A new family of elliptic curves with unbounded rank

Richard GRIFFON

Abstract −   Let $\mathbb{F}_q$ be a finite field of odd characteristic and $K = \mathbb{F}_q(t)$. For any integer $d \geq 1$, consider the elliptic curve E_d over K defined by $y^2 = x \cdot \left(x^2 + t^{2d} \cdot x - 4t^{2d}\right)$. We show that the rank of the Mordell–Weil group $E_d(K)$ is unbounded as d varies. The curve E_d satisfies the BSD conjecture, so that its rank equals the order of vanishing of its L-function at the central point. We provide an explicit expression for the L-function of E_d, and use it to study this order of vanishing in terms of d.

Keywords: Elliptic curves over function fields, Explicit computation of L-functions, BSD conjecture, Unbounded ranks, Explicit Jacobi sums.

2010 Math. Subj. Classification: 11G05, 11M38, 11G40, 14G10, 11L05.

Introduction

Let $\mathbb{F}_q$ be a finite field of characteristic $p \geq 3$ and $K := \mathbb{F}_q(t)$. It has been known for a while that there are elliptic curves over K with arbitrary large Mordell–Weil ranks. The first examples were provided in [ST67] by Shafarevich and Tate: they construct a sequence $\{E_n\}_{n \geq 1}$ of *isotrivial* elliptic curves over K such that rank $E_n(K) \to \infty$. The first instance of a sequence of *non-isotrivial* elliptic curves with unbounded ranks is due to Ulmer in [Ulm02]. Ulmer subsequently proved a rather general theorem (see [Ulm07]) which ensures, under a parity condition on the degree of the conductor, that certain so-called Kummer families of elliptic curves over K have unbounded *analytic* ranks. In parallel, Berger proposed in [Ber08] a construction of Kummer families of elliptic curves for which the BSD conjecture holds for each curve in the family: in these cases, Ulmer's 'unbounded *analytic* rank' result mentioned above can be translated into a 'unbounded *algebraic* rank' theorem.

In [Ber08], Berger gives three examples of families of elliptic curves to which her construction applies: for all but one of them, she concludes about unboundedness of the algebraic rank using Ulmer's result in [Ulm07]. In this article, we treat the remaining example, to which [Ulm07] does not apply. Specifically, for any integer $d \geq 1$, consider the elliptic curve E_d/K given by the affine Weierstrass model:

$$E_d : \qquad Y^2 + 2t^d \cdot XY - 4t^{2d} \cdot Y = X^3 - 6t^d \cdot X^2 + 8t^{2d} \cdot X.$$

The main goal of this article is to prove that:

Theorem A − *As $d \geq 1$ varies, the ranks of the Mordell–Weil groups $E_d(K)$ are unbounded; i.e.,*

$$\limsup_{d \geq 1} \operatorname{rank}(E_d(K)) = +\infty.$$

Further, the average Mordell–Weil rank of $E_d(K)$ is unbounded.

We prove the two assertions of Theorem A separately (see Theorems 7.4 and 7.7). First, we will construct several sequences of 'special' integers $(d_n)_{n \geq 1}$ for which we show that

$$\operatorname{rank}\left(E_{d_n}(K)\right) \gg_q d_n / \log d_n.$$

More precisely, we exhibit sequences integers d_n's such that this lower bound holds (see Theorem 7.4). We further show that one may retain the lower bound even if one restricts the parity of d_n. Secondly, we will use a result from [PS10] to prove that the average rank of $E_d(K)$ is unbounded: more precisely, we will show (in Theorem 7.7) that

$$\exists \alpha > 1/2, \qquad \frac{1}{x} \sum_{d \leq x} \operatorname{rank}\left(E_d(K)\right) \geq x^{\alpha} \qquad (\text{as } x \to \infty).$$

Of course, the second assertion implies the first one, and our treatment might appear redundant. However, the two proofs shed a different light on the behaviour of the sequence $d \mapsto \operatorname{rank}\big(E_d(K)\big)$. Indeed, for the explicitly constructed $(d_n)_{n\geq 1}$ in Theorem 7.4, the corresponding curves E_{d_n} have 'very large' ranks (as large as allowed by Brumer's bound, *cf.* [Bru92] and our Remark 7.6(b)). However, these integers d_n are very far apart from each other, and they cannot be deemed representative of the 'typical' size of $\operatorname{rank}\big(E_d(K)\big)$. The average result fills in that gap by showing that the rank of E_d is 'usually large'; but one then loses the explicit and precise character of the first construction.

The second proof also reveals that the sequence $\{E_d\}_d$ at hand is quite special: indeed, Brumer has proved that the average rank of elliptic curves over $\mathbb{F}_q(t)$ is bounded (see [Bru92]).

Let us now explain the strategy of the proof of Theorem A as we give the plan of the paper. In section 1, we start by introducing the elliptic curves E_d and by computing their relevant invariants. We also recall one of the results in [Ulm07] and explain why it cannot be used here. In section 2, we then completely describe the torsion subgroup $E_d(K)_{\mathrm{tors}}$ (Theorem 2.1) and provide a point of infinite order in $E_d(K)$ (Corollary 2.2).

Our first step towards the proof of Theorem A will be to give an explicit formula for the L-function $L(E_d/K, T)$ of E_d/K. To avoid introducing too many notations here, let us only state the following special case of our result (see Theorem 4.1 for the general version):

Theorem B − *Let $\mathbb{F}_q$ be a finite field of odd characteristic. For any integer $d \geq 1$ such that $2d \mid q - 1$, choose a character $\boldsymbol{\chi} : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ of exact order $2d$. The L-function of the elliptic curve E_d/K is given by*

$$L(E_d/K, T) = (1 - qT) \cdot \prod_{\substack{1 \leq n \leq 2d-1 \\ n \neq d/2, 3d/2}} \left(1 - B(n) \cdot T\right),$$

where, for all $n \in \{1, \ldots, 2d-1\}$ with $n \neq d/2, 3d/2$, we let

$$B(n) := \boldsymbol{\chi}^n(16) \cdot \left(\sum_{u \in \mathbb{F}_q} \boldsymbol{\chi}^n(u(1-u))\right)\left(\sum_{v \in \mathbb{F}_q} \boldsymbol{\chi}^{2n+d}(v)\boldsymbol{\chi}^{-n}(1-v)\right).$$

The relevant objects are introduced in section 3 and the proof of Theorem 4.1 is given in section 4. It is based on direct manipulations of character sums related to 'counting points' on the various reductions of E_d. Given that there are very few elliptic curves over K for which the L-function is explicitly known, this Theorem may be of independent interest.

The expression of $L(E_d/K, T)$ in Theorem B is sufficiently explicit that one can study its order of vanishing at $T = q^{-1}$ (see Corollary 4.3). Our main interest in doing so is that the BSD conjecture is known to hold for E_d/K *i.e.*, one has:

$$\operatorname{ord}_{T=q^{-1}} L(E_d/K, T) = \operatorname{rank}\big(E_d(K)\big).$$

This fact has been proved by Berger in [Ber08], and we sketch her proof in section 5. To this effect, we also briefly recall there how the curves E_d are constructed.

The expression for $\operatorname{ord}_{T=q^{-1}} L(E_d/K, T)$ obtained in Corollary 4.3 becomes more tractable for certain values of d: specifically, for those $d \geq 1$ such that $2d$ is *supersingular*. We give more details about this in section 6, recalling results from [ST67] and [Ulm02]. Our main result (Theorem A) is finally proved in section 7: the unboundedness of the rank is first proved in §7.1, we then discuss the unboundedness of the average rank in §7.2. We conclude the paper by an observation in §7.3 (Theorem 7.9) providing a third proof of Theorem A which is conditional on a certain hypothesis about primes.

1. The curves E_d and their invariants

Throughout this article, we fix a finite field $\mathbb{F}_q$ of characteristic $p \geq 3$, and we denote by $K = \mathbb{F}_q(t)$.

For any integer $d \geq 1$, consider the elliptic curve E_d/K defined by the affine Weierstrass model:

$$E_d : \qquad Y^2 + 2t^d \cdot XY - 4t^{2d} \cdot Y = X^3 - 6t^d \cdot X^2 + 8t^{2d} \cdot X.$$

The sequence $\{E_d\}_{d \geq 1}$ is an example of a *Kummer family* of elliptic curves over K (see §1.2). This sequence corresponds to the special case '$a = 1/2$' of Berger's example[1] (6) in §4.3 of [Ber08], further studied in §4.4 *loc. cit.* as example (2). The family $\{E_d\}_{d \geq 1, (d,q)=1}$ was also studied in [Gri16, Chap. 7], where E_d is denoted by $B_{1/2,d}$. In section 5 below, we will recall how these curves E_d are constructed in [Ber08].

---

[1] Note that Berger assumes that d is coprime to p, which we don't. We also point out a small typo in the Weierstrass model of E_1 given p. 3029 of [Ber08]: in standard notation, the coefficient a_2 should be $-(a+1)t$ instead of $-(a+1)$.

The above model of E_d has discriminant $2^8 t^{6d}(t^{2d} + 16)$ and a straightforward computation shows that the j-invariant of E_d is

$$j(E_d) = \frac{2^4 \cdot (t^{2d} + 12)^3}{t^{2d} + 16}.$$

We observe that $j(E_d) \in K$ is clearly not constant, so that E_d/K is non-isotrivial. Writing $d = p^e d'$ where $e \geq 0$ and d' is relatively prime to p, we see that the inseparability degree of the extension $K/\mathbb{F}_q(j(E_d))$ is p^e. In particular, the j-invariant of E_d is separable if and only if d is coprime to p.

The change of variables $(x, y) = (X - 2t^d, Y + t^d(X - 2t^d))$ changes the above model of E_d into a short Weierstrass model for E_d:

$$E_d : \qquad y^2 = x \cdot \left(x^2 + t^{2d} \cdot x - 4t^{2d}\right). \tag{1.1}$$

From now on, we work with this model of E_d, unless otherwise specified. The discriminant of (1.1) is easily seen to be

$$\Delta_d = 2^8 \cdot t^{6d}(t^{2d} + 16).$$

Remark 1.1 We point out that our point of view on Kummer families is slightly different from that of Ulmer's and Berger's. In their articles [Ber08, Ulm07, Ulm13], they fix an elliptic curve $E/\mathbb{F}_q(t)$ and consider the variation of the rank of $E(\mathbb{F}_q(t^{1/d}))$ as d varies. In the present paper, the base field $\mathbb{F}_q(t)$ is fixed and, for all d, we study the ranks of $E_d(\mathbb{F}_q(t))$ as d varies, where the elliptic curve $E_d/\mathbb{F}_q(t)$ is obtained from E_1 by 'replacing each occurence of t in a Weierstrass model of E_1 by t^d'. These two points of view are formally equivalent; we chose the latter because it is better suited to our purpose.

Remark 1.2 Let $d \geq 1$ be an integer: one can write $d = p^e d'$ for some integers $e \geq 0$ and $d' \geq 1$ such that $\gcd(d', p) = 1$. The elliptic curves E_d and $E_{d'}$ are then isogenous over K. Indeed, the p^e-th power Frobenius F_{p^e} provides a (purely inseparable) K-isogeny $F_{p^e} : E_{d'} \to E_d$.

Being K-isogenous, the elliptic curves $E_{d'}$ and E_d have the same conductor (see [Gro11, App. C], or [Sil09, Coro. VII.7.2] and [Sil94, Ex. IV.40]), the same L-function (see [Mil06, Chap. I, Lemma 7.1]) and the same Mordell–Weil rank (because the kernel of an isogeny is finite).

1.1. Conductor of E_d. $-$ Let us first describe the bad reduction of E_d and deduce the degree of the conductor of E_d. We identify, as we may, the finite places of K with monic irreducible polynomials in $\mathbb{F}_q[t]$.

For any integer $d \geq 1$, let M_d denote the set of (finite) places of K that divide $t^{2d} + 16$; the set M_d can be also be viewed as the set of closed points of $\mathbb{P}^1_{/\mathbb{F}_q}$ corresponding to $2d$-th roots of -16.

Proposition 1.3 $-$ *For any integer $d \geq 1$, the elliptic curve E_d given by (1.1) has good reduction outside $S = \{0\} \cup M_d \cup \{\infty\}$, and*

- *At $v = 0$, E_d has good (resp. additive) reduction when d is even (resp. d odd),*

- *At $v \in M_d$, E_d has split multiplicative reduction,*

- *At $v = \infty$, E_d has split multiplicative reduction.*

Proof: This can be proved directly by applying Tate's algorithm to E_d (see [Sil94, Chap. IV, §9]). This algorithm actually yields more information about the bad reduction of E_d: at $v = 0$, E_d has either good reduction (type $\mathbf{I}_0$) or additive reduction of type $\mathbf{I}_0^*$ depending on whether d is even or odd, respectively. At $v \in M_d$ (resp. at $v = \infty$), E_d has split multiplicative reduction of type $\mathbf{I}_1$ (resp. of type $\mathbf{I}_{4d}$). $\square$

Corollary 1.4 $-$ *Let $d \geq 1$ be an integer, and E_d/K the elliptic curve defined by (1.1). We denote by $\mathcal{N}_d$ the conductor divisor of E_d, and by $\mathcal{N}_d^f$ the part of $\mathcal{N}_d$ which is prime to 0 and ∞.*

Writing $d = p^e d'$ where $e \geq 0$ and $\gcd(d', p) = 1$, one has

$$\deg \mathcal{N}_d = \deg \mathcal{N}_{d'} = \begin{cases} 2d' + 1 & \text{if } d' \text{ is even,} \\ 2d' + 3 & \text{if } d' \text{ is odd,} \end{cases} \quad and \quad \deg \mathcal{N}_d^f = \deg \mathcal{N}_{d'}^f = 2d'. \tag{1.2}$$

Proof: When d is coprime to p, the result directly follows from the Proposition above and from the observation that one has $\sum_{v \in M_d} \deg v = \deg(t^{2d} + 16) = 2d$ because $t^{2d} + 16$ is then squarefree in $\mathbb{F}_q[t]$. The case of a general d reduces to this first case: indeed, E_d and $E_{d'}$ have the same conductor since they are isogenous *via* the p^e-th Frobenius isogeny (see Remark 1.2). $\square$

Remark 1.5 The application of Tate's algorithm at each place v of K also provides us with a minimal v-integral model of E_d. From the proof of the above Proposition and the expression of the discriminant of (1.1), one already deduces that the model (1.1) is integral and minimal at all places $v \neq 0, \infty$ of K. At $v = 0$, the model (1.1) is integral but is never minimal: the application of Tate's algorithm yields that

- When d is even, a minimal model of E_d at $v = 0$ is given by $y^2 = x(x^2 + t^d \cdot x - 4)$.

- When d is odd, a minimal model of E_d at $v = 0$ is given by $y^2 = x(x^2 + t^{d+1} \cdot x - 4t^2)$.

1.2. Ulmer's theorem on unbounded ranks. $-$ Let $\mathbb{F}_q$ be a finite field of characteristic $p \geq 3$ and $K = \mathbb{F}_q(t) = \mathbb{F}_q(\mathbb{P}^1)$. For any elliptic curve E/K, we denote by $\mathcal{N}^f_{E/K}$ be the part of the conductor $\mathcal{N}_{E/K} \in \text{Div}(\mathbb{P}^1)$ that is prime to 0 and ∞.

Given a non-isotrivial elliptic curve E' over K, one can construct as follows a sequence $\{E'_d\}_{d\geq 1}$ of elliptic curves over K, which we call the *Kummer family built from E'*. For any integer $d \geq 1$, let E'_d/K be the pullback of E'/K under the Kummer map $\mathbb{P}^1 \to \mathbb{P}^1$ given by $t \mapsto t^d$. In down-to-earth words: given a Weierstrass model $\mathcal{W}$ of E'/K, define E'_d by the Weierstrass model obtained by replacing each occurence of t in $\mathcal{W}$ by t^d. One of the main results of [Ulm07] can be stated as follows:

Theorem 1.6 (Ulmer) $-$ *Let E'/K be a non-isotrivial elliptic curve: we assume that the degree of $\mathcal{N}^f_{E'/K}$ is* odd *and we denote by $\{E'_d\}_{d\geq 1}$ be the Kummer family built from E'. Then the sequence of analytic ranks $(\text{ord}_{T=q^{-1}} L(E'_d/K, T))_{d\geq 1}$ is unbounded. Moreover, for $d_n := q^n + 1$ where $n \geq 1$ is an integer, one has*

$$\text{ord}_{T=q^{-1}} L(E'_{d_n}/K, T) \geq \frac{q^n + 1}{2n} - C,$$

where the constant C depends at most on q and E'.

The sequence $\{E_d\}_{d\geq 1}$ of elliptic curves E_d defined by (1.1) is an example of a Kummer family: it is the one built from $E_1 : y^2 = x(x^2 + t^2 x - 4t^2)$. As was noted in [Ber08, §4.4], the Theorem above *does not* apply to the Kummer family at hand, because $\deg \mathcal{N}^f_1 = \deg \mathcal{N}^f_{E_1/K}$ is even (see Corollary 1.4).

2. Some rational points on E_d

When one looks for non-trivial K-rational points on E_d, one quickly finds at least two: $P_0 = (0, 0)$ and $P_d = (2t^d, 2t^{2d})$ on the model (1.1). The point P_0 is clearly 2-torsion, and we show in this section that P_0 is 'usually' the only K-rational torsion point on E_d:

Theorem 2.1 $-$ *Let $d \geq 1$ be an integer. Unless $p = 3$ and d is divisible by 3, one has $E_d(K)_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z}$ and $E_d(K)_{\text{tors}}$ is generated by $P_0 = (0,0)$. If $p = 3$ and 3 divides d, the torsion subgroup is generated by $P_1 = (-t^{4d/3}, t^{5d/3}(1 + t^{2d/3}))$, and one has $E_d(K)_{\text{tors}} \simeq \mathbb{Z}/6\mathbb{Z}$.*

We can then immediately deduce that the point P_d has infinite order:

Corollary 2.2 $-$ *For any integer $d \geq 1$, the point $P_d = (2t^d, 2t^{2d}) \in E_d(K)$ has infinite order. In particular, the elliptic curve E_d has positive rank.*

This section is devoted to the proof of Theorem 2.1, which we have split in several parts. The main difficulty in the proof is to bound the p-part of $E_d(K)_{\text{tors}}$.

2.1. Preliminaries. $-$ Let $p \geq 3$ be an odd prime number, and put $m = (p-1)/2$. In the polynomial ring $\mathbb{F}_p[U]$, consider the polynomial

$$G_p(U) = \sum_{0 \leq k \leq m/2} \beta_p(k) U^k, \quad \text{where } \beta_p(k) = 4^{-k} \cdot \binom{m}{2k}\binom{2k}{k} \in \mathbb{F}_p$$

Note that this definition makes sense ($k!$ is non-zero in $\mathbb{F}_p$ for $k \leq p - 1$). Since $\beta_p(0) = 1$, it is immediate that $G_p(0) = 1$. If $p = 3$, note that $G_p(U) = 1$ is constant, so we will now concentrate on the case when $p > 3$. By definition, we have the following identity relating $\beta(k+1)$ to $\beta(k)$:

$$\beta(k+1) = \frac{(m - 2k - 1)(m - 2k)}{4 \cdot (k+1)^2} \cdot \beta(k). \tag{2.1}$$

Let us prove the following:

Lemma 2.3 $-$ *If $p > 3$, one has $G_p(1) = (-1)^{\lfloor (p-1)/4 \rfloor} \in \mathbb{F}_p$.*

Proof: First of all, note that $(-1)^{\lfloor (p-1)/4 \rfloor}$ equals $+1$ precisely when $p \equiv 1$ or $3 \mod 8$, and is -1 otherwise. By quadratic reciprocity, -2 is a square modulo p if and only if $p \equiv 1, 3 \mod 8$. Since $1/4$ is always a square modulo p, we obtain the following identity in $\mathbb{F}_p$:

$$(-1)^{\lfloor (p-1)/4 \rfloor} = (-2)^{(p-1)/2} = (-1/2)^{(p-1)/2}.$$

Let $m = (p-1)/2$ and
$$N_p := \left| \left\{ (a,b) \in \mathbb{F}_p^2 : a^2 = b(b+1/2)^2 \right\} \right|.$$
A straightforward counting argument shows that N_p equals $p-1$ (resp. $p+1$) if $-1/2$ is a square (resp. not a square) in $\mathbb{F}_p^{\times}$. Hence $N_p \equiv -(-1/2)^{(p-1)/2} \bmod p$.

On the other hand, it is known that $\left| \{ x \in \mathbb{F}_p : x^2 = y \} \right| \equiv 1 + y^m \bmod p$ for any $y \in \mathbb{F}_p$. We deduce that

$$N_p = \sum_{b \in \mathbb{F}_p} \left| \left\{ a \in \mathbb{F}_p : a^2 = b^3 + b^2 + b/4 \right\} \right| \equiv p + \sum_{b \in \mathbb{F}_p^{\times}} \left(b^3 + b^2 + b/4 \right)^m.$$

The sum on the right-hand side decomposes as a $\mathbb{F}_p$-linear combination of sums of the form $\sum_{b \in \mathbb{F}_p^{\times}} b^n$ for $1 \le n \le 3m$. Since $\mathbb{F}_p^{\times}$ is cyclic, these sums $\sum_{b \in \mathbb{F}_p^{\times}} b^n$ all vanish in $\mathbb{F}_p$, except the one with $n = 2m = (p-1)$ which equals -1. Letting A_{p-1} denote the coefficient of b^{p-1} in the expansion of $(b^3 + b^2 + b/4)^m$ as a polynomial in b, we have thus proved that $N_p \equiv -A_{p-1}$. Using the binomial theorem, one can show that

$$A_{p-1} = \sum_{0 \le k \le m/2} \binom{m}{2k} \binom{2k}{k} 4^{-k} = \sum_{0 \le k \le m/2} \beta(k) = G_p(1).$$

Putting these results together yields the desired equality: $G_p(1) = -N_p = (-2)^{(p-1)/2} = (-1)^{\lfloor (p-1)/4 \rfloor}$. $\qquad \square$

Lemma 2.4 $-$ *If $p > 3$, the polynomial $G_p(U)$ has simple roots in $\overline{\mathbb{F}_p}$.*

Proof: Consider the differential operator $\mathcal{D} : \mathbb{F}_p[U] \to \mathbb{F}_p[U]$ given by

$$\forall P \in \mathbb{F}_p[U], \quad \mathcal{D}P := 16U(1-U)\frac{\mathrm{d}^2 P}{\mathrm{d}U^2} + 16(1 - 2U)\frac{\mathrm{d}P}{\mathrm{d}U} - 3P.$$

A simple computation using identity (2.1) and the fact that $m = (p-1)/2$ shows that

$$\mathcal{D}G_p(U) = p \cdot \sum_{k=0}^{M} \{-8k + p - 4\} \cdot \beta(k) U^k = 0 \quad \text{in } \mathbb{F}_p[U].$$

Since G_p is a non-zero solution of the second order linear differential equation described by $\mathcal{D}$, its only possible multiple roots in $\overline{\mathbb{F}_p}$ are the 'singular points' 0 and 1 of $\mathcal{D}$. Since we have shown that G_p does not vanish at 0 or 1 (see the previous Lemma), G_p only has simple roots in $\overline{\mathbb{F}_p}$ and the proof is complete. $\qquad \square$

2.2. Rational p-torsion on E_d. $-$ Let $d \ge 1$ be an integer, written as $d = p^e d'$ with $e \ge 0$ and d' coprime to p. To describe the p-torsion on E_d, it will be useful to compute the Hasse invariant of E_d. Recall that, if an elliptic curve E/K is given by a short Weierstrass model $y^2 = f(x)$, its Hasse invariant $A(E)$ can be described as the coefficient of x^{p-1} in $f(x)^{(p-1)/2}$ (see [Ulm11, Lect. I, §3] for more details). This definition clearly depends on the choice of $f(x)$, but it is easy to see that changing the short Weierstrass model of E amounts to multiplying $A(E)$ by a $(p-1)$-st power in $K^{\times}$. The Hasse invariant is thus a well-defined element of $K/(K^{\times})^{p-1}$.

We denote by $A_d \in K$ the Hasse invariant of E_d (or rather, one of its lift from $K/(K^{\times})^{p-1}$). To compute it, we describe E_d by a short minimal integral Weierstrass model at the place ∞ of K: putting $u = 1/t$, the curve E_d is given by

$$E_d : \qquad y^2 = x(x^2 + x - 4u^{2d}).$$

This model is easily obtained from (1.1) by the change of variables $(x,y) \mapsto (u^{2d}x, u^{3d}y)$. By the recipe described above, we have

$$\begin{aligned}
A_d &= \text{coefficient of } x^{p-1} \text{ in } x^{(p-1)/2}(x^2 + x - 4u^{2d})^{(p-1)/2} \\
&= \text{coefficient of } x^{(p-1)/2} \text{ in } (x^2 + x - 4u^{2d})^{(p-1)/2} \\
&= \sum_{\substack{0 \le j \le m \\ j \text{ even}}} \binom{m}{j}\binom{j}{j/2} \cdot (-4u^{2d})^{2j} = \sum_{0 \le k \le m/2} \binom{m}{2k}\binom{2k}{k} \cdot (-4u^{2d})^k = G_p(-16u^{2d}),
\end{aligned}$$

where G_p is the polynomial defined in the previous subsection. This follows directly from the binomial theorem.

By Proposition 7.3 in [Ulm11, Lecture I], the curve E_d possesses a non-trivial K-rational p-torsion point if and only if $j(E_d)$ is a p-th power in K and the Hasse invariant of E_d is a $(p-1)$-st power in $K^{\times}$. If d is coprime to d, the j-invariant is not a p-th power in K (see §1); the preceding criterion then implies that

$E_d(K)[p] = \{\mathcal{O}\}$. We now assume that p divides d: the j-invariant *is* a p-th power and we need to elucidate whether A_d is a $(p-1)$-st power in $K^\times$ or not.

We first assume that $p > 3$. We have shown in Lemma 2.4 that $G_p(u)$ has no multiple root in $\overline{\mathbb{F}_p}$. Since $A_d(u) = G_p(-16u^{2d}) \in \mathbb{F}_p[u]$, we note that $A_d(u) = A_{d'}(u)^{p^e}$. It follows from Lemma 2.4 that $G_p(U)^{p^e}$ is not a $(p-1)$-st power in $\mathbb{F}_q(U)$: indeed, the multiplicity of its roots in $\overline{\mathbb{F}_p}$ is p^e. Since the map $u \mapsto -16u^{2d'}$ is unramified outside $0, \infty$, we deduce that the roots of A_d in $\overline{\mathbb{F}_p}$ have multiplicity p^e. In particular, A_d is not a $(p-1)$-st power in $K^\times$.

Finally, if $p = 3$ and if d is divisible by 3, then the criterion ensures that $E_d(K)[3]$ is non-trivial. By direct inspection, we find that the point P_2 with coordinates $(t^{2d/3}, t^d + t^{5d/3})$ in the model (1.1) is a 3-torsion point on E_d.

We have therefore proven

Lemma 2.5 – $E_d(K)[p^\infty]$ *is trivial, unless* $p = 3$ *and* 3 *divides* d.

2.3. Prime-to-p part of $E_d(K)_{\mathrm{tors}}$.

– Let $d \geq 1$ be an integer, written as $d = p^e d'$ as before. The goal of this section is to describe the subgroup $G'_d \subseteq E_d(K)_{\mathrm{tors}}$ of points whose order is prime to p:

Lemma 2.6 – *The group* G'_d *is generated by* $P_0 = (0,0)$ *and thus* $G'_d \simeq \mathbb{Z}/2\mathbb{Z}$.

Proof: We start by describing the 2-torsion in G'_d: in the homogenised version of the model (1.1), the four $\overline{K}$-rational 2-torsion points on E_d are given by $[0:1:0] = \mathcal{O}$, $[0:0:1] = P_0$, $[-t^d(t^d + \sqrt{t^d + 16})/2 : 0 : 1]$ and $[-t^d(t^d - \sqrt{t^d + 16})/2 : 0 : 1]$. Only the first two are K-rational (since $t^d + 16 \in \mathbb{F}_q[t]$ is squarefree), hence $G'_d[2] = \{\mathcal{O}, P_0\}$.

For any place v of K, we let Γ_v denote the group of components of the special fibre at v of the Néron model of E_d (so that $\Gamma_v = \{1\}$ for all but finitely many places). Our proof of Proposition 1.3 and the table in [SS10, §7.2] provide explicit descriptions of the groups Γ_v for E_d.

When d is odd, the curve E_d has additive reduction at the place 0: Lemma 7.8 in [SS10] shows that the prime-to-p part of $E_d(K)_{\mathrm{tors}}$ embeds into $\Gamma_0 \simeq (\mathbb{Z}/2\mathbb{Z})^2$. We thus infer that G'_d is 2-torsion, so that $G'_d = G'_d[2] = \{\mathcal{O}, P_0\}$ by the computation in the previous paragraph.

This complete the proof of Theorem 2.1 in this case.

We now turn to the case when d is even. Corollary 7.5 in [SS10] shows that the whole of $E_d(K)_{\mathrm{tors}}$ embeds as a subgroup of $\Gamma := \prod_v \Gamma_v$. More explicitly, this result here yields that $E_d(K)_{\mathrm{tors}}$ is isomorphic to a subgroup of $\mathbb{Z}/4d\mathbb{Z}$. By the structure theorem for finite abelian groups, G'_d is then isomorphic to a subgroup of $\mathbb{Z}/4d'\mathbb{Z}$. In particular, G'_d has to be cyclic, and we let g' denote its order. Upon carrying out an explicit version of the proof of Proposition 7.1 in [Ulm11, Lect. 1], one can show that $1 \leq g' \leq 12$ (see the proof of [Gri18b, Prop. 1.5]). Given the previous constraints on g', we obtain that $g' \in \{2, 4, 6, 8, 10, 12\}$. If the characteristic p of K is 3, we still need to check that $E_d(K)$ has no non-trivial 4-torsion or 5-torsion points. If the characteristic is 5, we have to rule out non-trivial 3-torsion or 4-torsion points. And if the characteristic is > 5, the Lemma will follow once we have checked that $E_d(K)$ contains no non-trivial 3-torsion, 4-torsion or 5-torsion.

We carry out this last step by considering *division polynomials*: for any $n \geq 1$, there is a rational map ψ_n on E_d (which can be explicitly given in terms of Weierstrass coefficients of E_d) with the following property. The zeroes of ψ_n are simple and they are exactly the non-trivial n-torsion points on E_d, and ψ_n has a pole of the appropriate order at the neutral element $\mathcal{O}$. The reader is referred to [Sil09, Chap. III, Ex. 3.7] for more details.

First we note that, when d is even, the Weierstrass equation $W' : y^2 = x(x^2 + t^d x - 4)$ is a minimal integral model of E_d at all finite places of K (by 'scaling' (1.1) *via* $(x, y) \mapsto (t^d x, t^{3d/2} y)$). The formulae in [Sil09, Chap. III, Ex. 3.7] here read:

$$\psi_3 = 3x^4 + 4t^d \cdot x^3 - 24 \cdot x^2 - 16,$$
$$\psi_4 = 4y(x^6 + 2t^d \cdot x^5 - 20 \cdot x^4 - 80 \cdot x^2 - 32t^d \cdot x + 64),$$
$$\psi_5 = 5x^{12} + 20t^d \cdot x^{11} + 8t^d(2t^d - 31) \cdot x^{10} - 320t^d \cdot x^9 - 1680 \cdot x^8 - 5760t^d \cdot x^7 - 3840(t^{2d} - 5) \cdot x^6$$
$$- 1024t^d(t^{2d} - 23) \cdot x^5 + 1280(t^{2d} - 3125) \cdot x^4 - 35840t^d \cdot x^3 + 51200 \cdot x^2 + 4096.$$

Therefore, to conclude our proof, it remains to show that, for all $P = (x_P, y_P) \in E_d(K) \smallsetminus \{\mathcal{O}\}$ one has $\psi_n(x_P, y_P) \neq 0$ for $n \in \{3, 4, 5\}$ (with suitable restriction on the characteristic of K).

Assume that $p \neq 3$, and suppose that there exists a non-trivial 3-torsion point $P = (x_P, y_P) \in E_d(K)$. By construction of the polynomial ψ_3, we have $\psi_3(P) = 0$ *i.e.*, we have

$$x_P^4 + \tfrac{4}{3}t^d \cdot x_P^3 - 8 \cdot x_P^2 - \tfrac{16}{3} = 0.$$

In particular, $x_P \in \mathbb{F}_q(t)$ is integral over $\mathbb{F}_q[t]$ and we obtain that $x_P \in \mathbb{F}_q[t]$. Now, the equation above can be rewritten as: $x_P^2 \cdot (3x_P^2 + 4t^d \cdot x_P - 24) = 16$. For degree reasons, the polynomials x_P and $x_P^2 + 4t^d x_P - 24$ must both be constant and non-zero, which is impossible. This contradiction shows that $E_d(K)$ has no non-trivial 3-torsion. The same argument also excludes 5-torsion in case $p \neq 5$: if there were a non-trivial 5-torsion point $P = (x_P, y_P) \in E_d(K)$, then x_P would be in $\mathbb{F}_q[t]$ and would satisfy

$$\left(5x_P^{10} + 20t^d \cdot x_P^9 + 8t^d(2t^d - 31) \cdot x_P^8 + \cdots - 35840t^d \cdot x_P + 51200\right) \cdot x_P^2 = -4096.$$

Such an equality is never satisfied, so that $E_d(K)[5] = \{\mathcal{O}\}$. Finally, assume that there is a point $P = (x_P, y_P) \in E_d(K)$ of exact order 4. By construction $\psi_4(P) = 0$ but, since P is not 2-torsion, one has $y_P \neq 0$. By the same argument as above, x_P is an element of $\mathbb{F}_q[t]$ and is a solution of

$$\left(x_P^5 + 2t^d \cdot x_P^4 - 20 \cdot x_P^3 - 80 \cdot x_P - 32t^d\right) \cdot x_P = -64.$$

Since no element of $\mathbb{F}_q[t]$ can satisfy such a relation, P cannot exist and we have shown that $G_d'[4] = \{\mathcal{O}\}$. This concludes the proof that $G_d' = \{\mathcal{O}, P_0\}$ in the case when d is even. $\qquad\square$

2.4. Proof of Theorem 2.1. $-$ Let $d \geq 1$ be an integer: as above, we write $G_d' \subseteq E_d(K)_{\text{tors}}$ for the subgroup of torsion points whose order is prime to p. Note that $E_d(K)_{\text{tors}} \simeq G_d' \times E_d(K)[p^\infty]$.

Assume first that $p \neq 3$ and that d is arbitrary. By Lemma 2.5, $E_d(K)_{\text{tors}}$ does not have any non-trivial point of pth power order. Lemma 2.6 then tells us that $G_d' \simeq \mathbb{Z}/2\mathbb{Z}$. This proves Theorem 2.1 in this case. The proof extends to the case where $p = 3$ and d is coprime to 3.

There remains to treat the case where $p = 3$ and 3 divides d. We know by Lemma 2.6 that $G_d' \simeq \mathbb{Z}/2\mathbb{Z}$ is generated by $P_0 = (0,0)$. We also know, as a consequence of the Mordell-Weil theorem, that the group $E_d(K)[3^\infty]$ must be a finite cyclic group *i.e.* it is of the form $\mathbb{Z}/3^n\mathbb{Z}$ for some $n \geq 1$. By Lemma 2.5, the p-part $E_d(K)[3^\infty]$ contains the subgroup generated by $P_2 = (t^{2d/3}, t^d + t^{5d/3})$, which is isomorphic to $\mathbb{Z}/3\mathbb{Z}$. Hence, to complete the proof of Theorem 2.1, we only have to ensure that $E_d(K)$ contains no non-trivial 3^n-torsion points for any $n \geq 2$. Again, we write $d = 3^e d'$ with $e \geq 1$ and d' coprime to 3.

The proof of Lemma 14 in [GS95] shows that the order of $E_d(K)[3^\infty]$ is bounded by the inseparability degree of the j-invariant of E_d, which equals 3^e here (see §1). This concludes the proof of the Theorem if $e = 1$ (*i.e.*, if d is divisible by 3 but not by 3^2), and we now assume that $e \geq 2$.

In general, a result of Levin asserts that, if 3^n divides $|E_d(K)_{\text{tors}}|$ then $n \leq 2$ (see p. 461 in [Lev68]). Therefore, the Theorem will be proved once we have shown that $E_d(K)[9]$ is trivial. We proceed as follows to rule out 9-torsion. Let $d'' = d/9$, we first 'scale' the Weierstrass model (1.1), via $(x, y) \mapsto (t^{-2d/3}x, t^{-d}y)$, into the model $y_0^2 = x_0(x_0^2 + t^{4d/3}x_0 - 4t^{2d/3})$ which we denote by (W_0). In this model, the 3-torsion point P_2 we found above has coordinates $(1, 1 + t^{2d/3})$. Suppose that there were a K-rational point $Q \in E_d(K)$ of exact order 9; we could then choose Q so that $[3]Q = P_2$. Let $x_Q \in K$ be the first coordinate of Q in the model (W_0). By the formula for multiplication by 3 in characteristic 3 (see [Sil09, Chap. III, Ex. 3.7(d)]), the first coordinate of $[3]Q$ in the model (W_0) is given by

$$x([3]Q) = \frac{x_Q^3(x_Q^3 + t^{18d''})^2}{(t^{4d''}(x_Q - 1))^6} = \left\{\frac{x_Q(x_Q + t^{6d''})^2}{t^{8d''}(x_Q - 1)^2}\right\}^3.$$

Identifying $x([3]Q)$ with $x(P_2) = 1$, we obtain that x_Q would satisfy $x_Q(x_Q + t^{6d''})^2 = t^{8d''}(x_Q - 1)^2$. In other words,

$$x_Q \cdot \left(x_Q^2 - t^{6d''}(t^{2d''} + 1)x_Q + t^{8d''}(t^{4d''} + 1)\right) = t^{8d''}.$$

In particular, $x_Q \in \mathbb{F}_q(t)$ would be integral over $\mathbb{F}_q[t]$ and therefore would lie in $\mathbb{F}_q[t]$. However, as can easily be seen, the equation $X \cdot \left(X^2 - t^{6d''}(t^{2d''} + 1)X + t^{8d''}(t^{4d''} + 1)\right) = t^{8d''}$ has no solution $X \in \mathbb{F}_q[t]$. This shows that no such point Q can exist.

We conclude that $E_d(K)[p^\infty]$ consists only of the subgroup generated by P_2 (isomorphic to $\mathbb{Z}/3\mathbb{Z}$). Hence, by our previous results, $E_d(K)_{\text{tors}}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z}$ in this case. Moreover, it can be generated by $P_0 + P_2 = (-t^{4d/3}, t^{5d/3}(1 + t^{2d/3}))$. $\qquad\square$

Remark 2.7 Note that the full strength of Theorem 2.1 is not required to prove Corollary 2.2. More precisely, one can already deduce that $P_d = (2t^d, 2t^{2d}) \in E_d(K)$ has infinite order for all integers d from the assertion that $E_{d'}(K)_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z}$ for integers d' which are coprime to p. The argument goes as follows.

Let d be an integer and write $d = p^e d'$ with $e \geq 0$ and d' coprime to p. Let $F_{p^e} : E_{d'} \to E_d$ denote the p^e-th power Frobenius isogeny, $V_{p^e} : E_d \to E_{d'}$ its dual and $[p^e] : E_{d'} \to E_{d'}$ the multiplication-by-p^e map on $E_{d'}$.

By construction, one has $P_d = (2t^{p^e \cdot d'}, 2t^{p^e \cdot 2d'}) = F_{p^e}(P_{d'})$, so that $V_{p^e}(P_d) = V_{p^e} \circ F_{p^e}(P_{d'}) = [p^e]P_{d'}$. If P_d were torsion of order $m \geq 2$, one would have

$$\mathcal{O} = V_{p^e}(\mathcal{O}) = V_{p^e}([m]P_d) = [m]V_{p^e}(P_{d'}) = [m][p^e]P_{d'} = [p^e]([m]P'_d).$$

Since $E_{d'}(K)$ contains no p-th power torsion point, this would imply that $[m]P_{d'} = \mathcal{O}$, which is a contradiction. Therefore $P_d \in E_d(K)$ has infinite order.

3. Characters of order dividing $2d$ and some character sums

The goal of the next section will be to give an explicit expression for the L-function of E_d: the result will be expressed in terms of certain character sums, which we start by introducing and relating to products of some Jacobi sums.

3.1. Jacobi sums. — Let $\mathbb{F}$ be a finite field of odd characteristic. There is a unique non-trivial character of order 2 on $\mathbb{F}^\times$, which we denote by[2] $\lambda_{\mathbb{F}} : \mathbb{F}^\times \to \{\pm 1\}$. We follow the convention that non-trivial multiplicative characters $\chi : \mathbb{F}^\times \to \overline{\mathbb{Q}}^\times$ are extended to the whole of $\mathbb{F}$ by $\chi(0) := 0$, and the trivial character $\mathbb{1}$ by $\mathbb{1}(0) := 1$. To any pair of multiplicative characters χ_1, χ_2 on $\mathbb{F}^\times$, we associate a Jacobi sum

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

We refer to [Coh07, Chap. II, §5.3 - §5.4] for more details about these sums. For further use, we recall the following facts:

(Jac 1) For any non-trivial character χ, one has $\mathbf{j}_{\mathbb{F}}(\mathbb{1}, \chi) = 0$.

(Jac 2) For any non-trivial character χ such that $\chi \neq \lambda$, one has $\mathbf{j}_{\mathbb{F}}(\chi, \lambda) = \chi(4) \cdot \mathbf{j}_{\mathbb{F}}(\chi, \chi)$.

(Jac 3) One has $\mathbf{j}_{\mathbb{F}}(\lambda, \lambda) = \lambda(-1)$.

(Jac 4) For any characters χ_1, χ_2 on $\mathbb{F}^\times$ and any finite extension $\mathbb{F}'/\mathbb{F}$, one has

$$\mathbf{j}_{\mathbb{F}'}(\chi_1 \circ \mathbf{N}_{\mathbb{F}'/\mathbb{F}}, \chi_2 \circ \mathbf{N}_{\mathbb{F}'/\mathbb{F}}) = \mathbf{j}_{\mathbb{F}}(\chi_1, \chi_2)^{[\mathbb{F}':\mathbb{F}]},$$

where $\mathbf{N}_{\mathbb{F}'/\mathbb{F}} : \mathbb{F}' \to \mathbb{F}$ denotes the relative norm of the extension $\mathbb{F}'/\mathbb{F}$. This identity is often called the Hasse–Davenport relation for Jacobi sums (see [Coh07, Coro III.5.7]).

(Jac 5) For any characters χ_1, χ_2 on $\mathbb{F}^\times$ such that none of χ_1, χ_2, and $\chi_1\chi_2$ is trivial, one has

$$|\mathbf{j}_{\mathbb{F}}(\chi_1, \chi_2)| = |\mathbb{F}|^{1/2},$$

in any complex embedding of $\overline{\mathbb{Q}}$.

3.2. Two identities with character sums. — In this subsection, $\mathbb{F}$ denotes a finite field of odd characteristic. For any multiplicative character $\chi : \mathbb{F}^\times \to \overline{\mathbb{Q}}^\times$, we consider the double character sum

$$B(\mathbb{F}, \chi) := \sum_{x \in \mathbb{F}} \sum_{z \in \mathbb{F}^\times} \chi(z) \cdot \lambda\left(x^3 + x^2 z - 4xz\right). \tag{3.1}$$

Let us first prove the following:

Proposition 3.1 — *Let $\chi : \mathbb{F}^\times \to \overline{\mathbb{Q}}^\times$ be a multiplicative character. Then*

$$B(\mathbb{F}, \chi) = \begin{cases} |\mathbb{F}| & \text{if } \chi = \mathbb{1} \text{ is trivial,} \\ 1 & \text{if } \chi = \lambda \text{ has order 2,} \\ \mathbf{j}_{\mathbb{F}}(\chi, \chi) & \text{if } \chi \text{ has order exactly 4,} \\ \chi(16) \cdot \mathbf{j}_{\mathbb{F}}(\chi, \chi) \cdot \mathbf{j}_{\mathbb{F}}(\lambda\chi^2, \overline{\chi}) & \text{otherwise.} \end{cases}$$

Note that characters $\chi : \mathbb{F}^\times \to \overline{\mathbb{Q}}^\times$ of exact order 4 exist if and only if $|\mathbb{F}| \equiv 1 \bmod 4$ (by cyclicity of the group $\mathbb{F}^\times$). If this is the case, there are exactly two such characters.

---

[2]or simply by λ when no confusion is likely.

Proof: Notice that the terms with $x = 0$ do not contribute to the sum (3.1) because $\lambda(0) = 0$, therefore

$$B(\mathbb{F}, \chi) = \sum_{x \in \mathbb{F}^\times} \lambda(x) \left(\sum_{z \in \mathbb{F}^\times} \chi(z) \cdot \lambda\big((x-4)z + x^2\big) \right).$$

For a given $x \neq 0$, consider the inner sum in the above equality: if $x = 4$, then

$$\sum_{z \in \mathbb{F}^\times} \chi(z) \cdot \lambda\big((x-4)z + x^2\big) = \lambda(4)^2 \cdot \sum_{z \neq 0} \chi(z) = \begin{cases} |\mathbb{F}| - 1 & \text{if } \chi = \mathbb{1}, \\ 0 & \text{otherwise.} \end{cases}$$

If $x \neq 4$, we let $A_x := x^2/(x-4)$ and we obtain that

$$\sum_{z \in \mathbb{F}^\times} \chi(z) \cdot \lambda\big((x-4)z + x^2\big) = \lambda(x-4) \cdot \sum_{z \neq 0} \chi(z)\lambda(z + A_x).$$

If $\chi = \mathbb{1}$, it is not hard to check that $\sum_{z \neq 0} \chi(z)\lambda(z + A_x) = -1$. If χ is non-trivial, we can add the term $z = 0$ (which does not contribute) and reindex the sum by letting $(u_1, u_2) = (-z/A_x, 1 + z/A_x)$. This leads to

$$\sum_{z \neq 0} \chi(z)\lambda(z + A_x) = \chi(-A_x)\lambda(A_x) \cdot \sum_{\substack{u_i \in \mathbb{F} \\ u_1 + u_2 = 1}} \chi(u_1)\lambda(u_2) = -\chi(-1)\lambda(A_x)\chi(A_x) \cdot \mathbf{j}_\mathbb{F}(\chi, \lambda).$$

Besides, one can show that $\sum_x \lambda(x(x-4)) = -1$ (see [LN97, Theorem 5.48]). If $\chi = \mathbb{1}$ is trivial, this identity and what we have just proved yield that

$$B(\mathbb{F}, \mathbb{1}) = -\sum_{x \neq 0, 4} \lambda(x)\lambda(x-4) + \lambda(4) \cdot (|\mathbb{F}| - 1) = 1 + |\mathbb{F}| - 1 = |\mathbb{F}|,$$

as was to be shown. We now assume that $\chi \neq \mathbb{1}$: using the expression of A_x and the fact that $\lambda(x^2) = \lambda(x-4)^2 = 1$ for all $x \neq 0, 4$, we have obtained thus far that

$$B(\mathbb{F}, \chi) = -\chi(-1) \cdot \mathbf{j}_\mathbb{F}(\chi, \lambda) \cdot B'(\mathbb{F}, \chi), \quad \text{with } B'(\mathbb{F}, \chi) := \sum_{x \neq 0, 4} \lambda(x)\chi(x^2)\overline{\chi}(x-4). \tag{3.2}$$

It remains to express $B'(\mathbb{F}, \chi)$ in terms of a Jacobi sum, and we distinguish several cases.

We first assume that $\chi = \lambda$ has order exactly 2: in this case, one has $\lambda(x)\chi(x^2)\overline{\chi}(x-4) = \lambda(x)\lambda(x-4)$ for all $x \in \mathbb{F} \smallsetminus \{0, 4\}$. Hence, $B'(\mathbb{F}, \chi) = \sum_{x \in \mathbb{F}} \lambda(x(x-4)) = -1$ by the same identity as before. Moreover, (Jac 3) yields that $\mathbf{j}_\mathbb{F}(\lambda, \lambda) = \lambda(-1)$ so that $B(\mathbb{F}, \chi) = \lambda(-1)^2 = 1$.

Next, we assume that $\chi \notin \{\mathbb{1}, \lambda\}$ and that $\lambda\chi^2$ is the trivial character: this happens exactly when χ has exact order 4. For all $x \in \mathbb{F} \smallsetminus \{0, 4\}$, we now have $\lambda(x)\chi(x^2)\overline{\chi}(x-4) = \overline{\chi}(x-4)$. Hence $B'(\mathbb{F}, \chi) = -\overline{\chi}(-4)$ and we have $B(\mathbb{F}, \chi) = \overline{\chi}(4) \cdot \mathbf{j}_\mathbb{F}(\chi, \lambda)$ which, by (Jac 2), can be rewritten as $B(\mathbb{F}, \chi) = \mathbf{j}_\mathbb{F}(\chi, \chi)$.

Finally, we deal with the case where $\chi^4 \neq \mathbb{1}$. Then $\lambda\chi^2$ is non-trivial and, by setting $x = 4x'$, we obtain that

$$B'(\mathbb{F}, \chi) = \sum_{x \in \mathbb{F}} (\lambda\chi^2)(x)\overline{\chi}(x-4) = \lambda(4) \cdot \chi(-4) \cdot \sum_{x' \in \mathbb{F}} (\lambda\chi^2)(x')\overline{\chi}(1 - x') = -\chi(-4) \cdot \mathbf{j}_\mathbb{F}(\lambda\chi^2, \overline{\chi}).$$

Appealing to (Jac 2) again, we conclude that

$$B(\mathbb{F}, \chi) = \chi(-1)^2\chi(4) \cdot \mathbf{j}_\mathbb{F}(\chi, \lambda) \cdot \mathbf{j}_\mathbb{F}(\lambda\chi^2, \overline{\chi}) = \chi(16) \cdot \mathbf{j}_\mathbb{F}(\chi, \chi) \cdot \mathbf{j}_\mathbb{F}(\lambda\chi^2, \overline{\chi}). \qquad \square$$

From (Jac 4) and the above Proposition, one deduces the following:

Corollary 3.2 – *Let $\chi : \mathbb{F}^\times \to \overline{\mathbb{Q}}^\times$ be a multiplicative character. For any finite extension $\mathbb{F}'/\mathbb{F}$, one has*

$$B(\mathbb{F}', \chi \circ \mathbf{N}_{\mathbb{F}'/\mathbb{F}}) = B(\mathbb{F}, \chi)^{[\mathbb{F}' : \mathbb{F}]},$$

where $\mathbf{N}_{\mathbb{F}'/\mathbb{F}} : \mathbb{F}' \to \mathbb{F}$ denotes the relative norm of the extension.

We end this subsection by showing that:

Proposition 3.3 – *Let $\mathbb{F}$ be a finite field of odd characteristic. Then one has*

$$\sum_{x \in \mathbb{F}} \lambda\big(x(x^2 - 4)\big) = -\sum_{\substack{\chi^4 = \mathbb{1} \\ \chi^2 \neq \mathbb{1}}} \mathbf{j}_\mathbb{F}(\chi, \chi), \tag{3.3}$$

where the sum on the right-hand side is over all multiplicative characters of exact order 4 (hence it vanishes if $|\mathbb{F}| \not\equiv 1 \bmod 4$).

Proof: We denote by $S_\mathbb{F}$ the sum on the left-hand side of (3.3). We note that $\lambda(-1) = (-1)^{(|\mathbb{F}|-1)/2}$, so that $\lambda(-1) = 1$ if and only if $|\mathbb{F}| \equiv 1 \bmod 4$. This happens if and only if there exist characters $\chi : \mathbb{F}^\times \to \overline{\mathbb{Q}}^\times$ of exact order 4. Reindexing the sum $S_\mathbb{F}$ by setting $x' = -x$, we obtain that $S_\mathbb{F} = \lambda(-1) \cdot S_\mathbb{F}$. Hence, $S_\mathbb{F} = 0$ when $\lambda(-1) = -1$; and (3.3) is proved in this case, since the right-hand side is then an empty sum.

We now assume that $|\mathbb{F}| \equiv 1 \bmod 4$ and denote by $\theta : \mathbb{F}^\times \to \overline{\mathbb{Q}}^\times$ one of the two characters of order exactly 4 (the other such one being $\lambda\theta$). Since $\lambda = \theta^2$, the sum $S_\mathbb{F}$ can be rewritten as

$$S_\mathbb{F} = \sum_{x \in \mathbb{F}} \lambda(x)\lambda(x^2 - 4) = \sum_{x \in \mathbb{F}} \theta(x^2)\lambda(x^2 - 4) = \sum_{z \in \mathbb{F}} (1 + \lambda(z)) \cdot \theta(z)\lambda(z - 4) = \sum_{\chi \in \{\theta, \lambda\theta\}} \left(\sum_{z \in \mathbb{F}} \chi(z)\lambda(z - 4) \right).$$

Indeed, for any $z \in \mathbb{F}$, the number of $x \in \mathbb{F}$ such that $x^2 = z$ equals $1 + \lambda(z)$. For a non-trivial character $\chi : \mathbb{F}^\times \to \overline{\mathbb{Q}}^\times$, setting $(u_1, u_2) = (z/4, 1 - z/4)$ allows to identify the following sum with a Jacobi sum:

$$\sum_{z \in \mathbb{F}} \chi(z)\lambda(z - 4) = \chi(4)\lambda(-4) \cdot \sum_{\substack{u_i \in \mathbb{F} \\ u_1 + u_2 = 1}} \chi(u_1)\lambda(u_2) = -\chi(4)\lambda(-4) \cdot \mathbf{j}_\mathbb{F}(\chi, \lambda).$$

Hence, using (Jac 2) and noting that $\lambda(-4) = 1$ and $\theta^2(4) = \lambda(4) = 1$, the above equality applied successively to $\chi = \theta$ and $\chi = \lambda\theta$ implies that

$$-S_\mathbb{F} = \theta(4)\lambda(-4) \cdot \mathbf{j}_\mathbb{F}(\theta, \lambda) + \theta(4)\lambda(4)\lambda(-4) \cdot \mathbf{j}_\mathbb{F}(\lambda\theta, \lambda) = \mathbf{j}_\mathbb{F}(\theta, \theta) + \mathbf{j}_\mathbb{F}(\lambda\theta, \lambda\theta). \qquad \square$$

3.3. Action of q on $\mathbb{Z}/2d\mathbb{Z}$. $-$ For any integer $D \geq 1$ coprime to q, there is a natural action of the subgroup $\langle q \rangle_d \subseteq (\mathbb{Z}/D\mathbb{Z})^\times$ generated by q on $\mathbb{Z}/D\mathbb{Z}$ by multiplication[3]. For any subset $Z \subseteq \mathbb{Z}/D\mathbb{Z}$ which is stable under this action, we denote by $\mathcal{O}_q(Z)$ the set of orbits of Z. Given such a $Z \subseteq \mathbb{Z}/D\mathbb{Z}$ and an orbit $\mathbf{m} \in \mathcal{O}_q(Z)$, we will often need to choose a representative $m \in Z$ of this orbit: we make the convention that orbits in $\mathcal{O}_q(Z)$ are always denoted by a bold letter ($\mathbf{m}$, $\mathbf{n}$, ...) and that the corresponding normal letter (m, n, ...) designates any choice of representative in Z of this orbit.

For any integer $n \geq 1$ coprime to q, we denote the (multiplicative) order of q modulo n by $o_q(n)$ *i.e.*, the order of the subgroup $\langle q \rangle_n \subseteq (\mathbb{Z}/n\mathbb{Z})^\times$ generated by q. For any orbit $\mathbf{n} \in \mathcal{O}_q(Z)$, its length $|\mathbf{n}| = \left| \{n, qn, q^2n, \dots\} \right|$ is equal to

$$|\mathbf{n}| = \min\left\{ \nu \in \mathbb{Z}_{\geq 1} \mid q^\nu n \equiv n \bmod D \right\},$$

which, in turn, equals $|\mathbf{n}| = o_q(D/\gcd(D, n))$ for any $n \in \mathbf{n}$. For any power q^v of q, the definition of the order of q modulo $D/\gcd(D, n)$ implies that $q^v n \equiv n \bmod D$ if and only if $|\mathbf{n}|$ divides v, *i.e.*, if and only if $\mathbb{F}_{q^v}$ is an extension of $\mathbb{F}_{q^{|\mathbf{n}|}}$.

For any integer $d \geq 2$ which is coprime to q, we will be particularly interested in the subset

$$Z_{2d} := \begin{cases} \mathbb{Z}/2d\mathbb{Z} \smallsetminus \{0, d/2, d, 3d/2\} & \text{if } d \text{ is even,} \\ \mathbb{Z}/2d\mathbb{Z} \smallsetminus \{0, d\} & \text{if } d \text{ is odd} \end{cases}$$

of $\mathbb{Z}/2d\mathbb{Z}$ (which is stable under multiplication by q because $\gcd(2d, q) = 1$) and in the corresponding set of orbits $\mathcal{O}_q(Z_{2d})$.

Remark 3.4 In the special case when $2d$ divides $q - 1$ (*i.e.* when $q \equiv 1 \bmod 2d$), the action of q on Z_{2d} is trivial and the natural map $m \mapsto \mathbf{m}$ is a bijection between Z_{2d} and $\mathcal{O}_q(Z_{2d})$.

3.4. Characters of order dividing $2d$. $-$ Let us fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ and a prime ideal $\mathfrak{P}$ above p in the ring of algebraic integers $\overline{\mathbb{Z}} \subseteq \overline{\mathbb{Q}}$. The residue field $\overline{\mathbb{Z}}/\mathfrak{P}$ can be viewed as an algebraic closure $\overline{\mathbb{F}_p}$ of $\mathbb{F}_p$. Moreover, the reduction map $\overline{\mathbb{Z}} \to \overline{\mathbb{Z}}/\mathfrak{P}$ induces an isomorphism between the group $\mu_{\infty, p'} \subseteq \overline{\mathbb{Z}}^\times$ 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, and we denote by the same letter the restriction of $\mathbf{t}$ to any finite field $\mathbb{F}_q$ (which we view as as a subfield of $\overline{\mathbb{Z}}/\mathfrak{P}$). Note that any non-trivial multiplicative character on any finite extension of $\mathbb{F}_q$ is then a power of $\mathbf{t}$.

Suppose we are given a prime-to-p integer $d \geq 1$; for any $n \in \mathbb{Z}/2d\mathbb{Z} \smallsetminus \{0\}$, let $\mathbf{n} \in \mathcal{O}_q(\mathbb{Z}/2d\mathbb{Z})$ be the corresponding orbit and define a multiplicative character $\mathbf{t}_n : \mathbb{F}_{q^{|\mathbf{n}|}}^\times \to \overline{\mathbb{Q}}^\times$ by

$$\forall x \in \mathbb{F}_{q^{|\mathbf{n}|}}^\times, \quad \mathbf{t}_n(x) = \mathbf{t}(x)^{(q^{|\mathbf{n}|}-1)n/2d} \quad \text{and put } \mathbf{t}_n(0) := 0.$$

---

[3] We will simply say that 'q acts on $\mathbb{Z}/D\mathbb{Z}$ by multiplication'.

Further, if $s \geq 1$, we 'lift' $\mathbf{t}_n$ to a character $\mathbf{t}_n^{(s)} : \mathbb{F}_{q^s|\mathbf{n}|}^\times \to \overline{\mathbb{Q}}^\times$ via the relative norm $\mathbb{F}_{q^s|\mathbf{n}|} \to \mathbb{F}_{q|\mathbf{n}|}$, *i.e.*, we let $\mathbf{t}_n^{(s)} := \mathbf{t}_n \circ \mathbf{N}_{\mathbb{F}_{q^s|\mathbf{n}|}/\mathbb{F}_{q|\mathbf{n}|}}$.

The order of $\mathbf{t}_n$ obviously divides $2d$ and a more careful computation shows that $\mathbf{t}_n$ has exact order $2d/\gcd(2d, n)$. Note that the order of $\mathbf{t}_n$ does not divide 4 when $n \in Z_{2d} \subseteq \mathbb{Z}/2d\mathbb{Z}$. Since the norm is surjective, $\mathbf{t}_n^{(s)}$ has the same order as $\mathbf{t}_n$ for all $s \geq 1$.

The interest of the characters $\mathbf{t}_n^{(s)}$ (with $n \in \mathbb{Z}/2d\mathbb{Z} \smallsetminus \{0\}$, $s \geq 1$) lies in the following result:

Lemma 3.5 $-$ *Let $d \geq 2$ be coprime to q, and $\mathbb{F}$ be a finite extension of $\mathbb{F}_q$. Denote by $X_{2d}(\mathbb{F})$ the set of non-trivial characters χ on $\mathbb{F}^\times$ such that $\chi^{2d} = \mathbb{1}$ and $\chi^4 \neq \mathbb{1}$. Then*

$$X_{2d}(\mathbb{F}) = \left\{ \mathbf{t}_n^{(s)}, \ n \in Z_{2d} \text{ and } s \geq 1 \text{ such that } s \cdot |\mathbf{n}| = [\mathbb{F} : \mathbb{F}_q] \right\}.$$

In particular, as n runs through Z_{2d} and s runs through the positive integers, $\mathbf{t}_n^{(s)}$ runs through all characters on all finite extensions of $\mathbb{F}_q$ whose order divides $2d$ and whose 4-th power is non-trivial.

Proof: The detailed proof of a very similar result can be found in [Gri18b, §2.2]. Let us write $\mathbb{F} = \mathbb{F}_{q^n}$, denote by C the (cyclic) group C of multiplicative characters on $\mathbb{F}_{q^n}^\times$ whose order divides $2d$ and $e_n := \gcd(2d, q^n - 1) = |C|$. The main point is to note that the character $\chi := \mathbf{t}^{(q^n-1)/e_n}$ on $\mathbb{F}_{q^n}^\times$ has exact order e_n. Therefore χ generates C: any element of C is of the form χ^k for $k \in \{0, \ldots, 2d-1\}$. To obtain the enumeration of $X_{2d}(\mathbb{F}_{q^n}) \subseteq C$, it only remains to exclude the characters in C whose order divide 4: these correspond to χ^k with $k \in \{0, d/2, d, 3d/2\}$. $\qquad\square$

Remark 3.6 In the special case when $2d$ divides $q-1$ (*i.e.*, when $q \equiv 1 \bmod 2d$), all the characters $\mathbf{t}_m$ (with $m \in Z_d$) are characters on $\mathbb{F}_q^\times$ because $|\mathbf{m}| = 1$ (see Remark 3.4). Moreover we remark that $\mathbf{t}_m = (\mathbf{t}_1)^m$ for all $m \in Z_d$, and that $\mathbf{t}_1$ has exact order $2d$. Hence, by the Lemma above, as m runs through Z_{2d}, the characters $(\mathbf{t}_1)^m$ enumerate all possible non-trivial characters χ on $\mathbb{F}_q^\times$ such that $\chi^{2d} = \mathbb{1}$ and $\chi^4 \neq \mathbb{1}$.

3.5. The sums $\beta(n)$.

$-$ We can finally introduce the following notation:

Definition 3.7 Let $d \geq 1$ be coprime to q. For any $n \in Z_{2d}$, we let $Q := q^{|\mathbf{n}|}$ and set

$$\beta(n) := \mathbf{t}_n(16) \cdot \mathbf{j}_{\mathbb{F}_Q}(\mathbf{t}_n, \mathbf{t}_n) \cdot \mathbf{j}_{\mathbb{F}_Q}(\lambda_{\mathbb{F}_Q} \cdot \mathbf{t}_n^2, \mathbf{t}_n^{-1}). \tag{3.4}$$

For an orbit $\mathbf{n} \in \mathcal{O}_q(Z_{2d})$, we let $\beta(\mathbf{n}) := \beta(n)$ for any choice of $n \in \mathbf{n}$.

We compile a few results about these numbers $\beta(n)$:

Proposition 3.8 $-$ *Let $d \geq 1$ be coprime to q. The following statements hold:*

(i) *For any $\mathbf{n} \in \mathcal{O}_q(Z_{2d})$, $\beta(\mathbf{n})$ is well-defined (i.e., $\beta(q \cdot n) = \beta(n)$ for all $n \in Z_{2d}$),*

(ii) *In the notation of §3.2, $\beta(n) = B(\mathbb{F}_{q|\mathbf{n}|}, \mathbf{t}_n)$ for all $n \in Z_{2d}$,*

(iii) *For all $n \in Z_{2d}$ and for any $s \geq 1$, we have $B\left(\mathbb{F}_{q^s \cdot |\mathbf{n}|}, \mathbf{t}_n^{(s)}\right) = \beta(n)^s$,*

(iv) *One has $|\beta(n)| = q^{|\mathbf{n}|}$ for all $n \in Z_{2d}$,*

Proof: Let $n \in Z_d$ and set $Q := q^{|\mathbf{n}|}$. The map $x \mapsto x^q$ is a bijection of $\mathbb{F}_Q$ and $\lambda_{\mathbb{F}_Q} = \lambda_{\mathbb{F}_Q}^q$, so that

$$\mathbf{j}_{\mathbb{F}_Q}(\mathbf{t}_n, \mathbf{t}_n) = \mathbf{j}_{\mathbb{F}_Q}(\mathbf{t}_{q \cdot n}, \mathbf{t}_{q \cdot n}) \quad \text{and} \quad \mathbf{j}_{\mathbb{F}_Q}(\lambda_{\mathbb{F}_Q} \mathbf{t}_n^2, \mathbf{t}_n^{-1}) = \mathbf{j}_{\mathbb{F}_Q}(\lambda_{\mathbb{F}_Q} \mathbf{t}_{q \cdot n}^2, \mathbf{t}_{q \cdot n}^{-1}).$$

Moreover, $\mathbf{t}_n(16) = \mathbf{t}_n(16)^q = \mathbf{t}_{q \cdot n}(16)$ since $16 \in \mathbb{F}_q^\times$, hence $\beta(n) = \beta(q \cdot n)$; a repeated application of this identity implies that the value of $\beta(n)$ is constant along the orbit $\mathbf{n}$, which shows that (i) holds.

Item (ii) is a direct consequence of Proposition 3.1 upon remarking that the order of $\mathbf{t}_n$ does not divide 4. Again by construction of Z_{2d}, none of $\mathbf{t}_n$, $\mathbf{t}_n^2$ and $\mathbf{t}_n^4$ is trivial, so that $|\beta(n)| = q^{|\mathbf{n}|}$ by combining Proposition 3.1 and (Jac 5); thus (iv) is proved.

Finally, we deduce from Corollary 3.2 that $B(\mathbb{F}_{Q^s}, \mathbf{t}_n^{(s)}) = B(\mathbb{F}_Q, \mathbf{t}_n)^s$ for all $s \geq 1$; item (ii) above then yields (iii). $\qquad\square$

4. The L-function

In this section, we give an explicit expression for the L-function of E_d/K. Before we do so, let us first recall the definition of $L(E_d/K, T)$.

Let $d \geq 1$ be an integer. For any place v of K, let q_v be the cardinality of the residue field $\mathbb{F}_v$ of K at v. For such a v, we denote by $\widetilde{(E_d)}_v$ the plane cubic curve over $\mathbb{F}_v$ obtained by reducing modulo v a minimal v-integral model of E_d, and we put $a_v := |\mathbb{F}_v| + 1 - |\widetilde{(E_d)}_v(\mathbb{F}_v)|$. If v is a place of bad reduction for E_d, notice that a_v is $0, +1$ or -1 depending on whether the reduction of E_d at v is additive, split multiplicative or nonsplit multiplicative, respectively. Recall that the L-function of E_d/K is the power series given by

$$L(E_d/K, T) = \prod_{v \text{ good}} \left(1 - a_v \cdot T^{\deg v} + q_v \cdot T^{2\deg v}\right)^{-1} \cdot \prod_{v \text{ bad}} \left(1 - a_v \cdot T^{\deg v}\right)^{-1}, \tag{4.1}$$

where the products are over places of K of good (resp. bad) reduction for E_d. The reader may consult [Ulm11, Lect. 1, §9] or [Gro11, Lect. 2, §2] for more details.

The curve E_d/K being non-isotrivial, a theorem of Grothendieck shows that $L(E_d/K, T)$ is actually a polynomial which has integral coefficients (see [Gro11, App. D]). In particular, it makes sense to consider the multiplicity $\mathrm{ord}_{T=q^{-1}} L(E_d/K, T) \in \mathbb{Z}_{\geq 0}$ of q^{-1} as a zero of this polynomial (see Corollary 4.3).

4.1. Explicit expression for $L(E_d/K, T)$. $-$ Our first main result is the following:

Theorem 4.1 $-$ *For any integer $d \geq 1$ coprime to q, consider the elliptic curve E_d/K defined by* (1.1). *Set*

$$Z_{2d} := \begin{cases} \mathbb{Z}/2d\mathbb{Z} \smallsetminus \{0, d/2, d, 3d/2\} & \text{if } d \text{ is even,} \\ \mathbb{Z}/2d\mathbb{Z} \smallsetminus \{0, d\} & \text{if } d \text{ is odd.} \end{cases}$$

The L-function of E_d admits the expression

$$L(E_d/K, T) = (1 - qT) \cdot \prod_{\mathbf{n} \in \mathcal{O}_q(Z_{2d})} \left(1 - \beta(\mathbf{n}) \cdot T^{|\mathbf{n}|}\right), \tag{4.2}$$

where $\beta(\mathbf{n})$ has been defined in (3.4).

Remark 4.2 (a) One can actually deduce from Theorem 4.1 an expression of $L(E_d/K, T)$ for *all* $d \geq 1$, as follows. For any integer $d \geq 1$, write $d = p^e d'$ where $e \geq 0$ and $d' \geq 1$ is coprime to p. As was pointed out earlier (Remark 1.2) the elliptic curves $E_{d'}$ and E_d, being isogenous, share the same L-function. Therefore, $L(E_d/K, T) = L(E_{d'}/K, T)$ can also be expressed with the help of Theorem 4.1.

(b) In the special case when $2d \mid q - 1$, one can choose a character $\chi : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}^\times$ of exact order $2d$. By Remarks 3.4 and 3.6, the expression (4.2) then simplifies to

$$L(E_d/K, T) = (1 - qT) \cdot \prod_{\substack{1 \leq n \leq 2d-1 \\ n \neq d/2, 3d/2}} (1 - B(\mathbb{F}_q, \chi^n) \cdot T).$$

This special case of Theorem 4.1 was announced as Theorem B in the introduction.

Before we start the proof of Theorem 4.1, we remark that it directly leads to the following 'combinatorial' expression of the analytic rank of E_d/K:

Corollary 4.3 $-$ *For any integer $d \geq 2$ coprime to q,*

$$\mathrm{ord}_{T=q^{-1}} L(E_d/K, T) = 1 + \left|\left\{\mathbf{n} \in \mathcal{O}_q(Z_{2d}) \ : \ \beta(\mathbf{n}) = q^{|\mathbf{n}|}\right\}\right| \tag{4.3}$$

Proof: Let us take a closer look at the factorisation (4.2) of $L(E_d/K, T)$. The factor $1 - qT$ clearly contributes 1 to the order of vanishing of $L(E_d/K, T)$ at $T = q^{-1}$. For an orbit $\mathbf{n} \in \mathcal{O}_q(Z_{2d})$, the factor $1 - \beta(\mathbf{n}) \cdot T^{|\mathbf{n}|}$ vanishes at order 1 at $T = q^{-1}$ if and only if $\beta(\mathbf{n}) = q^{|\mathbf{n}|}$, and does not vanish otherwise. Summing up these contributions yields (4.3). $\qquad\square$

4.2. Proof of Theorem 4.1. − In order to prove Theorem 4.1, it will be useful to have a more explicit definition of $L(E_d/K,T)$ at hand. For an integer $m \geq 1$ and a point $\tau \in \mathbb{P}^1(\mathbb{F}_{q^m}) \smallsetminus \{\infty\}$, let v_τ be the place of K corresponding to τ. One may choose a polynomial $f_{d,\tau} \in \mathbb{F}_q[t,x]$, monic of degree 3 in x, such that $y^2 = f_{d,\tau}(t,x)$ provides a minimal integral Weierstrass model of E_d at v_τ. One can then form the character sum

$$A_d(\tau, q^m) := - \sum_{x \in \mathbb{F}_{q^m}} \lambda_{\mathbb{F}_{q^m}}(f_{d,\tau}(\tau, x)),$$

where $\lambda_{\mathbb{F}_{q^m}}$ is the unique character of order 2 on $\mathbb{F}_{q^m}^\times$. By a classical computation, one has

$$q^m + 1 - |\widetilde{(E_d)}_\tau(\mathbb{F}_{q^m})| = q^m - \sum_{x \in \mathbb{F}_{q^m}} \left(1 + \lambda_{\mathbb{F}_{q^m}}(f_\tau(x))\right) = - \sum_{x \in \mathbb{F}_{q^m}} \lambda_{\mathbb{F}_{q^m}}(f_\tau(x)) = A_d(\tau, q^m). \qquad (4.4)$$

Since E_d has split multiplicative reduction at $v = \infty$, we have $q^m + 1 - |\widetilde{(E_d)}_\infty(\mathbb{F}_{q^m})| = q^m + 1 - |\mathbb{F}_{q^m}| = 1$ for all $m \geq 1$. Hence we are led to put $A_d(\infty, q^m) := 1$ for all $m \geq 1$.

Lemma 4.4 − *The L-function of E_d/K is given by*

$$\log L(E_d/K, T) = \sum_{m=1}^\infty \left(\sum_{\tau \in \mathbb{P}^1(\mathbb{F}_{q^m})} A_d(\tau, q^m) \right) \cdot \frac{T^m}{m}. \qquad (4.5)$$

Proof: We refer the reader to [BH12, §2.2] for a detailed proof. The result follows from expanding $\log L(E_d/K, T)$ as a power series in T (from its definition (4.1)), rearranging terms and using (4.4). □

Proof (of Theorem 4.1): Let $d \geq 1$ be coprime to q, and E_d/K be the elliptic curve defined by (1.1). We deduce the identity (4.2) from the expression for $L(E_d/K, T)$ displayed in Lemma 4.4 by making the double sum on the right-hand side of (4.5) more explicit. From the preceding discussion, we already know that, for any integer $m \geq 1$, we have

$$\sum_{\tau \in \mathbb{P}^1(\mathbb{F}_{q^m})} A_d(\tau, q^m) = A_d(\infty, q^m) - \sum_{\tau \in \mathbb{F}_{q^m}} \sum_{x \in \mathbb{F}_{q^m}} \lambda_{\mathbb{F}_{q^m}}(f_{d,\tau}(x)),$$

where $A_d(\infty, q^m) = 1$. In fact, we can also give a straightforward expression of $A_d(0, q^m)$: if d is odd, then E_d has additive reduction at 0 so that $A_d(0, q^n) = 0$; whereas when d is even E_d has good reduction, and $y^2 = x(x^2 - 4)$ is a model of the reduction of E_d modulo $v = 0$. Hence we have

$$A_d(0, q^m) = \begin{cases} - \sum_{x \in \mathbb{F}_{q^m}} \lambda_{\mathbb{F}_{q^m}}(x(x^2 - 4)) & \text{if } d \text{ is even,} \\ 0 & \text{if } d \text{ is odd.} \end{cases} \qquad (4.6)$$

Now, for any $\tau \in \mathbb{P}^1(\mathbb{F}_{q^m}) \smallsetminus \{0, \infty\} = \mathbb{F}_{q^m}^\times$, we have seen in Remark 1.5 that a minimal integral model for the curve E_d/K at v_τ is $y^2 = x^3 + t^{2d}x^2 - 4t^{2d}x$. Thus, we have

$$\sum_{\tau \in \mathbb{F}_{q^m}^\times} A_d(\tau, q^m) = - \sum_{\tau \in \mathbb{F}_{q^m}^\times} \sum_{x \in \mathbb{F}_{q^m}} \lambda_{\mathbb{F}_{q^m}}(x^3 + \tau^{2d} \cdot x^2 - 4\tau^{2d} \cdot x).$$

For any $z \in \mathbb{F}_{q^m}^\times$, recall from [Coh07, Lemma 2.5.21] that $\left|\{\tau \in \mathbb{F}_{q^m}^\times : \tau^{2d} = z\}\right|$ equals $\sum_{\chi^{2d}=1} \chi(z)$, where the sum is over the multiplicative characters $\chi : \mathbb{F}_{q^m}^\times \to \overline{\mathbb{Q}}^\times$ whose order divides $2d$. Using this identity, one can reindex the outer sum in the last displayed equality: after changing the order of summation, we obtain that

$$\sum_{\tau \in \mathbb{F}_{q^m}^\times} A_d(\tau, q^m) = - \sum_{\chi^{2d}=1} \left(\sum_{z \in \mathbb{F}_{q^m}^\times} \sum_{x \in \mathbb{F}_{q^m}} \chi(z) \cdot \lambda_{\mathbb{F}_{q^m}}(x^3 + z \cdot x^2 - 4z \cdot x) \right) = - \sum_{\chi^{2d}=1} B(\mathbb{F}_{q^m}, \chi),$$

where $B(\mathbb{F}_{q^m}, \chi)$ is the character sum studied in §3.2. To avoid multiple subscripts, for any character χ on $\mathbb{F}_{q^m}^\times$ we will denote in the present proof the sum $B(\mathbb{F}_{q^m}, \chi)$ by $B(q^m, \chi)$.

The last displayed identity and the previous remarks about $A_d(\infty, q^m)$, $A_d(0, q^m)$ lead to:

$$\sum_{\tau \in \mathbb{P}^1(\mathbb{F}_{q^m})} A_d(\tau, q^m) = A_d(\infty, q^m) + A_d(0, q^m) - \sum_{\chi^{2d}=1} B(q^m, \chi)$$

$$= 1 + A_d(0, q^m) - \sum_{\substack{\chi^{2d}=1 \\ \chi^4=1}} B(q^m, \chi) - \sum_{\substack{\chi^{2d}=1 \\ \chi^4 \neq 1}} B(q^m, \chi).$$

Now, by the first three cases of Proposition 3.1, we can write

$$\sum_{\substack{\chi^{2d}=\mathbb{1} \\ \chi^4=\mathbb{1}}} B(q^m, \chi) = |\mathbb{F}_{q^m}| + 1 + \sum_{\substack{\chi^{2d}=\mathbb{1} \\ \chi^2 \neq \mathbb{1}, \chi^4=\mathbb{1}}} \mathbf{j}_{\mathbb{F}_{q^m}}(\chi, \chi).$$

We note that the second sum is empty if d is odd. From (4.6) and Proposition 3.3, we then obtain that

$$1 + A_d(0, q^m) - \sum_{\substack{\chi^{2d}=\mathbb{1} \\ \chi^4=\mathbb{1}}} B(q^m, \chi) = \begin{cases} 1 + \sum_\theta \mathbf{j}_{\mathbb{F}_{q^m}}(\theta, \theta) - \left(q^m + 1 + \sum_\theta \mathbf{j}_{\mathbb{F}_{q^m}}(\theta, \theta)\right) & \text{if } d \text{ is even,} \\ 1 + 0 - (q^m + 1 - 0) & \text{if } d \text{ is odd.} \end{cases}$$

$$= -q^m \text{ in both cases,}$$

where the sums on the right-hand side are over characters θ on $\mathbb{F}_{q^m}^\times$ of exact order 4.

Regrouping our computations thus far, we have proved that:

$$-\sum_{\tau \in \mathbb{P}^1(\mathbb{F}_{q^m})} A_d(\tau, q^m) = q^m + \sum_{\chi \in X_{2d}(\mathbb{F}_{q^m})} B(q^m, \chi),$$

where the sum on the right-hand side is over the set $X_{2d}(q^m)$ consisting of characters χ of $\mathbb{F}_{q^m}^\times$ such that χ^{2d} is trivial and χ^4 is non-trivial. Plugging this equality in (4.5), we obtain that

$$-\log L(E_d/K, T) = \sum_{m \geq 1} \frac{(qT)^m}{m} + \sum_{m \geq 1} \left(\sum_{\chi \in X_{2d}(\mathbb{F}_{q^m})} B(q^m, \chi) \right) \cdot \frac{T^m}{m}.$$

$$= -\log(1 - qT) + \sum_{m \geq 1} \left(\sum_{\chi \in X_{2d}(\mathbb{F}_{q^m})} B(q^m, \chi) \right) \cdot \frac{T^m}{m}.$$

The first term on the right-hand side clearly leads to the factor $1 - qT$ on the right-hand side of (4.2). There remains to handle the second sum; using Lemma 3.5, we can 'reindex' the double sum to get

$$\sum_{m \geq 1} \left(\sum_{\chi \in X_{2d}(\mathbb{F}_{q^m})} B(q^m, \chi) \right) \cdot \frac{T^m}{m} = \sum_{n \in Z_{2d}} \sum_{s \geq 1} B\left(q^{s \cdot |\mathbf{n}|}, \mathbf{t}_n^{(s)}\right) \cdot \frac{T^{s \cdot |\mathbf{n}|}}{s \cdot |\mathbf{n}|}.$$

For any $n \in Z_{2d}$ and any $s \geq 1$, Proposition 3.8(iii) yields that $B\left(q^{s \cdot |\mathbf{n}|}, \mathbf{t}_n^{(s)}\right) = \beta(n)^s$: hence, we have

$$-\log \frac{L(E_d/K, T)}{1 - qT} = \sum_{n \in Z_{2d}} \sum_{s \geq 1} \beta(n)^s \cdot \frac{T^{s \cdot |\mathbf{n}|}}{s \cdot |\mathbf{n}|} = \sum_{n \in Z_{2d}} \frac{1}{|\mathbf{n}|} \sum_{s \geq 1} \frac{\left(\beta(n) \cdot T^{|\mathbf{n}|}\right)^s}{s}$$

$$= -\sum_{n \in Z_{2d}} \frac{\log\left(1 - \beta(n) \cdot T^{|\mathbf{n}|}\right)}{|\mathbf{n}|} = -\sum_{\mathbf{n} \in \mathcal{O}_q(Z_{2d})} \sum_{n \in |\mathbf{n}|} \frac{\log\left(1 - \beta(n) \cdot T^{|\mathbf{n}|}\right)}{|\mathbf{n}|}$$

$$= -\sum_{\mathbf{n} \in \mathcal{O}_q(Z_{2d})} \log\left(1 - \beta(\mathbf{n}) \cdot T^{|\mathbf{n}|}\right).$$

From which the desired expression for $L(E_d/K, T)$ follows immediately. □

5. Berger's construction and the BSD conjecture

Let $k = \mathbb{F}_q$ be a finite field of odd characteristic p. Consider the two rational functions $f, g : \mathbb{P}^1_{/k} \to \mathbb{P}^1_{/k}$ given by:

$$f(u) = \frac{2u - 1}{2u(u - 1)}, \qquad g(v) = v(v - 1).$$

For any integer $d \geq 1$ coprime to q, let C_d/k (resp. D_d/k) be a projective smooth model of the curve given affinely by $z^d = f(u)$ (resp. $w^d = g(v)$). In the notation of [Ber08], the pair (f, g) is of type $[1, 1][1, 1][1, 1][2]$ and we have chosen the value '$a = 1/2$' for the parameter in f; see example (6) in §4.3 and example (2) in §4.4 of [Ber08]. Let us summarise the main results of [Ber08] in this case (see also [Ulm13] for a more detailed account).

By a direct computation, Berger [Ber08, §3] shows that the smooth projective curve X_d over $K = k(t)$ which is a model of the curve given in affine coordinates by

$$f(u) = t^d \cdot g(v) \tag{5.1}$$

has genus 1. Clearing denominators, one obtains that X_d/K is given by

$$\left(u - \tfrac{1}{2}\right) = t^d \cdot v(v-1)u(u-1) \tag{5.2}$$

The curve X_d obviously admits a K-rational point – namely, $(u, v) = (1/2, 0)$ – so that it is actually an elliptic curve over K.

Let us first find a Weierstrass model for this elliptic curve. Changing coordinates in (5.2) by letting

$$(x, y) = \left(2t^d(u^{-1} - 1), \; 2t^d(u^{-1} - 1)(2v - 1)\right) := H(u, v),$$

we find that X_d/K admits the Weierstrass model

$$X_d: \qquad y^2 = x \cdot \left(x^2 + t^{2d} \cdot x - 4t^{2d}\right).$$

Moreover, the 'change of coordinates' map $H : X_d \to E_d$ is birational, with birational inverse given by $(x, y) \mapsto (u, v) = \left(2t^d \cdot (x + 2t^d)^{-1}, \; (x + y) \cdot (2x)^{-1}\right)$. Therefore the elliptic curves X_d and E_d are actually K-isomorphic.

We now describe in more details the geometry of the situation. For any $d \geq 1$ coprime to q, one can view (5.1) as the equation over k of an affine surface in $\mathbb{A}^3_{/k}$ (with coordinates t, u, v); we then let S_d denote the projective closure[4] in $\mathbb{P}^3_{/k}$ of that affine surface. There is a dominant rational map $\rho : C_d \times D_d \dashrightarrow S_d$, given in affine coordinates by $\rho : \left((u, z), (v, w)\right) \mapsto (t = z/w, u, v)$. The surface S_d also admits a natural morphism $\pi_0 : S_d \to \mathbb{P}^1$ extending the projection $(t, u, v) \mapsto t$. The generic fiber of $\pi_0 : S_d \to \mathbb{P}^1$ is clearly the elliptic curve X_d/K, a.k.a. E_d/K by the previous paragraph.

Besides, the group μ_d of d-th roots of unity in $\overline{k}$ acts on $C_d \times D_d$, via $\zeta \cdot (u, z, v, w) := (u, \zeta z, v, \zeta w)$. We denote the quotient surface by $(C_d \times D_d)/\mu_d$ and by $\sigma : C_d \times D_d \to (C_d \times D_d)/\mu_d$ the quotient morphism[5]. Given its definition, it is clear that the map ρ above factors through σ. Since both ρ and σ have degree d, the induced rational map $\tilde{\rho} : (C_d \times D_d)/\mu_d \dashrightarrow S_d$ is birational. By blowing up the singular points of $(C_d \times D_d)/\mu_d$, one can resolve it into a regular surface (in a minimal way). We denote by $\mathcal{E}_d/k$ that surface: by construction, the successive blow-ups provide a birational map $b : \mathcal{E}_d \dashrightarrow (C_d \times D_d)/\mu_d$. Composing this map with $\pi_0 \circ \tilde{\rho}$, one endows $\mathcal{E}_d$ with a morphism $\pi : \mathcal{E}_d \to \mathbb{P}^1$ which 'extends' $\pi_0 : S_d \to \mathbb{P}^1$. In particular, the generic fiber of π is the same as that of π_0, i.e., it is E_d/K. Hence, $\pi : \mathcal{E}_d \to \mathbb{P}^1$ is the minimal regular model of E_d/K. On the other hand, note that composing the birational inverse of b with σ yields a dominant rational map $w_d : C_d \times D_d \dashrightarrow \mathcal{E}_d$. Here is a diagram describing the situation:
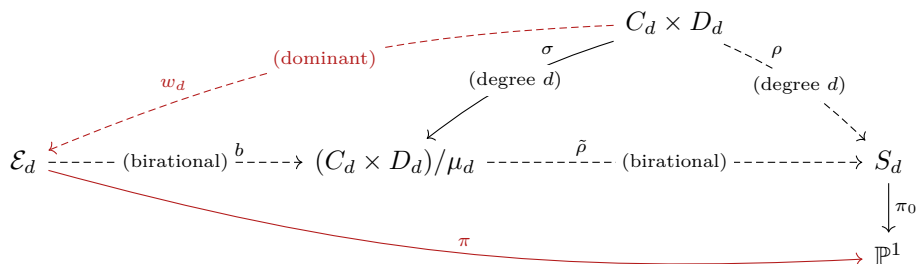
Summarising the discussion above, $\pi : \mathcal{E}_d \to \mathbb{P}^1$ is an elliptic surface (over k) with generic fiber E_d/K, and the surface $\mathcal{E}_d$ is dominated by a product of curves.

The most striking feature of Berger's construction is the following:

Theorem 5.1 (Berger) – *Let $d \geq 1$ be an integer. The elliptic curve E_d/K given by (1.1) satisfies the BSD conjecture. In particular, one has*

$$\operatorname{rank} E_d(K) = \operatorname{ord}_{T=q^{-1}} L(E_d/K, T).$$

---

[4]The surface S_d may be singular.
[5]The quotient surface $(C_d \times D_d)/\mu_d$ may be singular.

Proof: We only sketch the argument and refer the interested reader to [Ber08, §2] or [Ulm13] for a detailed proof. As before, we write $d = p^e d'$ where $e \geq 0$ and $d' \geq 1$ is coprime to q. The truth of the BSD conjecture is invariant under isogeny (see [Mil06, Chap. I, Thm. 7.3]): since E_d and $E_{d'}$ are isogenous (see Remark 1.2), it suffices to prove the Theorem in the case where $d = d'$ is coprime to q.

Hence we assume that $d \geq 1$ is coprime to q and we denote by $\pi : \mathcal{E}_d \to \mathbb{P}^1$ the minimal regular model of E_d/K. Proving the 'rank part' of the BSD conjecture for E_d/K is equivalent to proving the Tate conjecture for the surface $\mathcal{E}_d/\mathbb{F}_q$ (see [Tat66]). That conjecture is known to hold for surfaces which admit a dominant rational map from a product of curves (see [Tat94]). By the discussion above, $\mathcal{E}_d$ admits such a map $w_d : C_d \times D_d \dashrightarrow \mathcal{E}_d$, hence the Theorem. $\qquad\square$

More generally, the construction described by Berger in [Ber08, §2-§3] yields a number of examples of Kummer families of elliptic surfaces which are dominated by products of curves. For all these elliptic surfaces, the Tate conjecture holds. Therefore, for all the corresponding elliptic curves over K, the BSD conjecture is known to hold. Berger's construction thus provides a large range of examples where Ulmer's theorem about unbounded analytic ranks (see Theorem 1.6) can be unconditionally translated into an 'unbounded algebraic rank' result.

6. Supersingular integers and ranks

Let $\mathbb{F}_q$ be a finite field of characteristic $p \geq 3$ and $K = \mathbb{F}_q(t)$. For any integer $d \geq 1$, consider the elliptic curve E_d/K defined by (1.1). For the remainder of the article, we let

$$\varrho(d) := \mathrm{rank}\big(E_d(K)\big). \tag{6.1}$$

The goal of the next section will be to study the behaviour of the sequence $(\varrho(d))_{d \geq 1}$. In the present section, we first use the above results to give a combinatorial expression of $\varrho(d)$ for certain values of d.

6.1. Supersingular integers and Jacobi sums. $-$ Recall that an integer $D \geq 1$ is called *supersingular* if D divides $q^a + 1$ for some integer $a \geq 1$. We denote by $\mathcal{S}_q$ the set of supersingular integers. Since q is odd, note that $2d \in \mathcal{S}_q$ for any odd supersingular d.

Supersingular integers are of interest to us because of the following results:

Lemma 6.1 (Ulmer) $-$ *Let $D \geq 1$ be an* even *supersingular integer. Then the order of q modulo D is even. For any orbit $\mathbf{n} \in \mathcal{O}_q(\mathbb{Z}/D\mathbb{Z} \smallsetminus \{0, D/2\})$, its length $|\mathbf{n}|$ is even and D divides $n(q^{|\mathbf{n}|/2} + 1)$.*

Moreover, if $D = q^a + 1$ for some $a \geq 1$, the order of q modulo D equals $2a$.

For proofs of this lemma, we refer the reader to [Ulm02, Lemma 8.2] or to [Gri16, Lemmes 2.4.1 & 2.4.2] where a more detailed argument is given.

Lemma 6.2 (Shafarevich $-$ Tate / Ulmer) $-$ *Let $\mathbb{F}_{Q^2}/\mathbb{F}_Q$ be a quadratic extension of finite fields of odd characteristic. Let $\chi_1, \chi_2 : \mathbb{F}_{Q^2}^\times \to \overline{\mathbb{Q}}^\times$ be non-trivial characters on $\mathbb{F}_{Q^2}^\times$ such that $\chi_1\chi_2$ is non-trivial. If the restrictions of χ_1 and χ_2 to $\mathbb{F}_Q^\times$ are trivial, we have*

$$\mathbf{j}_{\mathbb{F}_{Q^2}}(\chi_1, \chi_2) = -Q = -\sqrt{Q^2}.$$

The proof can be found in [ST67, Lemma] or [Ulm02, Lemma 8.3]. In both references, the result is phrased in terms of Gauss sums, but is easily translated to the desired identity, see [Coh07, Prop. 2.5.14].

From the above lemmas, we deduce the following result about the sums $\beta(\mathbf{n})$ defined in §3.5:

Theorem 6.3 $-$ *Let $d \geq 1$ be a integer such that $2d \in \mathcal{S}_q$. Then, for all $\mathbf{n} \in \mathcal{O}_q(Z_{2d})$, we have $\beta(\mathbf{n}) = q^{|\mathbf{n}|}$.*

Proof: Let $n \in Z_{2d}$: by Lemma 6.1 applied to $D = 2d$), the length $|\mathbf{n}|$ of its orbit $\mathbf{n} \in \mathcal{O}_q(Z_{2d})$ is even. In particular, $Q := q^{|\mathbf{n}|/2}$ is an integral power of q, and the finite field extension $\mathbb{F}_{Q^2}/\mathbb{F}_Q$ is quadratic. By Lemma 6.1 again, $(Q+1)n/e$ is an integer and, by construction of $\mathbf{t}_n : \mathbb{F}_{Q^2}^\times \to \overline{\mathbb{Q}}^\times$, we deduce that

$$\forall x \in \mathbb{F}_Q^\times, \quad \mathbf{t}_n(x) = \mathbf{t}(x)^{(Q^2-1)n/e} = \mathbf{t}_n(x^{Q-1})^{(Q+1)n/e} = \mathbf{t}_n(1)^{(Q+1)n/e} = 1.$$

The character $\chi_1 = \mathbf{t}_n$ is thus a non-trivial character of $\mathbb{F}_{Q^2}^\times$ whose restriction to $\mathbb{F}_Q^\times$ is trivial; and the character $\chi_2 = \mathbf{t}_n^{-1}$ obviously has the same property. Consider now the character $\chi_3 = \lambda_{\mathbb{F}_{Q^2}} \mathbf{t}_n^2$: it cannot be trivial otherwise $\mathbf{t}_n$ would have order dividing 4, which does not happen for $n \in Z_{2d}$ (as was proved in §3.4). Nonetheless, χ_3 has trivial restriction to $\mathbb{F}_Q^\times$, being the product of two characters whose restrictions

to $\mathbb{F}_Q^\times$ are trivial, (the restriction of $\lambda_{\mathbb{F}_{Q^2}}$ is trivial because any element of $\mathbb{F}_Q^\times$ becomes a square in $\mathbb{F}_{Q^2}^\times$). Besides, note that $\boldsymbol{\chi}_1^2 = \mathbf{t}_n^2$ and $\boldsymbol{\chi}_2\boldsymbol{\chi}_3 = \lambda_{\mathbb{F}_{Q^2}}\mathbf{t}_n$ are non-trivial.

We can thus apply Lemma 6.2 and obtain that the Jacobi sums $\mathbf{j}_{\mathbb{F}_{Q^2}}(\boldsymbol{\chi}_1, \boldsymbol{\chi}_1)$ and $\mathbf{j}_{\mathbb{F}_{Q^2}}(\boldsymbol{\chi}_3, \boldsymbol{\chi}_2)$ both equal $-Q$. On the other hand, since the restriction of $\mathbf{t}_n$ to $\mathbb{F}_Q^\times$ is trivial and since $16 \in \mathbb{F}_Q^\times$, we have $\mathbf{t}_n(16) = 1$. Therefore, by its definition (see (3.4)) the sum $\boldsymbol{\beta}(n)$ satisfies:

$$\boldsymbol{\beta}(n) = \mathbf{t}_n(16) \cdot \mathbf{j}_{\mathbb{F}_{Q^2}}(\mathbf{t}_n, \mathbf{t}_n)\mathbf{j}_{\mathbb{F}_{Q^2}}(\lambda_{\mathbb{F}_{Q^2}} \cdot \mathbf{t}_n^2, \mathbf{t}_n^{-1}) = 1 \cdot \mathbf{j}_{\mathbb{F}_{Q^2}}(\boldsymbol{\chi}_1, \boldsymbol{\chi}_1)\mathbf{j}_{\mathbb{F}_{Q^2}}(\boldsymbol{\chi}_3, \boldsymbol{\chi}_2) = Q^2 = q^{|\mathbf{n}|},$$

as was to be shown. $\qquad\square$

Let us combine several of the results obtained so far. For any integer $d \geq 1$ coprime to q, the BSD conjecture (Theorem 5.1) ensures that $\varrho(d) = \mathrm{ord}_{T=q^{-1}} L(E_d/K, T)$. Besides, Corollary 4.3 yields an expression for $\mathrm{ord}_{T=q^{-1}} L(E_d/K, T)$ in terms of the number of $\mathbf{n} \in \mathcal{O}_q(Z_{2d})$ such that $\boldsymbol{\beta}(\mathbf{n}) = q^{|\mathbf{n}|}$. If we further assume that $d \geq 1$ is such that $2d \in \mathcal{S}_q$, the previous Theorem then implies:

Corollary 6.4 − *Let $d \geq 1$ be an integer such that $2d \in \mathcal{S}_q$. We have $\varrho(d) = 1 + |\mathcal{O}_q(Z_{2d})|$.*

Remark 6.5 Let $d \geq 1$ be an integer such that $2d \in \mathcal{S}_q$. Theorem 6.3 actually shows that the L-function of E_d/K admits the following expression:

$$L(E_d/K, T) = (1 - qT) \cdot \prod_{\mathbf{n} \in \mathcal{O}_q(Z_{2d})} \left(1 - (qT)^{|\mathbf{n}|}\right).$$

6.2. Structure of $\mathcal{O}_q(Z_{2d})$. − In order to make Corollary 6.4 more explicit, we describe in more detail the structure of $\mathcal{O}_q(Z_{2d})$. Let $d \geq 1$ be any integer coprime to q and define the set $Z_{2d} \subseteq \mathbb{Z}/2d\mathbb{Z}$ as in §3.3. For any divisor $e > 2$ of $2d$, consider the subset

$$Y_e := \{n \in Z_{2d} : \gcd(n, 2d) = 2d/e\} \subseteq Z_{2d};$$

since $\gcd(2d, q) = 1$, this subset is stable under the action of q. It is then clear that Z_{2d} is the disjoint union of the Y_e, and that the orbit set $\mathcal{O}_q(Z_{2d})$ is the disjoint union of the sets $\mathcal{O}_q(Y_e)$ as e runs through the divisors of $2d$ which are > 2.

We denote by ϕ Euler's totient function, and by $o_q(n)$ the multiplicative order of q modulo n, for any integer $n \geq 2$ coprime to q. Since $o_q(n)$ is the order of the subgroup generated by q in $(\mathbb{Z}/n\mathbb{Z})^\times$, we have $o_q(n) \mid \phi(n)$. In the notation of the previous paragraph, for any $e \mid 2d$ with $e > 2$, all orbits $\mathbf{n} \in \mathcal{O}_q(Y_e)$ have length $|\mathbf{n}| = o_q(e)$. Notice also that Y_e is in bijection with $(\mathbb{Z}/e\mathbb{Z})^\times$. These two observations show that

$$|\mathcal{O}_q(Y_e)| = |(\mathbb{Z}/e\mathbb{Z})^\times|/o_q(e) = \phi(e)/o_q(e).$$

This argument proves:

Lemma 6.6 − *Let $d \geq 1$ be an integer coprime to q. Then $|\mathcal{O}_q(Z_{2d})| = \displaystyle\sum_{\substack{e|2d \\ e>2}} \frac{\phi(e)}{o_q(e)}$.*

Following the notation of [PS10], for any integer D coprime to q, we now let

$$I_q(D) := \sum_{\substack{e|D \\ e>1}} \frac{\phi(e)}{o_q(e)}.$$

For all $d \geq 1$ such that $2d \in \mathcal{S}_q$, the results of Corollary 6.4 and of the above Lemma combine to yield that

$$\varrho(d) = 1 + |\mathcal{O}_q(Z_{2d})| = I_q(2d). \tag{6.2}$$

Notice indeed that $\phi(2)/o_q(2) = 1$. Using the obvious fact that one has $I_q(D) \geq I_q(E)$ for all divisors $E \geq 1$ of a prime-to-q integer D, we further obtain that, for all $d \geq 1$ such that $2d \in \mathcal{S}_q$,

$$\varrho(d) \geq I_q(d). \tag{6.3}$$

This inequality will be useful in the next section.

7. Unbounded rank for $\{E_d\}_{d \geq 1}$

In this section, we prove our second main result:

Theorem 7.1 − *Let $\mathbb{F}_q$ be a finite field of odd characteristic, and $K := \mathbb{F}_q(t)$. For any integer $d \geq 1$, consider as above the elliptic curve E_d defined by (1.1) over K. One has*

$$\limsup_{d \geq 1} \left(\operatorname{rank} E_d(K) \right) = +\infty.$$

We give two proofs of this result. In the first one, we exhibit various sequences $(d_n)_{n \geq 1}$ of integers such that $\varrho(d_n) \to \infty$ as $n \to \infty$. The second proof shows a stronger (but less explicit) result: we deduce from the work of Pomerance and Shparlinski that the average of $\varrho(d)$ is unbounded. We conclude the section by an amusing observation about a link between prime numbers and the sequence $(\varrho(d))_{d \geq 1}$.

Remark 7.2 In view of Remark 1.1, we note the following other way of stating Theorem 7.1. Let $E = E_1$ be the elliptic curve over $\mathbb{F}_q(t)$ defined by $y^2 = x(x^2 + t^2 \cdot x^2 - 4t^2)$. For any integer $d \geq 1$, consider the finite Kummer extension $K_d := \mathbb{F}_q(t^{1/d})$ of K. Theorem 7.1 asserts that $\limsup_{d \geq 1} \left(\operatorname{rank} E(K_d) \right) = +\infty$.

7.1. Unbounded ranks (I).

− Recall that $\mathcal{S}_q$ denotes the set of supersingular integers. Let us start by constructing some special sequences of integers:

Lemma 7.3 − *For all $n \geq 1$, consider $d_{\mathrm{e},n} := q^n + 1$ and $d_{\mathrm{o},n} := \sum_{i=0}^{2n} (-q)^i$.*

(i) *$d_{\mathrm{e},n}$ is an even integer such that $d_{\mathrm{e},n} \in \mathcal{S}_q$. Moreover, one has $I_q(d_{\mathrm{e},n}) \geq \log \sqrt[4]{q} \cdot d_{\mathrm{e},n} / \log d_{\mathrm{e},n}$.*

(ii) *$d_{\mathrm{o},n}$ is an odd integer such that $2d_{\mathrm{o},n} \in \mathcal{S}_q$. Moreover, one has $I_q(2d_{\mathrm{o},n}) \geq \log \sqrt[4]{q} \cdot d_{\mathrm{o},n} / \log d_{\mathrm{o},n}$.*

Proof: It is obvious that $d_{\mathrm{e},n} = q^n + 1$ is even and supersingular; by Lemma 6.1, the multiplicative order of q modulo $d_{\mathrm{e},n}$ equals $2n$. Moreover, for any divisor $e \mid d_{\mathrm{e},n}$, we have $o_q(e) \mid o_q(d_{\mathrm{e},n}) = 2n$ so that, in particular, $o_q(e) \leq o_q(d_{\mathrm{e},n})$. We obtain the chain of inequalities:

$$I_q(d_{\mathrm{e},n}) = \sum_{\substack{e \mid d_{\mathrm{e},n} \\ e > 1}} \frac{\phi(e)}{o_q(e)} \geq \frac{1}{o_q(d_{\mathrm{e},n})} \cdot \sum_{\substack{e \mid d_{\mathrm{e},n} \\ e > 1}} \phi(e) = \frac{d_{\mathrm{e},n} - 1}{o_q(d_{\mathrm{e},n})} = \frac{d_{\mathrm{e},n} - 1}{2n} \geq \frac{d_{\mathrm{e},n}}{4n}.$$

By construction, one has $n = \log(d_{\mathrm{e},n} - 1)/\log q \leq \log d_{\mathrm{e},n}/\log q$ and we immediately deduce item (i).

Being the sum of an odd number of odd integers, $d_{\mathrm{o},n}$ is clearly odd, and we note that

$$q^{2n+1} + 1 = (q+1) \cdot \sum_{i=0}^{2n} (-q)^i = \frac{q+1}{2} \cdot 2d_{\mathrm{o},n}.$$

This identity shows that $2d_{\mathrm{o},n}$ is supersingular and that $q^{2n+1} \equiv -1 \bmod 2d_{\mathrm{o},n}$, so that $o_q(2d_{\mathrm{o},n}) \leq 2(2n+1)$. As before, for any divisor $e \mid 2d_{\mathrm{o},n}$, we have $o_q(e) \leq o_q(2d_{\mathrm{o},n})$ and, by an argument similar to the above, we obtain that $I_q(2d_{\mathrm{o},n}) \geq (d_{\mathrm{o},n} - 1)/(2n+1)$. From the identity $d_{\mathrm{o},n} = (q^{2n+1} + 1)/(q+1)$, straightforward estimates imply that $(d_{\mathrm{o},n} - 1)/(2n+1) \geq \log \sqrt[4]{q} \cdot d_{\mathrm{o},n}/\log d_{\mathrm{o},n}$, which proves (ii). $\qquad \square$

Putting together our results so far, we obtain:

Theorem 7.4 − *Let $\mathbb{F}_q$ be a finite field of odd characteristic. For any integer $d \geq 1$, consider the elliptic curve E_d over $K = \mathbb{F}_q(t)$ defined by (1.1). There is an infinite sequence of integers $(d_n)_{n \geq 1}$ such that*

$$\varrho(d_n) = \operatorname{rank} \left(E_{d_n}(K) \right) \gg_q \frac{d_n}{\log d_n}.$$

More precisely,

(a) *there is an infinite sequence of odd integers $(d_{\mathrm{o},n})_{n \geq 1}$ such that $\varrho(d_{\mathrm{o},n}) \geq \log \sqrt[4]{q} \cdot d_{\mathrm{o},n}/\log d_{\mathrm{o},n}$.*

(b) *there is an infinite sequence of even integers $(d_{\mathrm{e},n})_{n \geq 1}$ such that $\varrho(d_{\mathrm{e},n}) \geq \log \sqrt[4]{q} \cdot d_{\mathrm{e},n}/\log d_{\mathrm{e},n}$.*

Proof: For any integer $d \geq 1$ such that $2d \in \mathcal{S}_q$, we know from (6.2) that $\varrho(d) = \operatorname{rank} \left(E_d(K) \right) = I_q(2d)$.

By Lemma 7.3(ii), there exists an infinite sequence of odd integers $d_{\mathrm{o},n} := \sum_{i=0}^{2n} (-q)^i$ such that $2d_{\mathrm{o},n}$ is supersingular and $I_q(2d_{\mathrm{o},n}) \geq \log \sqrt[4]{q} \cdot d_{\mathrm{o},n}/\log d_{\mathrm{o},n}$ for all $n \geq 1$. This proves assertion (a) of the Theorem.

Next, let $d_{\mathrm{e},n} := q^n + 1$ for any $n \geq 1$; note that $d_{\mathrm{e},n}$ is even and supersingular. By the small Lemma 7.5 below, one has $\varrho(d_{\mathrm{e},n}) \geq \varrho(d_{\mathrm{e},n}/2)$. Together with (6.2) applied for $d = d_{\mathrm{e},n}/2$, Lemma 7.3(i) then implies that

$$\varrho(d_{\mathrm{e},n}) \geq \varrho(d_{\mathrm{e},n}/2) = I_q(d_{\mathrm{e},n}) \geq \log \sqrt[4]{q} \cdot d_{\mathrm{e},n}/\log d_{\mathrm{e},n}.$$

This proves the Theorem, and concludes the first proof for Theorem 7.1. $\qquad \square$

Lemma 7.5 − *Let $d \geq 1$ be an integer. Then $\varrho(md) \geq \varrho(d)$ for all integers $m \geq 1$.*

Proof: For a given $m \geq 1$, we let $K_m := \mathbb{F}_q(t^m)$ be the subfield of $\mathbb{F}_q(t) = K$ consisting of rational functions in the variable t^m. Since $K_m \subseteq K$, it is clear that $E_{md}(K_m) \subseteq E_{md}(K)$. On the other hand, it is obvious that $E_{md}(K_m) \simeq E_d(K)$ as abelian groups. Hence, $E_d(K)$ is isomorphic to a subgroup of $E_{md}(K)$. □

Remark 7.6 (a) Given that the BSD conjecture holds for the curves E_d (see Theorem 5.1), the lower bound in Theorem 7.4(b) means that Ulmer's lower bound on the rank (Theorem 1.6) still holds for the sequence $\{E_d\}_{d \geq 1}$, even though its 'parity hypothesis' fails to be satisfied (see §1.2).

(b) Let us further compare the lower bounds in Theorem 7.4 to Brumer's upper bound on the rank. Proposition 6.9 in [Bru92] states that

$$\text{rank}\left(E(K)\right) \leq \log\sqrt{q} \cdot \frac{\deg \mathcal{N}_{E/K}}{\log \deg \mathcal{N}_{E/K}} \cdot \left(1 + o(1)\right) \quad (\text{as } \deg \mathcal{N}_{E/K} \to \infty), \tag{7.1}$$

for any non-isotrivial elliptic curve E/K. Applying this bound to $E = E_d$ and plugging in our computation of $\deg \mathcal{N}_{E_d/K}$ yields that $\varrho(d') \leq \log\sqrt{q} \cdot \frac{2d'}{\log d'} \cdot (1 + o(1))$, as $d' \to \infty$ runs through integers coprime to q. Combining this with the lower bounds on $\varrho(d_{\mathrm{x},n})$ provided by Theorem 7.4(a)-(b) for $\mathrm{x} \in \{\mathrm{o}, \mathrm{e}\}$ and all $n \geq 1$, we deduce that

$$\frac{\log q}{4} \cdot \frac{d_{\mathrm{x},n}}{\log d_{\mathrm{x},n}} \leq \varrho(d_{\mathrm{x},n}) \leq \log q \cdot \frac{d_{\mathrm{x},n}}{\log d_{\mathrm{x},n}} \cdot (1 + o(1)) \qquad (\text{as } n \to \infty).$$

In other words, the subsequences $\{E_{d_{\mathrm{x},n}}\}_{n \geq 1}$ for $\mathrm{x} \in \{\mathrm{o}, \mathrm{e}\}$ provide examples where Brumer's bound (7.1) is optimal, up to a small absolute constant.

7.2. Unbounded ranks (II).

− In [PS10], Pomerance and Shparlinski study the average behaviour of the Mordell–Weil ranks of the elliptic curves of [Ulm02]. In the introduction to their paper, they note that it would be interesting to extend their result to other families of elliptic curves. Motivated by this remark, we investigated the average rank of the sequence $\{E_d\}_{d \geq 1}$ under consideration here. Here is the outcome of this investigation:

Theorem 7.7 − *There exists an absolute constant $\alpha > 1/2$ such that, for all big enough x (depending on p) one has*

$$\frac{1}{x} \sum_{1 \leq d \leq x} \varrho(d) \geq x^\alpha.$$

In particular, the average rank of $\{E_d(K)\}_{d \geq 1}$ is unbounded.

It turns out that this result follows almost directly from the constructions in [PS10] (specifically, the proof of Theorem 1 there). For the convenience of the reader, we sketch a proof nonetheless; more details can be found on pp. 33 – 35 of *loc. cit.*.

Proof: Let x be a large real number (depending on p). Pomerance and Shparlinski show on p. 35 of [PS10] that there exist an absolute constant $\alpha > 1/2$ and a set S_x of integers, with the following properties:

(i) For all $d \in S_x$, $x^{1+o(1)} \leq d \leq x$,   (iii) For all $d \in S_x$, $o_q(d) \leq x^{o(1)}$,

(ii) $|S_x| \geq x^{\alpha+o(1)}$,   (iv) For all $d \in S_x$, d is odd and d is supersingular.

The construction of S_x is quite subtle (*cf.* pp. 32–34 *loc. cit.*) and relies on techniques from analytic number theory. We do not go into more details here and refer the reader to [PS10] for a complete proof.

Since it is known that $\phi(d) \gg d^{1+o(1)}$ for all $d \geq 1$, we deduce from properties (iii) and (i) of S_x that

$$\forall d \in S_x, \qquad I_q(d) \geq \frac{\phi(d)}{o_q(d)} \geq \frac{d^{1+o(1)}}{x^{o(1)}} \geq x^{1+o(1)}.$$

Hence, by (ii),

$$\frac{1}{x} \sum_{d \in S_x} I_q(d) \geq \frac{|S_x|}{x} \cdot x^{1+o(1)} \geq x^{\alpha+o(1)}.$$

By (iv), any $d \in S_x$ is odd and supersingular, so that $2d$ is supersingular for all $d \in S_x$. Thus, $\varrho(d) \geq I_q(d)$ by our inequality (6.3). From here, since $\varrho(d) \geq 1$, we deduce that

$$\frac{1}{x} \sum_{1 \leq d \leq x} \varrho(d) \geq \frac{1}{x} \sum_{d \in S_x} \varrho(d) \geq \frac{1}{x} \sum_{d \in S_x} I_q(d) \geq x^{\alpha+o(1)},$$

which concludes the proof of the Theorem. □

Remark 7.8 (a) Brumer has shown that the average rank of elliptic curves over K is bounded. More precisely, consider the sequence $\mathscr{E}\!\ell\!\ell$ of *all non-isotrivial* elliptic curves over K ordered by their naive height h: Theorem 7.11 in [Bru92] states that

$$\frac{1}{\left|\{E \in \mathscr{E} : h(E) \leq B\}\right|} \sum_{\substack{E \in \mathscr{E} \\ h(E) \leq B}} \operatorname{rank}\big(E(K)\big) \leq 2.3 + o(1) \qquad (\text{as } B \to \infty).$$

Comparing this result to our Theorem 7.7, one sees that the sequence $\{E_d\}_{d \geq 1}$ must be a very 'thin' subsequence of $\mathscr{E}\!\ell\!\ell$. It is also a quite special subsequence, in the sense that the average behaviour of its rank is atypical.

(b) From Theorem 7.7, one easily deduces the following statement: for x large enough, there are at least x^α integers $d \in [1, x]$ such that $\varrho(d) \gg_q \sqrt{d}/\log d$. In particular, 'large' ranks are relatively 'common' in the sequence $\{E_d\}_{d \geq 1}$. But actually, adapting Theorem 2 of [PS10] to the case at hand would show that a much stronger statement holds: this would prove that, for all $\epsilon > 0$, one has

$$\frac{1}{x} \cdot \left|\left\{d \in [1, x] : \varrho(d) \geq (\log d)^{(1/3-\epsilon)\log\log\log d}\right\}\right| = 1 - o_{p,\epsilon}(1) \qquad (\text{as } x \to \infty).$$

More vaguely, this tells us that the rank $\varrho(d)$ is 'reasonably large' for almost all integers d. Again, the proof of [PS10, Theorem 2] is quite subtle and we refer the reader to [PS10, pp. 36–39] for details.

7.3. An amusing fact. –
We conclude this paper by the following observation. In this section, we restrict to the case where $q = p$ is a prime number $p \geq 3$ and consider the elliptic curves E_d defined by (1.1) over $K = \mathbb{F}_p(t)$.

When $d = 1$ or 2, we know from Theorem 4.1 that $L(E_d/K, T) = 1 - pT$. In particular, the BSD conjecture (Theorem 5.1) here yields that $\varrho(1) = \varrho(2) = 1$. Since, for all $m \geq 1$, the p^m-th power Frobenius provides an isogeny $E_1 \to E_{p^m}$ (resp. $E_2 \to E_{2p^m}$) and since isogenous curves have the same Mordell–Weil rank, the groups $E_{p^m}(K)$ and $E_{2p^m}(K)$ also have rank one. Hence, we deduce that there exist infinitely many integers $d \geq 1$ such that E_d has Mordell–Weil rank 1 (namely $1, 2, p, 2p, p^2, 2p^2, p^3, \dots$). Combined with Corollary 2.2 – which implies that $\varrho(d) \geq 1$ for all $d \geq 1$, we have just shown that $\liminf_{d \geq 1} \varrho(d) = 1$.

One can generalise the above argument, as follows:

Theorem 7.9 – *Assume that there exists a prime number $\ell \neq 2, p$ such that p generates $(\mathbb{Z}/\ell^2\mathbb{Z})^\times$. For any odd integer $R \geq 1$, there are infinitely many integers $d \geq 1$ such that*

$$\operatorname{rank}\big(E_d(\mathbb{F}_p(t))\big) = R.$$

Given a prime $p \geq 3$, and assuming the existence of a prime $\ell \neq 2, p$ such that p generates $(\mathbb{Z}/\ell^2\mathbb{Z})^\times$, this Theorem gives a third proof of the unboundedness of $d \mapsto \operatorname{rank}\big(E_d(\mathbb{F}_p(t))\big)$ (Theorem 7.1).

Proof: The case $R = 1$ has already been handled above (without any assumption about primes), hence we can assume that $R \geq 3$ and let $r := (R-1)/2 \geq 1$.

Pick an odd prime ℓ such that the subgroup generated by p modulo ℓ^2 is the whole of $(\mathbb{Z}/\ell^2\mathbb{Z})^\times$. A classical argument shows that p then also generates $(\mathbb{Z}/\ell^b\mathbb{Z})^\times$ for all $b \geq 1$ (see [Hin11, Ex. I.6.2] for instance); and it is easily seen that, for all $b \geq 0$, p generates $(\mathbb{Z}/2\ell^b\mathbb{Z})^\times$ as well. Therefore, for this choice of ℓ, one has $o_p(\ell^b) = \phi(\ell^b)$ and $o_p(2\ell^b) = \phi(2\ell^b)$.

Since p generates $(\mathbb{Z}/2\ell^r\mathbb{Z})^\times$, there exists an integer $a \geq 1$ such that $p^a \equiv -1 \bmod 2\ell^r$ *i.e.*, such that $2\ell^r$ divides $p^a + 1$. Hence the integer $2\ell^r$ is supersingular. Moreover, we have

$$I_p(2\ell^r) = \sum_{\substack{e | 2\ell^r \\ e > 1}} \frac{\phi(e)}{o_p(e)} = \sum_{1 \leq b \leq r} \frac{\phi(\ell^b)}{o_p(\ell^b)} + \sum_{0 \leq b \leq r} \frac{\phi(2\ell^b)}{o_p(2\ell^b)} = r + (r+1) = R.$$

We deduce from Corollary 6.4 and (6.2) that one has $\operatorname{rank}\big(E_{\ell^r}(K)\big) = I_p(2\ell^r) = R$.

Now put $d_m := p^m \ell^r$ for all $m \geq 0$. Since $E_{p^m\ell^r}$ and E_{ℓ^r} are isogenous (*via* the p^m-th power Frobenius), their Mordell–Weil groups have the same rank. By the computation above, we thus have $\operatorname{rank}\big(E_{d_m}(K)\big) = R$ for all $m \geq 0$. $\qquad\square$

Remark 7.10 For an explicitly given prime p, it is rather easy to find primes ℓ such that p generates $(\mathbb{Z}/\ell^2\mathbb{Z})^\times$. Here is a sample for small values of p:

p	$\{\ell \neq 2, p \text{ prime} : \langle p \bmod \ell^2 \rangle = (\mathbb{Z}/\ell^2\mathbb{Z})^\times\}$
3	$\{5, 7, 17, 19, 29, 31, 43, 53, 79, 89, 101, 113, 127, 137, 139, ...\}$
5	$\{3, 7, 17, 23, 37, 43, 47, 53, 73, 83, 97, 103, 107, 113, 137, ...\}$
7	$\{11, 13, 17, 23, 41, 61, 67, 71, 79, 89, 97, 101, 107, 127, 151, ...\}$
11	$\{3, 13, 17, 23, 29, 31, 41, 47, 59, 67, 73, 101, 103, 109, 149, ...\}$
13	$\{5, 11, 19, 31, 37, 41, 47, 59, 67, 71, 73, 83, 89, 97, 109, 137, ...\}$
17	$\{5, 7, 11, 23, 31, 37, 41, 61, 97, 107, 113, 131, 139, 167, 173, ...\}$

Given a prime p, according to Artin's primitive root conjecture there should exist infinitely many primes ℓ such that p generates $(\mathbb{Z}/\ell\mathbb{Z})^\times$ (better, the set of such primes should have a positive density). Hooley [Hoo67] has proved Artin's conjecture under the assumption of GRH for the zeta function of certain number fields. We also note that Heath-Brown later proved (unconditionally) that there are at most two exceptional primes p for which the conjecture fails to hold, see [HB86]. Moreover, if p generates $(\mathbb{Z}/\ell\mathbb{Z})^\times$, one can show that p also generates $(\mathbb{Z}/\ell^2\mathbb{Z})^\times$ unless $p^{\ell-1} \equiv 1 \bmod \ell^2$. Experiments with small primes p and ℓ suggest that the latter happens only very rarely (when $p = 5$ for example, there are 30884 primes ℓ in the range $[3, 10^6]$ such that 5 generates $(\mathbb{Z}/\ell\mathbb{Z})^\times$, but only one with $5^{\ell-1} \equiv 1 \bmod \ell^2$, namely $\ell = 40487$). It thus seems quite plausible that, for each prime $p \geq 3$, there are infinitely many primes ℓ such that p generates $(\mathbb{Z}/\ell^2\mathbb{Z})^\times$.

Assuming that this is true, for all odd integers $R \geq 1$, one can exhibit infinitely many integers $(d_i)_{i \geq 1}$, *all coprime to p*, such that $\varrho(d_i) = R$ for all $i \geq 1$. This would provide a 'less artificial' construction of such a sequence than that given in the proof above.

References

[Ber08] Lisa Berger. Towers of surfaces dominated by products of curves and elliptic curves of large rank over function fields. *J. Number Theory*, 128(12):3013–3030, 2008. ↑ 1, 2, 3, 4, 14, 15, 16

[BH12] Salman Baig and Chris Hall. Experimental data for Goldfeld's conjecture over function fields. *Exp. Math.*, 21(4):362–374, 2012. ↑ 13

[Bru92] Armand Brumer. The average rank of elliptic curves. I. *Invent. Math.*, 109(3):445–472, 1992. ↑ 2, 19, 20

[Coh07] Henri Cohen. *Number theory. Vol. I. Tools and Diophantine equations*, volume 239 of *Graduate Texts in Mathematics*. Springer, New York, 2007. ↑ 8, 13, 16

[Gri16] Richard Griffon. *Analogues du théorème de Brauer-Siegel pour quelques familles de courbes elliptiques*. PhD thesis, Université Paris Diderot, July 2016. ↑ 2, 16, 21

[Gri18b] Richard Griffon. Explicit L-functions and a Brauer-Siegel theorem for Hessian elliptic curves. *Journal de Théorie des Nombres de Bordeaux*, (to appear), 2018. (Preprint ArXiv:1709.02761). ↑ 6, 11

[GS95] Dorian Goldfeld and Lucien Szpiro. Bounds for the order of the Tate-Shafarevich group. *Compositio Math.*, 97(1-2):71–87, 1995. ↑ 7

[Gro11] Benedict H. Gross. Lectures on the conjecture of Birch and Swinnerton-Dyer. In *Arithmetic of L-functions*, volume 18 of *IAS/Park City Math. Ser.*, pages 169–209. Amer. Math. Soc., Providence, RI, 2011. ↑ 3, 12

[HB86] Roger Heath-Brown. Artin's conjecture for primitive roots. *Quart. J. Math.*, 37(1):27–38, 1986. ↑ 21

[Hin11] Marc Hindry. *Arithmetics*. Universitext. Springer, London, 2011. (Trans. from the French by Sarah Carr). ↑ 20

[Hoo67] Christopher Hooley. On Artin's conjecture. *J. Reine Angew. Math.*, 225:209–220, 1967. ↑ 21

[Lev68] Martin Levin. On the Group of Rational Points on Elliptic Curves Over Function Fields. *American J. of Math.*, 90(2):456–462, 1968.↑ 7

[LN97] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, 2nd edition, 1997.↑ 9

[Mil06] J. S. Milne. *Arithmetic duality theorems*. Booksurge, LLC, 2nd edition, 2006.↑ 3, 16

[PS10] Carl Pomerance and Igor E. Shparlinski. Rank statistics for a family of elliptic curves over a function field. *Pure Appl. Math. Q.*, 6(1, Special Issue: In honor of John Tate. Part 2):21–40, 2010.↑ 1, 17, 19, 20

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.↑ 3

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, 2nd edition, 2009.↑ 3, 6, 7

[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.↑ 6

[ST67] Igor R. Shafarevich and John T. Tate. The rank of elliptic curves. *Dokl. Akad. Nauk SSSR*, 175:770–773, 1967.↑ 1, 2, 16

[Tat94] John T. Tate. Conjectures on algebraic cycles in *l*-adic cohomology. In *Motives (Seattle, WA, 1991)*, volume 55 of *Proc. Sympos. Pure Math.*, pages 71–83. Amer. Math. Soc., 1994.↑ 16

[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.↑ 16

[Ulm02] Douglas Ulmer. Elliptic curves with large rank over function fields. *Ann. of Math. (2)*, 155(1):295–315, 2002.↑ 1, 2, 16, 19

[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.↑ 1, 2, 3, 4

[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.↑ 5, 6, 12

[Ulm13] Douglas Ulmer. On Mordell-Weil groups of Jacobians over function fields. *J. Inst. Math. Jussieu*, 12(1):1–29, 2013.↑ 3, 14, 16

Departement Mathematik und Informatik, Universität Basel,
Spiegelgasse 1, 4051 Basel, Switzerland.
E-mail: richard.griffon@unibas.ch