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

Richard Griffon
Mathematisch Instituut, Universiteit Leiden

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

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

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

Keywords: 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.

2010 Math. Subj. Classification: 11G05, 11G40, 14G10, 11F67, 11M38.

Introduction

Let $\mathbb{F}_q$ be a finite field of characteristic $p \geq 5$, and $K = \mathbb{F}_q(t)$. For a non-isotrivial 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, whose degree is given in terms of the conductor of $E$, and for which the Riemann Hypothesis holds.

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 $L(E/K, T)$ on the critical line appears to be out of reach at the moment. In the meantime, 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 $d \geq 2$ that is coprime to $q$, consider the Hessian elliptic curve $E_d$ over $K$, whose affine Weierstrass model is:

$$E_d : \quad y^2 + xy - t^d y = x^3. \quad (1)$$

To give a flavour of our result (Theorem 3.1) without having to introduce too many notations, 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 $\chi : \mathbb{F}_q^\times \to \mathbb{Q}^\times$ of exact order $d$. In that case, our calculation then yields:

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

$$L(E_d/K, T) = \prod_{k=1}^{d-1} (1 - J_k \cdot T) \in \mathbb{Z}[T], \quad \text{where } J_k := \sum_{x_1, x_2, x_3 \in \mathbb{F}_q, \ x_1 + x_2 + x_3 = 1} \chi^k (-x_1 x_2 x_3).$$

*E-mail: r.m.m.griffon@math.leidenuniv.nl*
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 possibly nontrivial action of \( \text{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \) on the \( d \)-th roots of unity in \( \overline{\mathbb{F}_q} \), which leads to mild technical complications (see §2, §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 [Ulm07, §2-§4]).

In §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 \( \text{III}(E_d/K) \) is a finite group and, as \( d \to \infty \),

\[
\log \left( \left| \text{III}(E_d/K) \right| \cdot \text{Reg}(E_d/K) \right) \sim \log H(E_d/K),
\]

where \( \text{Reg}(E_d/K) \) 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

\[
\log \left( \left| \text{III}(E_d/K) \right| \cdot \text{Reg}(E_d/K) \right) \sim \frac{\log q}{d} \cdot d \quad (\text{as } d \to \infty),
\]

showing that the product \( |\text{III}(E_d/K)| \cdot \text{Reg}(E_d/K) \) grows exponentially fast with \( d \): see [Hin07] for an interpretation of this fact in terms of the “complexity of computing \( E_d(K) \)”.

Theorem B can also be restated as:

\[
\forall \epsilon > 0, \quad H(E_d/K)^{1+\epsilon} \ll_{q, \epsilon} |\text{III}(E_d/K)| \cdot \text{Reg}(E_d/K) \ll_{q, \epsilon} H(E_d/K)^{1+\epsilon}.
\]

The upper bound here essentially proves a conjecture of Lang (the formulation for elliptic curves over \( \mathbb{Q} \) is [Las83, Conj. 1]). Better yet, 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

\[
\log \left( |\text{Cl}(k)| \cdot \text{Reg}(k) \right) \sim \log \sqrt{\Delta_k} \quad (\text{as } \Delta_k \to \infty),
\]

where \( \text{Cl}(k) \) denotes the class-group of \( k \), and \( \text{Reg}(k) \) its regulator of units (see [Lan94, Chap. XVI]). At least in their formal structure, (2) and (3) look very similar and, following [HP16], we view Theorem B as an analogue of the Brauer-Siegel theorem for the Hessian elliptic curves.

Note that there are only six infinite families of elliptic curves where a complete analogue of the Brauer-Siegel is known to hold unconditionally: see [HP16, Thm. 1.4], [Gri17, Thm. 1.1], and four more examples in [Gri16a].

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 [Ulm07, §6]). In particular, the Tate-Shafarevich group \( \text{III}(E_d/K) \) is finite and, by bounding some of the terms appearing in the “BSD formula” (see Corollary 1.6), we get

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

where \( L^*(E_d/K, 1) \) denotes the special value of \( L(E_d/K, T) \) at \( T = q^{-1} \) (see Corollary 5.4). Given this link with \( L^*(E_d/K, 1) \), proving the estimate (2) is equivalent to the more analytic problem of showing that

\[
\frac{\log L^*(E_d/K, 1)}{\log H(E_d/K)} = o(1) \quad (\text{as } d \to \infty).
\]

In a previous article [Gri16b], 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. The resulting upper and lower bounds are enough to ensure that (4) holds (see §4).

\(^1\)henceforth abbreviated as BSD
The paper is organized as follows. We begin by giving, in §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 $E_d$: §2 introduces the necessary notations and tools while §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 §4, before recalling the BSD conjecture and concluding the proof of Theorem B in §5.

Notations For two functions $f(x), g(x)$ defined on $[0, \infty)$, we use both Landau’s “$f(x) = O_q(g(x))$” and Vinogradov’s “$f(x) \ll_q g(x)$” notations to mean that there exists a constant $C > 0$ depending at most on the mentioned parameters $a$ such that $|f(x)| \leq Cg(x)$ 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 $p \geq 5$, and we denote by $K = \mathbb{F}_q(t)$.

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

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

for some $A(t) \in \mathbb{F}_q[t]$ with $A(t)^3 \neq 1$ (see [SS10, §7.10]). This model is often called the Hessian normal form of $E$. 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:

$$E_d : y^2 + xy - t^d \cdot y = x^3,$$

which we call the $d$-th 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:

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

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

The reader is referred to [Ul14, Lecture 1] and [SS10] 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 [DO16]) from a different perspective: for many values of $d$, they have produced explicit $\mathbb{F}_q(t)$-rational points on $E_d$, which generate a full-rank subgroup of $E_d(\mathbb{F}_q(t))$. They use these explicit points to study the size of certain character sums over $\mathbb{F}_q^2$.

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 $v$ of $K$ | Type of $E_d$ at $v$ | $\text{ord}_v \Delta_{\text{min}}(E_d/K)$ | $\text{ord}_v N(E_d/K)$ | $c_v(E_d/K)$ |
|------------------|----------------------|--------------------------------------|----------------------|-------------|
| $0$              | $I_{3d}$             | $3d$                                 | $1$                  | $3d$        |
| $v \in B_d$      | $I_1$                | $1$                                  | $1$                  | $1$         |
| $\infty$         | $I_0$ if $d \equiv 0 \text{ mod } 3$ | $0$                                  | $0$                  | $1$         |
|                  | $IV$ if $d \equiv -1 \text{ mod } 3$ | $4$                                  | $2$                  | $3$         |
|                  | $IV^*$ if $d \equiv -2 \text{ mod } 3$ | $8$                                  | $2$                  | $3$         |
In this table, for all places \( v \) of \( K \) where \( E_d \) has bad reduction, we have denoted by \( \text{ord}_v(\Delta_{\text{min}}) \) (resp. \( \text{ord}_v(N) \)) the valuation at \( v \) of the minimal discriminant of \( E_d \) (resp. of the conductor of \( E_d \)), and by \( c_0(\mathcal{E}_d/K) \) the local Tamagawa number (see [Sil94, Chap. IV, §9] for definitions).

**Proof:** This follows from a routine application of Tate’s algorithm to \( E_d \) (see [Sil94, Chap. IV, §9]). \( \square \)

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

\[
\deg \Delta_{\text{min}}(E_d/K) = \begin{cases} 
4d & \text{if } d \equiv 0 \mod 3, \\
4(d+1) & \text{if } d \equiv -1 \mod 3, \\
4(d+2) & \text{if } d \equiv -2 \mod 3.
\end{cases}
\]

Indeed, note that \( \sum_{v \in \mathcal{B}_d} \deg v = d \). By definition, the exponential differential height of \( E_d/K \) is then

\[
H(E_d/K) = q^{\deg \Delta_{\text{min}}(E_d/K)} = q^{\lfloor \frac{d+2}{3} \rfloor},
\]

where \( \lfloor . \rfloor \) denotes the floor function.

**Remark 1.3** The following alternative definition of \( H(E_d/K) \) justifies its name (see §2 in [Ulm11, Lect. 3]). 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, if \( \Omega_{\mathcal{E}_d/\mathbb{P}^1} \) denotes the sheaf of relative differentials we let \( \omega = \omega_{\mathcal{E}_d/K} \) be the line bundle \( s_0^*(\Omega_{\mathbb{P}^1/\mathbb{P}^1}) \) on \( \mathbb{P}^1 \). Then the minimal discriminant divisor \( \Delta_{\text{min}}(E_d/K) \) corresponds to a section of \( \omega \otimes 12 \). In particular, one has \( 12 \deg \omega = \deg \Delta_{\text{min}}(E_d/K) \), and \( H(E_d/K) = q^{\deg \omega} \).

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

\[
E_d : \quad y^2 = x^3 + x^2 - 8t^d \cdot x + 16t^{2d}.
\]

The discriminant of this integral Weierstrass model is \( \Delta' = -2^{12}t^d(27t^d + 1) \). For all places \( v \neq \infty \) of \( K \), \( \text{ord}_v \Delta' = \text{ord}_v \Delta_{\text{min}}(E_d/K) \) 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 \( 3 | d \) (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 \( E_d(K)_{\text{tors}} \), as well as the Tamagawa number \( \tau(E_d/K) \).

**Proposition 1.5** – For any integer \( d \geq 1 \) coprime with \( q \), one has

\[
E_d(K)_{\text{tors}} \simeq \mathbb{Z}/3\mathbb{Z}.
\]

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

**Proof:** Let \( T := E_d(K)_{\text{tors}} \) 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 that the \( p \)-part \( T[p^\infty] \) of \( T \) must be trivial for \( j(E_d/K) \in K \) is not a \( p \)-th power in \( K \) (see [Ulm11, 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 [SS10, §7], [Sil94, Chapter IV, §9]). The table in [Sil94, p.365] gives that

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

We now distinguish two cases. First assume that \( 3 \nmid d \): by Proposition 1.2, \( E_d \) has additive reduction at the place \( \infty \) (with type \( \mathbb{II} \) or \( \mathbb{II}^* \)). Lemma 7.8 in [SS10] asserts that the non-\( p \)-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 [SS10], the torsion group $T$ injects into the product $\prod_{v \mid \Delta} G_v$ of the component groups. Therefore, $T$ is a subgroup of $\prod_{v \mid \Delta} G_v \approx \mathbb{Z}/3\mathbb{Z}$ (see (1.4)). 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. This can only happen for $M \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$ (see [Ulm11, Lect. 1, §7]). 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 $x_1 = u^{2d/3} \cdot x$ (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 $(4x_1^2 - 2u^{d/3} \cdot x_1 - 2u^{d/3}) \cdot x_1 = -1$. This contradiction shows that $E_d(K)$ has no nontrivial 2-torsion, so that $M = |T| = 3$ is odd.

Next suppose that there is a $K$-rational point $Q = (x, y) \in E_d$ of order exactly 9 on $E_d$. Up to replacing $Q$ by one of its multiples, we can assume that $3 \cdot Q = P_0$. Using the triplication formula (see [Sil09, Chap. III, Ex. 3.7 (d)]), it is possible to express the $x$-coordinate of $3Q = P_0$ in terms of $x$. By a rather tedious computation, one can show that $x$ must then satisfy:

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

Letting $u = 1/t$, $v = u^{d/3}$ and $x_2 = u^{d/3} \cdot x = v^2 \cdot x$, the above relation yields that $x_2 \in \mathbb{F}_q(u)$ is a solution of either $0 = x_2^3 + v \cdot x_2^2 - 3x_2^2 - v \cdot x_2 + 1$ or

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

Since none of these equations has any solution $x_2 \in \mathbb{F}_q(u)$, the 9-torsion in $E_d(K)$ has to be trivial. Therefore, $M = 3$ and $T \approx \mathbb{Z}/3\mathbb{Z}$ as claimed. \hfill \qed

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

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

In §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:

$$\frac{\log d}{d} \ll_q \frac{\log (\tau(E_d/K) \cdot q \cdot |E_d(K)_{\text{tors}}|^2)}{\log H(E_d/K)} \ll_q \frac{\log d}{d},$$  

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

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

**Remark 1.7** The above Corollary could also have been obtained as a special case of deep results in [HP16]. 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 notations and review the required facts about characters and Jacobi sums. The notations 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 $q$, $q$ acts naturally 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

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

(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 $m \in \mathcal{O}_q(Z_d)$, 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 $(m, \mathbf{n}, \ldots)$ and that the corresponding normal letter $(m, n, \ldots)$ designates any choice of representative of this orbit in $Z_d$.

We also identify without comment $\mathbb{Z}/d\mathbb{Z}$ with its lift $\{0, 1, 2, \ldots, d-1\}$ in $\mathbb{Z}$.

For any orbit $m \in \mathcal{O}_q(Z_d)$, its length $|m| = \left| \{m, qm, q^2m, \ldots \} \right|$ is equal to $|m| = \min \{ n \in \mathbb{Z}_{\geq 1} : q^n m \equiv m \mod d \}$,

which can equivalently be described as the multiplicative order of $q$ modulo $d/\gcd(d, m)$, for any $m \in \mathbf{m}$. By construction, the “lifted character” $\chi^{(s)} = (\chi(q^n m))^{(q^n m) - 1}/d$ is a character on $\mathbb{Z}/d\mathbb{Z}$.

Remark 2.1 In the special case when $d$ divides $q - 1$ (i.e. when $q \equiv 1 \mod d$), 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 $\mathbb{Z}$ of $\overline{\mathbb{Q}}$: the residue field $\mathbb{Z}/\mathfrak{p}$ is an algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$. The given finite field $\mathbb{F}_p$ and, more generally, any finite extension thereof will be seen as subfields of $\overline{\mathbb{F}}_p$. The reduction map $\mathbb{Z} \to \mathbb{Z}/\mathfrak{p}$ induces an isomorphism between the group $\mu_{\mathfrak{p}, \mathfrak{p}'} \subset \mathbb{Z}^\times$ of roots of unity of order prime to $p$ and the multiplicative group $\mathbb{F}_p^\times$. We let $t : \mathbb{F}_p^\times \to \overline{\mathbb{F}}_{\mathfrak{p}}^\times$ be the inverse of this isomorphism, and we denote by the same letter the restriction of $t$ to any finite extension of $\mathbb{F}_q$.

Any nontrivial multiplicative character on a finite extension of $\mathbb{F}_q$ is then a power of (a restriction of) $t$, cf. [Coh07, §3.6.2]. The trivial multiplicative character will be denoted by $1$.

Definition 2.2 For any $m \in \mathbb{Z}/d\mathbb{Z} \setminus \{0\}$ and any integer $s \geq 1$, define a character $t_m^{(s)} : \mathbb{F}_q^\times \to \overline{\mathbb{F}}_q^\times$ by

$$\forall x \in \mathbb{F}_q^\times, \quad t_m^{(s)}(x) = (t \circ N_{q^{|m|}/q^{|m|}}(x))^{(q^{|m|} - 1)/d} \quad \text{and we let } t_m^{(s)}(0) := 0.$$

Here, $N_{q^{|m|}/q^{|m|}} : \mathbb{F}_{q^{|m|}} \to \mathbb{F}_q$ denotes the norm of the extension $\mathbb{F}_{q^{|m|}}/\mathbb{F}_q$.

When $s = 1$, we denote $t_m^{(1)}$ by $t_m$ for short. Note that $t_m^{(s)}$ is indeed a character because $t$ and the norm $N_{q^{|m|}/q^{|m|}}$ are both multiplicative.

By construction, $t_m$ is a character on $\mathbb{F}_q^\times$ and its order divides $d$: more precisely, by noting that the restriction of $t$ to $\mathbb{F}_q^\times$ has exact order $q^{|m|} - 1$, it can be shown that the order of $t_m$ is exactly $d/\gcd(d, m)$.

The “lifted character” $t_m^{(s)}$ is defined on $\mathbb{F}_q^\times$, and has the same order as $t_m$ because the norm $N_{q^{|m|}/q^{|m|}}$ 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 $\mathbb{F}_{q^n}$ such that $\chi^d = 1$. Then

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

Proof: The characters $t_m^{(s)}$ appearing on the right-hand side all belong to $X(d, q^n)$ for they are all nontrivial characters on $\mathbb{F}_{q^n}$ with order dividing $d$. To prove the converse inclusion, let $d_n = \gcd(d, q^n - 1)$ and $\chi_0 = t^{(q^n - 1)/d_n}$. By the discussion above, $\chi_0$ is a character on $\mathbb{F}_{q^n}$ of exact order $d_n$. Thus, by cyclicity of the character group of $\mathbb{F}_{q^n}$, $\chi_0$ generates the group $X(d, q^n) \cup \{1\}$. 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 \( \chi = \chi_k^d = t^{(q^n-1)k/d_n} \). 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 \( \chi = t^{(q^n-1)m/d} \). Recall that \( [m] \) is the multiplicative order of \( q \) modulo \( d/\gcd(d, m) \): by definition, this implies that \( [m] \) divides \( n \) (see §2.1), so that we can write \( n = s \cdot [m] \) for some \( s \geq 1 \).

This shows that \( \chi = t^{(q^n-1)m/d} = t^{(q^{3n-1})m/d} \circ N_{\mathbb{F}_{q^n}/\mathbb{F}_{q^3}} = t^{(s)}_m \).

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 \( \chi^3 \neq 1 \). Then

\[
X_3(d, q^n) = \left\{ t^{(s)}_m, \ m \in \mathbb{Z}_d \text{ and } s \geq 1 \text{ such that } s \cdot [m] = n \right\}.
\]

**Proof:** We distinguish two cases. First, if \( \frac{m}{d} \) is not coprime to \( d \) and \( \gcd(d, m) \neq 1 \), then the characters \( t^{(s)}_m \) for \( m \in \mathbb{Z}/d\mathbb{Z} \setminus \{0\} \), and the preceding Lemma allows us to conclude in this case. In the remaining case when \( d \) divides \( m \), we have \( \mathbb{Z}_d = \mathbb{Z}/d\mathbb{Z} \setminus \{0, d/3, 2d/3\} \) and \( X_3(d, q^n) = X(d, q^n) \setminus \{ \chi : \chi^3 = 1 \} \). Since the order of \( t^{(s)}_m \) for \( m \in \mathbb{Z}/d\mathbb{Z} \setminus \{0\} \) is exactly \( d/\gcd(d, m) \), a direct inspection shows that \( (t^{(s)}_m)^3 = 1 \) if and only if \( m = d/3 \) or \( 2d/3 \). Which gives the desired result.

**Remark 2.5** In the special case when \( d \) divides \( q - 1 \), i.e. when \( q \equiv 1 \mod d \), the characters \( t_m \ (m \in \mathbb{Z}_d) \) are all nontrivial of \( \mathbb{F}_{q^3}^\times \), because \( [m] = 1 \). Since there are \( a \text{ priori} \ |\mathbb{Z}_d| \) nontrivial characters \( \chi \) on \( \mathbb{F}_q^\times \) such that \( \chi^d = 1 \) and \( \chi^3 \neq 1 \), 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 \( 1 \), and by \( \chi(0) = 1 \). For a character \( \chi : \mathbb{F}_r^\times \to \overline{\mathbb{Q}}^\times \) and an extension \( \mathbb{F}_r'/\mathbb{F}_r \) of degree \( s \), whose norm is denoted by \( N_{r/r'} : \mathbb{F}_r \to \mathbb{F}_r' \), we let \( \chi^{(s)} := \chi \circ N_{r/r'} \) 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

\[
J_r(\chi_1, \chi_2, \chi_3) := \sum_{\substack{x_1, x_2, x_3 \in \mathbb{F}_r \\ x_1+x_2+x_3=1}} \chi_1(x_1)\chi_2(x_2)\chi_3(x_3).
\]

Let us recall some classical facts about these sums (see [Coh07, §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 \( |J_r(\chi_1, \chi_2, \chi_3)| = r \). If \( \chi_1, \chi_2, \chi_3 \) are nontrivial but \( \chi_1\chi_2\chi_3 \) is trivial, the Jacobi sum “degenerates” to:

\[
J_r(\chi_1, \chi_2, \chi_3) = -\chi_3(-1) \sum_{\substack{x_1, x_2 \in \mathbb{F}_r \\ x_1+x_2=1}} \chi_1(x_1)\chi_2(x_2).
\]

(2.1)

Jacobi sums satisfy the Hasse-Davenport relation (see [Coh07, §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

\[
J_{r'}(\chi_1^{(s)}, \chi_2^{(s)}, \chi_3^{(s)}) = J_r(\chi_1, \chi_2, \chi_3)^s.
\]

(2.2)

We finally introduce the following notation:

**Definition 2.6** For any \( m \in \mathbb{Z}_d \), we let

\[
J(m) := J_{q^m}(t_m, t_m, t_m).
\]

(2.3)

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

By construction of \( \mathbb{Z}_d \), neither \( t_m \) nor \( (t_m)^3 \) is trivial, so that \( |J(m)| = q^{im} \) for all \( m \in \mathcal{O}_q(\mathbb{Z}_d) \).
3 The $L$-function

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

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

where the products are over the places of $K$, and where $a_v := q_v + 1 - |(\overline{E_d})_v(\mathbb{F}_{q_v})|$. Remark that, when $E$ 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 [Ulm11, Lect. 1, §9] for more details. With the notations 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

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

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

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

where $J(m)$ 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 [CHU14, Thm. 3.2.1]: we calculate $L(E_d/K, T)$ by manipulations of character sums. Note that an alternative, more cohomological, computation could be conducted (along the lines of [Ulm02, §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 the proof of Theorem 3.1. Indeed, one would then rely on the fact that the minimal regular model $E_d \to \mathbb{P}^1$ of $E_d/K$ is dominated by a quotient of the Fermat surface $F_d/F_q$ of degree $d$ (see [Ulm07] and [Ulm11, Lect. 3, §10]), whose zeta function is well-known and involves Jacobi sums.

**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 $\mathbb{F}_q^*$ of exact order $d$, one has

$$L(E_d/K, T) = \prod_{1 \leq k \leq d, k \neq d/2} (1 - \chi(-1)^kJ_k(\chi^k, \chi^k) \cdot T). \tag{3.3}$$

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 $\lambda : \mathbb{F}_r^* \to \{\pm 1\}$ the unique nontrivial character of order $2$ on $\mathbb{F}_r^*$ (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 $\chi : \mathbb{F}_r^* \to \mathbb{C}^*$,

$$\sum_{z \in \mathbb{F}_r} \chi(z) \cdot \lambda(x^3 + x^2 - 8zx + 16z^2) = \begin{cases} 0 & \text{if } \chi \text{ is trivial,} \\ \chi(-1)^3J_r(\chi, \chi, \chi) & \text{otherwise.} \end{cases} \tag{3.4}$$

**Proof:** Let $S_r(\chi)$ denote the double sum on the left-hand side of (3.4). We first put $z' = 4z$ in the outer sum, exchange the order of summation and split the sum according to whether $x = 0$ or not: we obtain that

$$S_r(\chi) = \chi^{-1}(4) \cdot \sum_{z' \in \mathbb{F}_r} \chi(z') \cdot \lambda(z')^2 + \chi^{-1}(4) \cdot \sum_{x \neq 0} \sum_{z'' \in \mathbb{F}_r} \chi(z') \cdot \lambda(x^3 + x^2 - 2z'x + z'^2)$$

$$= \chi^{-1}(4) \cdot \sum_{z' \in \mathbb{F}_r^2} \chi(z') + \chi^{-1}(4) \cdot \sum_{x \neq 0} \left(\sum_{z'' \in \mathbb{F}_r} \chi(z') \cdot \lambda(x^3 + (x - z')^2)\right)$$

8
To treat the sum over \( x \neq 0 \), note the following: for a given \( x \neq 0 \), by writing \( z' = x(y + 1) \), we obtain that

\[
\sum_{z' \in \mathbb{F}_r} \chi(z') \cdot \lambda(x^3 + (x - z')^2) = \chi(x) \cdot \sum_{y \in \mathbb{F}_r} \chi(y + 1) \cdot \lambda(x + y^2).
\]

Summing this identity over all \( x \neq 0 \) and exchanging the order of summation yields that

\[
S_q(\chi) = \chi^{-1}(4) \cdot \sum_{z' \neq 0} \chi(z') + \chi^{-1}(4) \cdot \sum_{y \in \mathbb{F}_r} \chi(y + 1) \left( \sum_{x \neq 0} \chi(x) \lambda(x + y^2) \right).
\]

If \( \chi \) is trivial, a straightforward evaluation of the sums leads to the desired result: \( S_r(\chi) = 0 \). From now on, we thus assume that \( \chi \) is nontrivial: in which case, \( \sum_{z' \neq 0} \chi(z') = 0 \) 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 \( 1 + \lambda(w) = |\{ t \in \mathbb{F}_r : t = w^2 \}| \) 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:

\[
\sum_{x \in \mathbb{F}_r} \chi(x) \lambda(x + y^2) = \sum_{x \in \mathbb{F}_r} \chi(x) \cdot (1 + \lambda(x + y^2)) = \sum_{x \in \mathbb{F}_r} \chi(x) \cdot |\{ t \in \mathbb{F}_q : x = t^2 - y^2 \}| = \sum_{t \in \mathbb{F}_r} \chi(t^2 - y^2).
\]

This leads to

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

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 \((y,t) \mapsto \left( \frac{t-y}{2}, \frac{y+t}{2}, y+1 \right)\) is a bijection, and this allows us to write the latter double sum as a Jacobi sum:

\[
\sum_{(y,t) \in \mathbb{F}_r^2} \chi(t - y) \chi(t + y) \chi(y + 1) = \chi(-4) \cdot \sum_{x_1 + x_2 + x_3 = 1, \ x_1, x_2, x_3 \in \mathbb{F}_r} \chi(x_1) \chi(x_2) \chi(x_3) = \chi(-4) \cdot J_r(\chi, \chi, \chi).
\]

Therefore, we have proved that \( S_r(\chi) = \chi(-1) \cdot J_r(\chi, \chi, \chi) \). This concludes the proof.

\[\square\]

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

\[
\sum_{x \in \mathbb{F}_r} \lambda(x^3 + a) = -\lambda(a) \cdot \sum_{\xi^3 = 1} \xi(4a) \cdot J_r(\xi, \xi, \xi),
\]

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

**Proof:** The sum over \( \xi \) in (3.5) contains 2 or 0 terms, depending on whether 3 divides \( |\mathbb{F}_r^\times| = r - 1 \) or not, respectively. For any \( z \in \mathbb{F}_r \), one has \( |\{ x \in \mathbb{F}_r : x = z^3 \}| = \sum_{\xi^3 = 1} \xi(z) \), where the sum is over characters \( \xi \) on \( \mathbb{F}_r^\times \) such that \( \xi^3 = 1 \) (see [Coh07, Lemma 2.5.21]). Therefore

\[
\sum_{x \in \mathbb{F}_r} \lambda(x^3 + a) = \sum_{z \in \mathbb{F}_r} \left|\{ x \in \mathbb{F}_r : x = z^3 \}\right| \cdot \lambda(z + a) = \sum_{z \in \mathbb{F}_r} \lambda(z + a) + \sum_{\xi^3 = 1} \xi(z) \lambda(z + a) \right). \] (3.6)

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

\[
\sum_{z \in \mathbb{F}_r} \xi(z) \lambda(z + a) = \sum_{x_1, x_2 \in \mathbb{F}_r, x_1 + x_2 = 1} \xi(-ax_1) \lambda(ax_2) = \xi(-a) \lambda(a) \cdot \sum_{x_1, x_2 \in \mathbb{F}_r, x_1 + x_2 = 1} \xi(x_1) \lambda(x_2)
\]

\[
= \xi(-4a) \lambda(a) \cdot \sum_{x_1, x_2 \in \mathbb{F}_r, x_1 + x_2 = 1} \xi(x_1) \xi(x_2) = -\xi(4a) \lambda(a) \cdot J_r(\xi, \xi, \xi).
\]

The penultimate equality follows from [Coh07, Prop. 2.5.18], and the last one from (2.1) because \( \xi^3 = 1 \). Plugging this result twice into (3.6) finishes the proof. \[\square\]
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 [CHU14, §3.2], one arrives at the following expression of \( L(E_d/K, T) \):

**Lemma 3.5** – Let \( n \geq 1 \). For any \( \tau \in \mathbb{P}^1(\mathbb{F}_{q^n}) \), denote by \( v_\tau \) the place of \( K \) corresponding to \( \tau \), and by \( (E_d)_\tau \) the reduction of a integral minimal model of \( E \) at \( v_\tau \). For all \( n \geq 1 \) and any \( \tau \in \mathbb{P}^1(\mathbb{F}_{q^n}) \), we let \( A_d(\tau, q^n) := q^n + 1 - |(E_d)_\tau(\mathbb{F}_{q^n})| \). Then, the L-function of \( E_d/K \) satisfies the formal identity

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

(3.7)

Our first step will be to find a more explicit expression of the inner sums in (3.7). For any finite extension \( \mathbb{F}_{q^n} \) of \( \mathbb{F}_q \), we again denote by \( \lambda : \mathbb{F}_{q^n}^* \rightarrow \{\pm 1\} \) (or by \( \lambda_{q^n} \) when confusion is possible) the quadratic character on \( \mathbb{F}_{q^n}^* \). For any \( \tau \in \mathbb{P}^1(\mathbb{F}_{q^n}) \), we fix an affine model \( y^2 = f_\tau(x) \) of \( (E_d)_\tau \) (with \( f_\tau(x) \in \mathbb{F}_{q^n}[x] \) of degree 3). A standard computation yields that

\[
A_d(\tau, q^n) = q^n + 1 - |(E_d)_\tau(\mathbb{F}_{q^n})| = q^n - \sum_{x \in \mathbb{F}_{q^n}} (1 + \lambda(f_\tau(x))) = - \sum_{x \in \mathbb{F}_{q^n}} \lambda(f_\tau(x)).
\]

(3.8)

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 \( (E_d)_\infty \) 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 \( (E_d)_\infty \) has affine model \( y^2 = x^3 + 1 \) over \( \mathbb{F}_q \) (see Remark 1.4). Therefore, by (3.8) and Proposition 3.4 (with \( r = q^n \) and \( a = 1/4 \)), one has

\[
A_d(\infty, q^n) = - \sum_{x \in \mathbb{F}_{q^n}} \lambda(x^3 + 1/4) = \sum_{(\xi, \xi, \xi) \neq (\xi, \xi)} j_\xi^\infty (\xi, \xi, \xi) = \sum_{(\xi, \xi, \xi) \neq (\xi, \xi)} j_\xi^\infty (\xi, \xi, \xi),
\]

where the sum is over nontrivial characters \( \xi \) of \( \mathbb{F}_{q^n}^* \) such that \( \xi^3 = 1 \) (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 \( f_\tau(x) = x^3 + x^2 - 8\tau^d \cdot x + 16\tau^{2d} \) and (3.8) here leads to

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

For any \( z \in \mathbb{F}_{q^n} \), one has \( |\{\tau \in \mathbb{F}_{q^n} : \tau^d = z\}| = \sum_{\chi^d = 1} \chi(z) \), where the sum is over all characters \( \chi \) of \( \mathbb{F}_{q^n} \), such that \( \chi^d = 1 \) (see [Coh07, Lemma 2.5.21]). After exchanging order of summation, we obtain that

\[
\sum_{\tau \in \mathbb{P}^1(\mathbb{F}_{q^n})} A(\tau, q^n) = - \sum_{\tau \in \mathbb{P}^1(\mathbb{F}_{q^n})} \sum_{x \in \mathbb{F}_{q^n}} \lambda(x^3 + x^2 - 8\tau^d \cdot x + 16\tau^{2d})
\]

\[
= - \sum_{z \in \mathbb{F}_{q^n}} \left( |\{\tau \in \mathbb{F}_{q^n} : \tau^d = z\}| \cdot \sum_{x \in \mathbb{F}_{q^n}} \lambda(x^3 + x^2 - 8zx + 16z^2) \right)
\]

\[
= - \sum_{\chi^d = 1} \sum_{z \in \mathbb{F}_{q^n}} \chi(z) \lambda(x^3 + x^2 - 8zx + 16z^2).
\]

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

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

where \( X(d, q^n) \) is the set of nontrivial characters \( \chi \) on \( \mathbb{F}_{q^n} \), such that \( \chi^d = 1 \). By our expression of \( A(\infty, q^n) \), it follows that

\[
\sum_{\tau \in \mathbb{P}^1(\mathbb{F}_{q^n})} A_d(\tau, q^n) = \begin{cases} 
\sum_{(\xi, \xi, \xi) \neq (\xi, \xi)} j_\xi^\infty (\xi, \xi, \xi) - \sum_{\chi \in X(d, q^n)} \chi(-1) \cdot j_\chi^\infty (\chi, \chi, \chi) & \text{if } 3 \mid d, \\
0 & \text{else.}
\end{cases}
\]
In both cases, one can rewrite this as
\[ \sum_{\tau \in \mathbb{F}_q^*} A_d(\tau, q^n) = - \sum_{\chi \in X_3(d, q^n)} \chi(-1) \cdot \mathfrak{j}_q^n(\chi, \chi, \chi), \]
where the sum is over the set \( X_3(d, q^n) \) of nontrivial characters \( \chi \) on \( \mathbb{F}_q^* \), such that \( \chi^d = 1 \) and \( \chi^3 \neq 1 \) (see §2.2). Plugging this last identity into (3.7), we obtain that
\[
- \log L(E_d/K, T) = \sum_{n \geq 1} \left( \sum_{\chi \in X_3(d, q^n)} \chi(-1) \cdot \mathfrak{j}_q^n(\chi, \chi, \chi) \right) \cdot \frac{T^n}{n}.
\]
We now perform a “reindexation” on this double sum: Lemma 2.4 allows us to rewrite (3.9) under the form:
\[
\sum_{n \geq 1} \left( \sum_{\chi \in X_3(d, q^n)} \chi(-1) \cdot \mathfrak{j}_q^n(\chi, \chi, \chi) \right) \cdot \frac{T^n}{n} = \sum_{m \in \mathbb{Z}_d} \left( \sum_{s \geq 1} t_{m}^{(s)}(1) \cdot \mathfrak{j}_{q^s \cdot m}(t_{m}^{(s)}, t_{m}^{(s)}, t_{m}^{(s)}) \cdot \frac{T^{s \cdot |m|}}{s \cdot |m|} \right).
\]
Further, \( t_{m}^{(s)}(1) = t_{m}(1)^s \) and the Hasse-Davenport relation (2.2) implies that
\[ \forall m \in \mathbb{Z}_d, \forall s \geq 1, \quad \mathfrak{j}_{q^s \cdot m}(t_{m}^{(s)}, t_{m}^{(s)}, t_{m}^{(s)}) = \mathfrak{j}_{q^1 \cdot m}(t_{m}, t_{m}, t_{m})^s = J(m)^s. \]
Therefore, we derive that
\[
\sum_{n \geq 1} \left( \sum_{\chi \in X_3(d, q^n)} \chi(-1) \cdot \mathfrak{j}_q^n(\chi, \chi, \chi) \right) \cdot \frac{T^n}{n} = \sum_{m \in \mathbb{Z}_d} \sum_{s \geq 1} \frac{(t_{m}(1)J(m) \cdot T^{s \cdot |m|})^s}{s \cdot |m|} \cdot \log \left( 1 - t_{m}(1)J(m) \cdot T^{s \cdot |m|} \right).
\]
In the right-most sum, notice that each term \( \log \left( 1 - t_{m}(1)J(m) \cdot T^{s \cdot |m|} \right) \) appears \( |m| \) times since \( J(q^k \cdot m) = J(m) \) for all \( k \geq 1 \). Thanks to the “weighting” by \( 1/|m| \), we may thus write the sum over \( m \in \mathbb{Z}_d \) as a sum over \( m \in \mathcal{O}_q(\mathbb{Z}_d) \). Finally, we have proved
\[ \log L(E_d/K, T) = \sum_{m \in \mathcal{O}_q(\mathbb{Z}_d)} \log \left( 1 - t_{m}(1)J(m) \cdot T^{s \cdot |m|} \right). \]
It remains to exponentiate this identity to complete the proof of Theorem 3.1. \( \square \)

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 \( \rho(E_d/K) := \text{ord}_{T = q^{-1}} L(E_d/K, T) \) is called the analytic rank of \( E_d \), and that the special value of \( L(E_d/K, T) \) at \( T = q^{-1} \) is the quantity
\[ L^*(E_d/K, 1) := \frac{L(E_d/K, T)}{(1 - qT)^{\rho}} \bigg|_{T = q^{-1}} \in \mathbb{Q}^* \quad \text{where } \rho = \rho(E_d/K). \]

**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 normalization of \( \text{Reg}(E_d/K) \) (see §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 [HP16, §7] for example, one readily obtains that
\[ -5 + o(1) \leq \frac{\log L^*(E_d/K, 1)}{\log H(E_d/K)} \leq o(1) \quad \text{(as } d \to \infty). \]
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:

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

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 [Gri16b]. 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 [Gri16b, §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

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

The group $(\mathbb{Z}/d\mathbb{Z})^\times$ acts on $G_d$ by coordinate-wise multiplication. In particular, $q$ acts by multiplication on $G_d$ and, for any nonempty subset $\Lambda \subset G_d$ which is stable under the action of $q$, we denote by $O_q(\Lambda)$ the set of orbits. For $a \in G_d$, we denote its orbit by $\Lambda = \{ a, qa, q^2a, \ldots \}$. We say that a nonempty subset $\Lambda \subset G_d$ satisfies hypothesis (II) if for all $\epsilon \in (0, 1/4)$, there exists $u \in (0, 1)$ such that

$$\left\{ \frac{(a_0, \ldots, a_3) \in \Lambda : d > \max_{0 \leq i \leq 3} \{ \gcd(d, a_i) \} > d^u} \right\} \leq c' \cdot |\Lambda| \cdot \left( \frac{\log \log d}{\log d} \right)^{1/4-\epsilon}, \quad (H)$$

for some constant $c'$. For $a = (a_0, \ldots, a_3) \in G_d$ with $a \neq 0 = (0, 0, 0, 0)$, whose orbit $A$ has length $|A|$, we define four characters on $\mathbb{F}_{q^{|A|}}^\times$:

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

One then defines a Jacobi sum:

$$J'(a_0, a_1, a_2, a_3) = \frac{1}{q^{|A|}-1} \sum_{x_0, \ldots, x_3 \in \mathbb{F}_{q^{|A|}}^\times} \chi_0(x_0)\chi_1(x_1)\chi_2(x_2)\chi_3(x_3) \in \mathbb{Q}(\zeta_d).$$

Since $a \in G_d$, the product $\chi_0\chi_1\chi_2\chi_3$ is the trivial character on $\mathbb{F}_{q^{|A|}}^\times$, and a classical calculation (cf. Lemma 2.5.13 in [Coh07]) relates $J'(a_0, a_1, a_2, a_3)$ to the Jacobi sums in Definition 2.6:

$$J'(a_0, a_1, a_2, a_3) = (\chi_0\chi_1\chi_2)(-1)\cdot j_{q^{|A|}}(\chi_0, \chi_1, \chi_2). \quad (4.3)$$

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

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

$$P(\Lambda, T) := \prod_{A \subset G_d} \left( 1 - J'(a) \cdot T^{|A|} \right),$$

where, for any orbit $A$, $a \in G_d$ denotes a choice of representative of $A$. Since the action of $\text{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q})$ on $\{ J'(a) \}_{a \in G_d}$ corresponds to the action of $(\mathbb{Z}/d\mathbb{Z})^\times$ on $G_d$ in the isomorphism $\text{Gal}(\mathbb{Q}(\zeta_d)/\mathbb{Q}) \simeq (\mathbb{Z}/d\mathbb{Z})^\times$, the assumption that $A$ is $(\mathbb{Z}/d\mathbb{Z})^\times$-stable ensures that $P(\Lambda, T) \in \mathbb{Z}[T]$. For $A$ as above, we finally introduce a special value:

$$P^*(\Lambda) := \frac{P(\Lambda, T)}{(1-qT)^{|\Lambda|-1}} \bigg|_{T=q^{-1}} \in \mathbb{Z}[q^{-1}] \setminus \{ 0 \} \quad \text{where } \rho = \text{ord}_{T=q^{-1}} P(\Lambda, T). \quad (4.4)$$

The following statement summarizes the main technical results of [Gri16b]:

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 (II) holds, the special value $P^*(\Lambda)$ satisfies

$$- C_3 \cdot \left( \frac{\log \log d}{\log d} \right)^{1/4-\epsilon} \leq \frac{\log |P^*(\Lambda)|}{\log q^{|A|}} \leq C_4 \cdot \frac{\log \log |A|}{\log |A|}. \quad (4.5)$$
This theorem is a concatenation of Theorems 5.1 and 6.2 in loc.cit.: the proof of the upper bound is relatively straightforward 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 [Gri16b, §4, §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 \( u = (1, 1, 1, -3) \) and we let

\[
\Lambda_d := H_d \setminus \{0\} = \{(m, m, m, -3m), m \in \mathbb{Z}/d\mathbb{Z}\} \setminus \{0\}, \tag{4.6}
\]

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 \( a = (a_0, \ldots, a_3) \) be an element of \( \Lambda_d \), so that \( a = m \cdot u \) for some \( m \in \mathbb{Z}/d\mathbb{Z} \setminus \{0\} \). Notice first that \(|A| = |m|\) because the coordinates of \( u \) are pairwise coprime. Also, all the \( a_i \) are nonzero if and only if \( m \in Z_d \). Furthermore, it follows from (4.3) that

\[
J'(a) = J'(m, m, m, -3m) = t_m(-1)^3 \cdot J_{d^m}(t_m, t_m, t_m) = t_m(-1) \cdot J(m).
\]

Consequently, in the notations of §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

\[
\left\lfloor \frac{\{a \in \Lambda_d : d > \max_i \gcd(d, a_i) > d^u\}}{d} \right\rfloor \ll u \cdot d^{-u/2} \cdot |\Lambda_d|.
\]

**Proof:** By construction of \( H_d \), any \( a = (a_0, \ldots, a_3) \in \Lambda_d \) is of the form \( a = (m, m, m, -3m) \) for some \( m \in \mathbb{Z}/d\mathbb{Z} \setminus \{0\} \). Thus, one has \( \max_i \gcd(d, a_i) \leq 3 \gcd(d, m) \). In particular, we obtain that

\[
\left\lfloor \frac{\{a \in \Lambda_d : d > \max_i \gcd(d, a_i) > d^u\}}{d} \right\rfloor \leq |\{m \in \mathbb{Z}/d\mathbb{Z} \setminus \{0\} : \gcd(d, m) > d^{u/3}\}|
\]

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,

\[
|\{m \in \mathbb{Z}/d\mathbb{Z} : \gcd(d, m) > d^{u/3}\}| = \sum_{e|d} \left\lfloor \frac{|\{m \in \mathbb{Z}/d\mathbb{Z} : \gcd(d, m) = e\}|}{d/e} \right\rfloor \leq \sum_{e|d} \frac{3\tau(d) \cdot d}{d^{u/3}}
\]

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 [HW08, Thm. 315]). In particular, for \( v = u/2 > 0 \), we have

\[
|\{a \in \Lambda_d : d > \max_i \gcd(d, a_i) > d^u\}| \leq 3\tau(d)d^{-u} \cdot |\Lambda_d| \ll u \cdot d^{-u/2} \cdot |\Lambda_d|.
\]

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 obtain that

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

By (1.3), we have

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

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 4.3 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. [Ulm11, Lect. 1, Thm. 5.1]). Furthermore, the group $E_d(K)$ is endowed with the canonical Néron–Tate height $h_{NT} : E_d(K) → \mathbb{Q}$. The quadratic map $h_{NT}$ induces a $\mathbb{Z}$-bilinear pairing $\langle -, - \rangle_{NT} : E_d(K) \times E_d(K) → \mathbb{Q}$, which is nondegenerate modulo $E_d(K)_{\text{tors}}$ (cf. [Sil94, Chap. III, Thm. 4.3]). The Néron–Tate regulator of $E_d/K$ is then defined as:

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

for any choice of a $\mathbb{Z}$-basis $P_1, \ldots, P_r ∈ E_d(K)$ of $E_d(K)/E_d(K)_{\text{tors}}$. Note that we normalize $\langle -, - \rangle_{NT}$ 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 [Sil94, Chap. III, §9]). Let us also recall that the Tate–Shafarevich group of $E_d/K$ is defined by

$$\Sha(E_d/K) := \ker \left( H^1(K, E_d) → \prod_v H^1(K_v, (E_d)_v) \right),$$

see [Ulm11, Lect. 1, §11] for more details. In Theorem 5.1 below, we will see that $\Sha(E_d/K)$ is finite.

5.1 The BSD conjecture

Inspired by the conjecture of Birch and Swinnerton-Dyer for elliptic curves over $\mathbb{Q}$, Tate gave a conjectural arithmetic interpretation of $\rho(E_d/K)$ and $L^*(E_d/K, 1)$ (see [Tat66]). 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 $d ≥ 1$, 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 $\Sha(E_d/K)$ is finite,
- the rank of $E_d(K)$ is equal to $\text{ord}_T-q^{-1} L(E_d/K, T)$,
- moreover, one has

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

(5.1)

We refer the reader to [Ulm07, §6] for the proof, or to [Ulm11, Lect. 3, §10] for a detailed sketch.

**Remark 5.2** Given Corollary 4.4, Lemma 3.5 in [Gri16b] yields fairly explicit expressions for $\rho(E_d/K)$ and $L^*(E_d/K, 1)$ as follows. For any integer $d ≥ 2$, in the notations of §2, consider the two subsets of $Z_d$ given by

$$V_d := \left\{ m ∈ Z_d : t_m(-1)J(m) = q^{|m|} \right\} \quad \text{and} \quad S_d := Z_d \setminus V_d.$$

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 $\rho(E_d/K) = |O_q(V_d)|$, and the special value $L^*(E_d/K, 1)$ has the following expression:

$$L^*(E_d/K, 1) = \prod_{m ∈ O_q(V_d)} |m| \cdot \prod_{m ∈ O_q(S_d)} \left( 1 - t_m(-1)J(m) \cdot q^{-|m|} \right).$$

(5.2)

**Remark 5.3** By Theorem 5.1 above, the analytic rank $\rho(E_d/K)$ is equal to $\text{rank}(E_d(K))$. The expression for $\rho(E_d/K)$ obtained in the previous remark allows us to retrieve a result of Ulmer on the ranks of $E_d(K)$ stating that as $d$ ranges through integers coprime to $q$, the ranks of $E_d(K)$ are unbounded (see [Ulm07, §2–§4], [Ulm11, Lect. 4, Thm. 3.11.1]). More precisely, one can show that there are infinitely many integers $d' ≥ 2$ coprime to $q$, such that $\text{rank}(E_{d'}(K)) \gg_{q} d'/\log d'$, where the implied constant is effective and depends only on $q$. We refer to [Gri16b, Prop. 7.3.5] for more details.

We conclude this subsection by recording the following estimate (see also §2 in [HP16]):

**Corollary 5.4** — When $d → ∞$ runs over the integers coprime to $q$, one has:

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

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


Proof: We first note that Theorem 5.1 ensures that \( \text{III}(E_d/K) \) 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

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

Corollary 1.6 then allows us to control the size of the right-most term. This yields the desired result. \( \square \)

### 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:

\[
\log \left( |\text{III}(E_d/K)| \cdot \text{Reg}(E_d/K) \right) \sim \log H(E_d/K) \quad (\text{as } d \to \infty).
\]

**Proof:** Given what has already been proved, the proof is almost clear: by Corollary 5.4, we know that

\[
\frac{\log \left( |\text{III}(E_d/K)| \cdot \text{Reg}(E_d/K) \right)}{\log H(E_d/K)} = 1 + \frac{\log L^*(E_d/K, 1)}{\log H(E_d/K)} + O \left( \frac{\log d}{d} \right) \quad (\text{as } d \to \infty).
\]

Further, Theorem 4.3 implies that, for all \( \epsilon \in (0, 1/4) \), there exists a constant \( C_5 > 0 \) such that

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

The concatenation of these two results thus yields that:

\[
\frac{\log \left( |\text{III}(E_d/K)| \cdot \text{Reg}(E_d/K) \right)}{\log H(E_d/K)} = 1 + O \left( \left( \frac{\log \log d}{\log d} \right)^{1/4-\epsilon} \right) = 1 + o(1) \quad (d \to \infty),
\]

where the implicit constant in the intermediate equality is effective and depends at most on \( q, p \) and \( \epsilon \). This is more than enough to prove Theorem 5.5. \( \square \)

**Remark 5.6** In [HP16], Hindry and Pacheco suggested to investigate the asymptotic behaviour of the Brauer-Siegel ratio

\[
\mathfrak{B}(E/K) := \log \left( |\text{III}(E/K)| \cdot \text{Reg}(E/K) \right) / \log H(E/K),
\]

as \( E \) runs through a family of non-isotrivial elliptic curves over \( K \). If \( \mathfrak{Ell} \) denotes the family of all such elliptic curves ordered by differential height, [HP16, Coro. 1.13] proves that

\[
0 \leq \liminf_{E \in \mathfrak{Ell} E \in \mathfrak{Ell}} \mathfrak{B}(E/K) \leq \limsup_{E \in \mathfrak{Ell} E \in \mathfrak{Ell}} \mathfrak{B}(E/K) = 1,
\]

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

**Acknowledgements** This article is based on results obtained by the author in his PhD thesis [Gri16a]. He thanks his supervisor Marc Hindry for his guidance and his encouragements. He also wishes to thank Douglas Ulmer and Michael Tsfasman for their interest in this work, for carefully reading a previous version, and for their helpful comments. The author is grateful to Universiteit Leiden for providing great working conditions during the writing of this article.

### References

[CHU14] Ricardo P. Conceição, Chris Hall, and Douglas Ulmer. Explicit points on the Legendre curve II. *Math. Res. Lett.*, 21(2):261–280, 2014. \( \dagger \)

[Coh07] Henri Cohen. *Number theory. Vol. I. Tools and Diophantine equations*, volume 239 of *Graduate Texts in Mathematics*. Springer, New York, 2007. \( \dagger \)

[DO16] Christopher Davis and Tommy Occhipinti. Explicit points on \( y^2 + xy - t^3 y = x^3 \) and related character sums. *J. Number Theory*, 168:13–38, 2016. \( \dagger \)
L-function and Brauer–Siegel for Hessian curves

Richard Griffon

[Gri16a] Richard Griffon. Analogues du théorème de Brauer–Siegel pour quelques familles de courbes elliptiques. PhD thesis, Université Paris Diderot, July 2016. (available at math.leidenuniv.nl/~griffonnmm/thesis/Griffon_thesis.pdf). ↑2, 14, 15

[Gri16b] Richard Griffon. A Brauer–Siegel theorem for Fermat surfaces over finite fields. (Preprint ArXiv:1612.08721), December 2016. ↑2, 12, 13, 14

[Gri17] Richard Griffon. Analogue of the Brauer–Siegel theorem for Legendre elliptic curves. (Preprint ArXiv:1706.07728), June 2017. ↑2

[Hin07] Marc Hindry. Why is it difficult to compute the Mordell–Weil group? In Diophantine geometry, volume 4 of CRM Series, pages 197–219. Ed. Norm., Pisa, 2007. ↑2

[HP16] Marc Hindry and Amielcar Pacheco. An analogue of the Brauer–Siegel theorem for abelian varieties in positive characteristic. Moscow Math. J., 16(1):45–93, January–March 2016. ↑2, 5, 11, 14, 15

[HW08] Godfrey H. Hardy and Edward M. Wright. An introduction to the theory of numbers. Oxford University Press, sixth edition, 2008. ↑13

[Lan83] Serge Lang. Conjectured Diophantine estimates on elliptic curves. In Arithmetic and geometry, Vol. I, volume 35 of Progr. Math., pages 155–171. Birkhäuser Boston, Boston, MA, 1983. ↑2

[Lan94] Serge Lang. Algebraic number theory, volume 110 of Graduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1994. ↑2

[Sil94] Joseph H. Silverman. Advanced topics in the arithmetic of elliptic curves, volume 151 of Graduate Texts in Mathematics. Springer-Verlag, New York, 1994. ↑4, 14

[Sil09] Joseph H. Silverman. The arithmetic of elliptic curves, volume 106 of Graduate Texts in Mathematics. Springer, Dordrecht, 2nd edition, 2009. ↑5

[SS10] Matthias Schütt and Tetsuji Shioda. Elliptic surfaces. In Algebraic geometry in East Asia—Seoul 2008, volume 60 of Adv. Stud. Pure Math., pages 51–160. Math. Soc. Japan, Tokyo, 2010. ↑3, 4, 5

[Tat66] John T. Tate. On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. In Séminaire Bourbaki, Vol. 9, pages 415–440 (Exp. No. 306). Soc. Math. France, Paris, 1965/66. ↑14

[Ulm02] Douglas Ulmer. Elliptic curves with large rank over function fields. Ann. of Math. (2), 155(1):295–315, 2002. ↑8

[Ulm07] Douglas Ulmer. L-functions with large analytic rank and abelian varieties with large algebraic rank over function fields. Invent. Math., 167(2):379–408, 2007. ↑2, 8, 14

[Ulm11] Douglas Ulmer. Elliptic curves over function fields. In Arithmetic of L-functions, volume 18 of IAS/Park City Math. Ser., pages 211–280. Amer. Math. Soc., Providence, RI, 2011. ↑3, 4, 5, 8, 14