Abstract. In 1985, Schoof devised an algorithm to compute zeta functions of elliptic curves over finite fields by directly computing the numerators of these rational functions modulo sufficiently many primes (see [11]). If $E/K$ is an elliptic curve with nonconstant $j$-invariant defined over a function field $K$ of characteristic $p \geq 5$, we know that its $L$-function $L(T, E/K)$ is a polynomial in $\mathbb{Z}[T]$ (see [5, p.11]). Inspired by Schoof, we study the reduction of $L(T, E/K)$ modulo integers. We obtain three main results. Firstly, if $E/K$ has non-trivial $K$-rational $N$-torsion for some integer $N$ coprime with $p$, we extend a formula for $L(T, E/K) \mod N$ due to Hall (see [4, p.133, Theorem 4]) to all quadratic twists $E_f/K$ with $f \in K^\times \setminus K^\times 2$. Secondly, without any condition on the 2-torsion subgroup of $E(K)$, we give a formula for the quotient modulo 2 of $L$-functions of any two quadratic twists of $E/K$. Thirdly, we use these results to compute the global root numbers of an infinite family of quadratic twists of an elliptic curve and in most cases find the exact analytic rank of each of these twists. We also illustrate that in favourable situations our second main result allows one to compute much more efficiently $L(T, E_f/K) \mod 2$ than an algorithm of Baig and Hall (see [1]). Finally, we use our formulas to compute directly some degree 2 $L$-functions.

1. Introduction

1.1. Motivation. Let $k$ be a finite field whose cardinality $q$ is a power of a prime $p$ and let $E/k$ be an elliptic curve defined over $k$. The zeta function of $E/k$ is a rational function of the form

$$Z(T, E/k) = \frac{L(T, E/k)}{(1-T)(1-qT)}.$$ 

Here, $L(T, E/k)$ is the quadratic polynomial $1 - \alpha T + qT^2$, with $\alpha$ the integer $1 + q - \#E(k)$ and where $\#E(k)$ is the cardinality of the set of $k$-rational points $E(k)$. For $p \geq 5$, the elliptic curve $E/k$ is given by a Weierstrass equation of the form $y^2 = x^3 + ax + b$ with $a, b \in k$ satisfying $-16(4a^3 + 27b^2) \neq 0$. If we want to compute the coefficient $\alpha$ in practice, we can test all pairs $(u, v)$ in $k \times k$ and determine which ones satisfy the equation $v^2 = u^3 + au + b$. As the cardinality of $q$ grows, this method becomes impractical. In 1985, Schoof [11] side-stepped this point-counting method. He took advantage of the fact that $\alpha$ was bounded in absolute value by $2\sqrt{q}$ (see [13, p.138, V. Theorem 1.1]) and devised an algorithm to directly compute the reduction of $\alpha$ modulo any prime $\ell$ different from $p$. If one performs this algorithm for sufficiently many primes $\ell_i$ so that their product $\prod_i \ell_i$ is strictly larger than $4\sqrt{q}$, then $\alpha$ is completely determined by its reduction modulo $\prod_i \ell_i$, thanks to the Chinese remainder theorem.

Suppose that $p \geq 5$ and let $C/k$ be a proper, smooth, and geometrically connected curve, with function field $K$. Let $E/K$ be an elliptic curve whose $j$-invariant is nonconstant. It follows from the work of Grothendieck, Deligne and others that the $L$-function of $E/K$ (defined in subsection [5]) is a polynomial in $1 + T \cdot \mathbb{Z}[T]$ (see [5, p.11]). In this paper, by analogy with Schoof, we begin a study of the problem of directly computing the reduction of $L(T, E/K)$ modulo an integer $N$ not divisible by $p$.

2020 Mathematics Subject Classification. 11G40.

Key words and phrases. Elliptic Curve, Function Field, $L$-Function, Torsion Subgroup.
1.2. Related Works. The problem of explicitly computing the $L$-function of an elliptic curve defined over a function field is difficult and currently very few strategies to compute it exist. To our knowledge, they all take advantage of the observation that an elliptic curve $E/K$ can be seen as an elliptic surface $E/k$ over the finite field $k$ (see [15] pp.250-252, Lecture 3).

One can compute the $L$-function using point-counting methods. The only implemented point-counting method that we are aware of can be found in the computer algebra system Magma [7] and is currently only available for the function field $K = k(t)$. The bulk of the work of the algorithm is to count points fiber-by-fiber on elliptic curves defined over finite fields that are finite extensions of $k$, up to some large enough degree. As the cardinality of $k$ grows, it becomes computationally difficult to compute $L$-functions with this technique.

In the direction of $p$-adic methods, one could consider the following idea, suggested by Andrew Sutherland (private communication) that we summarize here. In [2], Costa, Harvey and Kedlaya obtained a practical algorithm to compute zeta functions of varieties of some moderate dimension over finite fields which is much more efficient than naive-point counting. The idea would be to adapt their algorithm to compute the zeta function $Z(T, S/k)$ of the elliptic surface $S/k$ corresponding to the elliptic curve $E/K$. Let $Z(T, C/k)$ be the zeta function of the curve $C/k$ corresponding to the function field $K$ (see Definition 1). Sutherland’s idea can be justified by the fact that the $L$-function $L(T, E/K)$ is (see [15] p.257, Exercise 6.2), up to a finite product of rational functions indexed by the places of bad reduction, the quotient $Z(T, C/k)Z(qT, C/k)/Z(T, S/k)$.

There are various algorithms to compute the zeta function of the curve $C/k$ (for example [2]) and so to compute the $L$-function of $E/K$ it would essentially suffice to compute the zeta function of the elliptic surface. Costa pointed (private communication) that their method already applies if the elliptic surface is a toric 3-fold, for example a surface in a weighted projective space.

Finally, since the $L$-function of an elliptic curve $E/K$ with nonconstant $j$-invariant is a polynomial with integer coefficients, one can explore another approach in spirit of Schoof’s algorithm. The starting point of this exploration is the following key result by Hall [4] p.133, Theorem 4.

**Theorem 1.** Let $N ≥ 2$ be an integer coprime with $q$ and let $T$ be a finite subgroup of $E(K)$ of cardinality $N$. If $M^{\text{sp}}$, resp. $M^{\text{ns}}$, resp. $A$, denote the sets of places of $K$ over which $E$ has split multiplicative, resp. non-split multiplicative, resp. additive reduction, then

$L(T, E/K) ≡ Z(T, C/k)Z(qT, C/k) × \prod_{v ∈ M^{\text{sp}}} (1 − q^{dv}T^{dv})$

$× \prod_{v ∈ M^{\text{ns}}} \frac{(1 − T^{dv})(1 − q^{dv}T^{dv})}{(1 + T^{dv})}$

$× \prod_{v ∈ A} (1 − T^{dv})(1 − q^{dv}T^{dv}) \mod N$.

It is worth mentioning that this formula was not used to compute $L$-functions in Hall’s paper (see [4] p.139, Theorem 12 and [4] p.142, Theorem 16 for his main results). However, we illustrate in Proposition [20] how Theorem 1 can be used to compute some degree 2 $L$-functions.

1.3. Overview of the Results. Let $k$ be a finite field whose cardinality $q$ is a power of a prime $p ≥ 5$ and let $C/k$ be a proper, smooth and geometrically connected curve with function field $K$. Let $E$ be an elliptic curve over $K$ with nonconstant $j$-invariant and for each $f ∈ K^× \setminus K^{×2}$ let $E_f/K$ be its quadratic twist (see Subsection 2.1). Denote by $U$, $M$, $M^{\text{sp}}$, $M^{\text{ns}}$ and $A$ the subsets of closed points of $C$ corresponding to the loci of good, resp. multiplicative, resp. split multiplicative, resp. nonsplit multiplicative, resp. additive reduction of $E/K$. Let $f ∈ K^× \setminus K^{×2}$ and let $K_f$ be the quadratic extension of $K$ generated by a chosen square root of $f$. We decorate by a subscript $f$ the corresponding sets $U_f$, $M_f$, $M^{\text{sp}}_f$, $M^{\text{ns}}_f$ and $A_f$ when the reduction types of the places of $K$. 

2
are considered with respect to the quadratic twist $E_f/K$ of $E/K$. If $v$ is a place of $K$ (equivalently a closed point of $C$), then we write $k_v$ for the residue field of $v$ and $d_v$ for the degree of the finite extension $k_v/k$. Let $M^\text{ur}_{\text{fin}}$ (resp. $M^\text{ur}_{\text{inf}}$) be the subset of $M^\text{ur}$ (resp. of $M^\text{ur}$) whose elements are unramified in $K_f$. Finally, let $M^\text{split}$ and $M^\text{inert}$ be the subsets of places of $M$ which are respectively split and inert in $K_f$ and let $A_{\text{ur}}, A^\text{gd}_{\text{ram}}$ be subsets of places of $A$ which are respectively unramified in $K_f$ and ramified in $K_f$ over which $E/K$ has potentially good reduction. Our first main result, Theorem 2 gives, under the conditions of Theorem 1 a formula for $K$ the infinitely many extension sum of $N$ Theorem 2

Remark 1. In Theorem [16] we also provide formulas for $L(T, E_f/K) \mod N$ when $N \in \{2, 3, 4\}$. As a consequence, Corollary [15] gives a formula for $L(T, E_f/K) \mod 2$ that is slightly more precise than the one in [4], p.133, Theorem 4.

Remark 2. It is important to point that even if $E(K)$ has a subgroup of order $N$, the group $E_f(K)$ does not need to have a subgroup of order $N$. Indeed, one can show that for $N$ odd, the direct sum of $N$-torsion subgroups $E(K)[N] \oplus E_f(K)[N]$ of $E(K)$ and $E_f(K)$ is isomorphic to $N$-torsion subgroup $E(K_f)[N]$ of $E(K_f)$. Moreover, in [4], p.133, Theorem 4 only gives $L(T, E/K) \mod N$, while Theorem 2 gives $L(T, E_f/K) \mod N$ any of the infinitely many $f \in K^\times \setminus K^{\times 2}$.

The next result conveniently provides $\deg L(T, E_f/K)$, the degree of the $L$-function of a quadratic twist $E_f/K$, and its global root number $\varepsilon(E_f/K)$, in terms of the places of bad reduction of $E/K$, the decomposition types of these places in $K_f$, and the genus $g(C)$ of $C$.

Proposition 3 (Proposition [14]). Let $k'$ be the field of constants of $K_f$.

(i) The degree of $L(T, E_f/K)$ equals

$$\deg(M_{\text{ur}}) + \deg(A_{\text{ur}}) \text{ if } [k' : k] = 2,$$

$$2(2g(C) - 2) + 2 \sum_{v \in |C| \text{ ord}_v(f) \equiv 1 \mod 2} d_v + \deg(M_{\text{ur}}) + \deg(A_{\text{ur}}) - \deg(A^\text{gd}_{\text{ram}}) \text{ if } [k' : k] = 1.$$  

(ii) If $E(K)$ has a subgroup of order $N$ with $N \geq 2$ an integer coprime with $q$, then the global root number $\varepsilon(E_f/K)$ satisfies

$$\varepsilon(E_f/K) = \begin{cases} (-1)^{\#M_{\text{ur}}^\text{sp} + \#M_{\text{inert}}^\text{ns}}, & \text{mod } N \quad \text{if } [k' : k] = 2, \\ (-1)^{\#M_{\text{ur}}^\text{sp} + \#M_{\text{inert}}^\text{ns}}, & \text{mod } N \quad \text{if } [k' : k] = 1. \end{cases}$$

In our second main result we provide, unconditionally on the 2-torsion subgroup of $E(K)$, the ratio modulo 2 of the $L$-functions of any two quadratic twists of $E/K$. This ratio is well-defined. Indeed, let $f_1, f_2 \in K^\times$ and let $E_{f_1}$ and $E_{f_2}$ be the corresponding quadratic twists of

\[3\]
E. Since $E$ has nonconstant $j$-invariant $j(E)$, then $L(T, E/K) \in 1 + T \cdot \mathbb{Z}[T]$ (see [3, p.11]). By Lemma [11] we have $j(E) = j(E_1)$ and so $L(T, E_1/K) \in 1 + T \cdot \mathbb{Z}[T]$, for $i = 1, 2$. Therefore, $L(T, E_{f_1}/K) L(T, E_{f_2}/K) \in 1 + T \cdot \mathbb{Z}[[T]]$ and $L(T, E_{f_1}/K) L(T, E_{f_2}/K) \mod 2$ is a well-defined element of $1 + T \cdot (\mathbb{Z}/2\mathbb{Z})[[T]]$.

**Theorem 4** (Theorem 20). Let $f_1, f_2 \in K^\times$ and let

$$U_{f_1, f_2} := \left( |U_{f_1}| \cap |U_{f_2}| \right) \cup (M_{f_1} \cap M_{f_2}) \cup (A_{f_1} \cup A_{f_2}) .$$

Then,

$$L(T, E_{f_1}/K) \over L(T, E_{f_2}/K) = \prod_{v \in U_{f_1, f_2}} \left( L_v(T, E_{f_2}/K) \over L_v(T, E_{f_1}/K) \right) \mod 2. $$

In particular, when $K = k(t)$, we have the following.

**Corollary 5** (Corollary 23). Let $q$ be a power of a prime $p \geq 5$ and let $K = k(t)$. Suppose that $E/K$ has semistable reduction everywhere, with multiplicative reduction at $t = \infty$. Let $\Delta \in k[t]$ be the discriminant of a minimal Weierstrass equation for $E$ and let $f \in k[t]$ be a square-free polynomial of even degree which is coprime with $\Delta$. We have

$$L(T, E_f/K) \over L(T, E/K) = \prod_{v | f} \left( 1 + a_v T^{d_v} + T^{2d_v} \right) \mod 2,$$

where $a_v := 1 + q^{d_v} - \#E_v(k_v)$. Here, $E_v$ is the elliptic curve over $k_v$ obtained from $E$ by reducing modulo $v$ the coefficients of that minimal Weierstrass equation, and $\#E_v(k_v)$ is the cardinality of its set of $k_v$-rational points. See Corollary 23 for a more general expression.

A highlight of Equation (1) is its computability as we illustrate in Subsection 5.1. Given an elliptic curve $E/K$ with $L(T, E/K) = 1$, we discuss the efficiency to compute the reduction $L(T, E_f/K)$ modulo 2, when $f$ is a monic irreducible polynomial of even degree $d_f$, which is coprime to $\Delta$. More precisely, we show that employing Equation (1) is by far superior to computing $L(T, E/K)$ mod 2 than using a suitable version of the algorithm of Baig and Hall in [1]. The reason is roughly the following. Since $\text{char}(k) \neq 2, 3$, we can write a Weierstrass equation for $E/K$ in the form $y^2 = x^3 + Ax + B$ for some $A, B \in k[t]$. The comparison of the two approaches to compute $L(T, E_f/K)$ mod 2 amounts to decide whether the image of $x^3 + Ax + B$ in some finite fields is irreducible or not. With Corollary 23 we have $L(T, E_f/K) \equiv 1 + a_f T^{d_f} + T^{2d_f} \mod 2$ and we then only need to compute the reduction of $x^3 + Ax + B$ in the finite extension $k[t]/(f)$ of $k$ of degree $d_f$. In general, the algorithm of Baig and Hall requires to test, for most monic irreducible polynomials $v$ in $k[t]$ of degree $d_v \leq 2d_f$, the irreducibility of the image of $x^3 + Ax + B$ in the extensions of finite fields of $k$ defined by these polynomials $v$. As $d_f$ grows, the number of finite fields to consider for the algorithm of Baig and Hall becomes considerable (see Subsection 5.1 for more details).

In Subsection 5.2 we discuss an analogue approach to Schoof’s algorithm to compute polynomial $L$-functions of elliptic curves with nonconstant $j$-invariants. Although this analogous approach is currently in a primitive state, Theorem 1, Theorem 2 and Theorem 20 can be seen as first concrete steps. We also make the following elementary observation.

**Proposition 6** (Proposition 24 and Corollary 25). If $E/K$ is an elliptic curve with nonconstant $j$-invariant, with odd analytic rank, with a polynomial $L$-function of degree $d$ and coefficients $a_0 = 1, a_1, \ldots, a_n \in \mathbb{Z}$, then

$$L(T, E/K) = (1 - qT) \left( 1 + \sum_{n=1}^{d-2} \sum_{m=0}^{n} a_m q^{n-m} \right) T^n + q^{d-1} T^{d-1}.$$
As an illustration, we conclude Subsection 5.2 by using Theorem 1, Theorem 2, Proposition 3 and Corollary 5 to compute some degree 2 $L$-functions of elliptic curves.

**Proposition 7** (Proposition 26). Let $k$ be the field with 5 elements and let $f$ be a rational function of the form $f \in \{P(t), 1/Q(t), P(t)/Q(t), \text{ with } P(t), Q(t) \in k[t] \text{ coprime and of degree 1}\}$. An elliptic curve $E/k(t)$ given by a Weierstrass equation

$$E/k(t) : y^2 = (1 - a)xy - by = x^3 - bx^2,$$

with $a = (10 - 2f)/(f^2 - 9)$ and $b = -2(f - 1)/(f^2 - 9)^2$, has torsion subgroup $E(k(t))_{\text{tors}}$ isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Moreover, its $L$-function equals

$$L(T, E/k(t)) = (1 - 5T)(1 + 5T).$$

**Proposition 8** (Proposition 27). Suppose that $k$ is the field with 7 elements and let $f \in k[t]$ with degree 1. An elliptic curve $E/k(t)$ given by a Weierstrass equation

$$E/k(t) : y^2 + xy + \frac{f^2 + f + 1}{3(f + 2)^3} = x^3$$

has torsion subgroup $E(k(t))_{\text{tors}}$ isomorphic to $(\mathbb{Z}/3\mathbb{Z})^2$, bad reduction $M^s_p$ and $L$-function equal to 1. Moreover, for any finite place $h \in M^s_p$, the $L$-function of the quadratic twist $E_{h}/k(t)$ is

$$L(T, E_{h}/k(t)) = (1 - 7T)(1 + 7T).$$

Finally, in Subsection 5.3 we study, over an arbitrary field $k$ of characteristic $p \geq 5$, an infinite family of quadratic twists of the so-called universal elliptic curve $E$ over the function field $K$ of the modular curve $X_1(3)/k$. We obtain our third main theorem (detailed in Theorem 28) by using Theorem 2, Proposition 3 and Corollary 5 to compute the reduction modulo 2 and modulo 3 of the $L$-functions of the quadratic twists of that family, compute all the global root numbers and either give the exact analytic rank of the quadratic twists or a nontrivial upper bound on it.

**Theorem 9** (Theorem 28). Let $k$ be a finite field of cardinality $q$ such that $q \equiv 5, 11 \mod 12$. Consider the elliptic curve $E/k(t)$ given by the Weierstrass equation

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

and let $\Delta$ be the discriminant of this equation. The point $(0, 0) \in E(k(t))$ has order 3. If $f \in k[t]$ is a monic square-free polynomial of degree $d_f$, which is coprime to $\Delta$, then $L(T, E_f/K)$ has even degree. For $a \in \{0, 1\}$, we write $f(a) \in k^2$ to ask whether $f(a)$ is a square (Yes) or not (No) in $k$. We have

| $f(0) \in k^2$? | $f(1) \in k^2$? | $L(T, E_f/K) \mod 3$ |
|-----------------|-----------------|------------------|
| Yes             | Yes             | $L(T, K_f)L(-T, K_f)(1 - T)(1 + T)(1 + T^2)$ |
| Yes             | No              | $L(T, K_f)L(-T, K_f)(1 - T)^2(1 + T^2)$ |
| No              | Yes             | $L(T, K_f)L(-T, K_f)(1 - T)(1 + T)^3$ |
| No              | No              | $L(T, K_f)L(-T, K_f)(1 - T)(1 + T)(1 + T^2)$ |

**Table 1. Reduction $L(T, E_f/K) \mod 3$**

The global root number $\varepsilon(E_f/K)$ is given in Table 2 below.

Moreover, let $\text{Jac}(C_f)(k)$ be the set of $k$-rational points of the Jacobian of the (normalization of the) curve $C_f/k$ associated to the field $K_f$. If the 3-torsion subgroup of $\text{Jac}(C_f)(k)$ is trivial, then the fourth column of Table 2 gives the analytic rank, rank$^\text{an}(E_f/K)$ of the elliptic curve $E_f/K$ or an upper bound on it.

If $f$ is irreducible of odd degree, then we have the following.
Table 2. Global Root Number and Analytic Rank Using Reduction Modulo 3

| $f(0) \in k^2$? | $f(1) \in k^2$? | $\varepsilon(E_f/K)$ | rank_{an}(E_f/K) |
|-----------------|-----------------|---------------------|------------------|
| Yes             | Yes             | 1                   | 0                |
| Yes             | No              | 1                   | 0                |
| No              | Yes             | −1                  | ≤3               |
| No              | No              | −1                  | 1                |

Table 3. Analytic Rank using Reduction Modulo 2

| $a_{\infty} \mod 2$ | $a_f \mod 2$ | rank_{an}(E_f/K) |
|---------------------|--------------|------------------|
| 0                   | 0            | ≤4               |
| 0                   | 1            | ≤2               |
| 1                   | 0            | ≤2               |
| 1                   | 1            | 0                |

This paper is organized as follows. In Section 2, we introduce the notation used throughout the paper and recall some key concepts about zeta functions of curves and about quadratic twists and $L$-functions of elliptic curves. In Section 3 we prove our first and second main results, Theorem 16 and Theorem 20, as well as Corollary 18 and Proposition 14. In Section 4, we specialize to $K = k(t)$ the statements of Theorem 16 and Theorem 20 in Proposition 22 and Corollary 23, respectively. In Section 5, we discuss three applications of the results of Section 3 and Section 4. More precisely, we discuss in Subsection 5.1 the efficiency of Corollary 23 to compute $L(T, E_f/K) \mod 2$ and compare it with an algorithm of Baig and Hall. In Subsection 5.2, we discuss an analogue approach of Schoof’s algorithm to compute polynomial $L$-functions, observe an elementary identity on $L$-functions of elliptic curves with odd analytic rank (see Proposition 24) and compute some degree 2 $L$-functions with this Schoof’s like approach. In Subsection 5.3, we prove our third main result, Theorem 28. Finally, in Section 6, we prove some auxiliary results mentioned in Section 2 and in Section 3 for which we do not know a reference in the literature.

2. Notation and Prerequisites

In this section, we set up the notation that we use throughout this paper, introduce some basic concepts and prove some results which are certainly well-known but for which we could not find a proof in the literature.

Let $k$ be a finite field of cardinality a power $q$ of a prime $p \geq 5$. Let $C/k$ be a smooth, proper and geometrically connected curve $C$ defined over $k$ and of genus $g := g(C)$. Let $|C|$ be the the set of closed points of $C/k$ and let $K$ be its function field, which also has genus $g = g(K)$. The field $K$ is a finite algebraic extension of $k(t)$ for some transcendental element $t \in K$ over $k$. Given a field $L$, we fix an algebraic closure $\overline{L}$.

Now suppose that $K$ is the function field of a curve $C/k$ as introduced above. If $v$ is a place of $K$, then $K_v$ denotes the completion of $K$ at $v$ and we let ord$_v$ be the discrete valuation associated to $v$. Let $\mathcal{O}_v$ be the discrete valuation ring $\mathcal{O}_v = \{ \alpha \in K_v : \text{ord}_v(\alpha) \geq 0 \}$. The ring $\mathcal{O}_v$ is a local ring and we choose for generator of its unique maximal ideal $m_v = \{ \alpha \in K_v : \text{ord}_v(\alpha) > 0 \}$ a uniformizer $\pi_v$, normalized so that $\text{ord}_v(\pi_v) = 1$. We denote by $k_v$ the associated residue field $\mathcal{O}_v/m_v$, which is a finite extension of degree $d_v$ of $k$. Given an elliptic curve $E/K$, we let $E_v/k_v$ be the reduced curve defined over $k_v$ and we let $\Phi_v$ by the local group scheme of components defined over $k_v$. If $X$ is a scheme and $L$ is a field, then $X(L)$ denotes the set of $L$-rational points of $X$. If
G is a group and a positive integer N, then \( G[N] \) denotes the N-torsion subgroup of G. Finally, if S is a finite set, then \( \#S \) denotes its cardinality.

**Definition 1.** Let \( C/k \) be a proper, smooth, and geometrically connected curve of genus g. We define the zeta function of \( C/k \) as the Euler product

\[
Z(T, C/k) := \prod_{v \in |C|} (1 - T^{d_v})^{-1}.
\]

This zeta function can also be expressed as rational function

\[
Z(T, C/k) = \frac{L(T, C/k)}{(1 - T)(1 - qT)},
\]

where \( L(T, C/k) \) is a polynomial in \( 1 + T \cdot \mathbb{Z}[T] \) of degree 2g (see [10] p.53, Theorem 5.9).

**Definition 2.** Let \( E/K \) be an elliptic curve. Consider inside the locus of bad reduction \( Z \subset C \) all closed points \( v \) according to their reduction types with respect to \( E/K \). We write \( M \), resp. \( M^{sp} \), resp. \( M^{ns} \), resp. \( A \), for the set of points of multiplicative reduction, resp. of split multiplicative reduction, resp. of nonsplit multiplicative reduction, resp. of additive reduction. If \( S \) is any of these above sets, we sometimes abuse notation and consider \( S \) as the divisor \( \sum_{v \in S} d_v \cdot v \) and in this case define \( \deg(S) = \sum_{v \in S} d_v \).

The following result is certainly known, but we could not find it in the literature. Compare with the proof of [11] p.132, Lemma 3.

**Lemma 10.** Let \( K_v \) be a field complete with respect to a non-Archimedean place \( v \) whose residue field \( k_v \) has characteristic \( p \geq 0 \). If \( E/K_v \) is an elliptic curve with additive reduction over \( v \), then, the prime-to-\( p \)-torsion subgroup of \( E(K_v) \) injects into the group \( \Phi_v(k_v) \).

**Proof.** See Lemma 29 in the Appendix, Section 6

2.1. Quadratic Twists. We now briefly recall the notion of quadratic twists of elliptic curves and state some of their properties. For more details, we refer the reader to [13] X.2 and X.5. Let \( (E/K, O_E) \) be an elliptic curve \( E \) defined over \( K \) together with a rational point \( O_E \in E(K) \).

**Definition 3.** A twist of the elliptic curve \( E/K \) is the data of a second elliptic curve \( E'/K \) together with an isomorphism of elliptic curves \( \phi : E'/K \to E/K \) (so that \( \phi \) sends \( O_{E'} \) to \( O_E \)). On the set \( T(E/K) \) of twists of the elliptic curve \( E/K \), we introduce the equivalence relation \( \sim_k \) that two twists are equivalent if they are \( K \)-isomorphic and denote by \( \text{Tw}(E/K) \) the resulting quotient set.

The set \( \text{Aut}(E) \) of \( K \)-automorphisms of the group structure of the elliptic curve \( E/K \) forms an abelian group (see [13] p.69]). One obtains a canonical set bijection (see [13] p.319, X.2.2(c) and X.2.3]) from \( \text{Tw}(E/K) \) to the cohomology group \( H^1(\text{Gal}(K/K), \text{Aut}(E)) \). Now, let

\[
n := \begin{cases} 
2 & \text{if } j(E) \neq 0, 1728, \\
4 & \text{if } j(E) = 1728, \\
6 & \text{if } j(E) = 0.
\end{cases}
\]

Then, there is a canonical isomorphism of \( \text{Gal}(K/K) \)-modules \( \mu_n \overset{\cong}{\to} \text{Aut}(E) \) (see [13] p.104, III.10.2]). As a consequence of Hilbert’s Theorem 90, we have a canonical group isomorphism \( K^x/K^{x_n} \overset{\cong}{\to} H^1(\text{Gal}(K/K), \mu_n) \) (see [13] p.420, Appendix B, Proposition 2.5 (c))]. Therefore, the set \( \text{Tw}(E/K) \) is canonically isomorphic to the set \( K^x/K^{x_n} \). In this paper, an elliptic curve \( E/K \) is assumed to have nonconstant \( j \)-invariant and so we are only concerned with the case \( n = 2 \). In this situation, if we choose a Weierstrass equation of the form \( y^2 = x^3 + ax + b \) for \( E/K \) and an element \( f \in K^x \), then by [13] p.343, X.5.4], a representative \( E_f/K \) of a class in \( \text{Tw}(E/K) \)
corresponding to \( f \mod K \times 2 \) has a Weierstrass equation of the form \( y^2 = x^3 + f^2 ax + f^3 b \). We call the elliptic curve \( E_f/K \) the quadratic twist of \( E/K \) by \( f \). When \( f = 1 \), the curve \( E_f/K \) is precisely the “original” elliptic curve \( E/K \). An immediate application of the definitions of discriminant of a Weierstrass equation and of \( j \)-invariant of an elliptic curve yields the following result.

**Lemma 11.** Let \( L \) be any field of characteristic different from 2 and 3. Let \( E/L \) be an elliptic curve, let \( f \in L^* \) and let \( E_f/L \) be the corresponding quadratic twist. Choose a Weierstrass equation of the form \( W : y^2 = x^3 + ax + b \) for \( E/L \) and let \( \Delta_W \) be its discriminant. The corresponding Weierstrass equation for \( E_f/L \) is \( W_f : y^2 = x^3 + f^2 ax + f^3 b \) and we denote by \( \Delta_{W_f} \) its discriminant. We have \( \Delta_{W_f} = f^6 \Delta_W \) and in particular \( j(E_f) = j(E) \).

2.2. *L*-Function of an Elliptic Curve. Finally, we define the \( L \)-function of an elliptic curve defined over a function field. Let \( C \) be a smooth, proper and geometrically connected curve defined over a finite field \( k \) of characteristic \( p \geq 5 \) of genus \( g \). Let \( K \) be the function field of \( C/k \) and let \( E/K \) be an elliptic curve. For each place \( v \) of \( K \), we define the following integer.

\[
(4) \quad a_v := \begin{cases} 
1 + q^{dv} - \#E_v(k_v) & \text{if } E/K \text{ has good reduction over } v, \\
-1 & \text{if } E/K \text{ has split multiplicative reduction over } v, \\
1 & \text{if } E/K \text{ has nonsplit multiplicative reduction over } v, \\
0 & \text{if } E/K \text{ has additive reduction over } v.
\end{cases}
\]

**Definition 4.** For each place \( v \) of \( K \), we define, following [12, p.381, 10.2(b)] the local exponent of the conductor at \( v \) to be the integer

\[
(5) \quad n_v = \begin{cases} 
0 & \text{if } E/K \text{ has good reduction over } v, \\
1 & \text{if } E/K \text{ has multiplicative reduction over } v, \\
2 & \text{if } E/K \text{ has additive reduction over } v.
\end{cases}
\]

The global conductor of \( E/K \) is the divisor \( N(E/K) := \sum_{v \in |C|} n_v[v] \). Its degree equals

\[
\deg N(E/K) = \sum_v n_v \deg(v) = \deg(M) + 2 \deg(A),
\]

where \( M \) and \( A \) respectively denote the divisors of places of \( K \) over which \( E/K \) has multiplicative and additive reduction.

**Definition 5.** Given a formal indeterminate \( T \), set

\[
(6) \quad L_v(T^{dv}, E/K) := \begin{cases} 
1 - a_v T^{dv} + q^{dv} T^{2dv} & \text{if } E/K \text{ has good reduction over } v, \\
1 - a_v T^{dv} & \text{if } E/K \text{ has bad reduction over } v.
\end{cases}
\]

We define \( L \)-function of \( E/K \) is defined to be the Euler product

\[
(7) \quad L(T, E/K) := \prod_{v \in |C|} L_v(T^{dv}, E/K)^{-1}.
\]

Now assume that the \( j \)-invariant of \( E/K \) is nonconstant. It follows from the work of Grothendieck, Deligne and others (see [5, p.11]) that \( L(T, E/K) \) is a polynomial in \( 1 + T \cdot \mathbb{Z}[T] \) and has degree [15, p.232, Theorem 9.3]

\[
(8) \quad d = 2(2g - 2) + \deg N(E/K).
\]

Moreover, the leading coefficient of \( L(T, E/K) \) is \( \varepsilon(E/K) q^d \), where \( \varepsilon(E/K) \) is the global root number of \( E/K \). For this paper, it suffices to know that \( \varepsilon(E/K) = 1 \) precisely when \( \text{rank}^{an}(E/K) \), the analytic rank of \( E/K \), i.e., the order of vanishing of \( L(T, E/K) \) at \( T = q^{-1} \), is even and otherwise \( \varepsilon(E/K) = -1 \).
3. Function Fields of Arbitrary Genus

We assume throughout this section the following context.

**Context 12.** Let \( C/k \) be a proper, smooth and geometrically connected curve of genus \( g \) defined over a finite field \( k \) of characteristic \( p \geq 5 \) and let \( K \) be its function field. Let \( f \in K^\times \setminus K^{\times 2} \) be a non-square element and let \( E/K \) be an elliptic curve with nonconstant \( j \)-invariant. Modulo \( K^{\times 2} \), the element \( f \) determines a unique quadratic extension \( K_f \) of \( K \) as well as a unique quadratic twist \( E_f/K \). Let \( \theta \in \overline{K} \) be such that \( \theta^2 = f \) and so that \( K_f = K(\theta) \). Given a place \( v \) of \( K \), we let \( f_v \) be the image of \( f \) via a chosen field injection \( K \hookrightarrow K_v \) and we let \( \theta_v \) be the image of \( \theta \) via the corresponding field injection \( K \hookrightarrow K_v \). This yields a \( K \)-embedding \( \tau : K_f \hookrightarrow \overline{K_v} \). By abuse of notation, let \( v \) be the canonical extension to \( K_v \) of the place \( v \) and let \( \overline{\tau} \) be the unique extension of the place \( v \) of \( K_v \) to \( \overline{K_v} \). Then we have an extension \( w = \overline{\tau} \circ \tau \) of \( v \) to \( K_f \). Since the map \( \tau \) is continuous, it extends uniquely to a continuous \( K \)-embedding \( \tau : K_f \hookrightarrow \overline{K_v} \) and since \( K_f/K \) is finite, then \( K_{f,w} \) is the completion of \( K_f \) at \( w \). One then sees that \( K_{f,w} \) is the compositum field \( K_fK_v \) \([9, \text{p.161, II.8}]\) and the latter equals \( K_v(\theta_v) \) by definition of composition of fields.

Let \( \{ C \}_{\text{split}} \) (resp. \( \{ C \}_{\text{inert}} \), resp. \( \{ C \}_{\text{ram}} \)) be the subset of places of \( K \) which are split (resp. inert, resp. ramified) in \( K_f \), so that \( \{ C \} = \{ C \}_{\text{split}} \cup \{ C \}_{\text{inert}} \cup \{ C \}_{\text{ram}} \) is a disjoint union. Define \( \{ C \}_{\text{unr}} \):= \( \{ C \}_{\text{split}} \cup \{ C \}_{\text{inert}} \) and if \( S \in \{ M_{\text{sp}}, M_{\text{ns}}, A \} \) and \( r \in \{ \text{inert, ram, split, unr} \} \), set \( S_r := S \cap \{ C \}_{r} \).

Also, write \( A_{\text{ram}}^{sp} \), respectively \( A_{\text{ram}}^{ns} \), respectively \( A_{\text{ram}}^{ed} \), for the places of \( K \) which are ramified in \( K_f \) and such that, with respect to the elliptic curve \( E/K \), are places of additive reduction which are more precisely potentially multiplicatively split, respectively potentially multiplicative nonsplit, respectively potentially good. Finally, let \( A_{\text{ram}}^m \) be the union \( A_{\text{ram}}^{sp} \cup A_{\text{ram}}^{ns} \) and let \( A_{\text{ram}}^o \) be the complement in \( A_{\text{ram}} \) of \( A_{\text{ram}}^{sp} \cup A_{\text{ram}}^{ed} \).

For \( f \in K^\times \setminus K^{\times 2} \) we decorate the corresponding sets as \( S_{r,f} \), \( A_{f,\text{ram}}^{sp} \), \( A_{f,\text{ram}}^{ns} \), \( A_{f,\text{ram}}^{ed} \), \( A_{f,\text{ram}}^m \) and \( A_{f,\text{ram}}^o \), when these sets refer to places whose reduction types are considered with respect to the quadratic twist \( E_f/K \).

**Remark 3.** We have \( \{ C \}_{\text{ram}} = \{ v \in \{ C \} : \text{ord}_v(f) \equiv 1 \text{ mod } 2 \} \).

**3.1. General Results.** The following lemma holds in general and we use it in Subsection 5.3.

**Lemma 13.** We have

\[
L(-1, C/k) = q^g L(-q^{-1}, C/k).
\]

In particular, if \( N \) is a positive integer such that \( q \equiv -1 \text{ mod } N \), then

\[
L(-1, C/k) \equiv (-1)^g \# \text{Jac}(C)(k) \text{ mod } N,
\]

where \( \# \text{Jac}(C)(k) \) is the number of \( k \)-rational points of the Jacobian of \( C/k \).

**Proof.** This follows directly from the functional equation \( L(T, C/k) = q^g T^{2g} L(q^{-1}T^{-1}, C/k) \) (see \([10, \text{p.54, Proof of Theorem 5.9}]\)).

The following result gives a formula for the degree of \( L(T, E_f/K) \) and also extend \([4, \text{p.134, Corollary 5.9}]\) to quadratic twists. Moreover, the degree of the \( L \)-function of \( E_f/K \) and the global root number of \( E_f/K \) are expressed in terms of the data of \( E/K \) and of the decomposition behaviour of the places of \( K \) in \( K_f \).

**Proposition 14.** Let \( k' \) be the field of constants of the quadratic extension \( K_f \) of \( K \).

(i) The degree of \( L(T, E_f/K) \) equals

\[
\deg(M_{\text{unr}}) + \deg(A_{\text{unr}}) \text{ if } [k': k] = 2,
\]

9
\[2(2g(C) - 2) + \sum_{v \in |C|} d_v + \deg(M_{unr}) + \deg(A_{unr}) - \deg(A_{ram}^g) \text{ if } [k' : k] = 1.\]

(ii) If \(E(K)\) has a subgroup of order \(N\) with \(N \geq 2\) an integer coprime with \(q\), then the global root number \(\varepsilon(E_f/K)\) satisfies
\[
\varepsilon(E_f/K) = \begin{cases} 
(1-\#M_{ram}^g+\#M_{inert}^\mathfrak{p})^{-\deg(A_{unr})} \mod N & \text{if } [k' : k] = 2, \\
(1-\#M_{ram}^g+\#M_{inert}^\mathfrak{p})^{-\deg(A_{unr})+\deg(A_{ram}^g)} \mod N & \text{if } [k' : k] = 1.
\end{cases}
\]

Proof. If \([k' : k] = 2\), then \(K_f\) is the compositum \(k'K\), the extension \(K_f/K\) is unramified and \(g(K_f) = g(K) = g(C)\) (see [14, p.114, Theorem 3.6.3 (a),(b)]).

Now assume that \(k' = k\). Since \(p \geq 5\), then the extension \(K_f/K\) is tamely ramified. It follows from Remark 3 and from the Riemann-Hurwitz formula that
\[
g(K_f) = 2g(K) - 1 + \frac{1}{2} \sum_{\ord_v(f) \equiv 1 \mod 2} d_v.
\]

Let \(U^f\), \(M^f\) and \(A^f\) be the divisors of places of \(K_f\) over which the elliptic curve \(E\) has respectively good, multiplicative and additive reduction. For any quadratic extension \(K_f/K\), we have \(L(T, E_f/K) = L(T, E/K)L(T, E_f/K)\).

(i) From Equation (8) it follows that
\[
\deg(L(T, E_f/K)) = \deg(L(T, E/Kf)) - \deg(L(T, E/K))
\]
\[
= 4(g(K_f) - g(K)) + \left(\deg(M^f) - \deg(M)\right)
\]
\[
+ 2\left(\deg(A^f) - \deg(A)\right).
\]

Observe that if \(v \in M_{inert} \cup A_{inert}\) has degree \(d_v\), then the degree of the place \(w \in M^f\) equals \(2d_v\). Moreover, if \(v \in A_{ram}^g\), then a place \(w\) of \(K_f\) lying over \(v\) belongs to \(|U^f|\).

Finally, recall that \(M_{unr} = M_{split} \cup M_{inert}\). Then,
\[
\deg(M^f) = \begin{cases} 
2\deg(M_{unr}) & \text{if } [k' : k] = 2, \\
2\deg(M_{unr}) + \deg(M_{ram}) & \text{if } [k' : k] = 1,
\end{cases}
\]
\[
\deg(A^f) = \begin{cases} 
2\deg(A_{unr}) & \text{if } [k' : k] = 2, \\
2\deg(A_{unr}) + \deg(A_{ram}^g) + \deg(A_{ram}^g) & \text{if } [k' : k] = 1.
\end{cases}
\]

Thus,
\[
\deg(M^f) - \deg(M) = \deg(M_{unr}) \text{ for any } [k' : k] \in \{1, 2\}, \text{ and}
\]
\[
\deg(A^f) - \deg(A) = \begin{cases} 
\deg(A_{unr}) & \text{if } [k' : k] = 2, \\
\deg(A_{unr}) - \deg(A_{ram}^g) & \text{if } [k' : k] = 1.
\end{cases}
\]

Therefore, \(\deg(L(T, E_f/K))\) equals
\[
\deg(M_{unr}) + \deg(A_{unr}) \text{ if } [k' : k] = 2,
\]
\[
2(2g(C) - 2) + \sum_{\ord_v(f) \equiv 1 \mod 2} d_v + \deg(M_{unr}) + \deg(A_{unr}) - \deg(A_{ram}^g) \text{ if } [k' : k] = 1.
\]
(ii) We have \( \varepsilon(E/K_f) = \varepsilon(E/K)\varepsilon(E_f/K) \). Since \( N \) divides \( \#E(K) \), then \( N \) also divides \( E(K_f) \). Therefore, from [1] p.134, Corollary 5 we have
\[
\varepsilon(E/K_f) \equiv (-1)^{\#M_{sp}^f} q^{-\deg(A^f)} \mod N \quad \text{and} \quad \varepsilon(E/K) \equiv (-1)^{\#M_{sp}^f} q^{-\deg(A)} \mod N.
\]
Moreover, observe that \( \#M_{sp}^f = 2\#M_{sp} + \#M_{nsp} \). Therefore,
\[
\varepsilon(E_f/K) \equiv (-1)^{\#M_{sp}^f - \#M_{sp}^f - \deg(A) - \deg(A^f)} \mod N
\]
\[
\equiv \begin{cases} 
(-1)^{\#M_{sp}^f + \#M_{ns}^f} q^{-\deg(A_{unr})} \mod N & \text{if } [k' : k] = 2, \\
(-1)^{\#M_{sp}^f + \#M_{ns}^f} q^{-\deg(A_{unr}) + \deg(A_{ram}^f)} \mod N & \text{if } [k' : k] = 1.
\end{cases}
\]
\( \square \)

The following lemma is needed in our proofs of Theorem 16 and Theorem 20. It is certainly known but we could not find it in the literature. We refer the reader to Lemma 30 in the Appendix, Section 6 for our proof of the result.

**Lemma 15.** The reduction types of \( E/K \) and of \( E_f/K \) are related as follows.

(a) If \( v \in \mathbb{C} \backslash \mathbb{U} \),

(a1) then \( v \in U \cap U_f \) or \( v \in M \cap M_f \) or \( v \in A \cap A_f \).

(a2) Moreover, if \( v \in M \), then \( v \in M_{sp} \cap M_{sp}^f \) or \( M_{ns} \cap M_{ns}^f \) and only if \( v \in M_{split} \).

(b) If \( v \in \mathbb{C} \backslash \mathbb{U} \), then

| \( E/K \) | \( U \) \( | \) | \( M \) \( | \) | \( A_{sp}^d \) \( | \) | \( A_{ram}^m \) \( | \) | \( A_{ram}\) | \( A_{ram}^d \) | \( | \) |
|---|---|---|---|---|---|---|---|---|
| \( E_f/K \) | \( A_{sp}^d \) \( | \) | \( A_{ram}^m \) \( | \) | \( U_f \) \( | \) | \( M_{f,ram} \) \( | \) | \( A_{f,ram}^m \) | \( A_{f,ram}^d \) |

**Table 4. Reduction Types After Ramified Twist**

**Definition 6.** Given \( f \in K^\times \backslash K^{\times 2} \), we let \( \chi \) be the quadratic character associated to the quadratic extension \( K_f/K \). For each place \( v \) of \( K \), set
\[
L_v(T^{dv}, \chi) := \begin{cases} 
1 - T^{dv} & \text{if } v \in \mathbb{C} \backslash \mathbb{U}, \\
1 + T^{dv} & \text{if } v \in \mathbb{C} \backslash \mathbb{U}, \\
1 & \text{if } v \in \mathbb{C} \backslash \mathbb{U}.
\end{cases}
\]

The Artin L-function of \( \chi \) is the formal Euler product
\[
L(T, \chi) := \prod_{v \in \mathbb{C} \backslash \mathbb{U}} L_v(T^{dv}, \chi)^{-1}.
\]

Suppose that \( E(K) \) contains a subgroup of order \( N \geq 2 \) with \( N \) coprime with \( q \). Under this assumption, our first main result gives an explicit formula for \( L(T, E_f/K) \) modulo \( N \).

**Theorem 16.** If \( E(K) \) contains a subgroup \( T \) of order \( N \geq 2 \) with \( N \) coprime with \( q \), then
\[
L(T, E_f/K) \equiv L(T, \chi)L(qT, \chi) \times R(T) \times \gamma_{ram} \mod N,
\]
where
\[
R(T) \equiv \begin{cases} 
\prod_{v \in M_{unr}^{sp}} (1 + \alpha_v q^{dv} T^{dv}) \times \prod_{v \in M_{unr}^{ns}} \frac{(1 + \alpha_v q^{dv} T^{dv})(1 + \alpha_v q^{dv} T^{dv})}{(1 - \alpha_v T^{dv})(1 - \alpha_v T^{dv})} & \text{if } N \geq 5, \\
\prod_{v \in M_{unr}^{sp}} (1 + \alpha_v q^{dv} T^{dv}) \times \prod_{v \in M_{unr}^{ns}} \frac{(1 + \alpha_v q^{dv} T^{dv})}{1 - \alpha_v T^{dv}} & \text{if } N \in \{2, 3, 4\},
\end{cases}
\]

11
with
\[ \alpha_v = \begin{cases} 
1 & \text{if } v \in M_{\text{inert}} \cup A_{\text{inert}}, \\
-1 & \text{if } v \in M_{\text{split}} \cup A_{\text{split}},
\end{cases} \]
and \( \gamma_{\text{ram}} = 1 \) if \( N \geq 5 \) and
\[
\gamma_{\text{ram}} = \prod_{v \in A_{\text{ram}}^{\text{sp}}} (1 - T_{d v})^{-1} \times \prod_{v \in A_{\text{ram}}^{\text{ns}}} (1 + T_{d v})^{-1} \times \prod_{v \in A_{\text{ram}}^{\text{gd}}} (1 - T_{d v})^{-1} (1 + T_{d v})^{-1}
\]
if \( N \in \{2, 3, 4\} \). More precisely, for \( N \in \{2, 3, 4\} \) the possible Kodaira symbols of additive reduction with respect to \( E/K_v \) which contribute to \( L(T, E_f/K) \mod N \) are as follows.

| \( N \) | \( A_{\text{unr}} \) | \( A_{\text{ram}} \) |
|-------|---------|---------|
| 2     | \( \text{III}, \text{III}^*, I_n^* \), \( n \geq 0 \) | \( I_n^*, n \geq 0 \) |
| 3     | \( \text{IV}, \text{IV}^* \) | \( I_n^*, n \geq 0 \) |
| 4     | \( I_n^*, n \geq 0 \) | \( I_n^*, n \geq 0 \) |

Table 5. Kodaira Symbols of Additive Reduction Contributing to \( L(T, E_f/K) \mod N \)

Before proving Theorem 16, we recall and prove the following useful lemma.

**Lemma 17.** Let \( K_v \) be a complete field with respect to some non-Archimedean valuation and with finite residue field of characteristic \( p \). Let \( E/K_v \) be an elliptic curve with additive reduction and let \( T \) be a torsion subgroup of \( E(K_v) \) of order prime to \( p \). Then \( T \) has order at most 4. If it has order at least 2, then we have the following classification.

| \( \text{Isomorphism Type of } T \) | Possible Kodaira Symbols |
|-------------------------------|--------------------------|
| \( \mathbb{Z}/2\mathbb{Z} \)   | \( \text{III}, \text{III}^*, I_n^* \) with \( n \geq 0 \), \( I_{m,2}^* \) with \( m \geq 0 \) |
| \( \mathbb{Z}/3\mathbb{Z} \)   | \( \text{IV}, \text{IV}^* \) |
| \( \mathbb{Z}/4\mathbb{Z} \)   | \( I_{2n+1}, \text{ with } n \geq 1 \) |
| \( (\mathbb{Z}/2\mathbb{Z})^2 \) | \( I_{2n}^*, \text{ with } n \geq 0 \) |

Table 6. Local Torsion and Possible Additive Kodaira Symbols

**Remark 4.** In the notation of [6, p.497, 10.2.24], the symbol \( I_{m,2}^*, m \geq 0 \) is the Kodaira symbol \( I_n^*, m \geq 0 \) where the special fiber of the corresponding minimal model only has 2 irreducible components of multiplicity 1 defined over the residue field \( k_v \).

**Proof.** (of Lemma 17) By Lemma 10, the prime-to-\( p \) torsion of \( E(K_v) \) injects into \( \Phi_v(k_v) \). The first part of the statement follows from the fact that \( T \) is then identified with a subgroup \( \Phi_v(k_v) \) and the latter has order at most 4 (see [12, p.362, IV.9.2(d)]). To show the second part of the statement, we obtain the following classification for the isomorphism type of the group \( \Phi_v(k_v) \), based on the tables in [6, p.497, 10.2.24].

Finally, in order to include \( I_n^* \) with \( n \geq 0 \), where \( \Phi_v(k_v) = \Phi_v(\overline{k_v}) \), as possible Kodaira symbols for which \( T \) is isomorphic to \( \mathbb{Z}/2\mathbb{Z} \), we observe that the groups \( \mathbb{Z}/4\mathbb{Z} \) and \( (\mathbb{Z}/2\mathbb{Z})^2 \) have subgroups of order 2. \( \square \)
| Isomorphism Type of $\Phi_{v}(k_{v})$ | Possible Kodaira Symbols |
|-----------------------------------|---------------------------|
| $\mathbb{Z}/2\mathbb{Z}$          | $III, III^{s}, I_{m}^{s}, m \geq 0$ |
| $\mathbb{Z}/3\mathbb{Z}$          | $IV, IV^{s}$               |
| $\mathbb{Z}/4\mathbb{Z}$          | $I_{2n+1}$ with $n \geq 1$ |
| $(\mathbb{Z}/2\mathbb{Z})^{2}$   | $I_{2n}$ with $n \geq 0$   |

Table 7. Possible Kodaira Symbols for a Local Component Group of Additive Reduction

Proof. (of Theorem 16) The idea of the proof is as follows. We consider the quotient

$$
\frac{L(T, E_{f}/K)}{L(T, \chi)L(qT, \chi)} = \prod_{v \in |C|} \frac{L_{v}(T^{d_{w}}, \chi)L_{v}(q^{d_{w}}T^{d_{w}}, \chi)}{L_{v}(T^{d_{w}}, E_{f}/K)} \mod N
$$

and analyze the ratios of Euler factors according to the subsets $| C |_{\text{split}}, | C |_{\text{inert}}, | C |_{\text{ram}}$ of $| C |$.

We now prove the result. Using Lemma 15, we obtain $L_{v}(T^{d_{w}}, E_{f}/K)$ in terms of the reduction type of $E/K$ over $v \in | C |$.

First suppose that $v \in | C |_{\text{split}}$. Then, we obtain the following table.

| Reduction type of $E/K_{v}$ | $L_{v}(T^{d_{w}}, E_{f}/K) \mod N$ | $\frac{L_{v}(T^{d_{w}}, \chi)L_{v}(q^{d_{w}}T^{d_{w}}, \chi)}{L_{v}(T^{d_{w}}, E_{f}/K)} \mod N$ |
|-----------------------------|-----------------------------------|--------------------------------------------------------------------------------|
| $U_{\text{split}}$         | $(1 - T^{d_{w}})(1 - q^{d_{w}}T^{d_{w}})$ | $1$                                                                             |
| $M_{\text{split}}^{\text{sp}}$ | $1 - T^{d_{w}}$                  | $1 - q^{d_{w}}T^{d_{w}}$                                                         |
| $M_{\text{split}}^{\text{ns}}$ | $1 + T^{d_{w}}$                 | $(1 - T^{d_{w}})(1 - q^{d_{w}}T^{d_{w}})$                                       |
| $A_{\text{split}}$            | $1$                              | $(1 - T^{d_{w}})(1 - q^{d_{w}}T^{d_{w}})$                                       |

Table 8. Ratio of Euler Factors When the Place Splits in $K_{f}$

Second suppose that $v \in | C |_{\text{inert}}$. Then, we obtain the following table.

| Reduction type of $E/K_{v}$ | $L_{v}(T^{d_{w}}, E_{f}/K) \mod N$ | $\frac{L_{v}(T^{d_{w}}, \chi)L_{v}(q^{d_{w}}T^{d_{w}}, \chi)}{L_{v}(T^{d_{w}}, E_{f}/K)} \mod N$ |
|-----------------------------|-----------------------------------|--------------------------------------------------------------------------------|
| $U_{\text{inert}}$         | $(1 - T^{d_{w}})(1 - q^{d_{w}}T^{d_{w}})$ | $1$                                                                             |
| $M_{\text{inert}}^{\text{sp}}$ | $(1 + T^{d_{w}})$                | $1 + q^{d_{w}}T^{d_{w}}$                                                         |
| $M_{\text{inert}}^{\text{ns}}$ | $(1 - T^{d_{w}})$                 | $(1 + T^{d_{w}})(1 + q^{d_{w}}T^{d_{w}})$                                       |
| $A_{\text{inert}}$            | $1$                              | $(1 + T^{d_{w}})(1 + q^{d_{w}}T^{d_{w}})$                                       |

Table 9. Ratio of Euler Factors When the Place is Inert in $K_{f}$

Third suppose that $v \in | C |_{\text{ram}}$. In this case, $L_{v}(T^{d_{w}}, \chi)L_{v}(q^{d_{w}}T^{d_{w}}, \chi) = 1$. Then, we obtain the following table.

Only the last line of Table 10 requires a justification. Suppose that $E/K$ has additive potentially good reduction over $v$. Then, $E_{f}/K$ has good reduction over $v$ and by the theorem of semistable reduction, $E_{f}/K_{f}$ has good reduction over the place $w$ of $K_{f}$ lying above $v$. Since $E$ and $E_{f}$ are isomorphic over $K_{f}$, then $E_{f}(K_{f})[N] = E(K_{f})[N]$. Moreover, we have $E(K_{f})[N] \supset E(K)[N] \neq \{O\}$ by assumption and so $L_{w}(T^{d_{w}}, E_{f}/K_{f}) \equiv (1 - T^{d_{w}})(1 - q^{d_{w}}T^{d_{w}}) \mod N$ by \[ p.132, Lemma 3\]. Since $v$ ramifies in $K_{f}$, then $d_{w} = d_{v}$. Therefore, $\#E_{f,v}(k_{w}) = \#E_{w}(k_{w})$ and so $L_{v}(T^{d_{w}}, E_{f}/K) \equiv (1 - T^{d_{w}})(1 - q^{d_{w}}T^{d_{w}}) \mod N$.

Now, $E(K)$ has a subgroup $T$ of order $N \geq 2$ with $N$ coprime to $q$. For each place $v$ of $K$, $E(K)$ injects into $E(K_{v})$ and so does $T$. If $v$ is a place of additive reduction, then by Lemma 17.
Reduction type of $E/K_v$ & $L_v(T^d_v, E_f/K) \bmod N$ & $\frac{L_v(T^d_v, \chi)L_v(q^d_v T^d_v, \chi)}{L_v(T^d_v, E_f/K)} \bmod N$ & \\
| $U_{\text{ram}}$ & 1 & 1 & \\
| $M_{\text{ram}}$ & 1 & 1 & \\
| $A_{\text{ram}}$ & 1 & 1 & \\
| $A_{\text{ram}}^p$ & $(1 - T^d_v)^{-1}$ & $(1 - T^d_v)$ & \\
| $A_{\text{ram}}^{\psi}$ & $(1 + T^d_v)^{-1}$ & $(1 + T^d_v)^{-1}$ & \\
| $A_{\text{ram}}^d$ & $(1 - T^d_v)(1 + q^d_v T^d_v)$ & $(1 - T^d_v)^{-1}(1 + q^d_v T^d_v)^{-1}$ & \\

Table 10. Ratio of Euler Factors When the Place Ramifies in $K_f$

$\mathcal{T}$ has order at most 4. In particular, for $N \geq 5$, the elliptic curve $E/K$ has no place of additive reduction. Therefore, for $N \geq 5$ we ignore the rows regarding places of additive reduction in the previous tables.

The following corollary of Theorem 16 is a more precise version of [4, p.133, Theorem 4] in the case $N = 2$. More precisely, we note that places of additive reduction for $E_f/K$ which ramify in $K_f$ do not contribute to the reduction $L(T, E_f/K) \bmod 2$.

Corollary 18 (of Theorem 16). If $E(K)$ has nontrivial 2-torsion, then

$$L(T, E_f/K) \equiv Z(T, C/k)^2 \times \prod_{v \in M_f} (1 - T^d_v) \times \prod_{v \in A_{f,\text{anr}}} (1 - T^d_v)^2 \bmod 2.$$

Proof. Since $q$ is odd, it is congruent to 1 modulo 2. Moreover, $-1 \equiv 1 \bmod 2$ and so we do not distinguish between split and nonsplit multiplicative reduction modulo 2.

First, suppose that $v \in |C|_{\text{split}}$. Then, we obtain the following table.

| Reduction type of $E/K_v$ | $L_v(T^d_v, E_f/K) \bmod 2$ | $\frac{L_v(T^d_v, \chi)L_v(q^d_v T^d_v, \chi)}{L_v(T^d_v, E_f/K)} \bmod 2$ & \\
| $U|_{\text{split}}$ & 1 & 1 & \\
| $M_{\text{split}}$ & 1 & $1 - T^d_v$ & \\
| $A_{\text{split}}$ & $(1 - T^d_v)^2$ & $(1 - T^d_v)^2$ & \\

Table 11. Ratio Modulo 2 When the Place Splits in $K_f$

Second, suppose that $v \in |C|_{\text{inert}}$. Then, we obtain the following table.

| Reduction type of $E/K_v$ | $L_v(T^d_v, E_f/K) \bmod 2$ | $\frac{L_v(T^d_v, \chi)L_v(q^d_v T^d_v, \chi)}{L_v(T^d_v, E_f/K)} \bmod 2$ & \\
| $U|_{\text{inert}}$ & 1 & 1 & \\
| $M_{\text{inert}}$ & 1 & $1 - T^d_v$ & \\
| $A_{\text{inert}}$ & $(1 - T^d_v)^2$ & $(1 - T^d_v)^2$ & \\

Table 12. Ratio Modulo 2 When the Place is Inert in $K_f$

Third, suppose that $v \in |C|_{\text{ram}}$. Then, we obtain the following table.

Therefore,

$$\frac{L(T, E_f/K)}{L(T, \chi)L(q T, \chi)} \equiv \prod_{v \in M_{\text{anr}}} (1 - T^d_v) \times \prod_{v \in A_{\text{anr}}} (1 - T^d_v)^2 \times \prod_{v \in A_{\text{ram}}^{\psi}} (1 - T^d_v)^{-1} \times \prod_{v \in A_{\text{ram}}^{\psi}} (1 - T^d_v)^{-2} \bmod 2.$$
The ratio of Euler products modulo 2 is congruent to the product of the ratios modulo 2 of Euler products modulo 2.

**Proof.** See Lemma 31. □

**Lemma 19.** For each \( v \in |U|_{\text{unr}}=|U| \cap |U_f| \), we have \( a_v + a_{f,v} \equiv 0 \mod 2 \), where \( a_v \) and \( a_{f,v} \) are defined in Equation (4).

**Proof.** See Lemma 31. □

Let \( f_1, f_2 \in K^\times \) and let \( E_{f_1}/K \) and \( E_{f_2}/K \) be the corresponding quadratic twists of \( E/K \). Since \( E/K \) has nonconstant \( j \)-invariant \( j(E) \), then \( L(T, E/K) \in 1 + T \cdot Z[T] \) (see [5, p.11]). Since \( j(E) = j(E_{f_i}) \) for \( i \in \{1,2\} \) by Lemma 11, then \( L(T, E_{f_i}/K) \in 1 + T \cdot Z[T] \) for \( i \in \{1,2\} \). Therefore, \( L(T, E_{f_1}/K)/L(T, E_{f_2}/K) \in 1 + T \cdot Z[T] \) and the expression \( L(T, E_{f_1}/K)/L(T, E_{f_2}/K) \mod 2 \) is a well-defined element of \( 1 + T \cdot (Z/2Z)[T] \). In the second main result of this paper, we write explicitly the reduction modulo 2 of this quotient.

**Theorem 20.** Let \( f_1, f_2 \in K^\times \) and let

\[
U_{f_1,f_2} := (|U|_{f_1} \cap |U|_{f_2} ) \cup (M_{f_1} \cap M_{f_2}) \cup (A_{f_1} \cap A_{f_2}).
\]

Then,

\[
\frac{L(T, E_{f_1}/K)}{L(T, E_{f_2}/K)} \equiv \prod_{v \in U_{f_1,f_2}} \frac{L_v(T^{d_v}, E_{f_1}/K)}{L_v(T^{d_v}, E_{f_2}/K)} \mod 2.
\]

**Proof.** The ratio of Euler products modulo 2 is congruent to the product of the ratios modulo 2 of the Euler factors:

\[
\frac{L(T, E_{f_1}/K)}{L(T, E_{f_2}/K)} \equiv \prod_v \frac{L_v(T^{d_v}, E_{f_1}/K)}{L_v(T^{d_v}, E_{f_2}/K)} \mod 2.
\]

We show that if \( v \in U_{f_1,f_2} \), then \( L_v(T, E_{f_1}/K) \equiv L_v(T, E_{f_2}/K) \mod 2 \). If \( v \in A_{f_1} \cap A_{f_2} \), then the Euler factor is \( L_v(T, E_{f_i}/K) = 1 \) for \( i \in \{1,2\} \). Now, we can assume that \( f_1 = f \) and \( f_2 = 1 \).

Note that \( M \cap M_f = M_{\text{unr}} \) and \( |U| \cap |U_f| = |U|_{\text{unr}} \) by Lemma 15 (a1). If \( v \in M \cap M_f \), then by Lemma 19 (a2), we have \( L_v(T, E_{f}/K) \equiv L_v(T, E/K) \mod 2 \). Finally, if \( v \in |U| \cap |U_f| \), then by Lemma 19 we have \( a_v + a_{f,v} \equiv 0 \mod 2 \) and then from Equation (4) it follows that \( L_v(T, E_{f}/K) \equiv L_v(T, E/K) \mod 2 \). □

### Table 13. Ratio Modulo 2 When the Place Ramifies in \( K_f \)

| Reduction type of \( E/K_f \) | \( \frac{L_v(T^{d_v}, E_{f_1}/K)}{L_v(T^{d_v}, E_{f_2}/K)} \mod 2 \) |
|-------------------------------|---------------------------------|
| \( U \cap M_{f_1} \cap M_{f_2} \) | \( 1 \) |
| \( M_{f_1} \cap M_{f_2} \) | \( 1 \) |
| \( A_{f_1} \cap A_{f_2} \) | \( (1 - T^{d_v})^{-1} \) |
| \( A_{f_1} \cap A_{f_2} \) | \( (1 - T^{d_v})^{-2} \) |

Observe that \( L(T, \chi) \equiv Z(T, C/k) \times \prod_{v \in |C|_{\text{ram}}} (1 - T^{d_v}) \mod 2 \). Hence,

\[
L(T, E_{f_1}/K) \equiv Z(T, C/k)^2 \times \prod_{v \in A_{f_1}} (1 - T^{d_v})
\]

\[
\times \prod_{v \in M_{\text{unr}}} (1 - T^{d_v}) \times \prod_{v \in A_{\text{unr}}} (1 - T^{d_v})^2
\]

\[
\equiv Z(T, C/k)^2 \times \prod_{v \in M_f} (1 - T^{d_v}) \times \prod_{v \in A_{f,\text{unr}}} (1 - T^{d_v})^2 \mod 2.
\]
4. Function Fields of Genus 0

In this section, we illustrate some simplifications that occur in the statements of Theorems 16 and 20 when the curve \( C/k \) has genus 0. For simplicity, we restrict ourselves to the following context.

**Context 21.** Let \( K := k(t) \) be a rational function field and let \( E/K \) be an elliptic curve with non-constant \( j \)-invariant, semistable reduction and in particular either good or multiplicative reduction over \( \infty \). Suppose that over the affine plane \( \mathbb{P}^1_k \setminus \{\infty\} \), \( E/K \) is given by a minimal Weierstrass equation of the form \( y^2 = u(x) \), with \( u(x) := x^3 + ax + b \) irreducible in \( K[x] \) and \( a, b \in k[t] \). Let \( \Delta \) be the discriminant of this Weierstrass equation, which is also the discriminant of the cubic polynomial \( u(x) \). Finally, we let \( f \in k[t] \) be a monic square-free polynomial of degree \( d_f \) and let \( S \) be the set of distinct monic irreducible polynomials in \( k[t] \) dividing \( f \).

To ease the exposition, if \( K' \) is the function field of a curve \( C'/k' \) over a finite field \( k' \), we write \( Z(T, K') \) for the zeta function \( Z(T, C'/k') \). Let us first examine Theorem 16 in this context. For \( i \in \{0, 1\} \), let \( L(q^iT, K_f) \) be the numerator of the zeta function \( Z(q^iT, K_f) \) (see Definition 1).

**Proposition 22.** The following holds.

(i) We have the identity \( L(T, \chi)L(qT, \chi) = L(T, K_f)L(qT, K_f) \).

(ii) The set \( \{ v \in k[t] \setminus S \text{ monic irreducible} : x^2 - f \in k(t)[x] \text{ has a root in } k[t]/(v) \} \)
and the set \( \{ v \in k[t] \setminus S \text{ monic irreducible} : x^2 - f \in k(t)[x] \text{ has no roots in } k[t]/(v) \} \)

(iii) The set \( \{ v \in k[t] \setminus S \text{ monic irreducible} : x^2 - f \in k(t)[x] \text{ has a root in } k[t]/(v) \} \)
and the set \( \{ v \in k[t] \setminus S \text{ monic irreducible} : x^2 - f \in k(t)[x] \text{ has no roots in } k[t]/(v) \} \).

(iv) If \( d_f \) is even, then \( \infty \in C \text{ inert} \). If \( d_f \) is odd, then \( \infty \in C \text{ ram} \cap A_{f, \text{ram}} \).

**Proof.**

(i) Since the curve \( C/k \) has genus 0, the numerator of its zeta function equals 1. Moreover, for \( i \in \{0, 1\} \) the denominators of \( Z(q^iT, K) \) and \( Z(q^iT, K_f) \) are both equal to \( (1 - q^iT)(1 - q^{1+iT}) \). Therefore, the identity \( Z(q^iT, K_f) = Z(q^iT, K)L(q^iT, \chi) \) (see [9, p.524, (10.5) Corollary]) simplifies to \( L(q^iT, \chi) = L(q^iT, K_f) \).

(ii) A finite place of \( K \) corresponds to a monic irreducible polynomial in \( k[t] \). Let \( v \) be a finite place \( K \) which is unramified in \( K_f \). By the Dedekind-Kummer theorem (see [9] I.3.8, pp.47-48), \( v \) splits (resp. is inert) in \( K_f \) if and only if the polynomial \( x^2 - f \) has a root (resp. no roots) in the residue field \( k_v = k[t]/(v) \).

(iii) A finite place \( v \) of \( K \) which is ramified in \( K_f \) is characterized by the fact that \( \text{ord}_v(f) \) is odd. The valuation \( \text{ord}_v(f) \) is positive (and in fact equals 1) precisely for the finite places \( v \) which correspond to monic irreducible polynomials dividing \( f \).

(iv) The place at infinity \( \infty \) of \( k(t) \) corresponds to the maximal ideal \( (s) \) of \( k[s] \) if we set \( s := 1/t \). Let \( w_\infty \) be a place of \( K_f \) lying over the place \( \infty \). Then \( \text{ord}_{w_\infty}(f(t)) = \frac{2}{\gcd(d_f, 2)} \text{ord}_{1/t}(f(t)) \)
with \( 2/\gcd(d_f, 2) \) being the ramification index \( e(w_\infty | \infty) \) (see [14, p.125, Example 3.7.6]). So if \( d_f \) is even, then \( \infty \) is unramified in \( K_f \), while if \( d_f \) is odd, then \( t = \infty \) ramifies in \( K_f \) and by Lemma 15 (b) it becomes a place of additive reduction for \( E_f/K \).

We now consider Theorem 20 in Context 21.
Corollary 23 (of Theorem \textsuperscript{20}). We have
\[
\frac{L(T, E_f/K)}{L(T, E/K)} \equiv (1 - a_\infty T + T^2)^{\varepsilon_U} (1 - T)^{\varepsilon_M} \times \prod_{v \mid f} \left( \prod_{v \in U} (1 - a_v T^{d_v} + T^{2d_v}) \times \prod_{v \in M} (1 - T^{d_v}) \right) \pmod{2},
\]
where \((\varepsilon_U, \varepsilon_M) = \begin{cases} (0, 0) & \text{if } \deg(f) \text{ is even, } \\ (1, 0) & \text{if } \deg(f) \text{ is odd and } \infty \in |U|, \\ (0, 1) & \text{if } \deg(f) \text{ is odd and } \infty \in M. \end{cases}\)

In particular, the degree of \(L(T, E_f/K)\) is equal to
\[
\deg L(T, E_f/K) = 2\varepsilon_U + \varepsilon_M + \sum_{v \mid f} \left( 2 \sum_{v \in U} d_v + \sum_{v \in M} d_v \right) + \deg(M) + 2\deg(A) - 4.
\]

Proof. This follows directly from Theorem \textsuperscript{20} with \(f_1 = f, f_2 = 1\) and the following observations. If \(v \in U \cup M\) is a finite place which divides \(f\), then \(v \in A_f\) by Lemma \textsuperscript{15} (b). If \(d_f\) is odd, then \(\infty \in A_f\) as we just observed. Otherwise, a place of \(K\) which is unramified in \(K_f\) has the same reduction type before and after twisting by \(f\) by Lemma \textsuperscript{15} (a). The formula for the degree of \(L(T, E_f/K)\) follows immediately from the expression of \(L(T, E_f/K) \pmod{2}\) and Equation (8). \(\square\)

5. Applications

In this section, we discuss different applications of our results of Section \textsuperscript{3} and Section \textsuperscript{4}. In particular, we prove our third main theorem (see Theorem \textsuperscript{28}).

5.1. Remark on Computational Effort. Let \(E/k(t)\) be an elliptic curve with nonconstant \(j\)-invariant and \(L(T, E/k(t)) = 1\). If \(f \in k[t]\) is a monic irreducible polynomial of even degree \(d_f\) and coprime with \(\Delta\), then \(\deg L(T, E_f/K) = 2d_f\). Our goal is to compare the relative costs of computing \(L(T, E_f/K) \pmod{2}\) using Corollary \textsuperscript{23} and using the algorithm presented in \textsuperscript{11}. To avoid any ambiguity, let \(w\) denote the place corresponding to \(f\). In this case, Corollary \textsuperscript{23} gives
\[
L(T, E_f/K) \equiv 1 - a_w T^{d_f} + T^{2d_f} \pmod{2}.
\]

We need to compute the single term \(a_w \pmod{2}\). To do this, we can proceed as follows. Since \(f\) is coprime with \(\Delta\), then \(w \notin |U|\). The Weierstrass equation \(y^2 = x^3 - 27c_4 x - 54c_6\) that we gave above is minimal for the place \(w\). Let \(y^2 = x^3 - (27c_4 \mod \pi_w)x - (54c_6 \mod \pi_w)\) be the corresponding Weierstrass equation for the reduced elliptic curve \(E_w/k_w\). Since \(q\) is odd, then
\[
a_w = 1 + q^{d_f} - \#E_w(k_w) \equiv \#E_w(k_w) \pmod{2}.
\]

A non-identity point of order 2 in \(E_w(k_w)[2]\), if it exists, is of the form \((\alpha, 0)\), where \(\alpha \in k_w\) is a root of \(x^3 - (27c_4 \mod \pi_w)x - (54c_6 \mod \pi_w)\). Therefore, \(x^3 - (27c_4 \mod \pi_w)x - (54c_6 \mod \pi_w)\) is irreducible in \(k_w[x]\) if and only if \(a_w \equiv 1 \pmod{2}\).

Alternatively, we can adapt the algorithm of Baig and Hall (see \textsuperscript{11} pp.364-365)) to compute \(L(T, E_f/K) \pmod{2}\) as follows. One can write \(L(T, E_f/K) = \sum_{n=0}^{2d_f} c_n T^n\) with \(c_0 = 1\) and, for \(1 \leq n \leq 2d_f\), the coefficient \(c_n\) satisfies the recurrence relation (see \textsuperscript{11} pp.364-365, Lemma 2.2))
\[
c_n = \frac{1}{n} \sum_{m=1}^{n} b_m \cdot c_{n-m},
\]
where
\[ b_m = \sum_{v \in |U_f|_{d_v}|} d_v \cdot a_{v^m/d_v} + \sum_{v \in M_{f}^{sp}\ \text{d.c.}} d_v + \sum_{v \in M_{f}^{sp}\ \text{d.c.}} (-1)^{md_v} d_v, \]

with the meaning, as mentioned earlier, that the subscript \( f \) refers to the sets of places of \( K \) over which \( E_f \) has good, resp. split multiplicative, resp. nonsplit multiplicative reduction. The amount of effort to compute \( L(T, E_f/K) \mod 2 \) using this algorithm is bounded below by the computation, for each \( 1 \leq n \leq 2df \), of \( a_{v^m/d_v} \mod 2 \), for \( 1 \leq m \leq n \) and \( d_v \mid m \), where \( v \in |U_f| \). One can use the functional equation to roughly cut the number of computations in half (see [1, p.365]):

\[ c_n = \varepsilon(E_f/K)q^{2n-2df}c_{2df-n}, \ 0 \leq n \leq 2df. \]

For each degree \( d_v \), there are \( \frac{1}{d_v} \sum_{d \mid d_v} \mu(d_v) d \cdot q^{d} \) monic irreducible polynomials of degree \( d_v \) over the finite field \( k_v \) with \( q^d \) elements (see [3, pp.567-568, Chapter 14]), where \( \mu \) is the Möbius function. Most of these polynomials correspond to places of good reduction for \( E_f/K \) and we roughly need to compute half of the quantities of the form \( a_{v^m/d_v} \mod 2 \) that appears in the formulas for the \( b_m \)'s. Our formula is therefore clearly more efficient to compute \( L(T, E_f/K) \mod 2 \) than the algorithm in [1].

5.2. Computing \( L \)-Functions of Elliptic Curves à la Schoof. In this subsection, we discuss a general strategy to compute polynomial \( L \)-functions of elliptic curves. Our strategy is motivated by Schoof’s algorithm which computes zeta functions of elliptic curves over finite fields. We also prove the elementary Proposition 24 on elliptic curves of odd analytic rank that could improve our approach. We illustrate this strategy in Proposition 26 and in Proposition 27 by computing some degree 2 \( L \)-functions using Theorem 10, Theorem 16, Corollary 23 and Proposition 24.

Recall from Subsection 2.2 that the \( L \)-function of \( E/K \) is a polynomial \( L(T, E/K) = \sum_{n=0}^{d} a_n T^n \) in \( 1 + T \cdot Z[T] \) of degree \( d = 2g(C) - 2 + \deg(M) + 2 \deg(A) \) and the leading coefficient \( \varepsilon(E/K)q^{d} \). We can write \( L(T, E/K) = \prod_{i=1}^{d} (1 - \alpha_i T) \) as product of its reciprocal roots \( \alpha_1, \ldots, \alpha_d \). The reciprocal roots are algebraic integers which satisfy \( | \alpha_i | = q_i \), for each \( 1 \leq i \leq d \) and each complex embedding (see [15, p.267, Theorem 2.2.1]). Using this fact and expressing the coefficients of \( L(T, E/K) \) as symmetric polynomials in the \( \alpha_i \)'s, we deduce that

\[ | a_n | \leq \left( \begin{array}{c} d \\ n \end{array} \right) q^n \text{ for each } 1 \leq n \leq d. \]

Given an explicit Weierstrass equation for \( E/K \) we can already compute \( a_d = \varepsilon(E/K)q^{d} \) (using [1, p.365, Lemma 2.3]). Therefore, we only need to compute the coefficients \( a_1, 1 \leq i \leq d - 1 \). To guarantee in general that \( L(T, E/K) \) is completely determined by its reduction \( L(T, E/K) \mod M \) for some positive integer \( M \) coprime to \( q \), it suffices that \( M \) satisfies

\[ M > 2 \max_{1 \leq n \leq d-1} \left( \begin{array}{c} d \\ n \end{array} \right) q^n. \]

Remark 5. If \( E(K) \) has a subgroup of order \( N \geq 3 \), with \( N \) coprime to \( q \), then we can avoid the use of Tate’s algorithm (which is needed in [1, p.365, Lemma 2.3]), and compute global root numbers more directly. Indeed, expanding the formula for \( L(T, E_f/K) \mod N \) in Theorem 16 gives a relation of the form \( \varepsilon(E_f/K)q^{d} \equiv \pm q^{d} \mod N \) and so \( \varepsilon(E_f/K) \equiv \pm 1 \mod N \). This is sufficient to determine \( \varepsilon(E_f/K) \) since there is only one representative for the class \( \varepsilon(E_f/K) \mod N \) in the set \( \{-1, 1\} \). Alternatively, one could use [4, p.134, Corollary 5] and Proposition 14.

The following simple observation does not seem to be in the literature.
Proposition 24. If \( \varepsilon(E/K) = -1 \) and \( d = \deg(L(T, E/K)) \), then

\[
L(T, E/K) = (1 - qT) \left( 1 + \sum_{n=1}^{d-2} \left( \sum_{m=0}^{n} a_n q^{n-m} \right) T^n + q^{d-1}T^{d-1} \right).
\]

Proof. On one hand, since \( E/K \) has odd analytic rank, then

\[
0 = L(q^{-1}, E/K) = \sum_{n=1}^{d-1} a_n (q^{-1})^n \quad \text{and so } a_{d-1} = - \sum_{n=1}^{d-2} a_n q^{d-(n+1)}.
\]

On the other hand, expanding the right hand side of Equation (9), gives

\[
(1 - qT) \left( 1 + \sum_{n=1}^{d-2} \left( \sum_{m=0}^{n} a_n q^{n-m} \right) T^n + q^{d-1}T^{d-1} \right) = 1 + \sum_{n=1}^{d-2} a_n T^{d-2} - \left( \sum_{n=1}^{d-2} a_n q^{d-(n+1)} \right) T^{d-1} - q^d T^d.
\]

In particular, we have the following consequence.

Corollary 25. Under the assumptions of Proposition 24 we have

(i) If \( d = 1 \), then \( L(T, E/K) = 1 - qT \).

(ii) If \( d = 2 \), then \( L(T, E/K) = (1 - qT)(1 + qT) \).

(iii) If \( d = 3 \), then \( L(T, E/K) = (1 - qT)(1 + (q + a_1)T + q^2T^2) \) and \( a_2 = -7a_1 \).

Remark 6. A priori, if \( d = 3 \), then we have \( |a_1| \leq 3q \) and \( |a_2| \leq 3q^2 \). However, if \( E/K \) has odd analytic rank, then Corollary 25 (iii) shows that we only need to consider the bound \( |a_1| \leq 3q \) in order the compute \( L(T, E/K) \). More generally, Proposition 24 shows that if \( E/K \) has odd analytic rank and \( L(T, E/K) \) has degree \( d \), then in order to compute \( L(T, E/K) \), we only need to consider the bounds on \( |a_i| \), for \( 1 \leq i \leq d - 2 \).

Proposition 26. Let \( k \) be the field with 5 elements and let \( f \) be a rational function of the form \( f \in \{ P(t), 1/Q(t), P(t)/Q(t) \} \), with \( P(t), Q(t) \in k[t] \) coprime and of degree 1. An elliptic curve \( E/k(t) \) given by a Weierstrass equation

\[
E/k(t) : y^2 = (1-a)xy - by = x^3 - bx^2,
\]

with \( a = (10 - 2f)/(f^2 - 9) \) and \( b = -2(f - 1)^2(f - 5)/(f^2 - 9)^2 \), has torsion subgroup \( E(k(t))_{\text{tors}} \) isomorphic to \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \). Moreover, its L-function equals

\[
L(T, E/k(t)) = (1 - 5T)(1 + 5T).
\]

Proof. From [8] p.403, Table 3, the prime-to-5 torsion subgroup of \( E(k(t)) \) is isomorphic to \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \) and since the \( j \)-invariant of \( E \),

\[
j(E) = 4\frac{(f^2 + f + 1)^3(f^2 + 2f + 3)^3(f^2 + 4f + 1)^3(f^2 + 4f + 2)^3}{f^6(f + 1)^2(f + 2)^2(f + 3)^2(f + 4)^6},
\]

is not a 5th power in \( k(t) \), then the 5-torsion subgroup of \( E(k(t)) \) is trivial (see [15] p.229, Proposition 7.3). By direct computation, we see that the places of \( k(t) \) over which \( E \) has bad reduction is \( M \) and that \( \# M^p = \# M^{\infty} = 3 \) and so \( \deg(L(T, E/k(t))) = 2 \). Since \( k(t) \) has genus 0, then \( Z(T, k(t))Z(5T, k(t)) = 1/((1 - T)(1 - 5T)^2(1 - 5^2T)) \). Now, \( 5^2 \equiv 1 \mod 12 \) and that we have the
factorizations \((1 - 5T)^2 \equiv (1 + T)^2 \mod 12\) and \((1 - 5T)(1 - T) \equiv (1 + T)(1 + 5T) \mod 12\). It follows from Theorem 1 that

\[
L(T, E/k(t)) \equiv \frac{1}{(1 - T)^2(1 - 5T)^2} \times (1 - 5T)^3 \times \frac{(1 - T)^3(1 - 5T)^3}{(1 + T)^3} \\
\equiv \frac{(1 - T)(1 - 5T)^4}{(1 + T)^3} \\
\equiv (1 - 5T)(1 + 5T) \mod 12.
\]

Then, \(\varepsilon(E/k(t))^2 \equiv -5^2 \mod 12\) and so \(\varepsilon(E/k(t)) = -1\) (see Remark 3). To conclude that \(L(T, E/k(t)) = (1 - 5T)(1 + 5T)\), we can either use Corollary 25 (ii), or observe that since \(a_1 \equiv 0 \mod 12\) and \(|a_1| \leq 10\), then \(a_1 = 0\).

**Proposition 27.** Suppose that \(k\) is the field with 7 elements and let \(f \in k[t]\) be a polynomial of degree 1. An elliptic curve \(E/k(t)\) given by a Weierstrass equation

\[
E/k(t) : y^2 + xy + \frac{f^2 + f + 1}{3(f + 2)^2} = x^3
\]

has torsion subgroup \(E(k(t))_{\text{tors}}\) isomorphic to \((\mathbb{Z}/3\mathbb{Z})^2\), bad reduction \(M^{sp}\) and \(L\)-function equal to 1. Moreover, for any finite place \(h \in M^{sp}\), the \(L\)-function of the quadratic twist \(E_h/k(t)\) is

\[
L(T, E_h/k(t)) = (1 - 7T)(1 + 7T).
\]

**Proof.** Since \(\text{char}(k) \neq 3\) and \(\zeta_3 \in k\), then the prime-to-7 torsion subgroup of \(E(k(t))\) is isomorphic to \((\mathbb{Z}/3\mathbb{Z})^2\) (see [8], p.402, Table 1]). Since the \(j\)-invariant of \(E\),

\[
j(E) = 6 \frac{f^3(f + 1)^2(f + 2)^3(f + 4)^2}{(f + 6)^3},
\]

is not a 7th power in \(k(t)\), then the 7-torsion subgroup of \(E(k(t))\) is trivial (see [15], p.229, Proposition 7.3)). By direct computation, we see that the set of places of \(k(t)\) over which \(E\) has bad reduction is \(M^{sp}\) and the elements of this set are 3 finite places of degree 1 (none of which is a monic irreducible factor of \(f\)) and the place \(\infty\). In particular, \(\deg(L(T, E/k(t))) = 0\).

We now consider the quadratic twists \(E_h/k(t)\) for any finite place \(h \in M^{sp}\). Using Lemma 22, we see that \(#M^{sp}_{\text{split}} = #M^{sp}_{\text{inert}} = 1\) and \(M^{sp}_{\text{ram}} = \{h, \infty\}\). From Lemma 15 (a2), we have \(M^{sp}_{\text{split}} = M^{sp}_{h}\) and \(M^{sp}_{\text{inert}} = M^{sp}_{h}\) and from Lemma 22 (iv), we have \(A_h = \{h, \infty\}\). So \(\deg(L(T, E_h/k(t))) = -4 + 2 + 2(2) = 2\). By the Riemann-Hurwitz formula, we see that the quadratic extension \(k(t)/k(t)\) has genus 0 and so \(L(T, \chi) L(7T, \chi) = 1\). Therefore, Theorem 16 implies that

\[
L(T, E_h/k(t)) \equiv (1 - 7T)(1 + 7T) \mod 9.
\]

Then, \(\varepsilon(E_h/k(t))^2 \equiv -7^2 \mod 9\) and so \(\varepsilon(E_h/k(t)) = -1\) (see Remark 5). To conclude that \(L(T, E_h/k(t)) = (1 - 7T)(1 + 7T)\), we can either use Corollary 25 (ii) or proceed as follows. We have \(a_1 \equiv 0 \mod 9\) and since \(L(T, E/k(t)) = 1\), \(\deg(h) = 1\) and \(\infty \in M\), then Corollary 23 implies that

\[
L(T, E_h/k(t)) \equiv (1 - T)^2 \mod 2.
\]

Hence, \(a_1 \equiv 0 \mod 2\) and by the Chinese remainder theorem, \(a_1 \equiv 0 \mod 18\). Since \(|a_1| \leq 14\), we have \(a_1 = 0\).
5.3. Study of an Infinite Family of Quadratic Twists. In this subsection, we apply Theorem [16] Corollary 23, Lemma 13 and Proposition 14 to study an infinite family of quadratic twists of the so-called “universal” elliptic curve $E$ over the function field $K = k(t)$ of the “modular curve $X_1(3)/k$”. We suppose that $p \geq 5$. The elliptic curve $E/K$ is defined by the Weierstrass equation

$$y^2 + 3xy + (1 - t^3)y = x^3$$

(10)

together with the point at infinity $O = [0 : 1 : 0]$. Its discriminant is $\Delta = -3^3 t^3 (t - 1)^3 (t^2 + t + 1)^3$.

Since $\text{ord}_\infty(C)$ there is a Weierstrass equation over $K$ for which applying the change of variables $(t, x, y) \mapsto (1/s, x/s^e, y/s^e)$ to Equation (10) yields a Weierstrass equation over $k[s]$ that is minimal at $s : e = 1$. The resulting Weierstrass equation is

$$y^2 = x^3 - 27c_{4,\infty}x - 54c_{4,\infty},$$

where $c_{4,\infty} = 3^2(s^3 + 8)$ and $c_{6,\infty} = 3^3(s^6 - 20s^3 - 8)$.

The elliptic curve $E/K$ has good reduction above the place $\infty$. Indeed, there is a smallest integer $e \geq 1$ for which applying the change of variables $(t, x, y) \mapsto (1/s, x/s^e, y/s^e)$ to Equation (10) yields a Weierstrass equation over $k[s]$ that is minimal at $s : e = 1$. The resulting Weierstrass equation is

$$y^2 = x^3 - 27c_{4,\infty}x - 54c_{4,\infty},$$

where $c_{4,\infty} = 3^2(s^3 + 8)$ and $c_{6,\infty} = 3^3(s^6 - 20s^3 - 8)$.

Therefore, $E/K$ has good reduction over $\infty$. In particular, $\text{deg}(L(T, E/K)) = 0$.

We now assume that $q \equiv 5, 11 \mod 12$, so that the polynomial $t^2 + t + 1$ is irreducible in $k[t]$. We prove the following result.

**Theorem 28.** Let $E/K$ be the universal elliptic curve over the function field $K = k(t)$ of the modular curve $X_1(3)/k$, where $k$ is a finite field of cardinality $q$. Suppose that $q \equiv 5, 11 \mod 12$. Let $f \in k[t]$ be a monic square-free polynomial of degree $d_f$ which is coprime to $\Delta$. Then

$$\text{deg}(L(T, E_f/K)) = \begin{cases} 2d_f & \text{if } d_f \text{ is even}, \\
2(d_f + 1) & \text{if } d_f \text{ is odd} \end{cases}$$

is an even number. For $a \in \{0, 1\}$, we write $f(a) \in k^2$ to ask whether $f(a)$ is a square (Yes) or not (No) in $k$. We have

The global root number $\varepsilon(E_f/K)$ is given in Table 15 below.

Moreover, let $\text{Jac}(C_f)(k)$ be the set of $k$-rational points of the Jacobian of the (normalization of the) curve $C_f/k$ associated to the field $K_f$. If the 3-torsion subgroup of $\text{Jac}(C_f)(k)$ is trivial, then the fourth column of Table 15 gives the analytic rank, $\text{rank}^\text{an}(E_f/K)$, of the elliptic curve $E_f/K$ or an upper bound on it.
| $f(0) \in k^2?$ | $f(1) \in k^2?$ | $L(T, E_f/K)$ mod 3 |
|----------------|----------------|------------------|
| Yes            | Yes            | $L(T, K_f)L(-T, K_f)(1-T)(1+T)(1+T^2)$ |
| Yes            | No             | $L(T, K_f)L(-T, K_f)(1-T)^2(1+T^2)$ |
| No             | Yes            | $L(T, K_f)L(-T, K_f)(1-T)(1+T)^2$ |
| No             | No             | $L(T, K_f)L(-T, K_f)(1-T)^2(1+T^2)$ |

Table 14. Reduction $L(T, E_f/K)$ mod 3

| $f(0) \in k^2?$ | $f(1) \in k^2?$ | $\varepsilon(E_f/K)$ | $\text{ran}^{an}(E_f/K)$ |
|----------------|----------------|---------------------|--------------------------|
| Yes            | Yes            | 1                   | 0                        |
| Yes            | No             | 1                   | 0                        |
| No             | Yes            | -1                  | $\leq 3$                 |
| No             | No             | -1                  | 1                        |

Table 15. Global Root Number and Analytic Rank Using Reduction Modulo 3

We also have

$$L(T, E_f/K) \equiv (1 - a_\infty T + T^2)^{\varepsilon_U} \times \prod_{v \mid f} (1 - a_v T^{d_v} + T^{2d_v}) \mod 2,$$

where $\varepsilon_U = 1$ if $df$ is odd and $\varepsilon_U = 0$ if $df$ is even. If $df$ is odd, then

$$\text{rank}^{an}(E_f/K) \leq \begin{cases} 2\#\{v \mid f : a_v \equiv 0 \mod 2\} + 2 & \text{if } a_\infty \equiv 0 \mod 2, \\ 2\#\{v \mid f : a_v \equiv 0 \mod 2\} & \text{if } a_\infty \equiv 1 \mod 2. \end{cases}$$

In particular, if $f$ is irreducible of odd degree, then

$$\begin{array}{cc|c|c}
  a_\infty \mod 2 & a_f \mod 2 & \text{rank}^{an}(E_f/K) & \\
  0 & 0 & \leq 4 & \\
  0 & 1 & \leq 2 & \\
  1 & 0 & \leq 2 & \\
  1 & 1 & 0 & \\
\end{array}$$

Table 16. Analytic Rank using Reduction Modulo 2

If $f = \Delta$, then $\text{deg}(L(T, E_\Delta/K)) = 4$, $\varepsilon(E_\Delta/K) = 1$ and

$$L(T, E_\Delta/K) \equiv \begin{cases} L(T, K_f)L(-T, K_f) \mod 3, \\ (1-T)^4 \mod 2. \end{cases}$$

Proof. We first qualify the places of $K$ over which $E$ has bad reduction. The Weierstrass equation $y^2 = x^3 - 27c_4x - 54c_6$ is minimal for $v \in S := \{(t), (t-1), (t^2 + t + 1)\}$ since $-27c_4, -54c_6 \in k[t]$ and for each $v \in S, \text{ord}_v(\Delta) = 3 < 12$ (see [13] Remark 1.1, p.186). Moreover, for $v \in S, \text{ord}_v(c_4) = 0$ and so $M = S$ with $\text{deg}(M) = 4$ and $A = \emptyset$. From Equation (8), $\text{deg}(L(T, E/K)) = 0$ and thus $L(T, E/K) \equiv 1$. By [11] p.364, Lemma 2.1, a place $v \in M$ is in $M^{sp}$ if and only if the image of $6(-54c_6)$ in the residue field $k_v$ is a square. We have $6(-54c_6) \equiv -2^2 \cdot 3^7 \mod \pi_\tau$. This is not a square in $k_t$ since $-3$ is not a square in $k_t$ as we assumed that $q \equiv 5, 11 \mod 12$ (see Equation (11)). Now, if $v \in \{(t-1), (t^2 + t + 1)\}$, then $6(-54c_6) \equiv (2^2 \cdot 3^5)^2 \mod \pi_v$. Therefore, $M^{sp} = \{(t-1), (t^2 + t + 1)\}$ and $M^{ns} = \{(t)\}$. 

22
We now study the quadratic twists $E_f/K$ and their $L$-functions and first consider the reduction modulo 3. Suppose until further notice that $f \in k[t]$ is a monic square-free polynomial of degree $d_f$ that is coprime to $\Delta$. By Proposition [14] (i), we have

$$\deg (L(T, E_f/K)) = \begin{cases} 2d_f & \text{if } d_f \text{ is even}, \\ 2(d_f + 1) & \text{if } d_f \text{ is odd}, \end{cases}$$

which is in particular an even number. Moreover $M^{sp} = M^{sp}_{unr}$ and it follows from Lemma [22] that $M^{us}_{\text{inert}} = \{ t \}$ if and only if $f(0)$ is not a square in $k$. Therefore, from Proposition [14] (ii) we have

$$\varepsilon(E_f/K) = \begin{cases} -1 & \text{if } f(0) \in k \setminus k^2, \\ 1 & \text{if } f(0) \in k^2. \end{cases}$$

Since $q \equiv 5, 11 \mod 12$, then $q \equiv -1 \mod 3$. In this situation, Theorem [16] gives

$$L(T, E_f/K) \equiv L(T, K_f)L(-T, K_f)(1 + \alpha_tT)(1 - \alpha_{t-1}T)(1 + \alpha_{t^2+t+1}T^2) \mod 3,$$

where for $v \in M$, $\alpha_v = 1$ if $v \in M_{\text{inert}}$ and $\alpha_v = -1$ if $v \in M_{\text{split}}$. From Lemma [22] we see that

$$\alpha_t = \begin{cases} -1 & \text{if } f(0) \in k^2, \\ 1 & \text{if } f(0) \in k \setminus k^2 \end{cases} \quad \text{and} \quad \alpha_{t-1} = \begin{cases} -1 & \text{if } f(1) \in k^2, \\ 1 & \text{if } f(1) \in k \setminus k^2. \end{cases}$$

Now, we have $L(T, K_f)L(-T, K_f) = q^{g(K_f)T^{4g(K_f)}} + O(T^{4g(K_f)+1})$ (see [10] p.54, Proof of Theorem 5.9) and therefore we have

$$L(T, E_f/K) \equiv -\alpha_t\alpha_{t-1}\alpha_{t^2+t+1}T^{4g(K_f)+1} + O(T^{4g(K_f)+3}) \mod 3$$

and in particular

$$\varepsilon(E_f/K) \equiv -\alpha_t\alpha_{t-1}\alpha_{t^2+t+1} \mod 3.$$ 

Combining Equation [12] and Equation [13] we deduce the following.

| $f(0) \in k^2?$ | $f(1) \in k^2?$ | $(\alpha_t, \alpha_{t-1}, \alpha_{t^2+t+1})$ | $\varepsilon(E_f/K)$ |
| Yes | Yes | $(-1, -1, -1)$ | 1 |
| Yes | No | $(-1, 1, 1)$ | 1 |
| No | Yes | $(1, -1, -1)$ | -1 |
| No | No | $(1, 1, 1)$ | -1 |

**Table 17.** Decomposition of Unramified Places in $K_f$ and Global Root Number

Putting all these together, we conclude that

| $f(0) \in k^2?$ | $f(1) \in k^2?$ | $L(T, E_f/K) \mod 3$ | $\varepsilon(E_f/K)$ |
| Yes | Yes | $L(T, K_f)L(-T, K_f)(1 - T)(1 + T)(1 + T^2)$ | 1 |
| Yes | No | $L(T, K_f)L(-T, K_f)(1 - T)^2(1 + T^2)$ | 1 |
| No | Yes | $L(T, K_f)L(-T, K_f)(1 - T)(1 + T)^2$ | -1 |
| No | No | $L(T, K_f)L(-T, K_f)(1 - T)(1 + T)(1 + T^2)$ | -1 |

**Table 18.** Reduction $L(T, E_f/K) \mod 3$ and Global Root Number

Similarly to [1] p.134, Corollary 6], if $\#E(K)$ is divisible by 3, then we define, for any polynomial $P(T) \in 1 + T \cdot \mathbb{Z}[T]$, $v_3(P)$ as the $(1 + T)$-adic valuation of the image of $P$ in $1 + T \cdot \mathbb{F}_3[T]$ and extend it linearly to rational functions $P_1(T)/P_2(T)$. We have $L(1, C_f/k) = \#\text{Jac}(C_f)(k)$ (see [10] p.53, Theorem 5.9) and since $q \equiv -1 \mod 3$, then $L(-1, C_f/k) \equiv (-1)^{g(C_f)}\#\text{Jac}(C_f)(k) \mod 3$, by
Lemma 13. Therefore, we have $\text{Jac}(K_f)(k)[3] = \{O\}$ if and only if $v_3(L(T, K_f)) = v_3(L(-T, K_f)) = 0$. Hence, in general we have

$$\text{rank}^\text{an}(E_f(K)) \leq v_3(L(T, K_f)) + v_3(L(-T, K_f)) + v_3(R(T)),$$

where

| $f(0) \in k^2?$ | $f(1) \in k^2?$ | $v_3(R(T))$ | $\varepsilon(E_f/K)$ |
|-----------------|-----------------|--------------|------------------|
| Yes             | Yes             | 1            | 1                |
| Yes             | No              | 0            | 1                |
| No              | Yes             | 3            | $-1$             |
| No              | No              | 1            | $-1$             |

Table 19. $(1 + T)$-adic valuation in $\mathbb{F}_3[T]$ and Global Root Number

and in particular, if $\text{Jac}(K_f)[3] = \{O\}$, then we obtain Table 20.

| $f(0) \in k^2?$ | $f(1) \in k^2?$ | $\varepsilon(E_f/K)$ | $\text{ran}^\text{an}(E_f/K)$ |
|-----------------|-----------------|------------------|-----------------|
| Yes             | Yes             | 1                | 0               |
| Yes             | No              | 1                | 0               |
| No              | Yes             | $-1$             | $\leq 3$        |
| No              | No              | $-1$             | 1               |

Table 20. Global Root Number and Analytic Rank Using Reduction Modulo 3

Now suppose that $f = \Delta$. The set of places of $K$ over which $E$ has bad reduction is in $M$ and then by Lemma 22 (iii) these places ramify in $K_\Delta$ and acquire additive reduction with respect to $E_\Delta/K$. Therefore, $\deg(L(T, E_\Delta/K)) = -4 + 2(4) = 4$. By Theorem 16 we have

$$L(T, E_\Delta/K) \equiv L(T, C_f/k) L(-T, C_f/k) \mod 3,$$

with $L(T, C_f/k) = qT^2 + O(T)$. We have the relation $\varepsilon(E_\Delta/K)q^4 \equiv q^2 \mod 3$ and so $\varepsilon(E_\Delta/K) = 1$ (see Remark 5). If $\text{Jac}(C_f)(k)[3] = \{O\}$, then $\text{rank}^\text{an}(E_\Delta/K) = 0$.

We now consider the reduction modulo 2. The places of $K$ over which $E$ has bad reduction are all in $M$, and $\infty \notin |U|$. Moreover, we know that $L(T, E/K) = 1$. Corollary 23 allows us to describe $L(T, E_f/K)$ mod 2. More precisely, if $f$ is coprime with $\Delta$, then

$$L(T, E_f/K) \equiv (1 - a_\infty T + T^2)^{\varepsilon_U} \prod_{v|f} (1 - a_v T^{d_v} + T^{2d_v}) \mod 2,$$

$$\equiv (1 - a_\infty T + T^2)^{\varepsilon_U} \prod_{v|f} (1 - T)^2 (1 + T + \ldots + T^{d_v-1})^2 \times \prod_{a_v \equiv 1 \mod 2} (1 + T^{d_v} + T^{2d_v}) \mod 2,$$

where

$$\varepsilon_U = \begin{cases} 0 & \text{if } df \text{ is even}, \\ 1 & \text{if } df \text{ is odd}. \end{cases}$$

From this, we see for example that if $df$ is odd, then

$$\text{rank}(E_f/K) \leq \begin{cases} 2\#\{v \mid f : a_v \equiv 0 \mod 2\} + 2 & \text{if } a_\infty \equiv 0 \mod 2, \\ 2\#\{v \mid f : a_v \equiv 0 \mod 2\} & \text{if } a_\infty \equiv 1 \mod 2. \end{cases}$$
In particular, if $f$ is irreducible of odd degree, we have the following.

Finally, $f = \Delta$ has even degree and so

\begin{equation}
L(T, E_{\Delta}/K) \equiv (1 - T)^2 (1 - T^2) \equiv (1 - T)^4 \mod 2.
\end{equation}

Then the bound on the analytic rank provided by Equation (14) is $4 = \deg(\Delta)$. \hfill \Box

6. Appendix - Proofs of Some Lemmas

In this section we prove some lemmas which we believe are already known, at least in the folklore, but which we could not find in the literature.

Let $v$ be a place of $K$ and let $K_v$ be its $v$-adic completion. Let $\pi_v$ be a chosen normalized uniformizer. There is a well-defined reduction map $E(K_v) \to E_v(k_v)$ modulo $\pi_v$ (see [13] p. 187, VII.2]). The subset $E_{v,\text{sm}}(k_v)$ of smooth points of $E_v(k_v)$ forms a group (see [13] p. 56, III.2.5 and p. 105, Exercise 3.5]). Now, let $E_0(K_v)$ be the subset of points of $E(K_v)$ whose reduction is smooth and let $E_1(K_v)$ be the kernel of the reduction map. There is a short exact sequence of abelian groups

\begin{equation}
0 \to E_1(K_v) \to E_0(K_v) \to E_{v,\text{sm}}(k_v) \to 0,
\end{equation}

where the map $E_0(K_v) \to E_{v,\text{sm}}(k_v)$ is the reduction modulo the uniformizer $\pi_v$ (see [13] p. 188, VII.2.1]). Our proof of the following lemma uses the language of Néron models (See for example [12] pp. 361-364, IV.9.]).

**Lemma 29.** Let $K_v$ be a field complete with respect to a non-Archimedean place $v$ whose residue field $k_v$ has characteristic $p \geq 0$. Let $E/K_v$ be an elliptic curve with additive reduction over $v$. Then, the prime-to-$p$-torsion subgroup of $E(K_v)$ injects into the group $\Phi_v(k_v)$.

**Proof.** If $N$ is an integer coprime with $p$, then $E_1(k_v)[N] = \{0\}$ (see [13] p. 192, VII.3.1(a)]) and since $E/K_v$ has additive reduction, then $E_{v,\text{sm}}(k_v)$ is isomorphic to the additive $p$-group $k_v$ (see [13] p. 56, III.2.5 and p. 105, Exercise 3.5]). Therefore, $E_{v,\text{sm}}(k_v)[N] = \{0\}$. In view of the short exact sequence (15), we deduce that $E_0(k_v)[N] = \{0\}$. Now, there is a short exact sequence of abelian groups

\begin{equation}
0 \to E_0(K_v) \to E(K_v) \to E(K_v)/E_0(K_v) \to 0.
\end{equation}

Since $E_0(K_v)[N] = \{0\}$, then $E(k_v)[N]$ injects into $E(K_v)/E_0(K_v)$. Let $E_{k_v}$ (resp. $E_{k_v}^0$) be the special fiber of the Néron model $\mathcal{E}_v/\text{Spec}(O_v)$ of $E/K_v$ (resp. of the identity component $\mathcal{E}_v^0/\text{Spec}(O_v)$ of $\mathcal{E}_v/\text{Spec}(O_v)$). Since the field $K_v$ is complete (and in particular Henselian), then from [12] p. 362, 9.2(b)]) we have the group isomorphisms

\[ E(K_v)/E_0(K_v) \simeq E_{k_v}(k_v)/E_{k_v}^0(k_v) \simeq \Phi_v(k_v). \]

Therefore, the prime-to-$p$-part $\bigcup_{(N,p)=1} E(k_v)[N]$ of $E(K_v)$ injects into $\Phi_v(k_v)$. \hfill \Box

**Lemma 30.** Assuming Context 12, the reduction types of $E/K$ and of $E_f/K$ are related as follows.

(a) If $v \in \mathcal{C} \mid \mathcal{O}_{K_v}$,

(a1) then $v \in \big| \mathcal{U} \big| \cap \big| U_f \big|$ or $v \in M \cap M_f$ or $v \in A \cap A_f$.  

\begin{table}[h]
\centering
\begin{tabular}{|c|c|c|}
\hline
$a_\infty \mod 2$ & $a_f \mod 2$ & ran$_{an}(E_f/K)$ \\
\hline
0 & 0 & $\leq 4$ \\
0 & 1 & $\leq 2$ \\
1 & 0 & $\leq 2$ \\
1 & 1 & $= 0$ \\
\hline
\end{tabular}
\caption{Analytic Rank Using Reduction Modulo 2}
\end{table}
(a2) Moreover, if \( v \in M \), then \( v \in M^{sp} \cap M^{sp}_f \) or \( M^{ns} \cap M^{ns}_f \) if and only if \( v \in M^{\text{split}} \).

(b) If \( v \mid C \mid_{\text{ram}} \), then

\[
\begin{array}{|c|c|c|c|c|}
\hline
E/K_v & U_{\text{ram}} & M_{\text{ram}} & A^g_{\text{ram}} & A^m_{\text{ram}} & A^o_{\text{ram}} \\
\hline
E_f/K_v & A^g_{f,\text{ram}} & A^m_{f,\text{ram}} & | U_f |_{\text{ram}} & M_{f,\text{ram}} & A^o_{f,\text{ram}} \\
\hline
\end{array}
\]

Table 22. Reduction Types After Ramified Twist

Proof. Suppose that the elliptic curve \( E/K_v \) is given by a minimal Weierstrass equation

\[
y^2 = x^3 + a_v x + b_v
\]

and let \( \Delta_v \) be the discriminant associated to this equation. Then, \( E_{f_v}/K_v \) is given by the Weierstrass equation

\[
y^2 = x^3 + f_v^2 a_v x + f_v^3 b_v,
\]

and the discriminant of this equation is \( f_v^6 \Delta_v \) (see Lemma 11). However, Equation (17) might not be minimal. We will reduce to the case where it is minimal.

There exists an integer \( r \in \mathbb{Z} \) such that \( f_v^2 \pi_v^{-2r} \in O_v \). Under the change of variables \( (x, y) \mapsto (x/\pi_v^{2r}, y/\pi_v^{2r}) \) the Weierstrass equation (17) becomes

\[
y^2 = x^3 + f_v^2 \pi_v^{-4r} a_v x + f_v^3 \pi_v^{-6r} b_v,
\]

and has all its coefficients in \( O_v \) and therefore the discriminant of Equation (18), \( f_v^6 \pi_v^{-12r} \Delta_v \), also belongs to \( O_v \). Since \( \text{ord}_v \) is a discrete valuation, we can choose \( r \in \mathbb{Z} \) such that

\[
\text{ord}_v(f_v^6 \pi_v^{-12r} \Delta_v) = \text{ord}_v(f_v^6) - 2r + \text{ord}_v(\Delta)
\]

is minimized under the constraint that the coefficients of the Weierstrass equation (18) belong to \( O_v \), i.e., under the constraint that the integers

\[
2 \left( \text{ord}_v(f_v) - 2r \right) + \text{ord}_v(a_v) \text{ and } 3 \left( \text{ord}_v(f_v) - 2r \right) + \text{ord}_v(b_v)
\]

are nonnegative. For any such \( r \), the Weierstrass equation (18) is minimal.

Because twisting by an element in the square class of \( f_v \) yields an elliptic curve which is isomorphic to \( E_{f_v}/K_v \) (see Subsection 2.1), we can assume without loss of generality that the Weierstrass equation (17) is minimal and that either \( \text{ord}_v(f_v^2) = 0 \) (and so \( f_v \) is a unit) or that \( \text{ord}_v(f_v) \in \{ \pm 1 \} \) with \( f_v = \pi_v^\pm 1 \). Recall from Context 12 that \( K_{f, w} \simeq K_v(\theta_w) \). The integral closure \( O_w \) of \( O_v \) inside \( K_{f, w} \) is also the valuation ring of the place \( w \) lying over \( v \) and we let \( k_w \) be the residue field of \( w \).

Suppose further notice that \( f_v \) is a unit. Then, \( \text{ord}_v(f_v) = 0 \) and so the extension \( K_{f, w}/K_v \) is unramified. Therefore, the canonical surjective group morphism \( \text{Gal}(K_{f, w}/K_v) \to \text{Gal}(k_w/k_v) \) is an isomorphism (see [9] p.172, II, (9.9) Proposition).

From this observation one sees that \( f_v \) is a square in \( K_v \) if and only if \( v \) splits in \( K_{f, w} \) or equivalently that \( f_v \mod \pi_v \) is a square in \( k_v \). As \( f_v \) is a unit, it follows that

\[
\text{ord}_v(f_v^6 \Delta_v) = \text{ord}_v(\Delta_v), \quad \text{ord}_v(f_v^2 a_v) = \text{ord}_v(a_v) \text{ and } \text{ord}_v(f_v^3 b_v) = \text{ord}_v(b_v).
\]

Then \( E/K_v \) and \( E_f/K_v \) have the same reduction type (good, multiplicative, additive) over \( v \) (see [13] p.196, VII.5.1)). This proves Lemma 15 (a1).

Suppose that \( v \in M^{\text{unram}} \). By [1] p.364, Lemma 2.1, \( E_f/K_v \) has split multiplicative reduction over \( v \) if and only if the image \( f_v^3 6b_v \mod \pi_v \) of \( f_v^3 b_v \) in \( k_v \) is a square. This is equivalent to require that \( f_v 6b_v \mod \pi_v \) is a square in \( k_v \). But from [1] p.364, Lemma 2.1 we also know that \( E/K_v \) has split multiplicative reduction over \( v \) if and only if \( 6b_v \mod \pi_v \) is a square in \( k_v \). Hence, \( E/K_v \) and
$E_f/K_v$ have the same splitting behaviour (both split multiplicative or both nonsplit multiplicative) over $v$ if and only if $f_v \bmod \pi_v$ is a square in $k_v$. This completes the proof of Lemma \[15\] (a2).

We now assume that $f_v \in \{\pi_v^{\pm 1}\}$. In this situation, $v \in |C|_\text{ram}$. Remember that the Weierstrass equations (16) and (17) are minimal.

Suppose until further notice that (b1) holds. When $\text{ord}_v(E/K)$ reduction over $v$ in (b1.2.2). We are left to consider the situation where $\text{ord}_v(E/K)$ suppose until further notice that (b1) holds.

(b1.1) If $\text{ord}_v(\Delta_v) = 0$, then $E/K$ has good reduction over $v$ (see \[13\] p.196, VII.5.1(a)). In this case, $\text{ord}_v(\Delta_{v,f}) = 6 > 0$ and so $E/K_f$ has bad reduction over $v$. Since $j(E_f) = j(E)$, then

$$\text{ord}_v(j(E_f)) = 3 \text{ord}_v(a_v) - \text{ord}_v(\Delta_v) = 3 \text{ord}_v(a_v) \geq 0$$

by the minimality of Equation (16). Therefore, $j(E_f) \in \mathcal{O}_v$, and so $E_f/K_f$ has (additive) potential good reduction over $v$ (see \[13\] p.197, VII.5.5).

(b1.2) If $\text{ord}_v(\Delta) > 0$, then $E/K$ has bad reduction over $v$.

(b1.2.1) If $\text{ord}_v(a_v) = 0$, then $E/K$ has multiplicative reduction over $v$ by \[13\] p.196, VII.5.1(b)] and in this case $\text{ord}_v(f_v^2 a_v) = 2 > 0$. This implies that $E_f/K_f$ has additive reduction over $v$ (see \[13\] p.196, VII.5.1(c)]).

(b1.2.2) Suppose that $\text{ord}_v(a_v) > 0$. Then $E/K$ has additive reduction over $v$ (see \[13\] p.196, VII.5.1(c)]). Since $\text{ord}_v(f_v^2 a_v) = 2 + \text{ord}_v(a_v) > 0$, then $E_f/K$ also has additive reduction over $v$ (see \[13\] p.196, VII.5.1(c)]).

Now suppose that (b2) holds. Our case by case analysis of (b1) covers the following situations: When $\text{ord}_v(\Delta_v) = 0$, we conclude as in (b1.1) for $\text{ord}_v(a_v) \in \{0,1\}$. When $\text{ord}_v(\Delta_v) > 0$ and $\text{ord}_v(a_v) = 0$, then we conclude as in (b1.2.1). When $0 < \text{ord}_v(\Delta_v) < 6$ and $\text{ord}_v(a_v) = 1$, we conclude as in (b1.2.2). We are left to consider the situation where $\text{ord}_v(\Delta_v) \geq 6$ and $\text{ord}_v(a_v) = 1$. In this situation $E/K$ has additive reduction over $v$ and so does $E_f/K$.

Finally, assume that $\text{ord}_v(f_v) = -1$. Then, $\text{ord}_v(\Delta_{v,f}) \geq 0$ (resp. $\text{ord}_v(f_v^2 a_v) \geq 0$) implies that $\text{ord}_v(\Delta_v) \geq 6$ (resp. $\text{ord}_v(a_v) \geq 2$). Since Equation (16) is minimal, then $E/K$ has additive reduction over $v$. Since Equation (17) is minimal, then \[13\] p.186, VII.1.1] implies that we have the following (not necessarily mutually exclusively) two possibilities.

(b3) If $\text{ord}_v(\Delta_{v,f}) = -6 + \text{ord}_v(\Delta_v) < 12$, then $6 \leq \text{ord}_v(\Delta_v) < 18$.

(b4) If $\text{ord}_v(f_v^2 a_v) = -2 + \text{ord}_v(a_v) < 4$, then $2 \leq \text{ord}_v(a_v) < 6$.

Suppose that (b3) holds.

(b3.1) If $\text{ord}_v(\Delta_{v,f}) = 0$, then $\text{ord}_v(\Delta_v) = 6$. Since $E_f/K$ has good reduction over $v$, then $j(E_f) \in \mathcal{O}_v$ by \[13\] p.197, VII.5.5]. We also have $j(E_f) = j(E)$. Therefore,

$$\text{ord}_v(j(E_f)) = 3 \text{ord}_v(a_v) - 6 \geq 0$$

and so $\text{ord}_v(a_v) \geq 2$. Thus, by \[13\] p.197, VII.5.5] the elliptic curve $E/K$ has (additive) potential good reduction over $v$.

(b3.2) If $\text{ord}_v(\Delta_{v,f}) > 0$, then $E_f/K$ has bad reduction over $v$. Now, $\text{ord}_v(a_v) \geq 2$.

(b3.2.1) If $\text{ord}_v(a_v) = 2$, then $\text{ord}_v(f_v^2 a_v) = 0$ and so $E_f/K$ has multiplicative reduction over $v$ by \[13\] p.196, VII.5.1(c)] and $E/K$ has additive reduction. More precisely, if $\text{ord}_v(j(E_f)) = -\text{ord}_v(\Delta_{v,f}) = -n$ for some positive integer $n$, so that $E_f/K$ has Kodaira symbol $I_n$ over $v$, then $\text{ord}_v(j(E)) = -n$ as well and $E/K$ has potential multiplicative reduction over $v$ with Kodaira symbol $I_n$.  

27
(b3.2.2) If \( \text{ord}_v(a_v) > 2 \), then \( E_f/K \) has additive reduction over \( v \).

Finally, suppose that (b4) holds. If \( \text{ord}_v(\Delta_{e,f}) = 0 \), then we conclude as in (b1.1). Suppose that \( \text{ord}_v(\Delta_{e,f}) > 0 \). If \( \text{ord}_v(a_v) = 2 \), then we conclude as in (b3.2.1), while if \( \text{ord}_v(a_v) > 2 \), then we conclude as in (b3.2.2).

This ends our case by case analysis and our proof of Lemma 30.

**Lemma 31.** For each \( v \in | U |_{\text{unr}} = | U | \cap | U_f | \), we have \( a_v + a_{f,v} \equiv 0 \mod 2 \), where \( a_v \) and \( a_{f,v} \) are defined in Equation (7).

**Proof.** For each \( v \in | U |_{\text{unr}} \), let \( \chi_v : k_v^\times \to \{ \pm 1 \} \) be the unique character of order 2 defined by \( \chi_v(r) = 1 \) if and only if \( r \) is a square in \( k_v \), and \( \chi_v(r) = -1 \), otherwise, and extend \( \chi_v \) to \( k_v \) by setting \( \chi_v(0) := 0 \). Moreover, choose a Weierstrass equation \( y^2 = \alpha_v(x) \) for the elliptic curve \( E_v/k_v \). A corresponding Weierstrass equation for \( E_{f,v}/k_v \) is then given by \( y^2 = f_{v}^{-1}\alpha_v(x) \). Here, \( f_v \) is identified with the unit \( f_{v,v} \), which is the image of \( f \) in the local ring \( O_v \) (see the proof of Lemma 30). By [13 p.139, V.1.3], we have

\[
\#E_v(k_v) = 1 + q^{d_v} + \sum_{x \in k_v} \chi_v(\alpha_v(x)) \quad \text{and} \quad \#E_{f,v}(k_v) = 1 + q^{d_v} + \chi_v(f_{v}^{-1}) \sum_{x \in k_v} \chi_v(\alpha_v(x)).
\]

Since \( q \equiv 1 \mod 2 \), then

\[
\#E_v(k_v) + \#E_{f,v}(k_v) = 2(1 + q^{d_v}) + (1 + \chi_v(f_{v}^{-1})) \sum_{x \in k_v} \chi_v(\alpha_v(x)) \equiv 0 \mod 2.
\]

In particular, we have

\[
a_v + a_{f,v} = 2(1 + q^{d_v}) - (\#E_v(k_v) + \#E_{f,v}(k_v)) \equiv 0 \mod 2.
\]

□

**Acknowledgments**

This paper comes from Chapter 3 of the PhD thesis of the author, while at the University of Western Ontario. We acknowledge the support of the Natural Sciences and Engineering Research Council of Canada (NSERC), [PGSD2-535451-2019] during part of this period. The paper was completed at the University of Lethbridge where the author received financial support from the Pacific Institute for the Mathematical Sciences (PIMS) while he was a PIMS postdoctoral fellow. The author sincerely thanks his PhD supervisor Chris Hall for the many helpful discussions. The author also thanks Amir Akbary and Andrew Fiori for the useful feedback on preliminary versions of this paper.

**References**

[1] Baig, S., Hall, C.: Experimental Data for Goldfeld’s Conjecture over Function Fields, Exp. Math. 21 (2012), no. 4, 362-374. [https://doi.org/10.1080/10586458.2012.671638](https://doi.org/10.1080/10586458.2012.671638)

[2] Costa, E., Harvey, D., Kedlaya, K.: Zeta functions of non-degenerate hypersurfaces in toric varieties via controlled reduction in \( p \)-adic cohomology, Proceedings of the Thirteenth Algorithmic Number Theory Symposium, 221–238, Open Book Ser., 2, Math. Sci. Publ., Berkeley, CA, 2019. [https://doi.org/10.2140/obs.2019.2.221](https://doi.org/10.2140/obs.2019.2.221)

[3] Dummit, S. Foote, R.: Abstract algebra. Third edition, John Wiley & Sons, Inc., Hoboken, N, 2004, xii+932pp. 0-471-43334-9 00-01.

[4] Hall, C.: \( L \)-functions of twisted Legendre curves, J. Number Theory 119 (2006), no. 1, 128-147. [https://doi.org/10.1016/j.jnt.2005.10.004](https://doi.org/10.1016/j.jnt.2005.10.004)

[5] Katz, N. M.: Twisted \( L \)-functions and monodromy, Annals of Mathematics Studies, 150. Princeton University Press, Princeton, NJ, 2002. viii+249 pp. [https://doi.org/10.1515/9781400824885](https://doi.org/10.1515/9781400824885)

[6] Liu, Q.: Algebraic geometry and arithmetic curves, Oxford Graduate Texts in Mathematics 6, Oxford University Press, Oxford, Translated from the French by Reinie Erné, Oxford Science Publications (2002), xvi+576. 0-19-850284-2
[7] Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symbolic Comput., 24 (1997), 235–265. https://doi.org/10.1006/jsco.1996.0125

[8] McDonald, R. J. S.: Torsion subgroups of elliptic curves over function fields of genus 0, J. Number Theory 193 (2018), 395-423. https://doi.org/10.1016/j.jnt.2018.05.017

[9] Neukirch, J.: Algebraic Number Theory, Translated from the 1992 German original and with a note by Norbert Schappacher. With a foreword by G. Harder. Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 322. Springer-Verlag, Berlin, 1999. xviii+571 pp. https://doi.org/10.1007/978-3-662-03983-0

[10] Rosen, M.: Number theory in function fields, Graduate Texts in Mathematics, 210. Springer-Verlag, New York, 2002, xii+358 pp. https://doi.org/10.1007/978-1-4757-6046-0

[11] Schoof, R.: Elliptic Curves Over Finite Fields and the Computation of Square Roots mod p, Math. Comp. 44 (1985), no. 170, 483–494. https://doi.org/10.1090/S0025-5718-1985-0777280-6

[12] Silverman, J.: Advanced topics in the arithmetic of elliptic curves. Graduate Texts in Mathematics, 151, Springer New York, NY, 1994, xiv+525pp., 978-0-387-94325-1. https://doi.org/10.1007/978-1-4612-0851-8

[13] Silverman, J.: The Arithmetic of Elliptic Curves, Second edition. Graduate Texts in Mathematics, 106. Springer, Dordrecht, 2009, xx+513 pp. https://doi.org/10.1007/978-0-387-09494-6

[14] Stichtenoth, H.: Algebraic Function Fields and Codes, Second edition. Graduate Texts in Mathematics, 254, Springer Berlin, Heidelberg, 2009, XIV+360 pp. https://doi.org/10.1007/978-3-540-76878-4

[15] Ulmer, D.: Elliptic curves over function fields, In: Arithmetic of L-functions, IAS/Park City Math. Ser., 18, Amer. Math. Soc., Providence, RI, 2011, 211-280. https://doi.org/10.1090/pcms/018

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, UNIVERSITY OF LETHBRIDGE, 4401 UNIVERSITY DRIVE WEST, LETHBRIDGE, T1K 3M4, ALBERTA, CANADA

Email address: felix.barilboudreau@uleth.ca