let

$$\begin{aligned}\mathcal{E}_n(X) &:= \{(a,b) \in \mathcal{F}(X) :\ E_{a,b} \text{ is exceptional at } n\} \quad (n \geqslant 1),\\ \mathcal{E}_{\text{non-Serre}}(X) &:= \{(a,b) \in \mathcal{F}(X) :\ E_{a,b} \text{ is not a Serre curve}\}.\end{aligned}$$

In [9], Duke showed that there exists a positive constant γ such that, as $X \to \infty$,

$$\#\left(\bigcup_{\ell \geqslant 2} \mathcal{E}_\ell(X)\right) = \mathrm{O}(X^4 \log^\gamma X),$$

where ℓ denotes a prime. The O-constant, though ineffective in Duke's proof, can be made effective (see [35]); the constant γ can also be given explicitly (see [17]).

Duke's result was refined by Grant [10], who showed that, for any $\varepsilon > 0$ and as $X \to \infty$,

$$\#\left(\bigcup_{\ell \geqslant 2} \mathcal{E}_\ell(X)\right) = cX^3 + \mathrm{O}_\varepsilon(X^{2+\varepsilon}),$$

where $c = 2/\zeta(6) + (4\varepsilon_+ + 4\varepsilon_- + 6\log(\varepsilon_-/\varepsilon_+))/3\zeta(6)$, $\zeta(\cdot)$ is the Riemann zeta function, $\varepsilon_\pm$ are the real roots of $x^3 \pm x - 1 = 0$, and the O_ε-constant in the error term is ineffective. Grant's proof shows that the main term in this asymptotic comes from $\mathcal{E}_2(X)$ and $\mathcal{E}_3(X)$.

These results were generalized in two different directions. On the one hand, Jones [15] showed that for most elliptic curves in the above two-parameter family, *all* the nth division fields are as large as possible. More precisely, there exists an (explicit) positive constant γ such that, as $X \to \infty$,

$$\#\mathcal{E}_{\text{non-Serre}}(X) = \mathrm{O}(X^4 \log^\gamma X).$$

As in Duke's result, the O-constant can be made effective. Subsequently, Jones' result was strengthened by Radhakrishnan [27] to the asymptotic

$$\#\mathcal{E}_{\text{non-Serre}}(X) = cX^3 + \mathrm{O}_\varepsilon(X^{2+\varepsilon}),$$

where c is as in Grant's result and the O_ε-constant is ineffective.

On the other hand, Cojocaru and Hall [7] showed that most elliptic curves over $\mathbb{Q}$ in a *one-parameter* family have $c(E, \mathbb{Q}) = 17$, that is, they have no exceptional primes $\ell \geqslant 17$ (see equation (3)).

The purpose of this paper is to refine the above average results and show that almost all elliptic curves in a *one-parameter* family are *Serre curves*. For this, let $E/\mathbb{Q}(t)$ be an elliptic curve defined over $\mathbb{Q}(t)$, given by the Weierstrass equation

$$E : y^2 = x^3 + A(t)x + B(t), \tag{1}$$

where $A(t), B(t) \in \mathbb{Q}[t]$ are fixed polynomials (for which the associated discriminant

$$\Delta_E(t) = -16(4A(t)^3 + 27B(t)^2)$$

is not identically zero) and such that the j-invariant of E

$$j_E(t) := 1728 \cdot \frac{4A(t)^3}{4A(t)^3 + 27B(t)^2}$$

is non-constant, that is, $j_E \notin \mathbb{Q}$. We standardly call such an elliptic curve *non-isotrivial*.

For $T > 0$, let

$$\mathcal{F}_E(T) := \{t_0 \in \mathbb{Q} : \mathcal{H}(t_0) \leqslant T, E_{t_0}/\mathbb{Q} \text{ is an elliptic curve}\}, \tag{2}$$

where $\mathcal{H}(t_0)$ is the Mordell height of t_0 (defined as the maximum of the absolute values of the numerator and denominator of t_0) and E_{t_0} is the specialization of E at t_0. Note that, for all but finitely many $t_0 \in \mathbb{Q}$, E_{t_0} is an elliptic curve. Thus,

$$\#\mathcal{F}_E(T) \asymp T^2.$$

Similarly to the above, let

$$\mathcal{E}_{E,n}(T) := \{t_0 \in \mathcal{F}_E(T) : \ E_{t_0} \text{ is exceptional at } n\} \quad (n \geqslant 1),$$
$$\mathcal{E}_{E,\text{non-Serre}}(T) := \{t_0 \in \mathcal{F}_E(T) : E_{t_0} \text{ is not a Serre curve}\}.$$

In [7], Cojocaru and Hall showed that there exists an explicit positive constant γ such that, as $T \to \infty$,

$$\#\left(\bigcup_{\ell \geqslant 17} \mathcal{E}_{E,\ell}(T)\right) = \mathrm{O}_E(T^{3/2}\log^\gamma T), \tag{3}$$

where the implied O_E-constant depends on the polynomials $A(t), B(t)$ defining E, and, as in Duke's and Jones' aforementioned results, can be made effective.

In this paper, we will show that the order of magnitude of the above set, and, moreover, of $\mathcal{E}_{E,\text{non-Serre}}(T)$, is significantly smaller.

Since Galois groups do not increase under specialization, we need to assume from the start that the family $E/\mathbb{Q}(t)$ has the property that the image of the representation of the absolute Galois group of $\mathbb{Q}(t)$ on $E[n]$ is of index 1 or 2 in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ for all $n \geqslant 1$. Both the situations where this index is 1 for all $n \geqslant 1$ and where this index is 2 for some n can produce families $E/\mathbb{Q}(t)$ whose specializations are almost all Serre curves. However, in order to make notation and arguments less cumbersone, we shall henceforth assume that, for all $n \geqslant 1$,

$$\mathrm{Gal}(\mathbb{Q}(t)(E[n])/\mathbb{Q}(t)) \simeq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}). \tag{4}$$

Now let $\mathcal{X}$ denote the set of modular curves which parameterize non-Serre curves, as defined explicitly in Definition 17 of Section 6.

For $X \in \mathcal{X}$, let

$$C_{X,E} := X \times_{\mathbb{P}^1(j)} \mathbb{P}^1(t)$$

be the fiber product defined by the commutative diagram

$$\begin{array}{ccc} X \times_{\mathbb{P}^1(j)} \mathbb{P}^1(t) & \xrightarrow{\psi_{X,E}} & \mathbb{P}^1(t) \\ \downarrow & & \downarrow{\scriptstyle j_E} \\ X & \xrightarrow{j_X} & \mathbb{P}^1(j), \end{array} \tag{5}$$

where j_E is the map associated to the j-invariant of E, j_X is the j-map attached to X (see Section 6), and the remaining two maps are the canonical projections.

As will be explained in Proposition 20 of Section 6, hypothesis (4), for all $n \geqslant 1$, implies that $C_{X,E}$ are curves over $\mathbb{Q}$ which are irreducible over $\mathbb{Q}$. We then set

$$\mathcal{X}_E^0 := \{X \in \mathcal{X} : C_{X,E} \text{ is absolutely irreducible, has genus } 0, \text{ and } C_{X,E}(\mathbb{Q}) \neq \emptyset\},$$
$$\mathcal{X}_E^1 := \{X \in \mathcal{X} : C_{X,E} \text{ is absolutely irreducible, has genus } 1, \text{ and } C_{X,E}(\mathbb{Q}) \neq \emptyset\}.$$

Finally, we introduce the following definition.

Definition 3. Let $E/\mathbb{Q}(t)$ be a non-isotrivial elliptic curve. The elliptic curve E is called *j-unusual* if there exist a non-singular integral matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and a polynomial $P(t) \in \mathbb{Z}[t]$ such that $j_E(t) = P((at+b)/(ct+d))$. If E is not j-unusual, then it is called *j-usual*.

Main Theorem. *Let $E/\mathbb{Q}(t)$ be a non-isotrivial elliptic curve as in equation (1) such that hypothesis (4) holds for all $n \geqslant 1$. We keep the notation and terminology introduced above.*

(1) *Assume that E is j-usual and let $\varepsilon > 0$.*

(a) *If $\mathcal{X}_E^0 = \emptyset$, then, as $T \to \infty$,*

$$\#\mathcal{E}_{E,\text{non-Serre}}(T) = \mathrm{O}_{E,\varepsilon}(T^{\varepsilon}).$$

(b) *If $\mathcal{X}_E^0 \neq \emptyset$, then there is a positive constant $c(E)$ such that, as $T \to \infty$,*

$$\#\mathcal{E}_{E,\text{non-Serre}}(T) \sim c(E) \cdot T^{2/d_E},$$

where

$$d_E := \min\{\deg \psi_{X,E} : X \in \mathcal{X}_E^0\} \geqslant 2.$$

(2) *Assume that E is j-unusual. Then, for any $\varepsilon > 0$ and as $T \to \infty$,*

$$\#\mathcal{E}_{E,\text{non-Serre}}(T) = \mathrm{O}_{E,\varepsilon}(T^{1+\varepsilon}).$$

Note that, since $\bigcup_{\ell \geqslant 2} \mathcal{E}_{E,\ell}(T) \subseteq \mathcal{E}_{E,\text{non-Serre}}(T)$, our theorem substantially improves upon equation (3).

We conclude the introduction with a few remarks.

Remarks. (1) Hypothesis (4) of the Main Theorem asserts that

$$\forall n \geqslant 1, \quad \mathrm{Gal}(\mathbb{Q}(t)(E[n])/\mathbb{Q}(t)) \simeq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

As we will show in Section 3 (see Proposition 4), this is equivalent to the two assertions

$$\forall n \in \{36\} \cup \{\ell : \ell \text{ prime}, \ 5 \leqslant \ell \leqslant 13\}, \quad \mathrm{Gal}(\mathbb{Q}(t)(E[n])/\mathbb{Q}(t)) \simeq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

and

$$\mathbb{Q}(t)(\sqrt{\Delta_E(t)}) \cap \overline{\mathbb{Q}} = \mathbb{Q}.$$

In particular, equation (4) needs only to be verified for n in a finite set.

(2) By results of Dennin [8], for any fixed g, the set of genus g modular curves, of all levels, is finite. In particular, the sets $\mathcal{X}_E^0$ and $\mathcal{X}_E^1$ are finite; see [5] for the list of all genus 0 modular curves of all levels.

(3) The situation $\mathcal{X}_E^0 = \emptyset$ is the typical one. Indeed, for $X \in \mathcal{X}$, j_X is ramified only at 0, 1, ∞. Using the Riemann–Hurwitz formula, one can then show that if j_E has degree $D_E > 1$ and is unramified over 0, 1, ∞, then the genus of $C_{X,E}$ is positive. Therefore, we consider $\mathcal{X}_E^0 = \emptyset$ the *genus usual* case. Likewise, we consider, when equation (4) holds for all $n \geqslant 1$, the *Galois usual* case. The theorem can be paraphrased by saying that non-Serre curves are extremely

rare in a one-parameter family, unless something unusual happens, namely the family is genus unusual, j-unusual, or Galois unusual. None of these phenomena has to be contended with when studying the two-parameter family of elliptic curves.

(4) Naturally, one may ask what the true order of magnitude of $\#\mathcal{E}_{E,\text{non-Serre}}(T)$ is. An affirmative answer to Serre's Uniformity Question leads to the following prediction.

Let $E/\mathbb{Q}(t)$ be a non-isotrivial elliptic curve such that hypothesis (4) holds for all $n \geqslant 1$.

(a) If $\mathcal{X}_E^0 = \emptyset$ but $\mathcal{X}_E^1 \neq \emptyset$, then

$$\#\mathcal{E}_{E,\text{non-Serre}}(T) \sim c(E)(\log T)^{\rho_E/2},$$

for some positive constant depending on E, where ρ_E is the maximum of the Mordell–Weil ranks of $C_{X,E}$ for $X \in \mathcal{X}_E^1$. If $\rho_E = 0$, we interpret the asymptotic as saying that at most finitely many (depending on E) specializations E_t in our family are non-Serre curves.

(b) If $\mathcal{X}_E^0 = \emptyset$ and $\mathcal{X}_E^1 = \emptyset$, then

$$\#\mathcal{E}_{E,\text{non-Serre}}(T) \leqslant c(E),$$

for some positive constant depending on E.

(c) If $\mathcal{X}_E^0 \neq \emptyset$, then

$$\#\mathcal{E}_{E,\text{non-Serre}}(T) \sim c(E)T^{2/d_E},$$

for some positive constant depending on E, where d_E is the minimum of $\deg \psi_{X,E}$ for $X \in \mathcal{X}_E^0$, which is at least 2.

In particular, we believe our bound is far from best possible in the j-unusual case.

(5) When the one-parameter family of elliptic curves is not galois usual, one can still consider whether almost all specializations have galois representations whose image is as large as possible given this constraint. We call such optimal specializations *relative Serre curves* and study them in [**16**]. Likewise, studying families of elliptic curves over number fields other than $\mathbb{Q}$ requires a more delicate analysis, which we address in a coming paper.

(6) One can view our Main Theorem in the spirit of Hilbert Irreducibility, that for the *infinite* Galois extension $\text{Gal}(\mathbb{Q}(t)(E_{\text{tors}})/\mathbb{Q}(t))$, its geometric specializations are typically as large as the arithmetic of $\mathbb{Q}$ will allow. Note however, that in contrast to Hilbert Irreducibility, we do not have $\text{Gal}(\mathbb{Q}((E_t)_{\text{tors}})/\mathbb{Q}) = \text{Gal}(\mathbb{Q}(t)(E_{\text{tors}})/\mathbb{Q}(t))$ for any specialization.

NOTATION. Throughout the paper, we use the following (standard) notation. The letters ℓ and p denote rational primes. For a non-zero integer m, $\nu(m)$ denotes the number of its distinct prime divisors and $\tau(m)$ the number of its divisors. We write

$$\text{rad}(m) := \prod_{\ell \mid m} \ell,$$

for the radical of m. For a prime p, we let $\mathbb{Z}_p$ and $\mathbb{Q}_p$ denote, respectively, the p-adic integers and numbers, and for any finite extension L of $\mathbb{Q}_p$ whose ring of integers has maximal ideal $\mathfrak{p}$, we let $\text{ord}_{\mathfrak{p}}(x)$ denote the $\mathfrak{p}$-adic valuation of any $x \in L^*$. Given an integer $r \geqslant 1$, we write $c_r(m)$ and $d_r(m)$ for the odd r-full part and r-free part of m, respectively, that is,

$$c_r(m) := \prod_{\substack{\ell \neq 2 \\ \text{ord}_\ell(m) \geqslant r}} \ell^{\text{ord}_\ell(m)}, \quad d_r(m) := \prod_{\substack{\ell \neq 2 \\ \text{ord}_\ell(m) < r}} \ell^{\text{ord}_\ell(m)}.$$

For real-valued functions f and g, with g positive, we write $f = \text{O}(g)$ or $f \ll g$ if there exists a positive constant M such that $|f(x)| \leqslant Mg(x)$ for all x. If $f = \text{O}(g)$ and $g = \text{O}(f)$, then we write $f \asymp g$. We write $f = \text{O}_C(g)$ when the constant M implied in the O-notation depends on another quantity C. If $\lim_{x\to\infty} f(x)/g(x) = 1$, then we write $f \sim g$.

As usual, we let GL_2 and SL_2 denote the 2×2 general linear group and the special linear group, respectively.

2. *Outline of the proof of the Main Theorem*

In this section, we outline the proof of the Main Theorem of the paper. We start by fixing the setting and notation, and continue with a summary of the main steps of the proof.

2.1. *Setting/notation*

Let $E/\mathbb{Q}(t)$ be a non-isotrivial elliptic curve as in equation (1). Throughout the paper, we keep the notation associated to $E/\mathbb{Q}(t)$ introduced in Section 1. In addition, we write

$$j_E(t) = \frac{f(t)}{g(t)} \in \mathbb{Q}(t), \tag{6}$$

where $f(t), g(t) \in \mathbb{Z}[t]$ are such that $f(t)$ and $g(t)$ are relatively prime in $\mathbb{Q}[t]$ and have relatively prime content. We let

$$D_E := \max\{\deg f(t), \deg g(t)\}, \tag{7}$$

that is, D_E is the degree of j_E as a rational map. We let $F(R,S), G(R,S) \in \mathbb{Z}[R,S]$ be the homogeneous polynomials defined by

$$F(R,S) = S^{D_E} f\left(\frac{R}{S}\right), \quad G(R,S) = S^{D_E} g\left(\frac{R}{S}\right). \tag{8}$$

2.2. *Proof outline*

The proof of the Main Theorem can be summarized in four principal steps, as follows. The first step consists of a characterization of a Serre curve in terms of its exceptional integers, which is achieved by means of group theory. In brief, it is stated as follows.

Step 1. For any $T > 0$,

$$\mathcal{E}_{E,\text{non-Serre}}(T) = \mathcal{E}_{E,\text{non-Serre},36}(T) \cup \left(\bigcup_{\ell \geqslant 5} \mathcal{E}_{E,\ell}(T) \right),$$

where

$$\mathcal{E}_{E,\text{non-Serre},36}(T) := \mathcal{E}_{E,\text{non-Serre}}(T) \cap \mathcal{E}_{E,36}(T).$$

This follows from Corollary 8 of Section 3.

The second step consists of embedding the infinite union $\bigcup_\ell \mathcal{E}_{E,\ell}(T)$ into a finite union of similar sets. The underlying idea is that an elliptic curve over $\mathbb{Q}$ with non-integral j-invariant cannot have large exceptional primes. To be precise, let R_0, S_0 denote relatively prime integers, and for an arbitrary fixed integer $r \geqslant 1$, let

$$\mathcal{E}^r_{E,\text{int}}(T) := \left\{ t_0 = \frac{R_0}{S_0} \in \mathcal{F}_E(T) : d_r(G(R_0,S_0)) | F(R_0,S_0) \right\},$$

where $d_r(G(R_0,S_0))$ denotes the odd r-free part of $G(R_0,S_0)$ (see the notation at the end of Section 1). Using Tate's theory of q-curves and Mazur's work on rational isogenies of prime degree, we show the following.

STEP 2. Let $r \geqslant 13$ be an integer. Then, for any $T > 0$,

$$\bigcup_{\ell} \mathcal{E}_{E,\ell}(T) \subset \left(\bigcup_{\ell \leqslant r} \mathcal{E}_{E,\ell}(T) \right) \cup \mathcal{E}^r_{E,\mathrm{int}}(T).$$

This is Corollary 10 of Section 4.

The third step consists of estimating the set $\mathcal{E}^r_{E,\mathrm{int}}(T)$ by using work of Bombieri and Schmidt on the Thue equation, Bezout's theorem, and the theory of norm-form equations in quadratic fields.

STEP 3. We assume that $E/\mathbb{Q}(t)$ is non-isotrivial. Let $\varepsilon > 0$ and let $r = r(E,\varepsilon) := \lceil 3D_E \log(\max\{D_E, 2\})/\varepsilon \log 2 \rceil$. For any $T > 0$, we have:

(1) if $E/\mathbb{Q}(t)$ is j-usual, then

$$\#\mathcal{E}^r_{E,\mathrm{int}}(T) = \mathrm{O}_{E,\varepsilon}(T^{\varepsilon});$$

(2) if $E/\mathbb{Q}(t)$ is j-unusual, then

$$\#\mathcal{E}^r_{E,\mathrm{int}}(T) = \mathrm{O}_{E,\varepsilon}(T^{1+\varepsilon}).$$

This is Corollary 15 of Section 5.

The fourth (and final) step consists of estimating the sets $\mathcal{E}_{E,\text{non-Serre},36}(T)$ and $\mathcal{E}_{E,\ell}(T)$ (for $\ell \leqslant r$) by using the theory of modular curves and results on counting rational points of bounded height on curves. To state the fourth step precisely, we need the following piece of notation: for an integer $r \geqslant 5$, let $\mathcal{X}_r$ denote the subset of $\mathcal{X}$ consisting of curves of prime level $5 \leqslant \ell \leqslant r$ or level $n = 36$, as defined explicitly in Definition 17 of Section 6.

STEP 4. Let $E/\mathbb{Q}(t)$ be a non-isotrivial elliptic curve. Let $r \geqslant 5$ be an integer. We assume that hypothesis (4) holds for any prime n with $5 \leqslant n \leqslant \min\{r, 13\}$ and for $n = 36$. For any $T > 0$, we have:

(1) if $\mathcal{X}_r \cap (\mathcal{X}^0_E \cup \mathcal{X}^1_E) = \emptyset$, then

$$\# \left(\mathcal{E}_{E,\text{non-Serre},36}(T) \cup \left(\bigcup_{5 \leqslant \ell \leqslant r} \mathcal{E}_{E,\ell}(T) \right) \right) = \mathrm{O}_{E,r}(1);$$

(2) if $\mathcal{X}_r \cap \mathcal{X}^0_E = \emptyset$, but $\mathcal{X}_r \cap \mathcal{X}^1_E \neq \emptyset$, then

$$\# \left(\mathcal{E}_{E,\text{non-Serre},36}(T) \cup \left(\bigcup_{5 \leqslant \ell \leqslant r} \mathcal{E}_{E,\ell}(T) \right) \right) \sim c(E)(\log T)^{\rho_{E,r}/2},$$

for some positive constant $c(E)$ depending on E, where $\rho_{E,r}$ is the maximum of the Mordell–Weil ranks of $C_{X,E}/\mathbb{Q}$ for $X \in \mathcal{X}_r \cap \mathcal{X}^1_E$;

(3) if $\mathcal{X}_r \cap \mathcal{X}^0_E \neq \emptyset$, then

$$\# \left(\mathcal{E}_{E,\text{non-Serre},36}(T) \cup \left(\bigcup_{5 \leqslant \ell \leqslant r} \mathcal{E}_{E,\ell}(T) \right) \right) \sim c(E) T^{2/d_{E,r}},$$

for some positive constant $c(E)$ depending on E, where $d_{E,r} := \min\{\deg \psi_{X,E} : X \in \mathcal{X}_r \cap \mathcal{X}^0_E\}$.

This is an immediate consequence of Proposition 20 of Section 6.

The proof of the Main Theorem is completed by combining the above four steps and by noting that $d_{E,r} \geqslant 2$ (see part (2) of Proposition 20 of Section 6).

3. *Serre curves and exceptional numbers*

The goal of this section is to prove Proposition 4, which characterizes a Serre curve in terms of its exceptional numbers, thus proving the claim of Step 1 of Section 2, and which also justifies the first remark after the Main Theorem.

The main result we require is the following theorem, in whose statement we use the standard notation $[G, G] := \langle ghg^{-1}h^{-1} : g, h \in G\rangle$ for the commutator subgroup of a finite group G.

PROPOSITION 4. (a) *An elliptic curve E over $\mathbb{Q}$ is a Serre curve if and only if*

$$\forall n \in \{36\} \cup \{\ell : \ell \text{ prime}, \ \ell \geqslant 5\}, \ [\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}), \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})] = [\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}), \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})].$$

(b) *A non-isotrivial elliptic curve E over $\mathbb{Q}(t)$ satisfies*

$$\mathrm{Gal}(\mathbb{Q}(t)(E[n])/\mathbb{Q}(t)) = \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}), \tag{9}$$

for every positive integer n if and only if:

(A1) *E satisfies equation (9) for $n \in \{36\} \cup \{\ell : \ell \text{ prime}, 5 \leqslant \ell \leqslant 13\}$, and*

(A2) *the extension $\mathbb{Q}(t)(\sqrt{\Delta_E(t)})$ is geometric over $\mathbb{Q}(t)$, that is, $\mathbb{Q}(t)(\sqrt{\Delta_E(t)}) \cap \overline{\mathbb{Q}} = \mathbb{Q}$.*

Proof. For (a), see [16]. For (b), suppose that E is an elliptic curve over $\mathbb{Q}(t)$ satisfying assumptions (A1) and (A2). We adopt a more global viewpoint. Recall that $\hat{\mathbb{Z}}$ denotes the inverse limit of the projective system $\{\mathbb{Z}/n\mathbb{Z} : n \geqslant 1\}$, ordered by divisibility. Under the isomorphism of the Chinese remainder theorem, we have $\hat{\mathbb{Z}} \simeq \prod_\ell \mathbb{Z}_\ell$. Consider the action of $G_{\mathbb{Q}(t)} := \mathrm{Gal}(\overline{\mathbb{Q}(t)}/\mathbb{Q}(t))$ on the torsion subgroup E_{tors} of E over $\overline{\mathbb{Q}(t)}$. If we choose a basis of E_{tors} over $\hat{\mathbb{Z}}$, then this gives a continuous group homomorphism

$$\varphi_E : G_{\mathbb{Q}(t)} \longrightarrow \mathrm{GL}_2(\hat{\mathbb{Z}}),$$

which is related to the division fields by the equation

$$\overline{\mathbb{Q}(t)}^{\ker(\pi_n \circ \varphi_E)} = \mathbb{Q}(t)(E[n]),$$

where $\pi_n : \mathrm{GL}_2(\hat{\mathbb{Z}}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ denotes the canonical projection. Note also that equation (9) holds for every $n \geqslant 1$ if and only if $\varphi_E(G_{\mathbb{Q}(t)}) = \mathrm{GL}_2(\hat{\mathbb{Z}})$. Thus, our goal is to show that $\varphi_E(G_{\mathbb{Q}(t)}) = \mathrm{GL}_2(\hat{\mathbb{Z}})$.

The following theorem restates [7, Theorem 1.1], taking into account the subsequent remark.

THEOREM 5. *Let F be any perfect field, C/F be a proper, smooth, geometrically connected curve, and let $K := F(C)$ be its function field. Then there exists a positive constant $c(K)$, depending at most on the genus of K, such that, for any non-isotrivial elliptic curve E/K and any rational prime $\ell \geqslant c(K)$ with $\ell \neq \mathrm{char}F$, the geometric Galois group of $K(E[\ell])/K$ is $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$. More precisely,*

$$c(K) := 2 + \max\left\{\ell : \ell \text{ prime}, \ \frac{1}{12}[\ell - (6 + 3e_2 + 4e_3)] \leqslant \mathit{genus}\,(K)\right\},$$

where $e_2 = +1$ if $\ell \equiv 1 \bmod 4$ and -1 otherwise, and $e_3 = +1$ if $\ell \equiv 1 \bmod 3$ and -1 otherwise.

To specialize to our situation, we take $F = \mathbb{Q}$ and $C = \mathbb{P}^1$, so that $c(K) = 15$. Thus, we derive the following corollary.

COROLLARY 6. *For any non-isotrivial elliptic curve E defined over $\mathbb{Q}(t)$ and any prime $\ell \geqslant 17$, one has*

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

Given assumption (A1), it follows that we must have equation (9) for $n \in \{36\} \cup \{\ell : \ell \text{ prime}, 5 \leqslant \ell\}$. We now apply the following theorem, which is proved by combining [**11**, Theorem 1.1, Corollaries 2.13 and 2.16]. Let $\pi_n : \mathrm{GL}_2(\hat{\mathbb{Z}}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ denote the canonical projection and let

$$\mathrm{sgn} : \mathrm{GL}_2(\hat{\mathbb{Z}}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \longrightarrow \frac{\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})}{[\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}), \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})]} \simeq \{\pm 1\}$$

denote the signature map.

THEOREM 7. *Let $H \subseteq \mathrm{GL}_2(\hat{\mathbb{Z}})$ be a closed subgroup. Then $H = \mathrm{GL}_2(\hat{\mathbb{Z}})$ if and only if the following conditions hold.*

(1) *For each prime $\ell \geqslant 5$, $\pi_\ell(H) = \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$.*
(2) *The group $\pi_{36}(H) = \mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z})$.*
(3) *The function $\mathrm{sgn} \times \det : \mathrm{GL}_2(\hat{\mathbb{Z}}) \longrightarrow \{\pm 1\} \times (\hat{\mathbb{Z}})^*$ satisfies $(\mathrm{sgn} \times \det)(H) = \{\pm 1\} \times (\hat{\mathbb{Z}})^*$.*

To complete the proof of (b), we would like to apply Theorem 7 with $H = \varphi_E(G_{\mathbb{Q}(t)})$. Conditions (1) and (2) of Theorem 7 have already been verified above. We now show that condition (3) must also hold. Suppose for the sake of contradiction that $(\mathrm{sgn} \times \det)(H) \subsetneq \{\pm 1\} \times (\hat{\mathbb{Z}})^*$. Recall that, because of the non-degeneracy of the Weil pairing and the irreducibility over $\mathbb{Q}$ of the nth cyclotomic polynomial for every n, we have

$$\det(\varphi_E(G_{\mathbb{Q}(t)})) = (\hat{\mathbb{Z}})^*. \tag{10}$$

Also, since $\varphi_E(G_{\mathbb{Q}(t)}) \bmod 2 = \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$, we have that $\mathrm{sgn}(\varphi_E(G_{\mathbb{Q}(t)})) = \{\pm 1\}$, and this character gives the Galois action on $\mathbb{Q}(\sqrt{\Delta_E(t)})$:

$$\sigma(\sqrt{\Delta_E(t)}) = \mathrm{sgn}(\varphi_E(\sigma)) \cdot \sqrt{\Delta_E(t)} \quad (\sigma \in G_{\mathbb{Q}(t)}).$$

Thus, we must have that

$$(\mathrm{sgn} \times \det)(\varphi_E(G_{\mathbb{Q}(t)})) = \{(x, y) \in \{\pm 1\} \times (\hat{\mathbb{Z}})^* : x = f(y)\},$$

for some group homomorphism $f : (\hat{\mathbb{Z}})^* \longrightarrow \{\pm 1\}$. Chasing through the definitions, we find that

$$\mathbb{Q}(t)(\sqrt{\Delta_E(t)}) = \overline{\mathbb{Q}(t)}^{\ker(\mathrm{sgn} \circ \varphi_E)} = \overline{\mathbb{Q}(t)}^{\ker(f \circ \det \circ \varphi_E)} \subseteq \overline{\mathbb{Q}(t)}^{\ker(\det \circ \varphi_E)} = \mathbb{Q}(t)^{\mathrm{cyc}},$$

which contradicts assumption (A2). Note also that one may reverse this argument to show that if $\mathbb{Q}(t)(\sqrt{\Delta_E(t)})$ is not geometric over $\mathbb{Q}(t)$, then $(\mathrm{sgn} \times \det)(\varphi_E(G_{\mathbb{Q}(t)})) \neq \{\pm 1\} \times (\hat{\mathbb{Z}})^*$, so that assumption (A2) is indeed necessary. This completes the proof of Proposition 4. □

As an immediate consequence of part (a) of Proposition 4, we have the following corollary.

COROLLARY 8.

$$\begin{aligned}\{E/\mathbb{Q} : E \text{ is not a Serre curve}\} &= \{E/\mathbb{Q} : [\mathrm{Gal}(\mathbb{Q}(E[36])\mathbb{Q}), \mathrm{Gal}(\mathbb{Q}(E[36])\mathbb{Q})] \subsetneq [\mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z}), \mathrm{GL}_2(\mathbb{Z}/36\mathbb{Z})]\} \\ &\cup \left(\bigcup_{\ell \geqslant 5} \{E/\mathbb{Q} : [\mathrm{Gal}(\mathbb{Q}(E[\ell])\mathbb{Q}), \mathrm{Gal}(\mathbb{Q}(E[\ell])\mathbb{Q})] \subsetneq [\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}), \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})]\} \right)\end{aligned}$$

For $\ell \geqslant 5$, one has $[\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}), \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})] = [\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}), \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})] = \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ (see, for example, [**15**, Lemma 19]), from which it follows that, for any subgroup $H \subseteq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$,

$$[H, H] = [\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}), \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})] \iff \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \subseteq H. \tag{11}$$

Applying equation (11) with $H = \mathrm{Gal}(\mathbb{Q}(E[n])\mathbb{Q})$ (and noting that $\det(\mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q})) = (\mathbb{Z}/n\mathbb{Z})^*$, for the same reason that equation (10) holds), we deduce from Corollary 8 the statement of Step 1.

4. *Elliptic curves with non-integral j-invariants*

In this section, we show that elliptic curves over $\mathbb{Q}$ with non-integral j-invariants cannot have large exceptional primes. As a corollary, we obtain the claim of Step 2 of the Main Theorem.

THEOREM 9. *Let $r \geqslant 13$ be an integer and let $E/\mathbb{Q}$ be an elliptic curve with j-invariant j_E. Assume that there exists an odd rational prime p such that*

$$-r < \mathrm{ord}_p(j_E) < 0.$$

If there exists an odd rational prime ℓ such that

$$\mathrm{Gal}(\mathbb{Q}(E[\ell])/\mathbb{Q}) \subsetneq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z}),$$

then $\ell \leqslant r$.

Proof. This is proved in [**10**, Section 4]. For the sake of clarity and completeness, we include the details below.

We assume that $\ell > r$ and reach a contradiction. Since $\mathrm{ord}_p(j_E) < 0$, Tate's theory of q-curves [**34**, Lemma 5.2, Theorem 5.3] implies that there exist a unique $q \in \mathbb{Q}_p^*$, with $\mathrm{ord}_p(q) > 0$, and a pair $(L, \mathfrak{p})$, with $\mathbb{Q}_p \subseteq L$ a field extension of degree at most 2 and $\mathfrak{p}$ a prime of L lying above p, such that the associated q-curve $E_q/\mathbb{Q}_p$ has j-invariant j_E, the curves E and E_q are isomorphic over L, and

$$\mathrm{ord}_{\mathfrak{p}}(q) = -\mathrm{ord}_{\mathfrak{p}}(j_E) = -e \cdot \mathrm{ord}_p(j_E), \tag{12}$$

for some $e \in \{1, 2\}$ (see also [**28**, IV-20]). We claim that

$$\ell \nmid \mathrm{ord}_{\mathfrak{p}}(j_E). \tag{13}$$

Indeed, if $\ell \mid \mathrm{ord}_{\mathfrak{p}}(j_E)$, then, since ℓ is odd, equation (12) implies that $\ell \mid \mathrm{ord}_p(j_E)$, and thus $\ell \leqslant -\mathrm{ord}_p(j_E)$. But $\ell > r$ and $-r < \mathrm{ord}_p(j_E)$, thus we reach a contradiction and establish condition (13).

Now, since $\ell \nmid \mathrm{ord}_{\mathfrak{p}}(j_E)$, the theory of q-curves implies that $\mathrm{Gal}(L(E_q[\ell])/L)$, and thus also $\mathrm{Gal}\,(\mathbb{Q}(E[\ell])/\mathbb{Q})$, contains a transvection [**28**, Lemma 1, IV-20]. However, by hypothesis, the

prime ℓ is such that $\mathrm{Gal}\,(\mathbb{Q}(E[\ell])/\mathbb{Q}) \subsetneq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$; thus, by [28, Lemma 2, IV-20], $E[\ell]$ is reducible as a $G_{\mathbb{Q}}$-module.

We recall Mazur's result [24, Corollary 3.3] that if $E[\ell]$ is reducible and $\ell \geqslant 17$, then E has potentially good reduction at all odd primes. Since $r \geqslant 13$ and $\ell > r$, the above applies to our situation, which implies, in particular, that $\mathrm{ord}_p(j_E) \geqslant 0$, contradicting the hypothesis. This completes the proof. □

Remark. It is because of the need to employ Mazur's theorem in the previous proof that we restrict our attention in this paper to families of elliptic curves over $\mathbb{Q}$.

Corollary 10. *Let $E/\mathbb{Q}(t)$ be an elliptic curve and let $r \geqslant 13$ be an integer. We keep the notation $\mathcal{E}_{E,n}(T)$, $\mathcal{E}^r_{E,\mathrm{int}}(T)$ introduced in Sections* 1 *and* 2.2. *Then, for any $T > 0$,*

$$\bigcup_{\ell} \mathcal{E}_{E,\ell}(T) \subseteq \left(\bigcup_{\ell \leqslant r} \mathcal{E}_{E,\ell}(T) \right) \cup \mathcal{E}^r_{E,\mathrm{int}}(T).$$

Proof. This is a direct consequence of the theorem, since, for every prime $\ell > r$ and every $t_0 \in \mathcal{E}_{E,\ell}(T) \backslash \mathcal{E}^r_{E,\mathrm{int}}(T)$, the pair (E_{t_0}, ℓ) satisfies the hypothesis of the theorem. □

5. *Elliptic curves with r-free-integral j-invariant*

In this section, we obtain an upper estimate for $\#\mathcal{E}^r_{E,\mathrm{int}}(T)$ for any $T > 0$ and any fixed positive integer r, and prove the claim of Step 3 of the Main Theorem. We start with a few preliminary results.

Lemma 11. *Let $E/\mathbb{Q}(t)$ be a non-isotrivial elliptic curve given by the Weierstrass equation* (1). *We keep all the related notation introduced in Sections* 1 *and* 2. *In particular, R_0, S_0 denotes a pair of relatively prime integers. Then there exists a positive integer $\mu = \mu(E)$, depending on j_E, such that, for any integer $r \geqslant 1$ and any $T > 0$, the following statements hold:*

(1) $d_r(G(R_0, S_0)) \mid \mu$ *for all* $R_0/S_0 \in \mathcal{E}^r_{E,\mathrm{int}}(T)$;
(2) $\#\mathcal{E}^r_{E,\mathrm{int}}(T) \leqslant \sum\limits_{\substack{G_0 \\ d_r(G_0) \mid \mu}} \#\{R_0/S_0 \in \mathcal{F}_E(T) : G(R_0, S_0) = G_0\}$.

Proof. Since f and g are relatively prime in $\mathbb{Q}[t]$, there exist $H, J, K, L \in \mathbb{Z}[R, S]$ and $\lambda', \lambda'' \in \mathbb{Z}, n', n'' \in \mathbb{N}$ such that

$$H(R,S)F(R,S) + J(R,S)G(R,S) = \lambda' R^{n'},$$
$$K(R,S)F(R,S) + L(R,S)G(R,S) = \lambda'' S^{n''}.$$

We set

$$\mu := \mathrm{lcm}\{\lambda', \lambda''\}, \tag{14}$$

and infer that every pair (R_0, S_0) of coprime integers satisfies

$$\gcd\{F(R_0, S_0), G(R_0, S_0)\} \mid \mu. \tag{15}$$

In particular, every $t_0 = R_0/S_0 \in \mathcal{E}^r_{E,\mathrm{int}}(T)$ satisfies $d_r(G(R_0, S_0)) \mid \mu$. The pair R_0, S_0 is determined up to sign by the choice of t_0, so the above implies that

$$\begin{aligned}\#\mathcal{E}^r_{E,\mathrm{int}}(T) &\leqslant \sum_{\substack{F_0, G_0\\ G_0\neq 0\\ d_r(G_0)\mid F_0}} \sum_{\substack{R_0/S_0\in\mathcal{F}_E(T)\\ F(R_0,S_0)=F_0\\ G(R_0,S_0)=G_0}} 1\\ &\leqslant \sum_{\substack{F_0, G_0\\ G_0\neq 0\\ d_r(G_0)\mid \mu}} \sum_{\substack{R_0/S_0\in\mathcal{F}_E(T)\\ F(R_0,S_0)=F_0\\ G(R_0,S_0)=G_0}} 1\\ &= \sum_{\substack{G_0\neq 0\\ d_r(G_0)\mid \mu}} \sum_{\substack{R_0/S_0\in\mathcal{F}_E(T)\\ G(R_0,S_0)=G_0}} 1, \end{aligned} \tag{16}$$

which completes the proof. □

We let

$$G(R, S) = m \cdot G_1(R, S)^{e_1} \dots G_k(R, S)^{e_k} \tag{17}$$

be the unique factorization of $G(R, S)$ into primitive irreducible polynomials of $\mathbb{Z}[R, S]$.

Proposition 12. *Let $E/\mathbb{Q}(t)$ be a non-isotrivial elliptic curve given by the Weierstrass equation (1). We keep all the related notation introduced in Sections 1 and 2. In particular, R_0, S_0 denotes a pair of relatively prime integers. Let G_0 be a non-zero integer. Then, for any $T > 0$, the following statements hold.*

(1) *If $k = 1$ and $\deg G_1 = 1$, then*

$$\#\left\{\frac{R_0}{S_0} \in \mathcal{F}_E(T) : G(R_0, S_0) = G_0\right\} = \mathrm{O}_E(T).$$

(2) *If $k = 1$ and $\deg G_1 = 2$, then, for any $\varepsilon > 0$,*

$$\#\left\{\frac{R_0}{S_0} \in \mathcal{F}_E(T) : G(R_0, S_0) = G_0\right\} = \mathrm{O}_{E,\varepsilon}(T^\varepsilon).$$

(3) *If $k = 1$ and $\deg G_1 \geqslant 3$, then*

$$\#\left\{\frac{R_0}{S_0} \in \mathcal{F}_E(T) : G(R_0, S_0) = G_0\right\} = \mathrm{O}(D_E{}^{1+\nu(G_0)}).$$

(4) *If $k \geqslant 2$, then, for any $\varepsilon > 0$,*

$$\#\left\{\frac{R_0}{S_0} \in \mathcal{F}_E(T) : G(R_0, S_0) = G_0\right\} = \mathrm{O}_{E,\varepsilon}(T^\varepsilon).$$

Proof. To prove statement (1), we assume that $k = 1$ and $\deg G_1 = 1$, thus

$$G(R, S) = m \cdot (cR + dS)^e, \tag{18}$$

for some integer $e \geqslant 1$ and m, c, $d \in \mathbb{Z}$ with $\gcd\{c, d\} = 1$. Part (1) of the proposition now follows.

To prove statement (2), we assume that $k = 1$ and $\deg G_1 = 2$. Thus,

$$G(R, S) = m \cdot (aR^2 + bRS + cS^2)^e,$$

for some integer $e \geqslant 1$ and $m, a, b, c \in \mathbb{Z}$ with $\gcd\{a, b, c\} = 1$.

The result in this case might be well known, but we were unable to find a suitable reference, so we include a proof (for example, the proof on [**31**, p. 135] gives an O-constant that depends on G_0).

Let $K := \mathbb{Q}(\sqrt{b^2-4ac})$ and $\theta := (-b+\sqrt{b^2-4ac})/2a$, $\theta' := (-b-\sqrt{b^2-4ac})/2a \in K$. Note that $[K:\mathbb{Q}] = 2$ and

$$aR^2 + bRS + cS^2 = a(R-\theta S)(R-\theta' S)$$

in $K[R,S]$. Also, note that there exists a positive integer n such that $n\theta$ is an algebraic integer. We choose $\widetilde{n}$ to be the least such n and set $\widetilde{\theta} := \widetilde{n}\theta \in \mathcal{O}_K$.

With this notation, we obtain

$$\begin{aligned}
&\#\left\{\frac{R_0}{S_0} \in \mathcal{F}_E(T) : G(R_0,S_0) = G_0\right\} \\
&\quad = \#\left\{\frac{R_0}{S_0} \in \mathcal{F}_E(T) : a(R_0-\theta S_0)(R_0-\theta' S_0) = \left(\frac{G_0}{m}\right)^{1/e}\right\} \\
&\quad \leqslant \#\left\{\frac{R_0}{S_0} \in \mathcal{F}_E(\widetilde{n}T) : (R_0-\widetilde{\theta} S_0)(R_0-\widetilde{\theta}' S_0) = \frac{\widetilde{n}^2}{a}\cdot\left(\frac{G_0}{m}\right)^{1/e}\right\}.
\end{aligned}$$

In case $\widetilde{n}^2/a \cdot (G_0/m)^{1/e} \notin \mathbb{Z}$, the set being counted is empty. Otherwise, we take

$$g_0 = g_0(E) := \frac{\widetilde{n}^2}{a}\cdot\left(\frac{G_0}{m}\right)^{1/e}$$

and

$$\widetilde{T} := \widetilde{n}T,$$

obtaining

$$\begin{aligned}
&\#\left\{\frac{R_0}{S_0} \in \mathcal{F}_E(\widetilde{T}) : (R_0-\widetilde{\theta} S_0)(R_0-\widetilde{\theta}' S_0) = \frac{\widetilde{n}^2}{a}\cdot\left(\frac{G_0}{m}\right)^{1/e}\right\} \\
&\quad \leqslant \sum_{\substack{I \subseteq \mathcal{O}_K \\ I \text{ principal} \\ N(I)=g_0}} \#\{\beta = R_0 - \widetilde{\theta} S_0 \in \mathcal{O}_K : \beta\mathcal{O}_K = I, |R_0| \leqslant \widetilde{T}, |S_0| \leqslant \widetilde{T}\},
\end{aligned}$$

where the summation is over principal ideals I of $\mathcal{O}_K$ of norm $N(I) = g_0$.

If K is imaginary quadratic, then the summand above is bounded by $|\mathcal{O}_K^*| \leqslant 6$, and if K is real quadratic, taking into account the action of a fundamental unit of $\mathcal{O}_K^*$, the summand is bounded by

$$\ll_\theta \log \widetilde{T} \ll \log T;$$

for a proof, see [14, Equation (27)]. Thus,

$$\begin{aligned}
&\sum_{\substack{I \subseteq \mathcal{O}_K \\ I \text{ principal} \\ N(I)=g_0}} \#\{\beta = R_0 - \widetilde{\theta} S_0 \in \mathcal{O}_K : \beta\mathcal{O}_K = I, |R_0| \leqslant \widetilde{T}, |S_0| \leqslant \widetilde{T}\} \\
&\quad \ll_E \log T \sum_{\substack{I \subset \mathcal{O}_K \\ I \text{ principal} \\ N(I)=g_0}} 1 \leqslant \log T \sum_{\substack{I \subset \mathcal{O}_K \\ N(I)=g_0}} 1.
\end{aligned}$$

Following [14, pp. 707–708], we will now show that

$$\sum_{\substack{I \subset \mathcal{O}_K \\ N(I)=g_0}} 1 \leqslant \sum_{d \mid g_0} 1 = \tau(g_0). \tag{19}$$

Indeed, writing $\tau_K(g_0)$ for the left-hand side of equation (19), we note that both sides are multiplicative in g_0, hence it suffices to prove the inequality when $g_0 = p^\alpha$ is a prime power.

In this case, one computes explicitly that

$$\tau_K(p^\alpha) = \begin{cases} 0 & \text{if } p \text{ is inert in } K \text{ and } \alpha \text{ is odd,} \\ 1 & \text{if } p \text{ is inert in } K \text{ and } \alpha \text{ is even,} \\ 1 & \text{if } p \text{ ramifies in } K, \\ \alpha+1 & \text{if } p \text{ splits in } K, \end{cases}$$

where, for instance, in the final case where $p\mathcal{O}_K = \mathfrak{P}\cdot\mathfrak{P}'$ we have

$$\{I \subseteq \mathcal{O}_K : N(I) = p^\alpha\} = \{\mathfrak{P}^i \cdot (\mathfrak{P}')^{\alpha-i} : 0 \leqslant i \leqslant \alpha\}.$$

Putting everything together, we infer that

$$\#\left\{\frac{R_0}{S_0} \in \mathcal{F}_E(T) : G(R_0,S_0) = G_0\right\} \ll_E \log T \cdot \tau(g_0).$$

Now we use the well-known estimate (see [12, p. 344]) that, for any $\varepsilon > 0$,

$$\tau(g_0) < \exp\left(\frac{2^{1/\varepsilon}}{\varepsilon \log 2}\right) \cdot g_0^{\varepsilon}, \tag{20}$$

as well as

$$|g_0| \ll_E |G_0| \ll_E T^{D_E}$$

(with explicit $\ll_E$-constants depending on $j_E(t)$), and conclude that

$$\#\left\{\frac{R_0}{S_0} \in \mathcal{F}_E(T) : G(R_0,S_0) = G_0\right\} \ll_{E,\varepsilon} T^{\varepsilon}.$$

To prove statement (3), we assume that $k = 1$ and $\deg G_1 \geqslant 3$, which puts us in the setting of the main result of Bombieri and Schmidt on Thue equations [2]. This gives us

$$\#\left\{\frac{R_0}{S_0} \in \mathcal{F}_E(T) : G(R_0,S_0) = G_0\right\} \ll {D_E}^{1+\nu(G_0)}.$$

To prove statement (4), we assume that $k \geqslant 2$. Then

$$\begin{aligned} &\#\left\{\frac{R_0}{S_0} \in \mathcal{F}_E(T) : G(R_0,S_0) = G_0\right\} \\ &\quad\leqslant \sum_{d_1,d_2 \mid G_0} \#\left\{\frac{R_0}{S_0} \in \mathcal{F}_E(T) : G_1(R_0,S_0) = d_1, G_2(R_0,S_0) = d_2\right\}. \end{aligned}$$

By Bezout's theorem, we have

$$\#\left\{\frac{R_0}{S_0} \in \mathcal{F}_E(T) : G_1(R_0,S_0) = d_1, G_2(R_0,S_0) = d_2\right\} \leqslant \deg G_1 \cdot \deg G_2.$$

Therefore, by invoking once again the estimate of equation (20) for the divisor function, we deduce that

$$\#\left\{\frac{R_0}{S_0} \in \mathcal{F}_E(T) : G(R_0,S_0) = G_0\right\} \leqslant {D_E}^2 \cdot \tau(G_0)^2 \ll_{E,\varepsilon} T^{\varepsilon},$$

with an explicit $\ll_{E,\varepsilon}$-constant. This completes the proof of Proposition 12. □

Lemma 13. *Let $E/\mathbb{Q}(t)$ be a non-isotrivial elliptic curve given by the Weierstrass equation (1). We keep all the related notation introduced in Sections 1 and 2. In particular, R_0, S_0 denotes a pair of relatively prime integers. Let $\mu = \mu(E)$ as in Lemma 11. Let r be a*

positive integer. Then, for any $T > 0$,

$$\#\left\{G_0 \in \mathbb{Z}, G_0 \neq 0 : d_r(G_0) \mid \mu, G_0 = G(R_0, S_0) \text{ for some } \frac{R_0}{S_0} \in \mathcal{F}_E(T)\right\} = \mathrm{O}_{E,r}(T^{D_E/r} \log T).$$

Proof. We write $G_0 = \pm 2^\alpha c_r(G_0) d_r(G_0)$ as in Section 2 and observe that $|G_0| \ll_E T^{D_E}$. Therefore, the number of values of α which may occur is $\mathrm{O}_E(D_E \log T) = \mathrm{O}_E(\log T)$. Since

$$\#\{n \leqslant x : n \text{ is } r\text{-full}\} = \mathrm{O}_r(x^{1/r})$$

(see [**32**, p. 297]), the number of values of $c_r(G_0)$ which may occur is $\mathrm{O}_{E,r}(T^{D_E/r})$. Therefore,

$$\#\left\{G_0 \in \mathbb{Z}, G_0 \neq 0 : d_r(G_0) \mid \mu, G_0 = G(R_0, S_0) \text{ for some } \frac{R_0}{S_0} \in \mathcal{F}_E(T)\right\} \ll_{E,r} \log T \cdot T^{D_E/r} \cdot \tau(\mu),$$

which completes the proof. □

We now show the following theorem.

THEOREM 14. *Let* $E/\mathbb{Q}(t)$ *be a non-isotrivial elliptic curve given by the Weierstrass equation* (1). *We keep all the related notation introduced in Sections* 1 *and* 2. *For any* $r \geqslant 1$ *and* $T > 0$, *the following statements hold.*

(1) *If* $k = 1$ *and* $\deg G_1 = 1$, *then*

$$\#\mathcal{E}^r_{E,\mathrm{int}}(T) = \mathrm{O}_{E,r}(T^{(D_E/r)+1} \log T).$$

(2) *If* $k \geqslant 2$, *or if* $k = 1$ *and* $\deg G_1 = 2$, *then, for any* $\varepsilon > 0$,

$$\#\mathcal{E}^r_{E,\mathrm{int}}(T) = \mathrm{O}_{E,r,\varepsilon}(T^{(D_E/r)+\varepsilon} \log T).$$

(3) *If* $k = 1$ *and* $\deg G_1 \geqslant 3$, *then*

$$\#\mathcal{E}^r_{E,\mathrm{int}}(T) = \mathrm{O}_{E,r}(T^{(D_E/r)(1+(\log D_E/\log 2))} \log T).$$

Proof. The proof is an immediate consequence of Lemma 11, Proposition 12, and Lemma 13, as follows.

For the proof of statement (1), we assume that $k = 1$ and $\deg G_1 = 1$. By Lemma 11, part (1) of Proposition 12, and Lemma 13,

$$\#\mathcal{E}^r_{E,\mathrm{int}}(T) \leqslant \sum_{\substack{G_0 \neq 0 \\ d_r(G_0) \mid \mu}} \#\left\{\frac{R_0}{S_0} \in \mathcal{F}_E(T) : G(R_0, S_0) = G_0\right\} \ll_{E,r} T^{(D_E/r)+1} \log T.$$

To prove statement (2), we assume that $k \geqslant 2$ or that $k = 1$ and $\deg G_1 = 2$. Again, by Lemma 11, Proposition 12 (parts (2) and (4)), and Lemma 13,

$$\#\mathcal{E}^r_{E,\mathrm{int}}(T) \ll_{E,r,\varepsilon} T^{(D_E/r)+\varepsilon} \log T.$$

To prove statement (3), we assume that $k = 1$ and $\deg G_1 = 3$. Then

$$\#\mathcal{E}^r_{E,\mathrm{int}}(T) \ll {\sum_{\substack{G_0 \\ d_r(G_0) \mid \mu}}}' D_E{}^{1+\nu(G_0)},$$

where the dash on the summation indicates that the integers G_0 in the summation occur as values of $G(R_0, S_0)$ for some $R_0/S_0 \in \mathcal{E}^r_{E,\mathrm{int}}(T)$. In particular, $|G_0| \ll_E T^{D_E}$ and

$$\begin{aligned}\nu(G_0) &\leqslant 1 + \nu(c_r(G_0)) + \nu(d_r(G_0))\\ &\leqslant 1 + \nu(\mathrm{rad}(c_r(G_0))) + \nu(\mu),\end{aligned}$$

where 1 occurs if G_0 is even.

We now recall the elementary estimate

$$\nu(m) \leqslant \frac{\log m}{\log 2}$$

and deduce that

$$\nu(G_0) \leqslant \frac{D_E \log T}{r \log 2} + \mathrm{O}_E(1).$$

This gives us that

$$D_E{}^{1+\nu(G_0)} \ll_E D_E{}^{D_E \log T/r \log 2} = T^{D_E \log D_E/r \log 2},$$

and so

$$\begin{aligned}&\#\mathcal{E}^r_{E,\mathrm{int}}(T)\\ &\ll_E T^{D_E \log D_E/r \log 2} \cdot \#\left\{G_0 \in \mathbb{Z}, G_0 \neq 0 : d_r(G_0) \mid \mu, G_0 = G(R_0, S_0) \text{ for some } \frac{R_0}{S_0} \in \mathcal{F}_E(T)\right\}.\end{aligned}$$

By Lemma 13, we now conclude that

$$\#\mathcal{E}^r_{E,\mathrm{int}}(T) \ll_{E,r} T^{(D_E/r)(1+(\log D_E/\log 2))} \log T.$$

This completes the proof of the theorem. □

Finally, we deduce Step 3 of the Main Theorem.

Corollary 15. *Let $E/\mathbb{Q}(t)$ be a non-isotrivial elliptic curve given by the Weierstrass equation (1). We keep all the related notation introduced in Sections 1 and 2. Let $\varepsilon > 0$ and set*

$$r = r(E, \varepsilon) := \left\lceil \frac{3D_E \log(\max(\{D_E, 2\}))}{\varepsilon \log 2} \right\rceil.$$

For any $T > 0$, the following statements hold.

(1) *If E is j-usual, then*

$$\#\mathcal{E}^r_{E,\mathrm{int}}(T) = \mathrm{O}_{E,\varepsilon}(T^{\varepsilon}).$$

(2) *If E is j-unusual, then*

$$\#\mathcal{E}^r_{E,\mathrm{int}}(T) = \mathrm{O}_{E,\varepsilon}(T^{1+\varepsilon}).$$

6. *Serre curves, modular curves, and thin sets in $\mathbb{P}^1$*

The goal of this section is to complete the proof of the Main Theorem by providing the estimates claimed in Step 4 of Section 2. We first relate Serre curves to $\mathbb{Q}$-rational points on modular curves and then use the theory of thin sets in $\mathbb{P}^1$ to count the $\mathbb{Q}$-rational points of bounded height on the corresponding modular curves.

6.1. *Serre curves and modular curves*

Let $n \geqslant 1$ be an integer and let $X(n)$ denote the complete modular curve of level n. We recall that $X(n)$ parameterizes elliptic curves, together with chosen bases of n-division points.

Moreover, if G is a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, such that $-I \in G$, and the determinant map

$$\det : G \longrightarrow (\mathbb{Z}/n\mathbb{Z})^*$$

is surjective, then:

(1) the quotient $X_G := X(n)/G$ is a curve over $\mathbb{Q}$;
(2) the non-cuspidal points of $X_G(\mathbb{Q})$ are in one-to-one correspondence with the ($\overline{\mathbb{Q}}$-isomorphism classes of) elliptic curves $E/\mathbb{Q}$ having the property that $\mathrm{Gal}\,(\mathbb{Q}(E[n])/\mathbb{Q})$ is contained in some conjugate of G in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$;
(3) the j-map associated to X_G, $j_{X_G} : X_G \longrightarrow \mathbb{P}^1$, defines a morphism over $\mathbb{Q}$ of degree $\#\,\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})/\#G$.

In part (2) above, if $E/\mathbb{Q}$ gives rise to a non-cuspidal point $P \in X_G(\mathbb{Q})$, then $j_{X_G}(P)$ is the j-invariant of E. For more details, see [**23**] and the references therein.

Recall that, for each positive integer n, we have

$$\det(\mathrm{Gal}\,(\mathbb{Q}(E[n])/\mathbb{Q})) = (\mathbb{Z}/n\mathbb{Z})^*.$$

With the notation of Section 3, and in the same spirit, we introduce the following definition.

Definition 16. For any positive integer n, we define

$$\mathcal{M}(n) := \{H \subsetneq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}) : \det(H) = (\mathbb{Z}/n\mathbb{Z})^* \text{ and } [H,H] \subsetneq [\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}), \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})]\}$$
$$\mathcal{M}_{\max}(n) := \{H \in \mathcal{M}(n) : \nexists H_1 \in \mathcal{M}(n) \text{ with } H \subsetneq H_1\}/\sim,$$

where $H \sim H'$ if $H' = gHg^{-1}$ for some $g \in \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$.

Now we define a set of modular curves.

Definition 17.

$$\mathcal{X} := \left(\bigcup_{\ell \geqslant 5} \{X_H : H \in \mathcal{M}_{\max}(\ell)\}\right) \cup \{X_H : H \in \mathcal{M}_{\max}(36)\}.$$

For an integer $r \geqslant 5$, let

$$\mathcal{X}_r := \left(\bigcup_{5 \leqslant \ell \leqslant r} \{X_H : H \in \mathcal{M}_{\max}(\ell)\}\right) \cup \{X_H : H \in \mathcal{M}_{\max}(36)\}.$$

It now follows from Corollary 8 that $\mathcal{X}$ is the set of modular curves parameterizing non-Serre curves; this is in agreement with the notation of Section 1. We state this formally as the following theorem.

Theorem 18. *Let $E/\mathbb{Q}$ be an elliptic curve. Then E is not a Serre curve if and only if E corresponds to a non-cuspidal $\mathbb{Q}$-rational point of X_H for some $X_H \in \mathcal{X}$.*

We deduce the following immediate corollary.

Corollary 19. *Let $E/\mathbb{Q}(t)$ be an elliptic curve. Then, for any $T > 0$,*

$$\mathcal{E}_{E,\text{non-Serre}}(T) = \bigcup_{X_H \in \mathcal{X}} \mathcal{E}_{E,X_H}(T),$$

where $\mathcal{X}$ is as in Definition 17, *$X_H = X(n)/H$ as above, and*

$$\mathcal{E}_{E,X_H}(T) := \{t_0 \in \mathcal{F}_E(T) : j_E(t_0) \in \mathbb{P}^1(j) \text{ is the image under } j_{X_H} \text{ of a non-cuspidal point of } X_H(\mathbb{Q})\}.$$

Moreover,

$$\mathcal{E}_{E,\text{non-Serre},36}(T) = \left(\bigcup_{H \in \mathcal{M}_{\max}(36)} \mathcal{E}_{E,X_H}(T) \right)$$

and

$$\mathcal{E}_{E,\ell}(T) = \bigcup_{H \in \mathcal{M}_{\max}(\ell)} \mathcal{E}_{E,X_H}(T) \quad \forall \ell \geqslant 5.$$

We note that $\mathcal{E}_{E,X_H}(T)$ consists of the $t_0 \in \mathcal{F}_E(T)$ covered by rational points in the fiber product $C_{X_H,E} = X_H \times_{\mathbb{P}^1(j)} \mathbb{P}^1(t)$.

6.2. *Thin sets in* $\mathbb{P}^1$

Finally, we are ready to use the theory of thin sets in $\mathbb{P}^1$ and prove the claim of Step 4 of Section 2. The main result of the section is the following proposition.

PROPOSITION 20. *Let $n \geqslant 1$ be an integer and let $G \subseteq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ be such that $-I \in G$ and $\det G = (\mathbb{Z}/n\mathbb{Z})^*$. Let X_G be the modular curve associated to G. Let $E/\mathbb{Q}(t)$ be a non-isotrivial elliptic curve such that*

$$\mathrm{Gal}(\mathbb{Q}(t)(E[n])/\mathbb{Q}(t)) \simeq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}). \tag{21}$$

Let $C_{X_G,E} := X_G \times_{\mathbb{P}^1(j)} \mathbb{P}^1(t)$ be the fiber product associated to E and X_G, as in Section 1. *Let $\mathcal{H}$ be the Mordell height on $\mathbb{P}^1$. With the notation introduced in Section* 1, *we have the following.*

(1) *The curve $C_{X_G,E}$ is irreducible over $\mathbb{Q}$. If $C_{X_G,E}$ is reducible over $\overline{\mathbb{Q}}$, then*

$$\#C_{X_G,E}(\mathbb{Q}) = \mathrm{O}_{G,E}(1),$$

where the $\mathrm{O}_{G,E}$-constant depends on the degrees of the polynomials defining the irreducible components of $C_{X_G,E}$.

(2) *Assume henceforth that $C_{X_G,E}$ is irreducible over $\overline{\mathbb{Q}}$. Then $\deg \psi_{X_G,E} = \#\,\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})/\#G$.*

(3) *If $C_{X_G,E}$ has genus* 0 *and $C_{X_G,E}(\mathbb{Q}) \neq \emptyset$, then there exists a positive constant $c(G,E)$, depending on $C_{X_G,E}$, such that, as $T \to \infty$,*

$$\#\{y_0 \in C_{X_G,E}(\mathbb{Q}) : \mathcal{H}(\psi_{X_G,E}(y_0)) \leqslant T\} \sim c(G,E) T^{2/d_{X_G,E}},$$

where $d_{X_G,E} = \deg \psi_{X_G,E}$.

(4) *If $C_{X_G,E}$ has genus* 1 *and $C_{X_G,E}(\mathbb{Q}) \neq \emptyset$, then there exists a positive constant $c(G,E)$, depending on $C_{X_G,E}$, such that, as $T \to \infty$,*

$$\#\{y_0 \in C_{X_G,E}(\mathbb{Q}) : \mathcal{H}(\psi_{X_G,E}(y_0)) \leqslant T\} \sim c(G,E) (\log T)^{\rho_{X_G,E}/2},$$

where $\rho_{X_G,E}$ is the Mordell–Weil rank of $C_{X_G,E}/\mathbb{Q}$.

(5) *If $C_{X_G,E}$ has genus at least* 2, *then there exists a positive constant $c(G,E)$, depending on $C_{X_G,E}$, such that, as $T \to \infty$,*

$$\#\{y_0 \in C_{X_G,E}(\mathbb{Q}) : \mathcal{H}(\psi_{X_G,E}(y_0)) \leqslant T\} \leqslant c(G,E).$$

The proposition is a consequence of the following upper bounds for the so-called thin sets in $\mathbb{P}^1$, as described in [**31**, p. 133].

THEOREM 21. *Let $C/\mathbb{Q}$ be a smooth, absolutely irreducible algebraic curve. Let $\psi : C \longrightarrow \mathbb{P}^1$ be a non-constant morphism defined over $\mathbb{Q}$, of degree d. Let $\mathcal{H}$ be the Mordell height on $\mathbb{P}^1$. The following statements hold.*

(1) *(Theory of heights). If C has genus 0 and $C(\mathbb{Q}) \neq \emptyset$, then there exists a positive constant $c = c(C)$, depending on the curve C, such that, as $T \to \infty$,*

$$\#\{t_0 \in \psi(C(\mathbb{Q})) : \mathcal{H}(t_0) \leqslant T\} \sim cT^{2/d}.$$

(2) *(Néron). If C has genus 1 and $C(\mathbb{Q}) \neq \emptyset$, then there exists a positive constant $c = c(C)$, depending on the curve C, such that, as $T \to \infty$,*

$$\#\{t_0 \in \psi(C(\mathbb{Q})) : \mathcal{H}(t_0) \leqslant T\} \sim c(\log T)^{\rho/2},$$

where ρ denotes the Mordell–Weil rank of $C/\mathbb{Q}$.

(3) *(Faltings). If C has genus at least 2, then there exists a positive constant $c = c(C)$, depending on the curve C, such that*

$$\#\{t_0 \in \psi(C(\mathbb{Q}))\} \leqslant c.$$

Proof of Proposition 20. To prove part (1), we must show that under hypothesis (21), the curve $C_{X_G,E} = X_G \times_{\mathbb{P}^1(j)} \mathbb{P}^1(t)$ is irreducible over $\mathbb{Q}$. If this were not the case, then $C_{X_G,E}$ would have an irreducible component W defined over $\mathbb{Q}$, whose function field $\mathbb{Q}(W)$ has a degree over $\mathbb{Q}(t)$ that is strictly less than the degree of $\mathbb{Q}(X_G)$ over $\mathbb{Q}(j)$. So *a fortiori*, $C_{X_G,E}$ has an irreducible component Y defined over $\mathbb{Q}(\zeta_n)$, where ζ_n is a primitive nth root of unity, whose function field $\mathbb{Q}(\zeta_n)(Y)$ has a degree over $\mathbb{Q}(\zeta_n)(t)$ that is strictly less than the degree of $\mathbb{Q}(\zeta_n)(X_G)$ over $\mathbb{Q}(\zeta_n)(j)$. Hence the curve $C_{X(n),E} := X(n) \times_{\mathbb{P}^1_{\mathbb{Q}(\zeta_n)}(j)} \mathbb{P}^1_{\mathbb{Q}(\zeta_n)}(t)$ has an irreducible component Z over $\mathbb{Q}(\zeta_n)$, whose function field $\mathbb{Q}(\zeta_n)(Z)$ has a degree over $\mathbb{Q}(\zeta_n)(t)$ that is strictly less than the degree of $\mathbb{Q}(\zeta_n)(X(n))$ over $\mathbb{Q}(\zeta_n)(j)$, which is $|\operatorname{SL}_2(\mathbb{Z}/n\mathbb{Z})|/2$.

On the other hand, if $\mathcal{F}_n$ denotes the Fricke functions of level n (for more details on Fricke functions, see, for instance, [**19**] or [**33**]), we have $\mathbb{Q}(\zeta_n)(X(n)) = \mathbb{Q}(\zeta_n)(j, \mathcal{F}_n)$, and so $\mathbb{Q}(\zeta_n)(Z) \cong \mathbb{Q}(\zeta_n)(t, \mathcal{F}_n) = \mathbb{Q}(\zeta_n)(t, E[n]^+)$, the field $\mathbb{Q}(\zeta_n)(t)$ adjoined with all the even functions of E evaluated at $E[n]$. If hypothesis (21) holds, this field is of index 2 in $\mathbb{Q}(t, E[n])$, which has degree $|\operatorname{SL}_2(\mathbb{Z}/n\mathbb{Z})|$ over $\mathbb{Q}(\zeta_n)(t)$. This contradiction shows that $C_{X_G,E}$ is irreducible over $\mathbb{Q}$.

Hence, if $C_{X,E}$ is not irreducible over $\overline{\mathbb{Q}}$, any $\mathbb{Q}$-point P of $C_{X,E}$ is contained in a component not defined over $\mathbb{Q}$ and so is contained in all the conjugate components under the action of $G_{\mathbb{Q}}$. Hence, the number of such P is bounded by the number of points in the intersection of distinct components of $C_{X,E}$, which is bounded by Bezout's theorem.

To prove part (2), we now assume that $C_{X,E}$ is absolutely irreducible, and so

$$\deg \psi_{X_G,E} = \deg j_{X_G} = \frac{\#\operatorname{GL}_2(\mathbb{Z}/n\mathbb{Z})}{\#G}.$$

For the proof of parts (3)–(5), we apply Theorem 21. □

The claim of Step 4 of Section 2 is an immediate consequence of Proposition 20 and Corollaries 19 and 6.

Acknowledgements. The authors are grateful to the following research institutes for funding and excellent work facilities during the preparation of the paper: Centre de Recherches Mathématiques, Montreal, QC, Canada; Hausdorff Research Institute for Mathematics, Bonn,

Germany; Institute for Advanced Study, Princeton, NJ, USA; Max Plank Institute for Mathematics, Bonn, Germany; Mathematical Sciences Research Institute, Berkeley, CA, USA; Park City Mathematics Institute, Park City, UT, USA. They would also like to thank Everett Howe for bringing [5] to their attention. Finally, they would like to thank the anonymous referee for a careful reading of the manuscript and for suggestions which improved its exposition.

References

1. Yu. Bilu and P. Parent, 'Serre's uniformity problem in the split Cartan case', *Ann. of Math.*, to appear, Preprint, 2008, arXiv:0807.4954.
2. E. Bombieri and W. M. Schmidt, 'On Thue's equation', *Invent. Math.* 88 (1987) 69–81.
3. A. Brumer, 'The average rank of elliptic curves. I', *Invent. Math.* 109 (1992) 445–472.
4. I. Chen, 'The Jacobians of non-split Cartan modular curves', *Proc. London Math. Soc.* (3) 77 (1998) 1–38.
5. K. Chua, M. Lang and Y. Yang, 'On Rademacher's conjecture: congruence subgroups of genus zero of the modular group', *J. Algebra* 277 (2004) 408–428.
6. A. C. Cojocaru, 'On the surjectivity of the Galois representations associated to non-CM elliptic curves', *Canad. Math. Bull.* 48 (2005) 16–31, with an appendix by E. Kani.
7. A. C. Cojocaru and C. Hall, 'Uniform results for Serre's theorem for elliptic curves', *Int. Math. Res. Not.* 50 (2005) 3065–3080.
8. J. B. Dennin, Jr., 'The genus of subfields of $K(n)$', *Proc. Amer. Math. Soc.* 51 (1975) 282–288.
9. W. D. Duke, 'Elliptic curves with no exceptional primes', *C. R. Math. Acad. Sci. Paris Sér. I*, 325 (1997) 813–818.
10. D. Grant, 'A formula for the number of elliptic curves with exceptional primes', *Compos. Math.* 122 (2000) 151–164.
11. A. Greicius, 'Elliptic curves with surjective adelic Galois representations', *Experiment. Math.*, to appear, Preprint, 2009, http://arxiv.org/abs/0901.2513
12. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 6th edn, revised by D. R. Heath-Brown and J. H. Silverman (Oxford University Press, Oxford, 2008).
13. N. Jones, 'A bound for the torsion conductor of a non-CM elliptic curve', *Proc. Amer. Math. Soc.* 137 (2009) 37–43.
14. N. Jones, 'Averages of elliptic curve constants', *Math. Ann.* 345 (2009) 685–710.
15. N. Jones, 'Almost all elliptic curves are Serre curves', *Trans. Amer. Math. Soc.* 362 (2010) 1547–1570.
16. N. Jones, 'GL_2-representations with maximal image', Preprint.
17. T. Kawamura, 'The effective surjectivity of mod ℓ Galois representations of 1- and 2-dimensional abelian varieties with trivial endomorphism ring', *Comment. Math. Helv.* 78 (2003) 486–493.
18. A. Kraus, 'Une remarque sur les points de torsion des courbes elliptiques', *C. R. Acad. Paris Sér. I*, 321 (1995) 1143–1146.
19. S. Lang, *Elliptic functions* (Addison-Wesley, Reading, MA, 1973).
20. S. Lang and H. Trotter, *Frobenius distributions in* GL_2*-extensions*, Lecture Notes in Mathematics 504 (Springer, Berlin, 1976).
21. D. W. Masser and G. Wüstholz, 'Galois properties of division fields of elliptic curves', *Bull. London Math. Soc.* 25 (1993) 247–254.
22. B. Mazur, 'Modular curves and the Eisenstein ideal', *Publ. Math. Inst. Hautes Études Sci.* 47 (1977) 33–186.
23. B. Mazur, *Rational points on modular curves*, Lecture Notes in Mathematics 601 (Springer, New York, 1977) 107–148.
24. B. Mazur, 'Rational isogenies of prime degree', *Invent. Math.* 44 (1978) 129–162.
25. B. Mazur and H. P. F. Swinnerton-Dyer, 'The arithmetic of Weil curves', *Invent. Math.* 25 (1974) 1–61.
26. L. Merel, 'Arithmetic of elliptic curves and diophantine equations', *J. Théor. Nombres Bordeaux* 11 (1999) 173–200.
27. V. Radhakrishnan, 'Asymptotic formula for the number of non-Serre curves in a two-parameter family', PhD Thesis, University of Colorado at Boulder, 2008.
28. J.-P. Serre, *Abelian ℓ-adic representations and elliptic curves* (Benjamin, New York, 1968).
29. J.-P. Serre, 'Propriétés galoisiennes des points d'ordre fini des courbes elliptiques', *Invent. Math.* 15 (1972) 259–311.
30. J.-P. Serre, 'Quelques applications du théorème de densité de Chebotarev', *Publ. Math. Inst. Hautes Études Sci.* 54 (1981) 123–201.
31. J.-P. Serre, *Lectures on the Mordell–Weil theorem*, Aspects of Mathematics (Vieweg, Braunschweig, 1989).
32. H. Shapiro, *Introduction to the theory of numbers* (Wiley, New York, 1983).
33. G. Shimura, *Introduction to the arithmetic theory of automorphic functions* (Princeton University Press, Princeton, NJ, 1971).
34. J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics 151 (Springer, New York, 1994).
35. D. Zywina, 'Elliptic curves with maximal Galois action on their torsion points', Preprint.

Alina-Carmen Cojocaru
Department of Mathematics
Statistics and Computer Science
University of Illinois at Chicago
851 S Morgan St, 322 SEO
Chicago, IL 60607
USA

Institute of Mathematics 'Simion Stoilow'
of the Romanian Academy
21 Calea Grivitei St
Bucharest 010702
Sector 1
Romania

Institute for Advanced Study
Einstein Drive
Princeton, NJ 08540
USA

cojocaru@math.uic.edu

Nathan Jones
Department of Mathematics
University of Mississippi
Hume Hall 305
PO Box 1848
University, MS 38677-1848
USA

ncjones@olemiss.edu

David Grant
Department of Mathematics
University of Colorado at Boulder
Campus Box 395
Boulder, CO 80309-0395
USA

grant@colorado.edu