JOURNAL
de Théorie des Nombres
de BORDEAUX
*anciennement Séminaire de Théorie des Nombres de Bordeaux*

Richard GRIFFON

**Explicit $L$-functions and a Brauer–Siegel theorem for Hessian elliptic curves**

Tome 30, n° 3 (2018), p. 1059-1084.

<http://jtnb.cedram.org/item?id=JTNB_2018__30_3_1059_0>

*Journal de Théorie des Nombres*
*de Bordeaux* **30** (2018), 1059–1084

# Explicit *L*-functions and a Brauer–Siegel theorem for Hessian elliptic curves

par Richard GRIFFON

Résumé. Étant donné un corps fini $\mathbb{F}_q$ de caractéristique $p \geq 5$, nous considérons la famille de courbes elliptiques $E_d$ définies sur $K = \mathbb{F}_q(t)$ par $E_d : \ y^2 + xy - t^d y = x^3$, pour tout entier $d \geq 1$ qui est premier à $q$.

Nous donnons une expression explicite des fonctions $L$ de ces courbes. De plus, nous déduisons de ce calcul que les courbes $E_d$ satisfont un analogue du théorème de Brauer–Siegel. Plus spécifiquement, nous montrons que, lorsque $d \to \infty$ parcourt les entiers premiers à $q$, l'on a

$$\log\left(|Ш(E_d/K)| \cdot \mathrm{Reg}(E_d/K)\right) \sim \log H(E_d/K),$$

où $H(E_d/K)$ désigne la hauteur différentielle exponentielle de $E_d$, $Ш(E_d/K)$ son groupe de Tate–Shafarevich et $\mathrm{Reg}(E_d/K)$ son régulateur de Néron–Tate.

Abstract. For a finite field $\mathbb{F}_q$ of characteristic $p \geq 5$ and $K = \mathbb{F}_q(t)$, we consider the family of elliptic curves $E_d$ over $K$ given by $y^2 + xy - t^d y = x^3$ for all integers $d$ coprime to $q$.

We provide an explicit expression for the $L$-functions of these curves. Moreover, we deduce from this calculation that the curves $E_d$ satisfy an analogue of the Brauer–Siegel theorem. Precisely, we show that, for $d \to \infty$ ranging over the integers coprime with $q$, one has

$$\log\left(|Ш(E_d/K)| \cdot \mathrm{Reg}(E_d/K)\right) \sim \log H(E_d/K),$$

where $H(E_d/K)$ denotes the exponential differential height of $E_d$, $Ш(E_d/K)$ its Tate–Shafarevich group and $\mathrm{Reg}(E_d/K)$ its Néron–Tate regulator.

## Introduction

Let $\mathbb{F}_q$ be a finite field of characteristic $p \geq 5$, and $K = \mathbb{F}_q(t)$. For a nonisotrivial elliptic curve $E$ over $K$, we denote by $L(E/K, T)$ its $L$-function: it is *a priori* defined as a formal power series in $T$. Deep theorems of Grothendieck and Deligne, however, show that $L(E/K, T)$ is actually a polynomial with integral coefficients, satisfying the expected functional equation (relating its behaviour at $T$ to that at $1/q^2T$), whose degree is

Manuscrit reçu le 11 décembre 2017, accepté le 6 juin 2018.
2010 *Mathematics Subject Classification.* 11G05, 11G40, 14G10, 11F67, 11M38.
*Mots-clefs.* Elliptic curves over function fields, Explicit computation of $L$-functions, Special values of $L$-functions and BSD conjecture, Estimates of special values, Analogue of the Brauer–Siegel theorem.

given in terms of the conductor of $E$, and for which the Riemann Hypothesis holds (i.e., complex zeros $z$ of $L(E/K,T)$ have magnitude $|z| = q^{-1}$).

In general, these facts are not sufficient to study finer analytic and arithmetic questions about $E$. For example, a general study of the distribution of zeros of $T \mapsto L(E/K,T)$ on the circle $\{z \in \mathbb{C} : |z| = q^{-1}\}$ on which they lie appears to be out of reach at the moment. In the meantine, partial evidence could be gathered by studying special families of elliptic curves $E/K$ for which $L(E/K,T)$ is explicitly known.

Our first goal in this article is thus to exhibit a new infinite family for which the $L$-functions can be explicitly calculated. Specifically, for any integer $d \geq 1$ coprime to $q$, consider the *Hessian elliptic curve* $E_d$ over $K$, whose affine Weierstrass model is:

$$E_d : \quad y^2 + xy - t^d \cdot y = x^3. \tag{0.1}$$

The curve $E_d$ can be viewed as the pullback under the Kummer map $t \mapsto t^d$ of $E_1$; the family $\{E_d\}_{d\geq 1,(d,q)=1}$ is therefore called the *Kummer family* built from $E_1$. We are thus studying a Kummer family of "universal" elliptic curves equipped with a rational 3-torsion point (much like the "Legendre curves" studied in [20, 2] form a Kummer family of universal elliptic curves with rational 2-torsion).

To give a flavour of our result (Theorem 3.1) without having to introduce too much notation, we restrict in this paragraph to the case where $d$ divides $|\mathbb{F}_q^\times| = q-1$: by cyclicity of $\mathbb{F}_q^\times$, we can choose a character $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ of exact order $d$. In that case, our calculation yields:

**Theorem A.** *For any integer $d$ dividing $q-1$, the $L$-function of $E_d/K$ is given by:*

$$L(E_d/K,T) = \prod_{\substack{k=1 \\ 3k\not\equiv 0 \bmod d}}^{d-1} (1 - J_k \cdot T) \in \mathbb{Z}[T],$$

*where, for all $k \in \{1,\dots,d-1\}$, we have set*

$$J_k := \sum_{\substack{x_1,x_2,x_3\in\mathbb{F}_q \\ x_1+x_2+x_3=1}} \chi^k\left(-x_1x_2x_3\right).$$

In Theorem 3.1, we provide a similar formula for $L(E_d/K,T)$ under the much lighter assumption that $d$ be coprime to the characteristic of $K$. In this more general setting, one has to account for the nontrivial action of $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ on the $d$th roots of unity in $\overline{\mathbb{F}_q}$, which leads to mild technical complications (see Sections 2 and 3).

We hope that the explicit expression for $L(E_d/K,T)$ can be of use for several applications. For example, using Theorem 3.1, one could reprove a result of Ulmer stating that as $d \geq 2$ ranges through integers coprime to

$q$, the ranks of the Mordell–Weil groups $E_d(K)$ are unbounded (see [18, §2-§4]).

In Sections 4 and 5, we then use our explicit knowledge of $L(E_d/K, T)$ to prove the following asymptotic estimate (see Theorem 5.5):

**Theorem B.** *Let $\mathbb{F}_q$ be a finite field of characteristic $p \geq 5$, and $K = \mathbb{F}_q(t)$. For any integer $d$ coprime with $q$, consider the Hessian elliptic curve $E_d/K$ as above. Then the Tate–Shafarevich group $Ш(E_d/K)$ is a finite group and, as $d \to \infty$, one has*

$$\log\left(|Ш(E_d/K)| \cdot \mathrm{Reg}(E_d/K)\right) \sim \log H(E_d/K), \tag{0.2}$$

*where $\mathrm{Reg}(E_d/K)$ denotes the Néron–Tate regulator of $E_d$, and $H(E_d/K)$ its exponential differential height.*

From the computation of $H(E_d/K)$, one further gets that

$$\log\left(|Ш(E_d/K)| \cdot \mathrm{Reg}(E_d/K)\right) \sim \tfrac{\log q}{3} \cdot d \qquad (\text{as } d \to \infty),$$

showing that the product $|Ш(E_d/K)| \cdot \mathrm{Reg}(E_d/K)$ grows exponentially fast with $d$; see [9] for an interpretation of this fact in terms of the "complexity of computing" the Mordell–Weil group $E_d(K)$.

Theorem B can also be restated as:

$$\forall\, \epsilon > 0, \quad H(E_d/K)^{1-\epsilon} \ll_{q,\epsilon} |Ш(E_d/K)| \cdot \mathrm{Reg}(E_d/K) \ll_{q,\epsilon} H(E_d/K)^{1+\epsilon}.$$

The upper bound here essentially proves a conjecture of Lang (the formulation for elliptic curves over $\mathbb{Q}$ is [11, Conj. 1]). Better still, our lower bound reveals that the exponent 1 is optimal (i.e., no smaller exponent would work in the upper bound).

**Remark 0.1.** The Brauer–Siegel theorem asserts that when $k$ runs through a sequence of number fields whose degrees over $\mathbb{Q}$ are bounded and such that the absolute values $\Delta_k$ of their discriminants tend to $+\infty$, one has the asymptotic estimate

$$\log\left(|\mathrm{C}l(k)| \cdot \mathrm{Reg}(k)\right) \sim \log\sqrt{\Delta_k} \qquad (\text{as } \Delta_k \to \infty), \tag{0.3}$$

where $\mathrm{C}l(k)$ denotes the class-group of $k$ and $\mathrm{Reg}(k)$ its regulator of units (see [12, Chap. XVI]). At least in their formal structure, (0.2) and (0.3) look very similar and, following [10], we view Theorem B as an analogue of the Brauer–Siegel theorem for the Hessian elliptic curves.

Note that, at present, there are only a handful of examples of families of elliptic curves for which (0.2) is known to hold. More specifically, there are six elliptic curves $E_1^{(i)}$ over $K = \mathbb{F}_q(t)$ (with $i = 1, \ldots, 6$) such that the Kummer families $\{E_d^{(i)}\}_{d \geq 1, (d,q)=1}$ built from $E_1^{(i)}$ satisfy a complete (and unconditional) analogue of the Brauer–Siegel theorem: the reader is referred to [10, Thm. 1.4], [5, Thm. 1.1], and [4] for four more examples.

The author has recently constructed an *Artin–Schreier family* of elliptic curves over $K$ for which (0.2) also holds (see [6]).

Let us give a rough sketch of how we prove Theorem B. General results of Ulmer for elliptic curves in "Kummer towers" imply that for all $d$ as above, $E_d/K$ satisfies the Birch and Swinnerton–Dyer conjecture[1] (see [18, §6]). In particular, the Tate–Shafarevich group $Ш(E_d/K)$ is finite and, by bounding some of the terms appearing in the "BSD formula" (see Corollary 1.6), we will see in Corollary 5.4 that

$$\frac{\log\left(|Ш(E_d/K)|\cdot \mathrm{Reg}(E_d/K)\right)}{\log H(E_d/K)} = 1 + \frac{\log L^*(E_d/K,1)}{\log H(E_d/K)} + o(1) \quad (\text{as } d\to\infty),$$

where $L^*(E_d/K,1)$ denotes the special value of $L(E_d/K,T)$ at $T=q^{-1}$ (i.e., the first nonzero coefficient in the Taylor expansion of $T\mapsto L(E_d/K,T)$ at $T=q^{-1}$, see (4.1)). Given this link with $L^*(E_d/K,1)$, proving the estimate (0.2) is equivalent to the more analytic problem of showing that

$$\left|\frac{\log L^*(E_d/K,1)}{\log H(E_d/K)}\right| = o(1) \qquad (\text{as } d\to\infty). \tag{0.4}$$

In a previous article [7], we have proved bounds on special values of $L$-functions of a certain type. Since $L(E_d/K,T)$ is explicitly known, we can check that it has the correct shape to apply these results. We derive upper and lower bounds that are enough to ensure that (0.4) holds (see Section 4).

The paper is organized as follows. We begin by giving, in Section 1, a detailed presentation of the curves $E_d$ and we compute the relevant invariants: height, conductor, torsion subgroup and Tamagawa number. The next two sections are devoted to the calculation of the $L$-functions of $E_d$: Section 2 introduces the necessary notation and tools while Section 3 contains the result and its proof. Finally, we show the analogue of the Brauer–Siegel theorem for $E_d$: we prove the necessary bounds on the special value in Section 4, before recalling the BSD conjecture and concluding the proof of Theorem B in Section 5.

**Notation.** For two functions $f(x), g(x)$ defined on $[0,\infty)$, we use Vinogradov's "$f(x)\ll_a g(x)$" notation to mean that there exists a constant $C>0$ depending at most on the mentioned parameters $a$ such that $|f(x)|\le Cg(x)$ for $x\to\infty$. Unless otherwise stated, all constants are effective and could be made explicit.

## 1. Hessian elliptic curves

*Throughout this article, we fix a finite field $\mathbb{F}_q$ of characteristic $p\ge 5$, and we denote by $K=\mathbb{F}_q(t)$.*

[1] henceforth abbreviated as BSD

Let $E/K$ be a nonconstant elliptic curve with a $K$-rational (nontrivial) 3-torsion point $P_0$. Translating $P_0$ to the origin $(0,0)$, we can assume that $E$ has an affine Weierstrass model of the form

$$E_A : \qquad y^2 + xy - A(t) \cdot y = x^3,$$

for some nonconstant $A(t) \in \mathbb{F}_q(t)$ (see [13, §7.10]). This model is often called the *Hessian normal form* of $E$. For varying nonconstant $A(t) \in \mathbb{F}_q[t]$, the curves $E_A$ provide a universal family of nonisotrivial elliptic curves endowed with a rational 3-torsion point.

In this article, we exclusively concentrate on the case when $A(t)$ is a monomial $A(t) = t^d$, for some integer $d \geq 1$ which we always assume to be coprime with $q$. For all such integers $d$, we thus denote by $E_d$ the elliptic curve over $K$ given by the affine Weierstrass model:

$$E_d : \quad y^2 + xy - t^d \cdot y = x^3, \tag{1.1}$$

which we call the *dth Hessian elliptic curve* over $K$. It can readily be seen that the model (1.1) has discriminant $\Delta = -t^{3d}(27t^d + 1)$, and that the $j$-invariant of $E_d$ is:

$$j(E_d/K) = -\frac{(24t^d + 1)^3}{t^{3d}(27t^d + 1)} \in K.$$

Viewed as a map $\mathbb{P}^1 \to \mathbb{P}^1$, the $j$-invariant $j(E_d/K)$ is plainly not constant, so that $E_d$ is not isotrivial. Note also that, since $p \geq 5$, the $j$-invariant is separable i.e., $j(E_d/K) \notin K^p$.

The reader is referred to [19, Lect. 1] and [13] for nice expositions of basic results about elliptic curves over function fields in positive characteristic.

**Remark 1.1.** These elliptic curves $E_d$ have previously been studied by Davis and Occhipinti (see [3]) from a different perspective: *via* a clever use of character sums they have produced, for many values of $d$, explicit $\mathbb{F}_{q^2}(t)$-rational points on $E_d$ which generate a full-rank subgroup of $E_d(\mathbb{F}_{q^2}(t))$.

**1.1. Bad reduction and invariants.** Let us start by describing the bad reduction of $E_d$ and by determining the relevant invariants thereof.

By inspection of the places of $K$ dividing the discriminant $\Delta$ of (1.1), one can see that $E_d$ has good reduction outside $\{0\} \cup B_d \cup \{\infty\}$, where $B_d$ is the set of places of $K$ that divide $27t^d + 1$ (i.e., $B_d$ is the set of closed points of $\mathbb{P}^1$ corresponding to $d$th roots of $-1/27$). More precisely, we have:

**Proposition 1.2.** *The elliptic curve $E_d$ has good reduction outside $S = \{0\} \cup B_d \cup \{\infty\}$. The reduction of $E_d$ at places $v \in S$ is as follows:*

| *Place $v$* | *Type of $E_d$ at $v$* | $\delta_v(E_d/K)$ | $\nu_v(E_d/K)$ | $c_v(E_d/K)$ |
|---|---|---|---|---|
| 0 | $\mathbf{I}_{3d}$ | $3d$ | 1 | $3d$ |
| $v \in B_d$ | $\mathbf{I}_1$ | 1 | 1 | 1 |
| $\infty$ | $\mathbf{I}_0$ *if* $d \equiv 0 \bmod 3$ | 0 | 0 | 1 |
| | $\mathbf{IV}$ *if* $d \equiv -1 \bmod 3$ | 4 | 2 | 3 |
| | $\mathbf{IV}^*$ *if* $d \equiv -2 \bmod 3$ | 8 | 2 | 3 |

*In this table, for all places $v$ of $K$, we have denoted by $\delta_v(E_d/K)$ (resp. by $\nu_v(E_d/K)$) the valuation at $v$ of the minimal discriminant $\Delta_{\min}(E_d/K)$ of $E_d$ (resp. of the conductor $\mathcal{N}(E_d/K)$ of $E_d$), and by $c_v(E_d/K)$ the local Tamagawa number (see* [14, Chap. IV, §9] *for definitions).*

*Proof.* This follows from a routine application of Tate's algorithm to $E_d$ (see [14, Chap. IV, §9]). □

With this Proposition, we can compute the *minimal discriminant divisor* $\Delta_{\min}(E_d/K)$ and the *conductor* $\mathcal{N}(E_d/K)$ of $E_d$. In particular, they have degree

$$\deg \Delta_{\min}(E_d/K) = \begin{cases} 4d & \text{if } d \equiv 0 \bmod 3, \\ 4(d+1) & \text{if } d \equiv -1 \bmod 3, \\ 4(d+2) & \text{if } d \equiv -2 \bmod 3, \end{cases} \tag{1.2}$$

$$\text{and } \deg \mathcal{N}(E_d/K) = \begin{cases} d+1 & \text{if } d \equiv 0 \bmod 3, \\ d+3 & \text{otherwise.} \end{cases}$$

Indeed, note that $\sum_{v \in B_d} \deg v = d$. By definition, the *exponential differential height of $E_d/K$* is then

$$H(E_d/K) := q^{\frac{1}{12}\deg \Delta_{\min}(E_d/K)} = q^{\lfloor (d+2)/3 \rfloor}, \tag{1.3}$$

where $\lfloor \cdot \rfloor$ denotes the floor function.

**Remark 1.3.** The following alternative definition of $H(E_d/K)$ justifies its name (see [19, III.§2]). Let $\pi : \mathcal{E}_d \to \mathbb{P}^1$ be the Néron model of $E_d/K$ and $s_0 : \mathbb{P}^1 \to \mathcal{E}_d$ be the unit section. Denoting by $\Omega^1_{\mathcal{E}_d/\mathbb{P}^1}$ the sheaf of relative diffentials, we let $\omega = \omega_{E_d/K}$ be the line bundle $s_0^* \Omega^1_{\mathcal{E}_d/\mathbb{P}^1}$ on $\mathbb{P}^1$. Then the minimal discriminant divisor $\Delta_{\min}(E_d/K)$ corresponds to a section of $\omega^{\otimes 12}$. In particular, one has $12 \deg \omega = \deg \Delta_{\min}(E_d/K)$, and $H(E_d/K) = q^{\deg \omega}$.

**Remark 1.4.** It will be convenient to have locally minimal integral "short" Weierstrass models of $E_d$ at our disposal (see Section 3.2). By a straightforward change of variables in (1.1), one shows that $E_d$ can be given by:

$$E_d : \qquad y^2 = x^3 + x^2 - 8t^d \cdot x + 16t^{2d}.$$

The discriminant of this integral Weierstrass model is

$$\Delta' = -2^{12}t^{3d}(27t^d + 1).$$

For all places $v \neq \infty$ of $K$, $\operatorname{ord}_v \Delta' = \operatorname{ord}_v \Delta_{\min}(E_d/K)$ so that this new model is minimal at all the finite places $v$ of $K$. At $v = \infty$, the application of Tate's algorithm when $3 \mid d$ (i.e., in the case of good reduction) proves that a minimal integral model of $E$ at $\infty$ is $y^2 + u^{d/3}xy - y = x^3$, where $u = 1/t$ is the uniformizer at $\infty$. This model is readily brought into "short" Weierstrass form:

$$E_d : \quad y^2 = x^3 + \frac{u^{2d/3}}{4}x^2 - \frac{u^{d/3}}{2}x + \frac{1}{4}.$$

**1.2. Torsion and Tamagawa number.** In this section, we compute the torsion subgroup $E_d(K)_{\mathrm{tors}}$, as well as the Tamagawa number $\tau(E_d/K)$.

**Proposition 1.5.** *For any integer $d \geq 1$ coprime with $q$, one has*

$$E_d(K)_{\mathrm{tors}} \simeq \mathbb{Z}/3\mathbb{Z}.$$

*More precisely, $E_d(K)_{\mathrm{tors}}$ is generated by $P_0 = (0, 0)$.*

*Proof.* Let $T := E_d(K)_{\mathrm{tors}}$ and $P_0 = (0, 0) \in E_d(K)$: it is easy to check that $2P_0 = (0, t^d) = -P_0$. In particular, the point $P_0$ is 3-torsion, and $T$ already contains a subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z}$.

We observe first that the $p$-part $T[p^\infty]$ of $T$ must be trivial for $j(E_d/K)$ is not a $p$-th power in $K$ (see [19, Lect. 1, Prop. 7.3]).

For any place $v$ of $K$, let $G_v$ be the component group of the fiber at $v$ of the Néron model of $E_d$ (see [13, §7], [14, Chapt. IV, §9]). The table on p. 365 of [14] gives that

$$G_v \simeq \begin{cases} \mathbb{Z}/n\mathbb{Z} & \text{if the fiber at } v \text{ has type } \mathbf{I}_n \ (n \geq 1), \\ \mathbb{Z}/3\mathbb{Z} & \text{if the fiber at } v \text{ has type } \mathbf{IV} \text{ or } \mathbf{IV}^*. \end{cases} \tag{1.4}$$

We now distinguish two cases. Assume first that $3 \nmid d$: by Proposition 1.2, $E_d$ has additive reduction at the place $\infty$, with a fiber of type **IV** or $\mathbf{IV}^*$. Lemma 7.8 in [13] asserts that the prime-to-$p$ part of $T$ injects into the component group $G_v$ at an additive place $v$. Here, this yields that the whole of $T$ injects into $G_\infty \simeq \mathbb{Z}/3\mathbb{Z}$, and we conclude that $T \simeq \mathbb{Z}/3\mathbb{Z}$ in this case.

We now turn to the case when $3 \mid d$. By Corollary 7.5 in [13], the torsion subgroup $T$ injects into the product $\prod_{v|\Delta} G_v$ of the component groups. Therefore, it follows from Proposition 1.2 and (1.4) that $T$ is a subgroup

of $\prod_{v|\Delta} G_v \simeq \mathbb{Z}/3d\mathbb{Z}$. From which we deduce that $T$ is cyclic of some order $M \in \mathbb{Z}_{\geq 1}$, with $3 \mid M \mid 3d$.

We denote by $X_1(M)$ the compactification of the modular curve classifying pairs $(E, P)$ where $E$ is an elliptic curve and $P$ is a rational point of order $M$. Choosing a generator $Q \in T$, we form a pair $(E_d, Q)$ which, by construction, corresponds to a $K$-rational (non-cuspidal) point on $X_1(M)$. Hence, there exists a morphism $j' : \mathbb{P}^1 \to X_1(M)$. As we have seen, the $j$-invariant $j(E_d/K) : \mathbb{P}^1 \to \mathbb{P}^1$ is non constant and separable, and so is the induced morphism $j'$. Applying the Riemann–Hurwitz formula to $j'$ yields that the genus of $X_1(M)$ has to be 0. By [19, Lect. 1, §7], this can only happen for $M \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$. Given that $M$ must be divisible by 3, there remains only four possible values: $M \in \{3, 6, 9, 12\}$. To conclude the proof in this case, it suffices to check that $M$ must be odd, and that $M$ cannot be 9.

If there were a point $P = (x, y) \in E_d(K)$ of exact order 2, then the $x$-coordinate of $P$ would satisfy $4x^3 - 2x^2 - 2t^d \cdot x + t^{2d} = 0$. Letting $u = 1/t$ and $x_1 = u^{2d/3}x$ (recall that $3 \mid d$), we would obtain that

$$4x_1^3 - 2u^{2d/3} \cdot x_1^2 - 2u^{d/3} \cdot x_1 + 1 = 0.$$

But the latter equation has no solution $x_1 \in \mathbb{F}_q(u)$ since it factors as $(4x_1^2 - 2u^{2d/3} \cdot x_1 - 2u^{d/3}) \cdot x_1 = -1$. This contradiction shows that $E_d(K)$ has no nontrivial 2-torsion, so that $M = |T|$ is odd.

Next we show that $E_d$ has no nontrivial 9-torsion $K$-rational point. To that end, recall that for all points $P = (x_P, y_P) \in E_d(K)$ such that $3P \neq \mathcal{O}$, the "triplication formula" expresses the $x$-coordinate $x_{3P}$ of $3P$ as a rational function $\phi_3(x)/\psi_3(x)^2$ of $x_P$, where $\phi_3, \psi_3 \in K[x]$ are relatively prime polynomials that can be explicitly computed in terms of the coefficients of the Weierstrass model (1.1), see [15, Chap. III, Ex. 3.7]. A tedious but straightforward computation with the formulae of loc. cit. shows that $\phi_3(x)$ is given by

$$\begin{aligned}\phi_3(x) = x^9 + 6t^d \cdot x^7 + t^d(1 - 24t^d) \cdot x^6 - 6t^{2d} \cdot x^5 + 3t^{3d} \cdot x^4 \\ + t^{3d}(3t^d - 1) \cdot x^3 + 3t^{4d} \cdot x^2 - 3t^{5d} \cdot x + t^{6d}.\end{aligned}$$

Now suppose that there exists a $K$-rational point $Q = (x_Q, y_Q)$ of exact order 9 on $E_d$. Up to replacing $Q$ by one of its multiples, we can assume that $3Q = P_0$; in particular, their $x$-coordinates agree i.e., $x_{3Q} = x_{P_0} = 0$. Hence $\phi_3(x)$ vanishes at $x_Q \in K$, and $x_Q$ must satisfy

$$\begin{aligned}x_Q^9 + 6t^d \cdot x_Q^7 + t^d(1 - 24t^d) \cdot x_Q^6 - 6t^{2d} \cdot x_Q^5 + 3t^{3d} \cdot x_Q^4 \\ + t^{3d}(3t^d - 1) \cdot x_Q^3 + 3t^{4d} \cdot x_Q^2 - 3t^{5d} \cdot x_Q + t^{6d} = 0.\end{aligned}$$

Letting $u = 1/t$, $v = u^{d/3}$ and $x_2 = u^{2d/3}x_Q = v^2 x_Q$, multiplying the above relation by $u^6 = v^{18}$ yields that $x_2 \in \mathbb{F}_q(u)$ is a solution of

$$x_2^9 + 6v \cdot x_2^7 + (v^3 - 24) \cdot x_2^6 - 6v^2 \cdot x_2 + 3v \cdot x_2^4 \\ + (3 - v^2) \cdot x_2^3 + 3v^2 \cdot x_2^2 - 3v \cdot x_2 + 1 = 0.$$

Since the left-hand side factors, $x_2$ satisfies

$$\text{either } 0 = x_2^3 + (v - 3) \cdot x_2^2 - v \cdot x_2 + 1, \\ \text{or } 0 = x_2^6 + (3 - v) \cdot x_2^5 + (v^2 + v + 9) \cdot x_2^4 + (v^2 - 3v + 2) \cdot x_2^3 \\ + (v^2 - v + 3) \cdot x_2^2 - 2v^2 \cdot x_2 + 1.$$

Neither of these equations has any solution $x_2 \in \mathbb{F}_q(u)$, hence the 9-torsion in $E_d(K)$ has to be trivial. Therefore, $M = 3$ and $T \simeq \mathbb{Z}/3\mathbb{Z}$ as claimed. □

The (global) *Tamagawa number* $\tau(E_d/K) := \prod_{v \in S} c_v(E_d/K)$ can be computed from the last column of the table in Proposition 1.2: we immediately get

$$\tau(E_d/K) = \begin{cases} 3d & \text{if } d \equiv 0 \bmod 3, \\ 9d & \text{otherwise.} \end{cases} \tag{1.5}$$

In Section 5.1, we will need the results of Proposition 1.5 and (1.5) in the form of the following bound:

**Corollary 1.6.** *For all integers $d \geq 2$, coprime with $q$, the following bound holds:*

$$\frac{\log d}{d} \ll_q \frac{\log\left(\tau(E_d/K) \cdot q \cdot |E_d(K)_{\mathrm{tors}}|^{-2}\right)}{\log H(E_d/K)} \ll_q \frac{\log d}{d}, \quad (\textit{as } d \to \infty),$$

*for some effective constants depending at most on $q$.*

This is a straightforward consequence of our computations of $H(E_d/K)$, $|E_d(K)_{\mathrm{tors}}|$ and $\tau(E_d/K)$.

**Remark 1.7.** The above Corollary could also have been obtained as a special case of deep results in [10]. In that paper, the authors prove upper bounds on the order of the torsion subgroup (loc. cit., Thm. 3.8) and on the Tamagawa number (loc. cit., Thm. 6.5), which are valid for abelian varieties over $K$, under mild semistability assumptions.

Note that their proof is much more involved and less explicit, which is why we chose to include a self-contained treatment here.

## 2. Preliminaries for the computation of the $L$-function

The goal of the next section is to calculate the $L$-function of $E_d$ in terms of Jacobi sums. In this section, we introduce the necessary notation and review the required facts about characters and Jacobi sums. The notation introduced in this section will be in force for the rest of the paper.

**2.1. Action of $q$ on $\mathbb{Z}/d\mathbb{Z}$.** For any integer $d \geq 2$ coprime to $q$, the subgroup $\langle q \rangle \subset (\mathbb{Z}/d\mathbb{Z})^\times$ generated by $q$ acts [2] on $\mathbb{Z}/d\mathbb{Z}$ by $n \mapsto q \cdot n$. For any subset $Z \subset \mathbb{Z}/d\mathbb{Z}$ which is stable under this action, we denote by $\mathcal{O}_q(Z)$ the set of orbits of $Z$. In what follows, we will be particularly interested in the set

$$Z_d := \begin{cases} \mathbb{Z}/d\mathbb{Z} \smallsetminus \{0, d/3, 2d/3\} & \text{if } d \equiv 0 \bmod 3, \\ \mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\} & \text{otherwise,} \end{cases}$$

(which is stable under multiplication by $q$ because $\gcd(d, q) = 1$) and in the corresponding set of orbits $\mathcal{O}_q(Z_d)$. Given an orbit $\mathbf{m} \in \mathcal{O}_q(Z_d)$, we will often need to make a choice of representative $m \in Z_d$ of this orbit: we make the convention that orbits in $\mathcal{O}_q(Z_d)$ are always denoted by a bold letter ($\mathbf{m}$, $\mathbf{n}$, ...) and that the corresponding normal letter ($m$, $n$, ...) designates any choice of representative of this orbit in $Z_d$. We also identify without comment $\mathbb{Z}/d\mathbb{Z}$ with its lift $\{0, 1, 2, \dots, d-1\}$ in $\mathbb{Z}$.

For any orbit $\mathbf{m} \in \mathcal{O}_q(Z_d)$, its length $|\mathbf{m}| = |\{m, qm, q^2m, \dots\}|$ equals

$$|\mathbf{m}| = \min \{n \in \mathbb{Z}_{\geq 1} : \ q^n m \equiv m \bmod d\},$$

which can equivalently be described as the multiplicative order of $q$ modulo $d/\gcd(d, m)$, for any $m \in \mathbf{m}$. By construction of the multiplicative order, we note that, for a power $q^n$ of $q$, one has $q^n m \equiv m \bmod d$ if and only if $|\mathbf{m}|$ divides $n$ i.e., if and only if $\mathbb{F}_{q^n}$ is an extension of $\mathbb{F}_{q^{|\mathbf{m}|}}$.

**Remark 2.1.** In the special case when $d$ divides $q - 1$, the action of $q$ on $Z_d$ is trivial and there is a bijection between $\mathcal{O}_q(Z_d)$ and $Z_d$.

**2.2. Characters of order dividing $d$.** Fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ and a prime ideal $\mathfrak{P}$ above $p$ in the ring of integers $\overline{\mathbb{Z}}$ of $\overline{\mathbb{Q}}$: the residue field $\overline{\mathbb{Z}}/\mathfrak{P}$ is an algebraic closure $\overline{\mathbb{F}_p}$ of $\mathbb{F}_p$. The given finite field $\mathbb{F}_q$ and, more generally, any finite extension thereof will be viewed as subfields of $\overline{\mathbb{F}_p}$. The reduction map $\overline{\mathbb{Z}} \to \overline{\mathbb{Z}}/\mathfrak{P}$ induces an isomorphism between the group $\mu_{\infty,p'} \subset \overline{\mathbb{Z}}^\times$ of roots of unity of order prime to $p$ and the multiplicative group $\overline{\mathbb{F}_p}^\times$. We let $\mathbf{t} : \overline{\mathbb{F}_p}^\times \to \mu_{\infty,p'}$ be the inverse of this isomorphism, viewed as a $\overline{\mathbb{Q}}^\times$-valued map, and we denote by the same letter the restriction of $\mathbf{t}$ to any finite extension of $\mathbb{F}_q$.

[2] For brevity, we will simply say that "$q$ acts on $\mathbb{Z}/d\mathbb{Z}$ by multiplication".

Any nontrivial multiplicative character on a finite extension of $\mathbb{F}_q$ is then a power of (a restriction of) $\mathbf{t}$, cf. [1, §3.6.2]. The trivial multiplicative character will be denoted by $\mathbb{1}$.

**Definition 2.2.** *For any $m \in \mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\}$ and any integer $s \geq 1$, define a character $\mathbf{t}_m^{(s)} : \mathbb{F}_{q^{s\cdot|\mathbf{m}|}}^{\times} \to \overline{\mathbb{Q}}^{\times}$ by setting*

$$\forall\, x \in \mathbb{F}_{q^{s\cdot|\mathbf{m}|}}^{\times}, \quad \mathbf{t}_m^{(s)}(x) := \left(\mathbf{t} \circ \mathbf{N}_{q^{s\cdot|\mathbf{m}|}/q^{|\mathbf{m}|}}(x)\right)^{(q^{|\mathbf{m}|}-1)m/d}$$

*Here, $\mathbf{N}_{q^{s\cdot|\mathbf{m}|}/q^{|\mathbf{m}|}} : \mathbb{F}_{q^{s\cdot|\mathbf{m}|}} \to \mathbb{F}_{q^{|\mathbf{m}|}}$ denotes the norm of the extension $\mathbb{F}_{q^{s\cdot|\mathbf{m}|}}/\mathbb{F}_{q^{|\mathbf{m}|}}$. When $s = 1$, we denote $\mathbf{t}_m^{(1)}$ by $\mathbf{t}_m$ for short.*

Note that $\mathbf{t}_m^{(s)}$ is indeed a multiplicative character on $\mathbb{F}_{q^{s\cdot|\mathbf{m}|}}^{\times}$, because $\mathbf{t}$ is one and the norm $\mathbf{N}_{q^{s\cdot|\mathbf{m}|}/q^{|\mathbf{m}|}}$ is multiplicative. We extend $\mathbf{t}_m^{(s)}$ to the whole of $\mathbb{F}_{q^{s\cdot|\mathbf{m}|}}^{\times}$ by putting $\mathbf{t}_m^{(s)}(0) := 0$.

By construction, $\mathbf{t}_m$ is a nontrivial character on $\mathbb{F}_{q^{|\mathbf{m}|}}^{\times}$ and its order divides $d$: more precisely, by noting that the restriction of $\mathbf{t}$ to $\mathbb{F}_{q^{|\mathbf{m}|}}^{\times}$ has exact order $q^{|\mathbf{m}|} - 1$, it can be shown that the order of $\mathbf{t}_m$ is exactly $d/\gcd(d, m)$. The "lifted character" $\mathbf{t}_m^{(s)}$ is defined on $\mathbb{F}_{q^{s\cdot|\mathbf{m}|}}^{\times}$ and has the same order as $\mathbf{t}_m$ because the norm $\mathbf{N}_{q^{s\cdot|\mathbf{m}|}/q^{|\mathbf{m}|}}$ is surjective.

Moreover, the following result shows that we can thus enumerate all characters of order dividing $d$ on finite extensions of $\mathbb{F}_q$:

**Lemma 2.3.** *Let $d \geq 2$ be coprime to $q$ and $\mathbb{F}_{q^n}$ be the extension of degree $n$ of $\mathbb{F}_q$. Denote by $X(d, q^n)$ the set of nontrivial characters $\chi$ on $\mathbb{F}_{q^n}^{\times}$ such that $\chi^d = \mathbb{1}$. Then*

$$X(d, q^n) = \left\{\mathbf{t}_m^{(s)},\ m \in \mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\} \text{ and } s \geq 1 \text{ such that } s \cdot |\mathbf{m}| = n\right\}.$$

*Proof.* The characters $\mathbf{t}_m^{(s)}$ appearing on the right-hand side all belong to $X(d, q^n)$ for they are all nontrivial characters on $\mathbb{F}_{q^n}^{\times}$ with order dividing $d$. To prove the converse inclusion, let $d_n = \gcd(d, q^n - 1)$ and $\chi_0 = \mathbf{t}^{(q^n-1)/d_n}$. By the discussion above, $\chi_0$ is a character on $\mathbb{F}_{q^n}^{\times}$ of exact order $d_n$. Thus, by cyclicity of the character group of $\mathbb{F}_{q^n}^{\times}$, $\chi_0$ generates the subgroup of characters of order dividing $d$, which is none other than $X(d, q^n) \cup \{\mathbb{1}\}$. Hence, for any $\chi \in X(d, q^n)$, there is a unique $k \in \mathbb{Z}$ such that $1 \leq k < d_n$ and $\chi = \chi_0^k = \mathbf{t}^{(q^n-1)\cdot k/d_n}$. Let $m = kd/d_n \in \mathbb{Z}$ and note that $1 \leq m < d$. By construction, $d$ divides $m(q^n - 1)$ and we have $\chi = \mathbf{t}^{(q^n-1)m/d}$. Recall that $|\mathbf{m}|$ is the multiplicative order of $q$ modulo $d/\gcd(d, m)$: by definition, this implies that $|\mathbf{m}|$ divides $n$ (see Section 2.1), so that we can write $n = s \cdot |\mathbf{m}|$ for some $s \geq 1$.

This shows that $\chi = \mathbf{t}^{(q^{s\cdot|\mathbf{m}|}-1)m/d} = \mathbf{t}^{(q|\mathbf{m}|-1)m/d} \circ \mathbf{N}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^{|\mathbf{m}|}}} = \mathbf{t}_m^{(s)}$. □

We will actually need the following, slightly more precise, result:

**Lemma 2.4.** *Let $d \geq 2$ be coprime to $q$ and $\mathbb{F}_{q^n}$ be the extension of degree $n$ of $\mathbb{F}_q$. Denote by $X_3(d, q^n)$ the set of $\chi \in X(d, q^n)$ such that $\chi^3 \neq \mathbb{1}$. Then*

$$X_3(d, q^n) = \left\{ \mathbf{t}_m^{(s)},\ m \in Z_d \text{ and } s \geq 1 \text{ such that } s \cdot |\mathbf{m}| = n \right\},$$

*where $Z_d$ is as defined in Section 2.1.*

*Proof.* We distinguish two cases. First, if $3 \nmid d$, there are no nontrivial character of order dividing $d$ whose third power is trivial (since 3 and $d$ are coprime), so that $X_3(d, q^n) = X(d, q^n)$. On the other hand, $Z_d = \mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\}$, and the preceding Lemma allows us to conclude in this case. In the remaining case when 3 divides $d$, we have $Z_d = \mathbb{Z}/d\mathbb{Z} \smallsetminus \{0, d/3, 2d/3\}$ and $X_3(d, q^n) = X(d, q^n) \smallsetminus \{\chi : \chi^3 = \mathbb{1}\}$. Since the order of $\mathbf{t}_m^{(s)}$ for $m \in \mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\}$ is exactly $d/\gcd(d, m)$, a direct inspection shows that $(\mathbf{t}_m^{(s)})^3 = \mathbb{1}$ if and only if $m = d/3$ or $2d/3$. This proves the claim. □

**Remark 2.5.** In the special case when $d$ divides $q - 1$, the characters $\mathbf{t}_m$ ($m \in Z_d$) are all characters of $\mathbb{F}_q^\times$ because $|\mathbf{m}| = 1$. Since there are *a priori* $|Z_d|$ nontrivial characters $\chi$ on $\mathbb{F}_q^\times$ such that $\chi^d = \mathbb{1}$ and $\chi^3 \neq \mathbb{1}$, we have enumerated all possible such characters.

**2.3. Jacobi sums.** Let $\mathbb{F}_r$ be a finite field of odd characteristic (in our applications, $\mathbb{F}_r$ will be a finite extension of $\mathbb{F}_q$). We extend the (multiplicative) characters $\chi : \mathbb{F}_r^\times \to \overline{\mathbb{Q}}^\times$ to the whole of $\mathbb{F}_r$ by setting $\chi(0) = 0$ if $\chi$ is not the trivial character $\mathbb{1}$, and by $\mathbb{1}(0) = 1$. For a character $\chi : \mathbb{F}_r^\times \to \overline{\mathbb{Q}}^\times$ and an extension $\mathbb{F}_{r'}/\mathbb{F}_r$ of degree $s \geq 1$, whose norm is denoted by $\mathbf{N}_{r'/r} : \mathbb{F}_{r'} \to \mathbb{F}_r$, we let $\chi^{(s)} := \chi \circ \mathbf{N}_{r'/r}$ be the "lifted" character.

To any triple of characters $\chi_1, \chi_2, \chi_3$ on $\mathbb{F}_r^\times$, we associate a Jacobi sum

$$\mathbf{j}_r(\chi_1, \chi_2, \chi_3) := \sum_{\substack{x_1, x_2, x_3 \in \mathbb{F}_r \\ x_1 + x_2 + x_3 = 1}} \chi_1(x_1)\chi_2(x_2)\chi_3(x_3).$$

Let us recall some classical facts about these sums (see [1, §2.5.3–§2.5.4] for details and proofs). If $\chi_1$, $\chi_2$, $\chi_3$ and $\chi_1\chi_2\chi_3$ are all nontrivial, one has $|\mathbf{j}_r(\chi_1, \chi_2, \chi_3)| = r$. If $\chi_1$, $\chi_2$, $\chi_3$ are nontrivial but $\chi_1\chi_2\chi_3$ is trivial, the Jacobi sum "degenerates" to:

$$\mathbf{j}_r(\chi_1, \chi_2, \chi_3) = -\chi_3(-1) \cdot \sum_{\substack{x_1, x_2 \in \mathbb{F}_r \\ x_1 + x_2 = 1}} \chi_1(x_1)\chi_2(x_2). \tag{2.1}$$

Besides, Jacobi sums satisfy the Hasse–Davenport relation (see [1, §3.7]): for any finite extension $\mathbb{F}_{r'}/\mathbb{F}_r$ of degree $s$, and any characters $\chi_1, \chi_2, \chi_3$ on $\mathbb{F}_r^\times$, one has

$$\mathbf{j}_{r'}(\chi_1^{(s)}, \chi_2^{(s)}, \chi_3^{(s)}) = \mathbf{j}_r(\chi_1, \chi_2, \chi_3)^s. \tag{2.2}$$

We finally introduce the following notation:

**Definition 2.6.** *For any $m \in Z_d$, we let*

$$\mathbf{J}(m) := \mathbf{j}_{q^{|\mathbf{m}|}}(\mathbf{t}_m, \mathbf{t}_m, \mathbf{t}_m). \tag{2.3}$$

*Notice that $\mathbf{J}(m) = \mathbf{J}(q \cdot m)$ since $x \mapsto x^q$ is a bijection of $\mathbb{F}_{q^{|\mathbf{m}|}}$. For an orbit $\mathbf{m} \in \mathcal{O}_q(Z_d)$, we can thus define $\mathbf{J}(\mathbf{m}) := \mathbf{J}(m)$ for any choice of $m \in \mathbf{m}$.*

By construction of $Z_d$, neither $\mathbf{t}_m$ nor $(\mathbf{t}_m)^3$ is trivial, so that $|\mathbf{J}(\mathbf{m})| = q^{|\mathbf{m}|}$ for all $\mathbf{m} \in \mathcal{O}_q(Z_d)$.

## 3. The *L*-function

For any place $v$ of $K$, let $q_v$ be the cardinality of the residue field $\mathbb{F}_v$ of $K$ at $v$, and denote by $(\widetilde{E_d})_v$ the reduction modulo $v$ of a minimal integral model of $E_d$ at $v$ (a plane cubic curve over $\mathbb{F}_v$). By definition, the $L$-function of $E_d$ is the power series given by

$$L(E_d/K, T) = \prod_{v \text{ good}} \left(1 - a_v \cdot T^{\deg v} + q_v \cdot T^{2 \deg v}\right)^{-1} \cdot \prod_{v \text{ bad}} \left(1 - a_v \cdot T^{\deg v}\right)^{-1} \in \mathbb{Q}[\![T]\!], \tag{3.1}$$

where the products are over the places of $K$ of good, resp. bad, reduction for $E_d$, and where $a_v := q_v + 1 - |(\widetilde{E_d})_v(\mathbb{F}_v)|$. Remark that, when $E_d$ has bad reduction at $v$, $a_v$ is $0, +1$ or $-1$ depending on whether the reduction of $E$ at $v$ is additive, split multiplicative or nonsplit multiplicative respectively. See [19, Lect. 1, §9] for more details.

With the notation introduced in the previous section, we can now state our main result:

**Theorem 3.1.** *Let $d \geq 2$ be an integer coprime with $q$, and set*

$$Z_d := \begin{cases} \mathbb{Z}/d\mathbb{Z} \smallsetminus \{0, d/3, 2d/3\} & \text{if } d \equiv 0 \bmod 3, \\ \mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\} & \text{otherwise.} \end{cases}$$

*The $L$-function of $E_d/K$ is given by*

$$L(E_d/K, T) = \prod_{\mathbf{m} \in \mathcal{O}_q(Z_d)} \left(1 - \mathbf{t}_m(-1)\mathbf{J}(\mathbf{m}) \cdot T^{|\mathbf{m}|}\right) \in \mathbb{Z}[T], \tag{3.2}$$

*where $\mathbf{J}(\mathbf{m})$ is the Jacobi sum defined in* (2.3).

The rest of the section is devoted to the proof of this Theorem. Our strategy is inspired by that of [2, Thm. 3.2.1]: we calculate $L(E_d/K,T)$ by manipulations of character sums. Let us note that an alternative, more cohomological, computation could be conducted (along the lines of [17, §7], which treats a different family of elliptic curves). The latter approach would be less elementary, but would have the advantage of "explaining" the appearance of Jacobi sums in $L(E_d/K,T)$. Indeed, one would then rely on the fact that the minimal regular model $\mathcal{E}_d \to \mathbb{P}^1$ of $E_d/K$ is dominated by a quotient of the Fermat surface $\mathcal{F}_d/\mathbb{F}_q$ of degree $d$ (see [18] and [19, Lect. 3, §10]), whose zeta function is well-known to involve Jacobi sums (see [7]).

**Remark 3.2.** In the special case when $d$ divides $q-1$, the expression in (3.2) above simplifies. Indeed, letting $\chi$ be a character on $\mathbb{F}_q^\times$ of exact order $d$, one has

$$L(E_d/K,T) = \prod_{\substack{1\le k\le d\\ 3k\not\equiv 0 \bmod d}} \left(1-\chi(-1)^k \mathbf{j}_q(\chi^k,\chi^k,\chi^k)\cdot T\right). \tag{3.3}$$

This was stated as Theorem A in the introduction; it follows from Theorem 3.1 with Remarks 2.1 and 2.5.

**3.1. Character sums identities.** The proof of Theorem 3.1 requires two identities about character sums, which we first establish.

For any finite field $\mathbb{F}_r$ of odd characteristic, we denote by $\lambda : \mathbb{F}_r^\times \to \{\pm 1\}$ the unique nontrivial character of order 2 on $\mathbb{F}_r^\times$ (the "Legendre symbol" of $\mathbb{F}_r$), extended by $\lambda(0)=0$.

**Proposition 3.3.** *Let $\mathbb{F}_r$ be a finite field of odd characteristic. For any character $\chi : \mathbb{F}_r^\times \to \overline{\mathbb{Q}}^\times$,*

$$\sum_{z\in\mathbb{F}_r}\sum_{x\in\mathbb{F}_r} \chi(z)\cdot\lambda(x^3+x^2-8zx+16z^2) = \begin{cases} 0 & \text{if } \chi \text{ is trivial,}\\ \chi(-1)\cdot \mathbf{j}_r(\chi,\chi,\chi) & \text{otherwise.}\end{cases}$$

*Proof.* Let $S_r(\chi)$ denote the double sum on the left-hand side of the identity in the Proposition. We first put $u=4z$ in the outer sum, exchange the order of summation and split the sum according to whether $x=0$ or not: we obtain that

$$\begin{aligned}\chi(4)\cdot S_r(\chi) &= \sum_{u\in\mathbb{F}_r}\chi(u)\lambda(u)^2 + \sum_{x\neq 0}\sum_{u\in\mathbb{F}_r}\chi(u)\lambda(x^3+x^2-2ux+u^2)\\ &= \sum_{u\neq 0}\chi(u) + \sum_{x\neq 0}\left(\sum_{u\in\mathbb{F}_r}\chi(u)\cdot\lambda(x^3+(x-u)^2)\right),\end{aligned}$$

since $\lambda(u)^2=1$ (resp. 0) for $u\neq 0$ (resp. for $u=0$).

To treat the sum over $x \neq 0$, we note the following: for a given $x \neq 0$, writing $u = x(y+1)$ yields that

$$\sum_{u \in \mathbb{F}_r} \chi(u) \cdot \lambda(x^3 + (x-u)^2) = \chi(x) \cdot \sum_{y \in \mathbb{F}_r} \chi(y+1) \cdot \lambda(x + y^2).$$

Summing this identity over all $x \neq 0$ and exchanging the order of summation leads to

$$\chi(4) \cdot S_r(\chi) = \sum_{u \neq 0} \chi(u) + \sum_{y \in \mathbb{F}_r} \chi(y+1) \left( \sum_{x \neq 0} \chi(x) \lambda(x + y^2) \right).$$

If $\chi$ is trivial, a straightforward evaluation of the sums leads to the desired result: namely that $S_r(\chi) = 0$. From now on, we thus assume that $\chi$ is nontrivial. In that case, $\sum_{u \neq 0} \chi(u) = 0$ and $\chi(0) = 0$, so that the last displayed identity reads:

$$S_r(\chi) = \chi^{-1}(4) \cdot \sum_{y \in \mathbb{F}_r} \chi(y+1) \left( \sum_{x \in \mathbb{F}_r} \chi(x) \lambda(x + y^2) \right).$$

Recall that $1 + \lambda(w) = |\{t \in \mathbb{F}_r : t^2 = w\}|$ for all $w \in \mathbb{F}_r$. Thus, for any $y \in \mathbb{F}_r$, one can rewrite the sums over $x$ under the form:

$$\begin{aligned} \sum_{x \in \mathbb{F}_r} \chi(x) \lambda(x + y^2) &= \sum_{x \in \mathbb{F}_r} \chi(x)(1 + \lambda(x + y^2)) \\ &= \sum_{x \in \mathbb{F}_r} \chi(x) \cdot \Big| \{t \in \mathbb{F}_r : x = t^2 - y^2\} \Big| = \sum_{t \in \mathbb{F}_r} \chi(t^2 - y^2). \end{aligned}$$

We derive that

$$S_r(\chi) = \chi^{-1}(4) \cdot \sum_{(y,t) \in \mathbb{F}_r^2} \chi(t-y) \chi(t+y) \chi(y+1).$$

Since the map $\mathbb{F}_r^2 \to \{(x_1, x_2, x_3) \in \mathbb{F}_r^3 : x_1 + x_2 + x_3 = 1\}$ given by $(y,t) \mapsto ((t-y)/2, -(y+t)/2, y+1)$ is a bijection, we can write the latter double sum as a Jacobi sum:

$$\begin{aligned} \sum_{(y,t) \in \mathbb{F}_r^2} \chi(t-y) \chi(t+y) \chi(y+1) &= \chi(-4) \cdot \sum_{\substack{x_1 + x_2 + x_3 = 1, \\ x_i \in \mathbb{F}_r}} \chi(x_1) \chi(x_2) \chi(x_3) \\ &= \chi(-4) \cdot \mathbf{j}_r(\chi, \chi, \chi). \end{aligned}$$

Therefore, we have proved that $S_r(\chi) = \chi(-1) \cdot \mathbf{j}_r(\chi, \chi, \chi)$ for a nontrivial character $\chi$. This concludes the proof. □

**Proposition 3.4.** *Let $\mathbb{F}_r$ be a finite field of odd characteristic, and $a \in \mathbb{F}_r^\times$. Then*

$$\sum_{x \in \mathbb{F}_r} \lambda(x^3 + a) = -\lambda(a) \cdot \sum_{\substack{\xi^3 = \mathbb{1} \\ \xi \neq \mathbb{1}}} \xi(4a) \cdot \mathbf{j}_r(\xi, \xi, \xi), \tag{3.4}$$

*where the sum on the right-hand side is over characters* $\xi : \mathbb{F}_r^\times \to \overline{\mathbb{Q}}^\times$ *of exact order* 3.

The sum over $\xi$ in (3.4) contains 2 or 0 terms, depending on whether 3 divides $|\mathbb{F}_r^\times| = r-1$ or not, respectively (because $\mathbb{F}_r^\times$ is cyclic).

*Proof.* For any $z \in \mathbb{F}_r$, one has $\big|\{x \in \mathbb{F}_r : x^3 = z\}\big| = \sum_{\xi^3=\mathbb{1}} \xi(z)$ where the sum is over characters $\xi$ on $\mathbb{F}_r^\times$ such that $\xi^3 = \mathbb{1}$ (see [1, Lem. 2.5.21]). Therefore

$$\sum_{x\in\mathbb{F}_r} \lambda(x^3+a) = \sum_{z\in\mathbb{F}_r} \big|\{x \in \mathbb{F}_r : x^3 = z\}\big| \cdot \lambda(z+a) \tag{3.5}$$
$$= \sum_{z\in\mathbb{F}_r} \lambda(z+a) + \sum_{\substack{\xi^3=\mathbb{1}\\ \xi\neq\mathbb{1}}} \left( \sum_{z\in\mathbb{F}_r} \xi(z)\lambda(z+a) \right).$$

The first sum on the right-hand side vanishes because $\lambda$ is nontrivial. Hence we are done if 3 does not divide $|\mathbb{F}_r^\times|$, since the sum over $\xi$ is then empty.

In the case where 3 divides $|\mathbb{F}_r^\times|$, let $\xi$ be one of the two characters of exact order 3 on $\mathbb{F}_r^\times$. Then,

$$\sum_{z\in\mathbb{F}_r} \xi(z)\lambda(z+a) = \sum_{\substack{x_1,x_2\in\mathbb{F}_r\\ x_1+x_2=1}} \xi(-ax_1)\lambda(ax_2) = \xi(-a)\lambda(a) \cdot \sum_{\substack{x_1,x_2\in\mathbb{F}_r\\ x_1+x_2=1}} \xi(x_1)\lambda(x_2)$$
$$= \xi(-4a)\lambda(a) \cdot \sum_{\substack{y_1,y_2\in\mathbb{F}_r\\ y_1+y_2=1}} \xi(y_1)\xi(y_2) = -\xi(4a)\lambda(a) \cdot \mathbf{j}_r(\xi,\xi,\xi).$$

The penultimate equality follows from [1, Prop. 2.5.18], and the last one from (2.1) because $\xi^3 = \mathbb{1}$.

Plugging this result twice into (3.5) finishes the proof. □

**3.2. Proof of Theorem 3.1.** From the definition (3.1) of the $L$-function, expanding $\log L(E_d/K,T)$ as a power series and rearranging terms as in [2, §3.2], one arrives at the following expression for $L(E_d/K,T)$:

**Lemma 3.5.** *For any* $\tau \in \mathbb{P}^1(\overline{\mathbb{F}_q})$*, denote by* $v_\tau$ *the place of* $K$ *corresponding to* $\tau$*, and by* $(\widetilde{E_d})_\tau$ *the reduction of an integral minimal model of* $E_d$ *modulo* $v_\tau$*. For all* $n \geq 1$ *and any* $\tau \in \mathbb{P}^1(\mathbb{F}_{q^n})$*, we let*

$$A_d(\tau, q^n) := q^n + 1 - |(\widetilde{E_d})_\tau(\mathbb{F}_{q^n})|.$$

*Then, the* $L$*-function of* $E_d/K$ *satisfies the formal identity*

$$\log L(E_d/K,T) = \sum_{n=1}^{\infty} \left( \sum_{\tau\in\mathbb{P}^1(\mathbb{F}_{q^n})} A_d(\tau,q^n) \right) \cdot \frac{T^n}{n}. \tag{3.6}$$

Our first step will be to find a more explicit expression for the inner sums in (3.6). For any finite extension $\mathbb{F}_{q^n}$ of $\mathbb{F}_q$, we again denote by $\lambda : \mathbb{F}_{q^n}^\times \to \{\pm 1\}$ the quadratic character on $\mathbb{F}_{q^n}^\times$. For any $\tau \in \mathbb{P}^1(\mathbb{F}_{q^n})$, we fix an affine model $y^2 = f_\tau(x)$ of $(\widetilde{E_d})_\tau$ with $f_\tau(x) \in \mathbb{F}_{q^n}[x]$ of degree 3. A standard computation yields that

$$\begin{aligned} A_d(\tau, q^n) &= q^n + 1 - |(\widetilde{E_d})_\tau(\mathbb{F}_{q^n})| \\ &= q^n - \sum_{x \in \mathbb{F}_{q^n}} (1 + \lambda(f_\tau(x))) = - \sum_{x \in \mathbb{F}_{q^n}} \lambda(f_\tau(x)). \end{aligned} \tag{3.7}$$

The value of $A_d(\infty, q^n)$ depends on the reduction of $E_d$ at $\tau = \infty$ which, by Proposition 1.2, is as follows. When $d$ is not divisible by 3, $E_d$ has additive reduction at $\infty$ and $(\widetilde{E_d})_\infty$ is a rational curve over $\mathbb{F}_q$, whence $A_d(\infty, q^n) = 0$ in that case. When 3 divides $d$, $E_d$ has good reduction at $\infty$ and the reduced curve $(\widetilde{E_d})_\infty$ has affine model $y^2 = x^3 + 1/4$ over $\mathbb{F}_q$ (see Remark 1.4). Therefore, by (3.7) and Proposition 3.4 (with $r = q^n$ and $a = 1/4$), one has

$$\begin{aligned} A_d(\infty, q^n) &= - \sum_{x \in \mathbb{F}_{q^n}} \lambda(x^3 + 1/4) \\ &= \sum_{\substack{\xi^3 = \mathbb{1} \\ \xi \neq \mathbb{1}}} \mathbf{j}_{q^n}(\xi, \xi, \xi) = \sum_{\substack{\xi^3 = \mathbb{1} \\ \xi \neq \mathbb{1}}} \xi(-1) \cdot \mathbf{j}_{q^n}(\xi, \xi, \xi), \end{aligned}$$

where the sum is over nontrivial characters $\xi$ of $\mathbb{F}_{q^n}^\times$ such that $\xi^3 = \mathbb{1}$ (note that $\xi(-1) = 1$ for such a $\xi$).

Next for any $\tau \in \mathbb{F}_{q^n}$, as was noted in Remark 1.4, one can take $f_\tau(x)$ to be $f_\tau(x) = x^3 + x^2 - 8\tau^d \cdot x + 16\tau^{2d}$, and (3.7) here leads to

$$A_d(\tau, q^n) = - \sum_{x \in \mathbb{F}_{q^n}} \lambda\left(x^3 + x^2 - 8\tau^d \cdot x + 16\tau^{2d}\right).$$

For any $z \in \mathbb{F}_{q^n}$, one has $\left|\left\{\tau \in \mathbb{F}_{q^n} : \tau^d = z\right\}\right| = \sum_{\chi^d = \mathbb{1}} \chi(z)$, where the sum is over all characters $\chi$ of $\mathbb{F}_{q^n}^\times$ such that $\chi^d = \mathbb{1}$ (see [1, Lem. 2.5.21]). After exchanging order of summation, we obtain that

$$\begin{aligned} \sum_{\tau \in \mathbb{F}_{q^n}} A(\tau, q^n) &= - \sum_{\tau \in \mathbb{F}_{q^n}} \sum_{x \in \mathbb{F}_{q^n}} \lambda\left(x^3 + x^2 - 8\tau^d \cdot x + 16\tau^{2d}\right) \\ &= - \sum_{z \in \mathbb{F}_{q^n}} \left|\{\tau \in \mathbb{F}_{q^n} : \tau^d = z\}\right| \cdot \sum_{x \in \mathbb{F}_{q^n}} \lambda\left(x^3 + x^2 - 8zx + 16z^2\right) \\ &= - \sum_{\chi^d = \mathbb{1}} \left( \sum_{z \in \mathbb{F}_{q^n}} \sum_{x \in \mathbb{F}_{q^n}} \chi(z) \lambda\left(x^3 + x^2 - 8zx + 16z^2\right) \right). \end{aligned}$$

Using Proposition 3.3 on the inner sums (with $r = q^n$), we find that

$$\sum_{\tau\in\mathbb{P}^1(\mathbb{F}_{q^n})} A(\tau, q^n) = A(\infty, q^n) - \sum_{\chi\in X(d,q^n)} \chi(-1)\cdot \mathbf{j}_{q^n}(\chi,\chi,\chi),$$

where, for all $e \geq 1$, we write $X(e, q^n)$ for the set of nontrivial characters $\chi$ on $\mathbb{F}_{q^n}^\times$ such that $\chi^e = \mathbb{1}$. By our expression of $A(\infty, q^n)$, it follows that

$$\sum_{\tau\in\mathbb{P}^1(\mathbb{F}_{q^n})} A_d(\tau, q^n)$$
$$= \begin{cases} \displaystyle\sum_{\chi\in X(3,q^n)} \xi(-1)\mathbf{j}_{q^n}(\xi,\xi,\xi) - \sum_{\chi\in X(d,q^n)} \chi(-1)\mathbf{j}_{q^n}(\chi,\chi,\chi) & \text{if } 3 \mid d, \\ \displaystyle 0 \qquad\qquad\qquad - \sum_{\chi\in X(d,q^n)} \chi(-1)\mathbf{j}_{q^n}(\chi,\chi,\chi) & \text{else.} \end{cases}$$

In both cases, one can rewrite this as

$$\sum_{\tau\in\mathbb{P}^1(\mathbb{F}_{q^n})} A_d(\tau, q^n) = - \sum_{\chi\in X_3(d,q^n)} \chi(-1)\cdot \mathbf{j}_{q^n}(\chi,\chi,\chi),$$

where the sum is over the set $X_3(d, q^n)$ of nontrivial characters $\chi$ on $\mathbb{F}_{q^n}^\times$ such that $\chi^d = \mathbb{1}$ and $\chi^3 \neq \mathbb{1}$ (see Section 2.2). Plugging this last identity into (3.6), we obtain that

$$-\log L(E_d/K, T) = \sum_{n\geq 1} \left( \sum_{\chi\in X_3(d,q^n)} \chi(-1)\cdot \mathbf{j}_{q^n}(\chi,\chi,\chi) \right) \cdot \frac{T^n}{n}. \tag{3.8}$$

We now perform a "reindexation" of this double sum: Lemma 2.4 allows us to rewrite (3.8) under the form:

$$-\log L(E_d/K, T) = \sum_{m\in Z_d} \left( \sum_{s\geq 1} \mathbf{t}_m^{(s)}(-1)\cdot \mathbf{j}_{q^{s\cdot|\mathbf{m}|}}(\mathbf{t}_m^{(s)}, \mathbf{t}_m^{(s)}, \mathbf{t}_m^{(s)}) \cdot \frac{T^{s\cdot|\mathbf{m}|}}{s\cdot|\mathbf{m}|} \right).$$

Further, $\mathbf{t}_m^{(s)}(-1) = \mathbf{t}_m(-1)^s$ and the Hasse–Davenport relation (2.2) implies that

$$\forall\, m \in Z_d, \forall\, s \geq 1, \quad \mathbf{j}_{q^{s\cdot|\mathbf{m}|}}(\mathbf{t}_m^{(s)}, \mathbf{t}_m^{(s)}, \mathbf{t}_m^{(s)}) = \mathbf{j}_{q^{|\mathbf{m}|}}(\mathbf{t}_m, \mathbf{t}_m, \mathbf{t}_m)^s = \mathbf{J}(m)^s.$$

Therefore, we derive that

$$\begin{aligned} -\log L(E_d/K, T) &= \sum_{m\in Z_d} \sum_{s\geq 1} \frac{\left(\mathbf{t}_m(-1)\mathbf{J}(m)\cdot T^{|\mathbf{m}|}\right)^s}{s\cdot|\mathbf{m}|} \\ &= -\sum_{m\in Z_d} \frac{1}{|\mathbf{m}|} \cdot \log\left(1 - \mathbf{t}_m(-1)\mathbf{J}(m)\cdot T^{|\mathbf{m}|}\right). \end{aligned}$$

In the right-most sum, notice that each term "$\log(1 - \mathbf{t}_m(-1)\mathbf{J}(m)\cdot T^{|\mathbf{m}|})$" appears $|\mathbf{m}|$ times since $\mathbf{J}(q^k\cdot m) = \mathbf{J}(m)$ for all $k \geq 1$. Thanks to the

"weighting" by $1/|\mathbf{m}|$, we may thus write the sum over $m \in Z_d$ as a sum over $\mathbf{m} \in \mathcal{O}_q(Z_d)$. Finally, we have proved

$$\log L(E_d/K, T) = \sum_{\mathbf{m} \in \mathcal{O}_q(Z_d)} \log\left(1 - \mathbf{t}_m(-1)\mathbf{J}(m) \cdot T^{|\mathbf{m}|}\right).$$

Exponentiating this last identity completes the proof of Theorem 3.1. □

## 4. Bounds on the special value

We now study in more detail the behaviour of $L(E_d/K, T)$ around the point $T = q^{-1}$. More specifically, recall that the *analytic rank* of $E_d$ is defined to be $\rho(E_d/K) := \mathrm{ord}_{T=q^{-1}} L(E_d/K, T)$, and that the *special value of* $L(E_d/K, T)$ *at* $T = q^{-1}$ is the quantity

$$L^*(E_d/K, 1) := \left.\frac{L(E_d/K, T)}{(1 - qT)^\rho}\right|_{T=q^{-1}} \quad \text{where } \rho = \rho(E_d/K). \tag{4.1}$$

By construction and by the Riemann Hypothesis $L^*(E_d/K, 1) \in \mathbb{Z}[q^{-1}]_{>0}$.

**Remark 4.1.** The special value is "usually" defined as the first nonzero coefficient in the Taylor expansion of $s \mapsto L(E_d/K, q^{-s})$ around $s = 1$: our definition (4.1) differs from this more "usual" one by a factor $(\log q)^\rho$, which we prefer to avoid in order to ensure that $L^*(E_d/K, 1) \in \mathbb{Q}^*$. Note that this is consistent with our normalisation of $\mathrm{Reg}(E_d/K)$ (see Section 5 below).

The goal of this section is to give an asymptotic estimate on the size of $L^*(E_d/K, 1)$ in terms of the height $H(E_d/K)$, as $d$ grows to $+\infty$. By a rather crude estimate, as in [10, §7] for example, one readily obtains that

$$-5 + o(1) \leq \frac{\log L^*(E_d/K, 1)}{\log H(E_d/K)} \leq o(1) \qquad (\text{as } d \to \infty).$$

Here, we prove the following improved bounds:

**Theorem 4.2.** *For all $\epsilon \in (0, 1/4)$, there exist positive constants $C_1, C_2$, depending at most on $p$, $q$ and $\epsilon$, such that for any integer $d \geq 2$ coprime to $q$, the special value $L^*(E_d/K, 1)$ satisfies:*

$$-C_1 \cdot \left(\frac{\log\log d}{\log d}\right)^{1/4-\epsilon} \leq \frac{\log L^*(E_d/K, 1)}{\log H(E_d/K)} \leq C_2 \cdot \frac{\log\log d}{\log d}. \tag{4.2}$$

In the next section, we will use the BSD conjecture to reveal the arithmetic significance of such an estimate. The rest of this section is dedicated to the proof of Theorem 4.2. Using Theorem 3.1, we notice that $L(E_d/K, T)$ is a polynomial of the type studied in [7]. The desired bounds on $L^*(E_d/K, 1)$ are then a direct consequence of the results of loc. cit., which we start by recalling.

**4.1. Framework for bounding some special values.** For the convenience of the reader, we briefly recall the setting introduced in [7, §3] to prove bounds on special values of polynomials of the type appearing in (3.2). For any integer $d \geq 2$ coprime to $q$, consider

$$G_d := \left\{ \mathbf{a} = (a_0, a_1, a_2, a_3) \in (\mathbb{Z}/d\mathbb{Z})^4 : a_0 + a_1 + a_2 + a_3 = 0 \right\}.$$

The group $(\mathbb{Z}/d\mathbb{Z})^\times$ acts on $G_d$ by coordinate-wise multiplication. In particular, the subgroup $\langle q \rangle \subset (\mathbb{Z}/d\mathbb{Z})^\times$ acts on $G_d$ and, for any nonempty subset $\Lambda \subset G_d$ which is stable under the action of $\langle q \rangle$, we denote by $\mathcal{O}_q(\Lambda)$ the set of orbits. For $\mathbf{a} \in G_d$, we denote its orbit by $\mathbf{A} = \{\mathbf{a}, q\mathbf{a}, q^2\mathbf{a}, \dots\}$.

We say that a nonempty subset $\Lambda \subset G_d$ satisfies hypothesis (H) if, for all $\epsilon \in (0, 1/4)$, there exists $u \in (0,1)$ such that

$$\text{(H)} \quad \left| \left\{ \mathbf{a} \in \Lambda : d > \max_{0 \leq i \leq 3} \{\gcd(d, a_i)\} > d^u \right\} \right| \leq c' \cdot |\Lambda| \cdot \left( \frac{\log\log d}{\log d} \right)^{1/4-\epsilon},$$

for some constant $c'$.

For $\mathbf{a} = (a_0, \dots, a_3) \in G_d$ with $\mathbf{a} \neq \mathbf{0} = (0,0,0,0)$, whose orbit $\mathbf{A}$ has length $|\mathbf{A}|$, we define four characters on $\mathbb{F}_{q^{|\mathbf{A}|}}^\times$:

$$\forall\, i \in \{0,1,2,3\}, \quad \boldsymbol{\chi}_i : \mathbb{F}_{q^{|\mathbf{A}|}}^\times \to \overline{\mathbb{Q}}^\times,\ x \mapsto \mathbf{t}(x)^{(q^{|\mathbf{A}|}-1)\cdot a_i/d}.$$

One then defines a Jacobi sum $\mathbf{J}'(a_0, a_1, a_2, a_3) \in \mathbb{Q}(\zeta_d)$ by:

$$\mathbf{J}'(a_0, a_1, a_2, a_3) := \frac{1}{q^{|\mathbf{A}|} - 1} \sum_{\substack{x_0, \dots, x_3 \in \mathbb{F}_{q^{|\mathbf{A}|}}^\times \\ x_0 + \cdots + x_3 = 0}} \prod_{i=0}^{3} \boldsymbol{\chi}_i(x_i).$$

Since $\mathbf{a} \in G_d$, the product $\boldsymbol{\chi}_0\boldsymbol{\chi}_1\boldsymbol{\chi}_2\boldsymbol{\chi}_3$ is the trivial character on $\mathbb{F}_{q^{|\mathbf{A}|}}^\times$, and a classical calculation (cf. [1, Lem. 2.5.13]) relates $\mathbf{J}'(a_0, a_1, a_2, a_3)$ to the Jacobi sums in Definition 2.6:

$$\mathbf{J}'(a_0, a_1, a_2, a_3) = (\boldsymbol{\chi}_0\boldsymbol{\chi}_1\boldsymbol{\chi}_2)(-1) \cdot \mathbf{j}_{q^{|\mathbf{A}|}}(\boldsymbol{\chi}_0, \boldsymbol{\chi}_1, \boldsymbol{\chi}_2). \tag{4.3}$$

For any $\mathbf{a} = (a_0, a_1, a_2, a_3) \in G_d \smallsetminus \{\mathbf{0}\}$, it is well-known that $\mathbf{J}'(\mathbf{a}) = 0$ as soon as some (but not all) of the $a_i$'s are 0 mod $d$, and that $|\mathbf{J}'(\mathbf{a})| = q^{|\mathbf{A}|}$ if all $a_i$'s are nonzero (see [1, §2.5]).

To any nonempty subset $\Lambda \subset G_d$ which is stable under the action of $(\mathbb{Z}/d\mathbb{Z})^\times$, we can associate a polynomial

$$P(\Lambda, T) := \prod_{\mathbf{A} \in \mathcal{O}_q(\Lambda)} \left( 1 - \mathbf{J}'(\mathbf{a}) \cdot T^{|\mathbf{A}|} \right),$$

where, for any orbit $\mathbf{A}$, $\mathbf{a} \in G_d$ denotes a choice of representative of $\mathbf{A}$. Since the action of $\mathrm{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q})$ on $\{\mathbf{J}'(\mathbf{a})\}_{\mathbf{a} \in G_d}$ corresponds to the action

of $(\mathbb{Z}/d\mathbb{Z})^\times$ on $G_d$ in the isomorphism $\mathrm{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q}) \simeq (\mathbb{Z}/d\mathbb{Z})^\times$, the assumption that $\Lambda$ is $(\mathbb{Z}/d\mathbb{Z})^\times$-stable ensures that $P(\Lambda, T) \in \mathbb{Z}[T]$. For $\Lambda$ as above, we finally introduce a *special value* $P^*(\Lambda) \in \mathbb{Z}[q^{-1}] \smallsetminus \{0\}$:

$$P^*(\Lambda) := \frac{P(\Lambda, T)}{(1-qT)^\rho}\bigg|_{T=q^{-1}} \qquad \text{where } \rho = \mathrm{ord}_{T=q^{-1}} P(\Lambda, T). \tag{4.4}$$

The following statement summarizes the main technical results of [7]:

**Theorem 4.3.** *For all $\epsilon \in (0, 1/4)$, there exist positive constants $C_3, C_4$, depending at most on $q$, $p$ and $\epsilon$, such that the following holds. For any integer $d \geq 2$ coprime to $q$, and any nonempty subset $\Lambda \subset G_d$ which is stable under the action of $(\mathbb{Z}/d\mathbb{Z})^\times$ and for which hypothesis* (H) *holds, the special value $P^*(\Lambda)$ satisfies*

$$-C_3 \cdot \left(\frac{\log\log d}{\log d}\right)^{1/4-\epsilon} \leq \frac{\log|P^*(\Lambda)|}{\log q^{|\Lambda|}} \leq C_4 \cdot \frac{\log\log|\Lambda|}{\log|\Lambda|}. \tag{4.5}$$

This theorem is a concatenation of Theorems 5.1 and 6.2 in loc.cit.: the proof of the upper bound is relatively straighforward but that of the lower bound is more delicate. It essentially involves two ingredients: the Stickelberger theorem about $p$-adic valuations of Jacobi sums and an average equidistribution theorem for subgroups of $(\mathbb{Z}/d\mathbb{Z})^\times$ (see [7, §4 and §6] for more details).

**4.2. Proof of Theorem 4.2.** In order to apply Theorem 4.3 to the special value $L^*(E_d/K, 1)$, we start by relating $L(E_d/K, T)$ to a certain $P(\Lambda, T)$ as in the last subsection. Namely, for any integer $d \geq 2$ coprime to $q$, we consider the subgroup $H_d \subset G_d$ generated by $\boldsymbol{u} = (1, 1, 1, -3)$ and we let

$$\Lambda_d := H_d \smallsetminus \{\mathbf{0}\} = \{(m, m, m, -3m),\ m \in \mathbb{Z}/d\mathbb{Z}\} \smallsetminus \{\mathbf{0}\}. \tag{4.6}$$

Being a subgroup of $G_d$, $H_d$ is nonempty and stable under multiplication by $(\mathbb{Z}/d\mathbb{Z})^\times$, and so is $\Lambda_d$. We clearly have $|\Lambda_d| = |\mathbb{Z}/d\mathbb{Z}| - 1 = d - 1$. Let $\mathbf{a} = (a_0, \ldots, a_3)$ be an element of $\Lambda_d$, so that $\mathbf{a} = m \cdot \boldsymbol{u}$ for some $m \in \mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\}$. Notice first that $|\mathbf{A}| = |\mathbf{m}|$ because the coordinates of $\boldsymbol{u}$ are pairwise coprime. Also, all the $a_i$'s are nonzero if and only if $m \in Z_d$. Furthermore, it follows from (4.3) that

$$\mathbf{J}'(\mathbf{a}) = \mathbf{J}'(m, m, m, -3m) = \mathbf{t}_m(-1)^3 \cdot \mathbf{j}_{q^{|\mathbf{m}|}}(\mathbf{t}_m, \mathbf{t}_m, \mathbf{t}_m) = \mathbf{t}_m(-1) \cdot \mathbf{J}(m).$$

Consequently, in the notation of Section 4.1, Theorem 3.1 translates as:

**Corollary 4.4.** *Let $d \geq 2$ be an integer coprime to $q$, define $\Lambda_d$ as in* (4.6). *Then the $L$-function of $E_d$ is given by*

$$L(E_d/K, T) = P(\Lambda_d, T) \in \mathbb{Z}[T].$$

In particular, since the definitions (4.1) and (4.4) of special values agree, we see that

$$L^*(E_d/K,1) = P^*(\Lambda_d).$$

Let us now check that the subset $\Lambda_d \subset G_d$ defined in (4.6) satisfies (a strong form of) hypothesis (H):

**Lemma 4.5.** *For all $u \in (0,1)$, one has*

$$\left|\{\mathbf{a} \in \Lambda_d : d > \max_i\{\gcd(d,a_i)\} > d^u\}\right| \ll_u d^{-u/2} \cdot |\Lambda_d|.$$

*Proof.* By construction of $H_d$, any $\mathbf{a} = (a_0,\dots,a_3) \in \Lambda_d$ is of the form $\mathbf{a} = (m,m,m,-3m)$ for some $m \in \mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\}$. Thus, $\max_i\{\gcd(d,a_i)\}$ is at most $3\gcd(d,m)$. In particular, we obtain that

$$\begin{aligned}\left|\{\mathbf{a} \in \Lambda_d : d > \max_i\{\gcd(d,a_i)\} > d^u\}\right| \\ \leq \left|\{m \in \mathbb{Z}/d\mathbb{Z} \smallsetminus \{0\} : \gcd(d,m) > d^u/3\}\right|.\end{aligned}$$

For any divisor $e$ of $d$, the number of $m \in \mathbb{Z}/d\mathbb{Z}$ such that $\gcd(d,m) = e$ is $\phi(d/e) \leq d/e$. Hence,

$$\begin{aligned}|\{m \in \mathbb{Z}/d\mathbb{Z} :\ \gcd(d,m) > d^u/3\}| &= \sum_{\substack{e|d \\ d^u/3<e}} |\{m \in \mathbb{Z}/d\mathbb{Z} :\ \gcd(d,m) = e\}| \\ &\leq \sum_{\substack{e|d \\ d^u/3<e}} \frac{d}{e} \leq \frac{3\tau(d)\cdot d}{d^u},\end{aligned}$$

where $\tau(d)$ is the number of divisors of $d$. By a classical theorem, for all $v > 0$, there is an explicit constant $c_v$ such that $\tau(d) \leq c_v \cdot d^v$ (see [8, Thm. 315] and its proof). In particular, for $v = u/2 > 0$, we have:

$$\left|\{\mathbf{a} \in \Lambda_d :\ d > \max_i\{\gcd(d,a_i)\} > d^u\}\right| \leq 3\tau(d)d^{-u}\cdot d \ll_u d^{-u/2}\cdot|\Lambda_d|.$$

This proves the Lemma, and shows that $\Lambda_d$ satisfies hypothesis (H). □

Together with Corollary 4.4, the previous Lemma implies that Theorem 4.3 applies to $P^*(\Lambda_d) = L^*(E_d/K,1)$. Remembering that $|\Lambda_d| = d-1$, we thus obtain that

$$-C_3 \cdot \left(\frac{\log\log d}{\log d}\right)^{1/4-\epsilon} \leq \frac{\log L^*(E_d/K,1)}{\log q^{d-1}} \leq C_4 \cdot \frac{\log\log d}{\log d}, \quad (\text{as } d \to \infty).$$

By (1.3), we have

$$\forall\, d \geq 2, \quad \frac{9}{4} \leq \frac{3(d+1)}{d+2} \leq \frac{\log q^{d-1}}{\log H(E_d/K)} = \frac{d-1}{\lfloor (d+2)/3 \rfloor} \leq \frac{3(d+1)}{d-1} \leq 9.$$

Combining the last two displayed sets of inequalities concludes the proof of Theorem 4.2.

## 5. Analogue of the Brauer–Siegel theorem

In this section, we reinterpret the bounds in Theorem 4.2 in terms of arithmetic invariants of $E_d/K$, which we first introduce.

By the analogue of the Mordell–Weil theorem for elliptic curves over $K$, the group $E_d(K)$ is finitely generated (cf. [19, Lect. 1, Thm. 5.1]). Furthermore, the group $E_d(K)$ is endowed with the canonical Néron–Tate height $\widehat{h}_{NT} : E_d(K) \to \mathbb{Q}$. The quadratic map $\widehat{h}_{NT}$ induces a $\mathbb{Z}$-bilinear pairing $\langle \cdot, \cdot \rangle_{NT} : E_d(K) \times E_d(K) \to \mathbb{Q}$, which is nondegenerate modulo $E_d(K)_{\mathrm{tors}}$ (cf. [14, Chap. III, Thm. 4.3]). The *Néron–Tate regulator* of $E_d/K$ is then defined as:

$$\mathrm{Reg}(E_d/K) := \left|\det\left(\langle P_i, P_j\rangle_{NT}\right)_{1\le i,j\le r}\right| \in \mathbb{Q}^*,$$

for any choice of a $\mathbb{Z}$-basis $P_1, \dots, P_r \in E_d(K)$ of $E_d(K)/E_d(K)_{\mathrm{tors}}$. Note that we normalize $\langle \cdot, \cdot \rangle_{NT}$ to have values in $\mathbb{Q}$: we may do so since, in our context, this height pairing has an interpretation as an intersection pairing on the minimal regular model of $E_d$ (see [14, Chap. III, §9]).

Let us also recall that the *Tate–Shafarevich group* of $E_d/K$ is defined by

$$Ш(E_d/K) := \ker\left(\mathrm{H}^1(K, E_d) \longrightarrow \prod_v \mathrm{H}^1(K_v, (E_d)_v)\right),$$

see [19, Lect. 1, §11] for more details.

In Theorem 5.1 below, we will see that $Ш(E_d/K)$ is finite.

**5.1. The BSD conjecture.** Inspired by the BSD conjecture for elliptic curves over $\mathbb{Q}$, Tate conjectured in [16] that $\rho(E_d/K)$ and $L^*(E_d/K, 1)$ have an arithmetic interpretation. The conjecture is still open in general, but has been proved in the case of $E_d$ by Ulmer. We state his result as follows:

**Theorem 5.1** (Ulmer)**.** *For all integers $d \ge 1$, coprime with $q$, let $E_d$ be the Hessian elliptic curve* (1.1) *as above. Then the full BSD conjecture is true for $E_d/K$. That is to say,*

- *the Tate–Shafarevich group $Ш(E_d/K)$ is finite,*
- *the rank of $E_d(K)$ is equal to $\mathrm{ord}_{T=q^{-1}} L(E_d/K, T)$,*
- *moreover, one has*

$$L^*(E_d/K, 1) = \frac{|Ш(E_d/K)| \cdot \mathrm{Reg}(E_d/K)}{H(E_d/K)} \cdot \frac{\tau(E_d/K) \cdot q}{|E_d(K)_{\mathrm{tors}}|^2}, \tag{5.1}$$

*where $\tau(E_d/K)$ denotes the global Tamagawa number of $E_d$ (as in Section 1.2) and $H(E_d/K)$ its exponential differential height (as in Section 1.1).*

We refer the reader to [18, §6] for the proof, or to [19, Lect. 3, §10] for a detailed sketch.

**Remark 5.2.** Given Corollary 4.4, Lemma 3.5 in [7] yields fairly explicit expressions for $\rho(E_d/K)$ and $L^*(E_d/K,1)$ as follows. For any integer $d \geq 2$, in the notation of Section 2, consider the two subsets of $Z_d$ given by

$$V_d := \left\{ m \in Z_d : \ \mathbf{t}_m(-1)\mathbf{J}(m) = q^{|\mathbf{m}|} \right\} \quad \text{and} \quad S_d := Z_d \smallsetminus V_d.$$

It is easy to check that the sets $V_d$ and $S_d$ are stable under multiplication by $q$. Then, the analytic rank is given by $\rho(E_d/K) = |\mathcal{O}_q(V_d)|$, and the special value $L^*(E_d/K,1)$ has the following expression:

$$L^*(E_d/K,1) = \prod_{\mathbf{m} \in \mathcal{O}_q(V_d)} |\mathbf{m}| \cdot \prod_{\mathbf{m} \in \mathcal{O}_q(S_d)} \left(1 - \mathbf{t}_m(-1)\mathbf{J}(m) \cdot q^{-|\mathbf{m}|}\right). \tag{5.2}$$

**Remark 5.3.** By Theorem 5.1 above, the analytic rank $\rho(E_d/K)$ is equal to $\mathrm{rank}(E_d(K))$. The expression for $\rho(E_d/K)$ obtained in the previous remark allows us to retrieve a result of Ulmer stating that the ranks of $E_d(K)$ are unbounded as $d$ ranges through integers coprime to $q$ (see [18, §2-§4] and [19, Lect. 4, Thm. 3.1.1]). More precisely, one can show that there are infinitely many integers $d' \geq 2$ coprime to $q$, such that $\mathrm{rank}(E_{d'}(K)) \gg_q d'/\log d'$, where the implied constant is effective and depends only on $q$.

We refer to [4, Prop. 7.3.5] for more details.

We conclude this subsection by recording the following estimate (see also [10, §2]):

**Corollary 5.4.** *When $d \geq 2$ runs over the integers coprime to $q$, one has*

$$\frac{\log\left(|Ш(E_d/K)| \cdot \mathrm{Reg}(E_d/K)\right)}{\log H(E_d/K)} = 1 + \frac{\log L^*(E_d/K,1)}{\log H(E_d/K)} + O\left(\frac{\log d}{d}\right),$$

*where the implicit constant is effective and depends at most on $q$.*

*Proof.* We first note that Theorem 5.1 ensures that $Ш(E_d/K)$ is a finite group, so that the quantity on the left-hand side makes sense. For any integer $d \geq 2$ coprime to $q$, we take the logarithm of (5.1) and divide throughout by $\log H(E_d/K)$. Reordering terms, we obtain that

$$\frac{\log\left(|Ш(E_d/K)| \cdot \mathrm{Reg}(E_d/K)\right)}{\log H(E_d/K)} = 1 + \frac{\log L^*(E_d/K,1)}{\log H(E_d/K)} + \frac{\log\left(\tau(E_d/K) \cdot q \cdot |E_d(K)_{\mathrm{tors}}|^{-2}\right)}{\log H(E_d/K)}.$$

Corollary 1.6 then allows us to control the size of the right-most term.

This yields the desired result. □

**5.2. Analogue of the Brauer–Siegel theorem.** We finally turn to the proof of the asymptotic estimate announced in Theorem B of the introduction:

**Theorem 5.5.** *When $d \geq 2$ ranges through integers coprime to $q$, one has the asymptotic estimate:*

$$\log\left(|Ш(E_d/K)| \cdot \mathrm{Reg}(E_d/K)\right) \sim \log H(E_d/K) \quad (\textit{as } d \to \infty). \tag{5.3}$$

*Proof.* Given what has already been proved, very little remains to be done: by Corollary 5.4, we know that

$$\frac{\log\left(|Ш(E_d/K)| \cdot \mathrm{Reg}(E_d/K)\right)}{\log H(E_d/K)} = 1 + \frac{\log L^*(E_d/K,1)}{\log H(E_d/K)} + O\left(\frac{\log d}{d}\right),$$

as $d$ tends to $+\infty$. Further, Theorem 4.2 implies that, for all $\epsilon \in (0, 1/4)$, there exists a constant $C_5 > 0$ such that

$$\left|\frac{\log L^*(E_d/K,1)}{\log H(E_d/K)}\right| \leq C_5 \cdot \left(\frac{\log\log d}{\log d}\right)^{1/4-\epsilon} \qquad (\text{as } d \to \infty).$$

The concatenation of these two results thus yields that, as $d \to \infty$, one has

$$\frac{\log\left(|Ш(E_d/K)| \cdot \mathrm{Reg}(E_d/K)\right)}{\log H(E_d/K)} = 1 + O\left(\left(\frac{\log\log d}{\log d}\right)^{1/4-\epsilon}\right)$$

where the implicit constant here is effective and depends at most on $q$, $p$ and $\epsilon$. This is more than enough to prove Theorem 5.5. □

**Remark 5.6.** In [10], Hindry and Pacheco suggest to investigate the asymptotic behaviour of the *Brauer–Siegel ratio*

$$\mathfrak{Bs}(E/K) := \log\left(|Ш(E/K)| \cdot \mathrm{Reg}(E/K)\right) / \log H(E/K),$$

as $E$ runs through a family of nonisotrivial elliptic curves over $K$.

If $\mathscr{E}\ell\ell$ denotes the family of all such elliptic curves ordered by differential height, they show (see [10, Coro. 1.13]) that

$$0 \leq \liminf_{E \in \mathscr{E}\ell\ell} \mathfrak{Bs}(E/K) \leq \limsup_{E \in \mathscr{E}\ell\ell} \mathfrak{Bs}(E/K) = 1,$$

conditionally to the BSD conjecture for all $E \in \mathscr{E}\ell\ell$.

In this terminology, Theorem 5.5 above can be rephrased as follows: the ratio $\mathfrak{Bs}(E_d/K)$ has a limit when $E_d$ ranges through the Hessian family of elliptic curves (with $d \to \infty$), and this limit is 1 (unconditionally).

**Acknowledgments.** This article is based on results obtained by the author in his PhD thesis [4]. He would like to thank his supervisor Marc Hindry for his guidance and his encouragements. He also wishes to thank Douglas Ulmer, Michael Tsfasman and the anonymous referee for their interest in this work, their careful reading of a previous version and for their

helpful comments. The author is grateful to Universiteit Leiden for providing financial support and great working conditions during the writing of this article.

## References

[1] H. Cohen, *Number theory. Vol. I. Tools and Diophantine equations*, Graduate Texts in Mathematics, vol. 239, Springer, 2007.
[2] R. P. Conceição, C. Hall & D. Ulmer, "Explicit points on the Legendre curve II", *Math. Res. Lett.* **21** (2014), no. 2, p. 261-280.
[3] C. Davis & T. Occhipinti, "Explicit points on $y^2 + xy - t^d y = x^3$ and related character sums", *J. Number Theory* **168** (2016), p. 13-38.
[4] R. Griffon, "Analogues du théorème de Brauer–Siegel pour quelques familles de courbes elliptiques", PhD Thesis, Université Paris Diderot (France), 2016.
[5] ———, "Analogue of the Brauer–Siegel theorem for Legendre elliptic curves", *J. Number Theory* **193** (2018), p. 189-212.
[6] ———, "Bounds on special values of $L$-functions of elliptic curves in an Artin-Schreier family", to appear in *European J. Math*, 2018.
[7] ———, "A Brauer–Siegel theorem for Fermat surfaces over finite fields", *J. Lond. Math. Soc.* **97** (2018), no. 3, p. 523-549.
[8] G. H. Hardy & E. M. Wright, *An introduction to the theory of numbers*, Oxford University Press, 2008.
[9] M. Hindry, "Why is it difficult to compute the Mordell–Weil group?", in *Diophantine geometry*, Centro di Ricerca Matematica Ennio De Giorgi (CRM), vol. 4, Edizioni della Normale, 2007, p. 197-219.
[10] M. Hindry & A. Pacheco, "An analogue of the Brauer–Siegel theorem for abelian varieties in positive characteristic", *Mosc. Math. J.* **16** (2016), no. 1, p. 45-93.
[11] S. Lang, "Conjectured Diophantine estimates on elliptic curves", in *Arithmetic and geometry, Vol. I*, Progress in Mathematics, vol. 35, Birkhäuser, 1983, p. 155-171.
[12] ———, *Algebraic number theory*, Graduate Texts in Mathematics, vol. 110, Springer, 1994.
[13] M. Schütt & T. Shioda, "Elliptic surfaces", in *Algebraic geometry in East Asia—Seoul 2008*, Advanced Studies in Pure Mathematics, vol. 60, Mathematical Society of Japan, 2008, p. 51-160.
[14] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer, 1994.
[15] ———, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer, 2009.
[16] J. T. Tate, "On the conjectures of Birch and Swinnerton-Dyer and a geometric analog", in *Séminaire Bourbaki, Vol. 9*, Société Mathématique de France, 1965, p. 415-440.
[17] D. Ulmer, "Elliptic curves with large rank over function fields", *Ann. Math.* **155** (2002), no. 1, p. 295-315.
[18] ———, "$L$-functions with large analytic rank and abelian varieties with large algebraic rank over function fields", *Invent. Math.* **167** (2007), no. 2, p. 379-408.
[19] ———, "Elliptic curves over function fields", in *Arithmetic of L-functions*, IAS/Park City Mathematics Series, vol. 18, American Mathematical Society, 2011, p. 211-280.
[20] ———, "Explicit points on the Legendre curve", *J. Number Theory* **136** (2014), p. 165-194.

Richard Griffon
Universiteit Leiden – Mathematisch Instituut
Postbus 9512
2300 RA Leiden, The Netherlands
*E-mail*: r.m.m.griffon@math.leidenuniv.nl
*URL*: http://pub.math.leidenuniv.nl/~griffonrmm/