

L -functions of Twisted Legendre Curves

Chris Hall

Abstract

Let K be a global field of char p and let \mathbb{F}_q be the algebraic closure of \mathbb{F}_p in K . For an elliptic curve E/K with non-constant j -invariant, the L -function $L(T, E/K)$ is a polynomial in $1 + T \cdot \mathbb{Z}[T]$. For any $N > 1$ invertible in K and finite subgroup $\mathcal{T} \subset E(K)$ of order N , we compute the mod N reduction of $L(T, E/K)$ and determine an upper-bound for the order of vanishing at $1/q$, the so-called analytic rank of E/K . We construct infinite families of curves of rank zero when q is an odd prime power such that $q \equiv 1 \pmod{\ell}$ for some odd prime ℓ . Our construction depends upon a construction of infinitely many twin-prime pairs $(\Lambda, \Lambda - 1)$ in $\mathbb{F}_q[\Lambda] \times \mathbb{F}_q[\Lambda]$. We also construct infinitely many quadratic twists with minimal analytic rank, half of which have rank zero and half have (analytic) rank one. In both cases we bound the analytic rank by letting $\mathcal{T} \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2$ and studying the mod-4 reduction of $L(T, E/K)$.

1 Overview

Let K be a global field of char p and $k = \mathbb{F}_q \subset K$ be the field of constants. Given an elliptic curve E/K let $L(T, E/K)$ denote its L -function. The well-known conjecture of Birch Swinnerton-Dyer asserts that the order of vanishing of $L(T, E/K)$ at the central value $T = 1/q$, which we denote the analytic rank, is equal to the Mordell-Weil rank of $E(K)$. From Tate's work [T2] we know that the (algebraic) rank is at most the analytic rank, but in general we know very little about $L(T, E/K)$ without explicitly computing it (e.g., by "point counting").

If the j -invariant $j(E/K)$ is non constant in K (a function-field analogue of an elliptic curve without complex multiplication), then we know that $L(T, E/K)$ lies in $1 + T \cdot \mathbb{Z}[T]$ (cf. page 11 of [K]). Therefore, given a positive integer N one may ask about the mod N reduction of $L(T, E/K)$, viewing the result as an element of $1 + T \cdot (\mathbb{Z}/N)[T]$. While it is easy to compute the reduction given

Email address: cjh@math.utexas.edu (Chris Hall).

$L(T, E/K)$, one may also ask whether it is possible to compute the reduction directly. Of course, for N sufficiently large one can recover $L(T, E/K)$ from the reduction, hence the question really only makes sense for small N .

The key observation which forms the basis for this paper is that, while $L(T, E/K)$ is difficult to compute in general, there are infinite families for which the mod N reduction is easily computable for one or more $N > 1$. More precisely, we will show that if $E(K)$ has a torsion subgroup of order N , then one can compute the mod N reduction *without* computing $L(T, E/K)$. In particular, when $N = \ell$ is a rational prime distinct from p , then the order of vanishing of the mod ℓ reduction at $T = 1/q$ gives an upper bound for the analytic rank. Aside from the intrinsic interest of such a bound, it can also be useful for studying the average rank in a family of curves.

Let $\mathcal{F} = \{E_\chi/K\}$ be a family of quadratic twists of E/K . There is a natural enumeration of the curves in \mathcal{F} in the form of an increasing filtration $\mathcal{F}_0 \subset \mathcal{F}_1 \subset \dots \subset \mathcal{F}$: we let $\deg(\chi)$ denote the degree of the ramification divisor of the quadratic extension K_χ/K corresponding to χ and define

$$\mathcal{F}_n = \{E_\chi/K : \deg(\chi) \leq n\}.$$

In particular, if we write $\text{rk}_{\text{an}}(E_\chi)$ for the analytic rank of E_χ/K , then we may form the sequence of average (analytic) ranks

$$R_n := \frac{1}{\#\mathcal{F}_n} \sum_{\mathcal{F}_n} \text{rk}_{\text{an}}(E_\chi)$$

and ask whether $\lim_{n \rightarrow \infty} R_n$ exists and its value if it does. Goldfeld first posed the question in [G] (when K is a number field) and he conjectured that the limit is $1/2$.

The computational evidence for the conjecture has raised a bit of controversy. Over number fields and function fields both, it appears there are far more rank two curves among all even rank curves than there are rank three curves among all odd rank curves. More precisely, using a computer to determine the first several terms of the sequence one finds that most odd rank curves have rank one while a non-negligible proportion, say 0.15, of even rank curves have rank two. If the proportion goes to zero as n goes to infinity, then it appears to do so very slowly compared to the odd rank curves.

By contrast, in this paper we construct families \mathcal{F} for which the conjecture is true. In fact, we can prove something stronger: half the curves in any \mathcal{F}_n have analytic rank zero and the other half have analytic rank one, so $R_n = 1/2$ for all n . First, we compute the mod ℓ reduction of the corresponding L -functions for an appropriate ℓ and use it to deduce that the analytic rank is at most one. Next we determine the sign of the functional equation in order to deduce the

parity of the analytic rank and hence distinguish between analytic rank zero and analytic rank one. Both calculations follow from the results in section 2 where we show how to compute the mod N reduction of $L(T, E/K)$ when N is invertible in K and $E(K)$ has a torsion subgroup of order N . We note that the sign of the functional equation has a simple form when $N > 2$: it is the unique square-root of unity congruent to $(-1)^{\#M_{\text{sp}}} q^{-\deg(A)}$ modulo N , which simplifies to $(-1)^{\#M_{\text{sp}}}$ for $N > 4$ (because E must have semistable reduction in that case).

Let C/k be the curve which corresponds to K . The L -function has an Euler product expansion indexed by the closed points of C (places of K), and there is a well-known recipe for the Euler factors given a minimal Weierstrass model $\mathcal{E} \rightarrow C$. In section 3 we focus on constructing these models for successive generalizations of the Legendre curve over $F = k(\lambda)$

$$E_{\text{Leg}}/F : y^2 = x(x-1)(x-\lambda).$$

The most general object we will encounter is a quadratic twist E_f/K of the pullback Legendre curve E_Λ/K , where C is a finite cover $\Lambda : C \rightarrow \mathbb{P}^1$ and $K = k(C)$. While any elliptic curve E/K with non-constant j -invariant and full K -rational 2-torsion is K -isomorphic to some E_f/K , we will restrict our attention to C and Λ such that the 2-part of $\text{Jac}(C)(k)$ is trivial and $\Lambda : C \rightarrow \mathbb{P}^1$ is what we call an odd twin-prime cover.

We say that $\Lambda : C \rightarrow \mathbb{P}^1$ is a twin-prime cover if 0 and 1 are “inert” and ∞ is “totally ramified” and write $\bar{0}, \bar{1}, \bar{\infty}$ for the unique point lying over each. We say that Λ is an *odd twin-prime cover* if, in addition, $\deg(\Lambda)$ is odd. If Λ is an odd twin-prime cover and the 2-part of $\text{Jac}(C)(k)$ is trivial, we call the pullback curve E_Λ/K an *odd twin-prime Legendre curve*. The interest of this notion is the following theorem.

Theorem 1 (cf. theorem 12) *If E_Λ/K is an odd twin-prime Legendre curve, then the “central value” $L(1/q, E_\Lambda/K)$ is an odd rational number.*

For $C = \mathbb{P}^1$, the twin-prime covers $\Lambda : C \rightarrow \mathbb{P}^1$ are in one-to-one correspondence with twin-prime pairs $(\Lambda, \Lambda - 1) \in k[\lambda] \times k[\lambda]$: the map $\lambda \mapsto \Lambda$ gives the corresponding map of function fields $\Lambda^* : F \rightarrow K$. We use Kummer theory to explicitly construct infinitely many twin-prime covers.

Given an odd twin-prime Legendre curve E_Λ/K we also study its quadratic twists. Let $\mathcal{O}_K \subset K$ be the functions regular away from $\bar{\infty}$. For $f \in \mathcal{O}_K - \{0\}$ define

$$\text{supp}_{\text{odd}}(f) := \{w \in |C| : \text{ord}_w(f) \equiv 1 \pmod{2}\}.$$

We say that the associated quadratic twist E_f/K (cf. section 3.4) is an irreducible twist of odd degree $d := -\text{ord}_{\bar{\infty}}(f)$ if $\text{supp}_{\text{odd}}(f) = \{\nu, \bar{\infty}\}$ for a unique point $\nu \in |C - \bar{\infty}|$. A key observation is that, in this case, ν is a point of odd

degree on C , simply because $\text{ord}_\nu(f) \cdot \deg(\nu) + (\text{even terms}) + \text{ord}_\infty(f) = 0$. Our second main theorem is the following.

Theorem 2 (cf. theorem 16) *Let E_Λ/K be an odd twin-prime Legendre curve. Fix $f \in \mathcal{O}_K - \{0\}$ such that $f(\bar{0}), f(\bar{1}) \neq 0$ and let E_f/K be the associated quadratic twist. If E_f/K is an irreducible twist of odd degree, then it has minimal analytic rank (as imposed by the sign of the functional equation).*

We note that the L -function of the quadratic twist of E_f by an element of $k^\times - k^{\times 2}$ is $L(-T, E_f/K)$, and that it has the opposite sign for its functional equation. In particular, exactly one of the curve and its (scalar) twist will have analytic rank zero and the other will have analytic rank one. It is an open problem to construct a point of infinite order when the analytic rank is one.

The first two sections of this paper are abridged version of the author's PhD thesis at Princeton University. We have eliminated some of the messy details involved in the successive applications of Tate's algorithm and have simply summarized the relevant results. The last section of this paper revisits the bounds for the analytic rank and eliminates one defect of the approach via L -functions. More precisely, we perform a cohomological 2-descent and derive stronger bounds (in general) for the analytic rank of a twisted Legendre curve. The new bounds are the same as the old when we consider an odd twin-prime Legendre curve or an irreducible twist of odd degree, hence this section may be safely omitted on a first read.

We gratefully acknowledge our advisor Nicholas M. Katz for suggesting that we study empirical evidence for Goldfeld's conjecture and for many helpful discussions during the course of our research. We would like to thank the referee for many helpful remarks and suggestions.

1.1 Notation

We use the following notation throughout this paper.

- q : odd prime power
- $k = \mathbb{F}_q$
- $k \rightarrow \bar{k}$: algebraic closure
- C/k : proper, smooth, geometrically-connected curve
- $F = k(\lambda) = k(\mathbb{P}^1)$
- $\mathcal{O}_F = k[\lambda]$: ring of integers
- $K = k(C)$
- $\text{Jac}(C)$: Jacobian of C
- $w \in |C|$: closed point

\mathcal{O}_w : completed local ring
 K_w : quotient field of \mathcal{O}_w
 $\pi_w \in \mathcal{O}_w$: uniformizer
 $k(w)$: residue field of \mathcal{O}_w
 $d_w = \deg(w) := [k(w) : k]$
 E/K : elliptic curve
 $\mathcal{E}^0 \rightarrow C$: minimal Weierstrass model
 $\mathcal{E} \rightarrow C$: Neronmodel
 M_{sp} : locus of split multiplicative reduction
 M_{ns} : locus of non-split multiplicative reduction
 A : locus of additive reduction
 $L(T, E/K)$: L -function
 $\text{rk}_{\text{an}}(E/K)$: analytic rank

2 L -Functions

Throughout this section C/k denotes a proper smooth geometrically connected curve with function field $K = k(C)$, and E/K denotes an elliptic curve with non-constant $j(E/K)$. Given a minimal Weierstrass model $\mathcal{E}^0 \rightarrow C$, there is a well-known recipe for computing $L(T, E/K)$. We review this recipe and apply it to E/K with level structure. In particular, if $\mathcal{T} \subset E(K)$ is finite subgroup and $N = |\mathcal{T}|$ is invertible in k , we deduce a formula for the mod N reduction $\bar{L}(T, E/K) \in 1 + T \cdot (\mathbb{Z}/N)[T]$. As a corollary, we also deduce the sign of the functional equation from the mod N reduction of the leading coefficient, when $N > 2$.

2.1 Reduction Theorem

Let E/K be an elliptic curve with non-constant j -invariant and minimal Weierstrass model $\mathcal{E}^0 \rightarrow C$. For each $w \in |C|$ there is a polynomial $P_w(T, E/K)$ in $\mathbb{Z}[T]$ such that the L -function $L(T, E/K)$ of E/K has the Euler product expansion

$$L(T, E/K) := \prod_{w \in |C|} 1/P_w(T^{d_w}, E/K), \quad d_w := \deg(w).$$

A priori $L(T, E/K)$ is an element of $1 + T \cdot \mathbb{Z}[[T]]$, but the assumption on $j(E/K)$ ensures it is an element of $1 + T \cdot \mathbb{Z}[T]$ (see page 11 of [K]).

Let $\mathcal{E}^0/\mathcal{O}_w$ denote the pullback under $\text{Spec}(\mathcal{O}_w) \rightarrow C$ and $\mathcal{E}^0/k(w)$ the special fiber of $\mathcal{E}^0/\mathcal{O}_w$. There is a recipe for $P_w(T)$ involving the reduction type of

$\mathcal{E}^0/\mathcal{O}_w$ and the trace of Frobenius

$$a_w := 1 + q^{d_w} - \#\mathcal{E}^0(k(w)).$$

Decompose C as a disjoint union of

$$\begin{aligned} U &:= \{w \in |C| : \mathcal{E}^0/\mathcal{O}_w \text{ has good reduction}\}, \\ M_{\text{sp}} &:= \{w \in |C| : \mathcal{E}^0/\mathcal{O}_w \text{ has split multiplicative reduction}\}, \\ M_{\text{ns}} &:= \{w \in |C| : \mathcal{E}^0/\mathcal{O}_w \text{ has non-split multiplicative reduction}\}, \\ A &:= \{w \in |C| : \mathcal{E}^0/\mathcal{O}_w \text{ has additive reduction}\}. \end{aligned}$$

Then

$$P_w(T, E/K) := \begin{cases} 1 - a_w T + q^{d_w} T^2 & w \in |U| \\ 1 - T & w \in M_{\text{sp}} \\ 1 + T & w \in M_{\text{ns}} \\ 1 & w \in A \end{cases}.$$

Lemma 3 *Let $\mathcal{T} \subset E(K)$ be a finite subgroup such that $N = |\mathcal{T}|$ is invertible in k and let w be in $|U|$. Then \mathcal{T} injects into $\mathcal{E}^0(k(w))$. In particular, $\#\mathcal{E}^0(k(w)) \equiv 0 \pmod{N}$ and*

$$P_w(T, E/K) \equiv (1 - T)(1 - q^{d_w} T) \pmod{N}.$$

PROOF. The first part is a well-known fact about the formal group of $\mathcal{E}^0/\mathcal{O}_w$, defined as $\text{Ker}(\mathcal{E}^0(\mathcal{O}_w) \rightarrow \mathcal{E}^0(k(w)))$: because N is invertible in k , multiplication by N is an automorphism of the formal group (see part 2, section 4.9, theorem 3 of [Se]). In particular, $\mathcal{T} \cap \text{Ker} = \{O\}$, so \mathcal{T} maps injectively to $\mathcal{E}^0(k(w))$. If G is a finite group and $H \subset G$ is a subgroup of size N , then $\#G \equiv 0 \pmod{N}$. \square

Let g be the genus of C and $Z(T, C/k)$ be its zeta function. It is a rational function

$$Z(T, C/k) = \frac{L(T, C/k)}{(1 - T)(1 - qT)}, \quad L(T, C/k) \in 1 + T \cdot \mathbb{Z}[T],$$

where $L(T, C/k)$ has degree $2g$. It also has an Euler product

$$Z(T, C/k) := \prod_{w \in |C|} 1/(1 - T^{d_w})$$

whose Euler factors are remarkably similar to those of the mod N reduction in the lemma. This is the crucial observation in the proof of the following theorem.

Theorem 4 *Suppose $N \geq 2$ is an integer invertible in k and $\mathcal{T} \subset E(K)$ is a finite subgroup of size N . Decompose $C = U \cup M_{\text{sp}} \cup M_{\text{ns}} \cup A$ as above. Then*

$$\begin{aligned} L(T, E/K) &\equiv Z(T, C/k)Z(qT, C/k) \\ &\times \prod_{M_{\text{sp}}} (1 - q^{d_w} T^{d_w}) \\ &\times \prod_{M_{\text{ns}}} \frac{(1 - T^{d_w})(1 - q^{d_w} T^{d_w})}{(1 + T^{d_w})} \\ &\times \prod_A (1 - T^{d_w})(1 - q^{d_w} T^{d_w}) \pmod{N}. \end{aligned}$$

Suppose $N = 2$ and let $M = M_{\text{sp}} \cup M_{\text{ns}}$. Then this simplifies to

$$L(T, E/K) \equiv Z(T, C/k)^2 \times \prod_M (1 - T^{d_w}) \times \prod_A (1 - T^{d_w})^2 \pmod{2}.$$

PROOF. This follows from the previous lemma:

$$\begin{aligned} \frac{L(T, E/K)}{Z(T, C/k)Z(qT, C/k)} &\equiv \prod_{w \in C-U} \frac{(1 - T^{d_w})(1 - q^{d_w} T^{d_w})}{P_w(T, E/K)} \\ &\equiv \prod_{M_{\text{sp}}} (1 - q^{d_w} T^{d_w}) \times \prod_{M_{\text{ns}}} \frac{(1 - T^{d_w})(1 - q^{d_w} T^{d_w})}{(1 + T^{d_w})} \\ &\quad \times \prod_A (1 - T^{d_w})(1 - q^{d_w} T^{d_w}) \pmod{N}. \end{aligned}$$

□

REMARK: Let $d := \deg(L(T, E/K))$ and $q = |k|$. The L -function satisfies a functional equation: there exists $\varepsilon \in \{1, -1\}$ such that

$$L(T, E/K) = \varepsilon \cdot (qT)^d \cdot L(1/(q^2T), E/K).$$

We call ε the *sign* of the functional equation. It was observed by Shimura (and related by him to Birch at the 1963 Boulder conference in the context of relating twists of modular forms and elliptic curves, cf. [BiSt]) that the analytic rank (the order of vanishing of $L(T, E/K)$ at $T = 1/q$) is even if $\varepsilon = 1$ and odd if $\varepsilon = -1$.

Given $L(T, E/K)$ one may recover the sign from the leading coefficient:

$$L(T, E/K) = \varepsilon q^d T^d + O(T^{d-1}).$$

We observe that the leading coefficient is a unit mod N , hence the degree of $L(T, E/K)$ does not drop when reducing mod N .

Corollary 5 *Let $N \geq 2$ be an integer invertible in k and $\mathcal{T} \subset E(K)$ a finite subgroup of size N . Decompose C as in the theorem and let $M = M_{\text{sp}} \cup M_{\text{ns}}$. Then*

$$d := \deg(L(T, E/K)) = 2(2g - 2) + \deg(M) + 2 \deg(A)$$

and

$$\varepsilon \equiv (-1)^{\#M_{\text{sp}}} q^{-\deg(A)} \pmod{N}.$$

PROOF. Recalling that $L(T, C/k) = q^g T^{2g} + O(T^{2g-1})$ (cf. bottom of page 54 of [R]) we apply the theorem to show that

$$\begin{aligned} L(T, E/K) &\equiv \frac{q^g}{q} \cdot \frac{q^{3g}}{q^3} \cdot \prod_{M_{\text{sp}}} (-q^{d_w}) \cdot \prod_{M_{\text{ns}}} q^{d_w} \cdot \prod_A q^{d_w} \cdot T^d + O(T^{d-1}) \\ &\equiv (-1)^{\#M_{\text{sp}}} \cdot q^{d-\deg(A)} \cdot T^d + O(T^{d-1}) \pmod{N}. \end{aligned}$$

The formula for d follows immediately from the congruence and the identity $\deg(Z(T, C/k)) = 2g - 2$. The asserted congruence for ε also follows. \square

Clearly $\deg(L(T, E/K))$ provides a weak upper bound on the analytic rank of E/K . One may deduce stronger bounds, though in the following corollary we restrict to $N = 2$.

Corollary 6 *Suppose $E(K)$ has a non-trivial element of 2-torsion. For any polynomial $F(T) \in 1 + T \cdot \mathbb{Z}[T]$ define $v(F)$ to be the $(1 - T)$ -adic valuation of its image in $1 + T \cdot \mathbb{F}_2[T]$ and extend it linearly to quotients $F_1(T)/F_2(T)$.*

- (1) $v(L(T, E/K)) = 2 \cdot (v(L(T, C/k)) - 2) + \sum_M v(1 - T^{d_w}) + 2 \cdot \sum_A v(1 - T^{d_w})$.
- (2) $v(L(T, C/k)) = 0$ if and only if $\text{Jac}(C)$ has no non-trivial k -rational 2-torsion.
- (3) If $\text{Jac}(C)$ has no k -rational 2-torsion, then

$$v(L(T, E/K)) = -4 + \sum_M 2^{\text{ord}_2(d_w)} + 2 \sum_A 2^{\text{ord}_2(d_w)},$$

where $\text{ord}_2(n)$ is the power of 2 dividing n in \mathbb{Z} .

PROOF. The first part follows immediately from the theorem. The second part follows from the fact that $\#\text{Jac}(C)(k) = L(1, C/k)$ (see theorem 5.9 of [R]). The last part follows from the identity $v(1 - T^{d_w}) = 2^{\text{ord}_2(d_w)}$: if $m > 0$ is an odd integer and $d = 2^r m$, then

$$1 - T^d = 1 - T^{2^r m} \equiv (1 - T^m)^{2^r} \pmod{2}$$

and

$$\frac{1 - T^m}{1 - T} \Big|_{T=1} = (1 + T + \cdots + T^{m-1}) \Big|_{T=1} = m.$$

□

REMARK: As we will show in section 4, the bound in part 1 of the corollary is not the best possible in general. In particular, by applying heavier machinery we can bound the analytic rank of E/K by $2(\delta_2 - 2) + \#M + 2\#A$, where δ_2 is the dimension of the k -rational 2-torsion of $\text{Jac}(C)$. On the other hand, the curves we focus on have odd d_w for all $w \in M \cup A$, in which case the two bounds are equivalent.

3 Curves and Twists

In the first two parts of this section we construct minimal Weierstrass models for the Legendre curve and a subset of its quadratic twists. We then apply the results of section 2 to bound the analytic rank of the curves and we isolate an infinite family for which we can compute the analytic rank exactly. In the last two parts of the section we generalize the results of the first two. We consider a larger family of curves, a tiny subset of which are the Legendre curve and its twists, and we isolate an infinite subfamily for which we can compute the analytic rank exactly.

3.1 Models of Twisted Legendre Curves

In this section we let $F = k(\lambda)$. The so-called Legendre curve has Weierstrass model

$$E_{\text{Leg}}/F : y^2 = x(x-1)(x-\lambda), \tag{1}$$

and to any $f \in F^\times$ we associate the twisted curve

$$E_f/F : y^2 = x(x-f)(x-f\lambda). \tag{2}$$

One may easily verify that it is the twist of E_{Leg} by the extension $F(\sqrt{f})/F$. We may assume without loss of generality that $f \in \mathcal{O}_F - \{0\}$ is square free of degree d . For ease of exposition we also assume f is relatively prime to $\lambda(\lambda-1)$.

REMARK: The twist by λ is isomorphic to the pullback of E_{Leg}/F along the F -automorphism $\lambda \mapsto 1/\lambda$ (cf. section 3.3). Similarly, the twist by $\lambda-1$ is the pullback along $\lambda \mapsto 1/(1-\lambda)$.

The (smooth) minimal Weierstrass model $\mathcal{E}^0 \rightarrow \mathbb{P}^1$ of E_f/F is the identity component of the Néron model $\mathcal{E} \rightarrow \mathbb{P}^1$. For every finite prime π in \mathcal{O}_F we may consider the reduction of (2) modulo π . In general, the resulting curve is an elliptic curve over the residue field $k(\pi)$, but for some π there is one non-smooth point: it is a node if π divides $\lambda(\lambda-1)$ and it is a cusp if π divides f . Using our assumptions on f one can easily show that the locus of smooth points (together with the point at infinity) is the special fiber of $\mathcal{E}^0 \rightarrow \mathbb{P}^1$ over π .

By an appropriate change of coordinates in (2) one may also construct the minimal Weierstrass model over $\lambda = \infty$. The corresponding canonical compactification of the special fiber of $\mathcal{E}^0 \rightarrow \mathbb{P}^1$ over $\lambda = \infty$ has one non-smooth point: it is a node if $d = \deg(f)$ is odd and a cusp otherwise.

3.2 Reduction of Twisted Legendre Curves

The next step in writing $L(T, E_f/F)$ is to analyze the reduction of a (smooth) minimal Weierstrass model $\mathcal{E}^0 \rightarrow \mathbb{P}^1$. We assume $f(0)f(1) \neq 0$ and define the loci

$$M, A := \begin{cases} \{0, 1, \infty\}, \{w : f(w) = 0\} & \text{if } \deg(f) \text{ is odd} \\ \{0, 1\}, \{w : f(w) = 0\} \cup \{\infty\} & \text{otherwise} \end{cases}.$$

As the following lemma shows, these are the loci of points over which the compactified special fiber of $\mathcal{E}^0 \rightarrow \mathbb{P}^1$ has a node or cusp respectively. We also write U for the open complement $\mathbb{P}^1 - M - A$.

Lemma 7 *The restriction $\mathcal{E}^0 \rightarrow U$ is an elliptic curve and the special fiber of $\mathcal{E}^0 \rightarrow \mathbb{P}^1$ over $w \in M \cup A$ has the following reduction.*

- (1) *If $w = 0 \in M$, then it has split multiplicative reduction if $-f(0)$ is a square in $k(w)^\times$ and non-split multiplicative reduction otherwise.*
- (2) *If $w = 1 \in M$, then it has split multiplicative reduction if $f(1)$ is a square in $k(w)^\times$ and non-split multiplicative reduction otherwise.*
- (3) *If $w = \infty \in M$, then it has split multiplicative reduction if minus the leading coefficient of f is a square in $k(w)^\times$ and non-split multiplicative reduction otherwise.*
- (4) *If $w \in A$, then it has additive reduction.*

Following Kodaira's classification, in the first three cases the fiber has type I_2 while in the last case it has type I_0^ if w is finite and I_2^* if $w = \infty$.*

This is a straightforward application of Tate's algorithm.

Applying the lemma and following the construction in Chapter 2 we associate to E_f/F the L -function $L(T, E_f/F)$.

Corollary 8 *If $f \in k^\times$, then $L(T, E_f/F) = 1$.*

PROOF. Let $\mathcal{E}^0 \rightarrow \mathbb{P}^1$ be a minimal Weierstrass model. By the previous lemma it has multiplicative reduction for $w \in M = \{0, 1\}$, additive reduction for $w \in A = \{\infty\}$ and good reduction everywhere else. Applying the degree formula in corollary 5 we obtain

$$\deg(L(T, E_f/F)) = -4 + 2 + 2 \cdot 1 = 0.$$

Hence $L(T, E_f/F) = 1$. \square

An immediate consequence of the corollary is that the Legendre curve and its scalar twist each have rank zero. In fact, it is well known that $E_f(F) \simeq \mathbb{Z}/2 \oplus \mathbb{Z}/2$ in both cases.

Theorem 9 *Let $f \in \mathcal{O}_F$ be a non-zero square-free polynomial of degree d and relatively prime to $\lambda(\lambda - 1)$. Let $f = \alpha \prod_i p_i$ be a factorization into monic irreducibles p_i of degree d_i and $\alpha \in k^\times$. Then*

$$L(T, E_f/F) \equiv \begin{cases} (1-T)^{-1} \prod_i (1-T^{d_i})^2 \pmod{2} & \text{if } d \text{ is odd} \\ \prod_i (1-T^{d_i})^2 \pmod{2} & \text{if } d \text{ is even} \end{cases}.$$

Let $\varepsilon \in \{1, -1\}$ be the sign of the functional equation. Then

$$\varepsilon = \begin{cases} +1 & \begin{array}{l} \text{if } d \text{ is odd and } -\alpha f(0)f(1) \notin k^{\times 2} \\ \text{or} \\ \text{if } d \text{ is even and } f(0)f(1) \in k^{\times 2} \end{array} \\ -1 & \text{otherwise} \end{cases}.$$

PROOF. By theorem 4 we have

$$\begin{aligned} L(T, E_f/F) &\equiv (1-T)^{-4} \prod_M (1-T) \prod_A (1-T^{d_w})^2 \\ &\equiv (1-T)^{-4+\deg(M)+2\deg(A \cap \infty)} \prod_i (1-T^{d_i})^2 \pmod{2}. \end{aligned}$$

By lemma 7, $M = \{0, 1, \infty\}$ if d is odd and $M = \{0, 1\}$ if d is even, hence

$$m = -4 + \deg(M) + 2\deg(A \cap \infty) = \begin{cases} = -4 + 3 + 0 = -1 & \text{if } d \text{ is odd} \\ = -4 + 2 + 2 = 0 & \text{if } d \text{ is even} \end{cases}$$

and the first part of the lemma follows. Our assumptions on f imply that $\deg(A)$ is always odd, hence the second part of the lemma follows once we analyze the congruence $\varepsilon \equiv q(-1)^{\#M_{\text{sp}}} \pmod{4}$ of corollary 5.

If d is odd, then lemma 7 implies $\#M_{\text{sp}}$ is odd if $(-\alpha)(-f(0))f(1) \in k^{\times 2}$ and even otherwise. We note that $-1 \in k^{\times 2}$ if and only if $q \equiv 1 \pmod{4}$. Therefore $\varepsilon = -1$ if $-\alpha f(0)f(1) \in k^{\times 2}$ and $\varepsilon = 1$ otherwise. Similarly, if d is even, then lemma 7 implies $\#M_{\text{sp}}$ is even if $(-f(0))f(1) \in k^{\times 2}$ and odd otherwise. Therefore $\varepsilon = 1$ if $f(0)f(1) \in k^{\times 2}$ and $\varepsilon = -1$ otherwise. \square

Corollary 10 *Let E_f/F be the twisted Legendre curve associated to an irreducible polynomial $f \in \mathcal{O}_F$ of odd degree d with leading coefficient α . Then*

$$L(T, E_f/F) \equiv (1 - T)(1 + T + \cdots + T^{d-1})^2 \pmod{2},$$

hence E_f/F has analytic rank at most one. It has analytic rank zero if $-\alpha f(0)f(1) \notin k^{\times 2}$ and analytic rank one otherwise. In particular, precisely one of E_f/F and its constant field twist will have analytic rank zero and the other will have analytic rank one.

PROOF. The first two statements follow from the theorem. For the last statement we note that the scalar twist of E_f/F corresponds to multiplying α by a non square in k^\times . \square

REMARK: One may apply the theorem to other f prime to $\lambda(\lambda - 1)$, but the resulting bound on the analytic rank will no longer be sharp in general. Let $d := \deg(f)$ and $\text{rk}_{\text{an}}(E_f/F)$ denote the analytic rank. Then by theorem 9

$$\text{rk}_{\text{an}}(E_f/F) \leq \begin{cases} -1 + 2 \sum_i 2^{\text{ord}_2(d_i)} & \text{if } d \text{ is odd} \\ 2 \sum_i 2^{\text{ord}_2(d_i)} & \text{if } d \text{ is even} \end{cases}.$$

We will improve these bounds in section 4 using heavier machinery, but it is worth noting that the above bound will usually be better than the naive bound $D := \deg(L(T, E_f/F))$ or Brumer's sharper bound $D/(2 \log_q(D - 4g + 4)) + o(D/(2 \log_q(D - 4g + 4)))$ (e.g., if some d_i is divisible by a large odd number). Cf. (5.2) of [U].

3.3 Pullback Legendre Curves

In this section we consider the pullback of Legendre curve by a finite flat map $\Lambda : C \rightarrow \mathbb{P}^1$. Writing Λ as an element of K^\times , the induced inclusion of function

fields $F \rightarrow K$ is given by $\lambda \mapsto \Lambda$, and the pullback Legendre curve has induced Weierstrass model

$$E_\Lambda/K : y^2 = x(x-1)(x-\Lambda). \quad (3)$$

It is well known that the construction of the minimal Weierstrass model is not stable under ramified base change (unless the original curve has semistable reduction), therefore we must study the effect of ramification on the reduction of (3).

For $w \in \mathbb{P}^1$ and $\bar{w} \in C$ we write $\bar{w}|w$ if $\Lambda(\bar{w}) = w$. We also write D_w for the fibral divisor

$$D_w := \Lambda^*(w) = \sum_{\bar{w}|w} e_{\bar{w}} [\bar{w}] \in \text{Div}(C).$$

We fix a uniformizer $\pi_{\bar{w}} \in \mathcal{O}_{\bar{w}}$ for each $\bar{w} \in |C|$, and to any $\bar{w}|\infty$ we associate the character $\chi_{\text{sign},\bar{w}} : K^\times \rightarrow k(\bar{w})^\times$ given by

$$\chi_{\text{sign},\bar{w}}(f) := f/\pi_{\bar{w}}^{\text{ord}_{\bar{w}}(f)} \pmod{k(\bar{w})}.$$

Lemma 11 *Let $\mathcal{E}^0 \rightarrow C$ be a minimal Weierstrass model of E_Λ/K . Fix $w \in \mathbb{P}^1$ and $\bar{w}|w$ of ramification index $e = e_{\bar{w}}$. If $w \in \mathbb{P}^1 - \{0, 1, \infty\}$, then the special fiber $\mathcal{E}_{\bar{w}}^0$ has good reduction. Otherwise it has the following reduction:*

- (1) *If $w = 0$, then $\mathcal{E}_{\bar{w}}^0$ has Kodaira type I_{2e} . It has split multiplicative reduction if -1 is a square in $k(\bar{w})^\times$ and non-split multiplicative reduction otherwise.*
- (2) *If $w = 1$, then $\mathcal{E}_{\bar{w}}^0$ has Kodaira type I_{2e} and split multiplicative reduction.*
- (3) *If $w = \infty$ and e is even, then $\mathcal{E}_{\bar{w}}^0$ has Kodaira type I_{2e} . It has split multiplicative reduction if $-\chi_{\text{sign},\bar{w}}(\Lambda)$ is a square in $k(\bar{w})^\times$ and non-split multiplicative reduction otherwise.*
- (4) *If $w = \infty$ and e is odd, then $\mathcal{E}_{\bar{w}}^0$ has Kodaira type I_{2e}^* .*

This is an application of Tate's algorithm.

We say that $\Lambda : C \rightarrow \mathbb{P}^1$ is a *twin-prime cover* if it is totally ramified at ∞ and the fibral divisors D_0, D_1 are inert, and we write $\bar{0}, \bar{1}, \bar{\infty}$, respectively, for the unique points lying over $0, 1, \infty$, respectively. We say the map Λ is an *odd twin-prime cover* if it is a twin-prime cover and $\deg(\Lambda)$ is odd. The reason for isolating the notion of "odd twin-prime cover" is the following theorem about $L(T, E_\Lambda/K)$.

Theorem 12 *Let $\Lambda : C \rightarrow \mathbb{P}^1$ be an odd twin-prime cover of degree d and E_Λ/K the pullback Legendre curve. Let $L(T, C/k)$ denote the numerator of the zeta function $Z(T, C/k)$. Then*

$$L(T, E_\Lambda/K) \equiv L(T, C/k)^2 (1 + T + \cdots + T^{d-1})^2 \pmod{2}.$$

For $F(T) \in 1 + T \cdot \mathbb{Z}[T]$ define $v(F)$ to be the $(1 - T)$ -adic valuation of its

image in $1 + T \cdot \mathbb{F}_2[T]$. Then

$$\mathrm{rk}_{\mathrm{an}}(E_\Lambda/K) \leq v(L(T, E_\Lambda/K)) = 2 \cdot v(L(T, C/k)).$$

In particular, if the 2-part of $\mathrm{Jac}(C)(k)$ is trivial, the central value $L(1/q, E_\Lambda/K)$ is an odd rational number.

PROOF. By lemma 11, $M_\Lambda = \{\bar{0}, \bar{1}\}$ is the locus of multiplicative reduction. The curve has additive reduction over $\bar{\infty}$, hence applying the last part of theorem 4 with $M = M_\Lambda$ and $A = \{\bar{\infty}\}$ we obtain

$$L(T, E_\Lambda/K) \equiv \frac{L(T, C/k)^2}{(1-T)^4} \cdot (1-T^d)^2 \cdot (1-T)^2 \pmod{2}.$$

Finally, we recall that $L(1, C/k)$ is an odd integer precisely when the 2-part of $\mathrm{Jac}(C)(k)$ is trivial. \square

REMARK: One could relax the conditions to having unique points $\bar{0}, \bar{1}, \bar{\infty}$ over $0, 1, \infty$, i.e., allow $e_{\bar{0}} > 1$, $e_{\bar{1}} > 1$ or $f_{\bar{\infty}} > 1$. However, we point out that for $C = \mathbb{P}^1$ the twin-prime covers correspond bijectively to pairs of irreducible polynomials $(\Lambda, \Lambda - 1) \in \mathcal{O}_F \times \mathcal{O}_F$, while the relaxed conditions correspond to a seemingly less natural collection of polynomial pairs.

Given an odd twin-prime cover $\Lambda : C \rightarrow \mathbb{P}^1$ we call the corresponding pullback Legendre curve E_Λ/K an *odd twin-prime Legendre curve*. For the remainder of the section we show that there are infinitely many such curves in general. If $q = |k| \equiv 1 \pmod{\ell}$ for some odd prime ℓ , then as a corollary to the following lemma we see that there are infinitely many twin-prime pairs.

Lemma 13 *If $q \equiv 1 \pmod{\ell}$ for an odd prime ℓ and $\beta \in \mathbb{F}_q^\times - \mathbb{F}_q^{\times \ell}$, then $x^{l^m} - \beta \in \mathbb{F}_q[x]$ is irreducible for all $m \geq 0$.*

PROOF. cf. Theorem 9.1 of [La]. \square

Corollary 14 *If $q = |k| \equiv 1 \pmod{\ell}$ for an odd prime ℓ , then for every $m \geq 0$ there are twin-prime pairs $(\Lambda, \Lambda - 1)$ of polynomials such that $\deg(\Lambda) = \deg(\Lambda - 1) = \ell^m$.*

PROOF. There is at least one pair $(\alpha, \alpha + 1) \in k^\times \times k^\times$ such that $\alpha, \alpha + 1 \in k^\times - k^{\times \ell}$ because $k^{\times \ell}$ has index $\ell > 2$ in k^\times . \square

REMARK: If $q = 1 + 2^N$ for $N \geq 2$, then one may apply similar methods to show that there are twin-prime pairs $(\Lambda, \Lambda - 1)$ for every degree 2^m , $m \geq 2$. It is an open problem for such q to construct infinitely many with $\deg(\Lambda)$ odd. Paul Pollack has pointed out (personal communication) that one may use similar ideas to construct infinitely many twin-prime pairs for $q = 3$. The key idea is to find one twin-prime pair $(\Lambda, \Lambda - 1)$ and one rational prime ℓ dividing $q^{\deg(\Lambda)} - 1$ such that $(\Lambda \circ x^\ell, \Lambda \circ x^\ell - 1)$ is also a twin-prime pair. A slight variant of the proof of the above lemma allows one to show that $(\Lambda \circ x^{\ell^n}, \Lambda \circ x^{\ell^n} - 1)$ is a twin-prime pair for $n \geq 1$.

REMARK: For $q \gg 0$, $\ell \gg 0$ one may even use the lemma to construct infinitely many prime $m + 1$ -tuples $(\Lambda, \Lambda - a_1, \dots, \Lambda - a_m)$ where $a_1, \dots, a_m \in \mathbb{F}_q^\times$ are distinct elements. While not directly relevant to our applications, this technique is useful when considering pullbacks of curves with more points of bad reduction.

REMARK: In the previous discussion we considered $C = \mathbb{P}^1$. For other C we do not know much about twin-prime covers. One sort of example is the following. Let $(f, f - 1) \in k[x] \times k[x]$ be a twin prime pair such that $\deg(f) = \deg(f - 1)$ is odd. Then the y -coordinate of the hyperelliptic curve

$$C/k : y^2 = f(x)$$

gives a twin-prime cover $\Lambda = y : C \rightarrow \mathbb{P}^1$. One may also show that the 2-part of $\text{Jac}(C)(k)$ is trivial.

3.4 Twisted Odd Twin-Prime Legendre Curves

We combine the ideas of the previous sections and consider quadratic twists of an odd twin-prime Legendre curve E_Λ/K . We associate to $f \in \mathcal{O}_K - \{0\}$ the twisted curve

$$E_f/K : y^2 = x(x - f)(x - f\Lambda). \quad (4)$$

Unfortunately, when the genus $g = p_g(C)$ is positive there is no longer a good notion of “square free” in general: there exist $f \in \mathcal{O}_K$ of positive degree such that $\text{div}(f) = mD \in \text{Div}^0(C)$ for some $m > 1$, yet nD is not principal for $1 \leq n < m$. In particular, for every $g \in K^\times$ representing the coset $fK^{\times 2}$, there exists $w \in |C|$ such that $|\text{ord}_w(g)| \geq 2$. Nonetheless, the parity of $\text{ord}_w(f)$ for $w \in |C|$ is what really matters, so we define, for $f \in \mathcal{O}_K - \{0\}$,

$$\text{supp}_{\text{odd}}(f) := \{w \in |C| : \text{ord}_w(f) \equiv 1 \pmod{2}\}.$$

We call E_f/K an *irreducible twist of odd degree* $d := -\text{ord}_{\infty}(f)$ if $\text{supp}_{\text{odd}}(f) = \{\nu, \infty\}$ for a unique $\nu \in |C - \infty|$, necessarily itself of odd degree.

It is worth noting that if the 2-part of $\text{Jac}(C)(k)$ is trivial, then there are infinitely many irreducible twists of prime degree. First, there is an explicitly computable constant γ such that for all prime l

$$|C(\mathbb{F}_{q^l}) - C(\mathbb{F}_q)| > (1/2)q^l - \gamma.$$

Hence for prime $l \gg 0$ there is at least one $\nu \in C(\mathbb{F}_{q^l})$ such that $\deg(\nu) = l$. Further, because the 2-part of $\text{Jac}(C)(k)$ is trivial, there is a smallest odd integer $m > 0$ such that $m([\nu] - l[\infty]) = \text{div}(g_\nu)$ for some $g_\nu \in \mathcal{O}_K - \{0\}$. Such a g_ν gives an irreducible twist of odd degree lm .

REMARK: An alternate approach, as explained on page 15 of [K], is to fix an effective divisor D on C and to consider only $f \in K^\times$ whose divisor of poles is exactly D and which have $\deg(D)$ distinct zeros (over \bar{k}), none of which lie in a prespecified finite set $S \subset |C|$. In order to force twisting at a point $w \in |C|$ one chooses a D such that $\text{ord}_w(D)$ is odd. The advantage of such an approach is that it allows one to work with a set of functions which naturally form the set of k -points of a smooth, geometrically connected k -scheme, which in turn imposes a “uniformity” on the corresponding set of L -functions: they have a common degree.

Let $f \in \mathcal{O}_K - \{0\}$ subject only to the condition that $\text{supp}(f)$ is disjoint from $\{\bar{0}, \bar{1}\}$, i.e., $f(\bar{0}), f(\bar{1}) \neq 0$. We define the finite loci

$$M, A := \begin{cases} \{\bar{0}, \bar{1}, \infty\}, \text{supp}_{\text{odd}}(f) - \{\infty\} & \text{if } \infty \in \text{supp}_{\text{odd}}(f) \\ \{\bar{0}, \bar{1}\}, \text{supp}_{\text{odd}}(f) \cup \{\infty\} & \text{otherwise} \end{cases}.$$

As the following lemma shows, these are the loci of multiplicative and additive reduction respectively and the open complement $U = C - M - A$ is the locus of good reduction.

Lemma 15 *Let $\mathcal{E}^0 \rightarrow C$ be a minimal Weierstrass model of E_f/K . The restriction $\mathcal{E}^0 \rightarrow U$ is an elliptic curve, and otherwise the special fiber of $\mathcal{E}^0 \rightarrow C$ over $w \in |C|$ has the following reduction.*

- (1) *If $w = \bar{0}$, then $\mathcal{E}_{\bar{0}}^0$ has split multiplicative reduction if $-f(\bar{0}) \in k(\bar{0})^{\times 2}$ and non-split multiplicative reduction otherwise.*
- (2) *If $w = \bar{1}$, then $\mathcal{E}_{\bar{1}}^0$ has split multiplicative reduction if $f(\bar{1}) \in k(\bar{1})^{\times 2}$ and non-split multiplicative reduction otherwise.*
- (3) *If $w = \infty \in M$, then \mathcal{E}_{∞}^0 has split multiplicative reduction if $-\chi_{\text{sign}, \infty}(f\Lambda)$ is a square in $k(w)^\times$ and non-split multiplicative reduction otherwise, where $\chi_{\text{sign}, \infty} : K^\times \rightarrow k(\infty)^\times$ is the character given in the previous section.*
- (4) *If $w \in A$, then \mathcal{E}_w^0 has additive reduction.*

The first two cases have Kodaira type I_2 and the third has type $I_{2\deg(\Lambda)}$. The

last has type I_0^* if w is finite and $I_{2\deg(\Lambda)}^*$ if $w = \overline{\infty}$.

Once again this is an application of Tate's algorithm.

REMARK: Because $\text{ord}_{\overline{\infty}}(f\Lambda)$ is even, whether or not $-f_{\text{sign},\overline{\infty}}(f\Lambda)$ is a square in $k(\overline{\infty})^\times$ is independent of the choice of the uniformizer $\pi_{\overline{\infty}}$.

Theorem 16 *Let E_f/K be an irreducible twist of odd degree of an odd twin-prime Legendre curve E_Λ/K . Suppose $f(\overline{0}), f(\overline{1}) \neq 0$ and let $\{\nu\} := \text{supp}_{\text{odd}}(f) - \overline{\infty}$. Let $L(T, C/k)$ denote the numerator of the zeta function $Z(T, C/k)$, $d_\Lambda := \deg(\Lambda)$ and $d_\nu := \deg(\nu)$. Then*

$$L(T, E_f/K) \equiv (1 - T) L(T, C/k)^2 \prod_{d=d_\Lambda, d_\nu} (1 + T + \cdots + T^{d-1})^2 \pmod{2}.$$

In particular, if the 2-part of $\text{Jac}(C)(k)$ is trivial, then E_f/K has the minimal analytic rank imposed by the sign of the functional equation of $L(T, E_f/K)$.

PROOF. By the previous lemma $M = \{\overline{0}, \overline{1}, \overline{\infty}\}$ and $A = \{\nu\}$ are the loci of multiplicative and additive reduction respectively. Applying theorem 4 we obtain

$$L(T, E_f/K) \equiv (1 - T)^{-4} L(T, C/k)^2 \cdot (1 - T^{d_\Lambda})^2 (1 - T) \cdot (1 - T^{d_\nu})^2 \pmod{2}.$$

Finally, $v(L(T, C/k)) = 0$ precisely when the 2-part of $\text{Jac}(C)(k)$ is trivial (cf. the proof of theorem 12). \square

If we assume that the Birch and Swinnerton-Dyer conjecture is true, then any elliptic curve which has analytic rank one has algebraic rank one as well. It is an open problem to construct a point of infinite order when E_f/K is known to have analytic rank one. As discussed in [U] an appropriate Gross-Zagier formula would allow us to use the Heegner point. Ulmer has announced a proof of such a formula, though his paper has not yet appeared in the literature. The only published results are those of [RT], which are insufficient for our purpose: they work only for $E/k(\mathbb{P}^1)$ with semistable reduction (and some other properties), hence do not apply to E_f/K .

4 Etale Descent

Throughout this section we fix a global field $K = k(C)$ of char p and an elliptic curve E/K with non-constant j -invariant. We write $\mathcal{E}^0 \rightarrow C$ for the (smooth) minimal Weierstrass model of E/K and $\mathcal{E} \rightarrow C$ for the Néron model, and we

regard them as both group schemes and etale sheaves over C . As we plan to perform ℓ^n -descent for some rational prime $\ell \neq p$, this will be justified. Rather than performing the descent using Galois cohomology we have used the more modern theory of Neron models and etale cohomology because we feel that it more accurately reflects the ‘geometrical’ nature of the arguments in section 2 and is more amenable to generalization.

There is a short exact sequence of etale sheaves

$$0 \longrightarrow \mathcal{E}^0 \longrightarrow \mathcal{E} \longrightarrow \Phi \longrightarrow 0,$$

where Φ is the component sheaf of \mathcal{E} . For any subgroup $\Psi \subset \Phi$ we write \mathcal{E}^Ψ for the corresponding subgroup of \mathcal{E} , so that

$$0 \longrightarrow \mathcal{E}^0 \longrightarrow \mathcal{E}^\Psi \longrightarrow \Psi \longrightarrow 0$$

is exact. If we write $M, A \subset C$, respectively, for the locus of multiplicative and additive reduction of $\mathcal{E} \rightarrow C$, respectively, then Ψ is a skyscraper sheaf supported on $Z = M \cup A$.

Fix a rational prime $\ell \neq p$. Multiplication by ℓ^n is an etale map on E/K . It extends to a homomorphism of $\mathcal{E} \rightarrow C$ and we write $\mathcal{E}_{\ell^n} \rightarrow C$ for the kernel. Similarly, for any subgroup $\Psi \subset \Phi$, we write $\mathcal{E}_{\ell^n}^\Psi, \Psi_{\ell^n}$, respectively, for the kernel of multiplication by ℓ^n on \mathcal{E}^Ψ, Ψ , respectively. For every positive m, n , there is an exact sequence

$$0 \longrightarrow \mathcal{E}_{\ell^m}^\Psi \longrightarrow \mathcal{E}_{\ell^{m+n}}^\Psi \xrightarrow{\times \ell^m} \mathcal{E}_{\ell^n}^{\ell^m \Psi} \longrightarrow 0. \quad (5)$$

We will only be interested in this sequence when $\Psi = 0$. However, we point out that $\mathcal{E}_{\ell^i}^{\Phi_{\ell^j}} = \mathcal{E}_{\ell^i}$ for all $i \leq j$, so the sequences for $\Psi = \Phi_{\ell^{m+n}}$ and $\Psi = \Phi$ are isomorphic.

The following ‘Kummer square’ replaces the usual Kummer sequence of Galois

cohomology:

$$\begin{array}{ccccccc}
& & 0 & & 0 & & 0 \\
& & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \mathcal{E}_{\ell^n}^0 & \longrightarrow & \mathcal{E}^0 & \xrightarrow{\times \ell^n} & \mathcal{E}^0 \longrightarrow 0 \\
& & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \mathcal{E}_{\ell^n} & \longrightarrow & \mathcal{E} & \xrightarrow{\times \ell^n} & \mathcal{E}^{\ell^n} \Phi \longrightarrow 0 \\
& & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \Phi_{\ell^n} & \longrightarrow & \Phi & \xrightarrow{\times \ell^n} & \ell^n \Phi \longrightarrow 0 \\
& & \downarrow & & \downarrow & & \downarrow \\
& & 0 & & 0 & & 0
\end{array} \tag{6}$$

It is relatively easy to show that the rows and last two columns are exact. With a little work, one can also show that the first column is exact.

Lemma 17 *The sequence $0 \rightarrow \mathcal{E}_{\ell^n}^0 \rightarrow \mathcal{E}_{\ell^n} \rightarrow \Phi_{\ell^n} \rightarrow 0$ is exact.*

PROOF. It is easy to show that the sequence is left exact. To show right exactness we consider every $w \in Z$ and show that $\mathcal{E}_{\ell^n}(\mathcal{O}'_w) \rightarrow \Phi_{\ell^n}(\mathcal{O}'_w) \rightarrow 0$ is exact, where K_w is the w -adic completion of K , L_w/K_w is a ‘sufficiently large’ unramified extension of local fields, and \mathcal{O}'_w is the valuation ring of L_w . Replacing L_w be a quadratic extension if necessary, we may assume \mathcal{E} has split multiplicative or addition reduction over \mathcal{O}'_w . Therefore there is a section $\Phi_{\ell^n}(k'(w)) \rightarrow \mathcal{E}_{\ell^n}(k'(w))$, where $k'(w)$ is the residue field of \mathcal{O}'_w , and the ‘Teichmuller lift’ $\mathcal{E}_{\ell^n}(k'(w)) \rightarrow \mathcal{E}_{\ell^n}(\mathcal{O}'_w)$ gives a section $\Phi_{\ell^n}(\mathcal{O}'_w) = \Phi_{\ell^n}(k'(w)) \rightarrow \mathcal{E}_{\ell^n}(\mathcal{O}'_w)$. \square

One may extract the following short exact sequence of \mathbb{Z}/ℓ^n -modules from the cohomology sequence of the first row of (6):

$$0 \longrightarrow \mathcal{E}^0(C)/\ell^n \mathcal{E}^0(C) \longrightarrow H^1(\mathcal{E}_{\ell^n}^0) \longrightarrow H^1(\mathcal{E}^0)_{\ell^n} \longrightarrow 0, \tag{7}$$

where $H^i(\cdot)$ is the etale cohomology group $H^i(C, \cdot)$. In Shioda’s work (e.g., page 475 of [Sh]) one finds that $\mathcal{E}^0(C)$ is a free \mathbb{Z} -module of finite rank r — the Mordell-Weil rank of $E(K)$ — hence the first term of (7) is a free \mathbb{Z}/ℓ^n -module of rank r . On the other hand, $H^1(\mathcal{E}_{\ell^n}^0)$ is finitely generated because $\mathcal{E}_{\ell^n}^0 \rightarrow C$ is a quasi-finite group scheme, hence the last two terms are finite as well.

The fact that $\mathcal{E}_{\ell^n}^0(C) = 0$ for all n implies that the cohomology sequence of

(5) for $\Psi = 0$ simplifies to

$$0 \longrightarrow H^1(\mathcal{E}_{\ell^m}^0) \longrightarrow H^1(\mathcal{E}_{\ell^{m+n}}^0) \xrightarrow{\ell^m} H^1(\mathcal{E}_{\ell^n}^0) \longrightarrow \dots .$$

We write $H^1(\mathcal{E}_{\ell^\infty}^0)$ for the inductive limit of $H^1(\mathcal{E}_{\ell^n}^0)$ with respect to n , noting that $H^1(\mathcal{E}_{\ell^n}^0) = H^1(\mathcal{E}_{\ell^\infty}^0)_{\ell^n}$. Taking the inductive limit of (7) with respect to n we obtain the exact sequence of torsion \mathbb{Z}_ℓ -modules

$$0 \longrightarrow \mathcal{E}^0(C) \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell \longrightarrow H^1(\mathcal{E}_{\ell^\infty}^0) \longrightarrow H^1(\mathcal{E}^0)_{\ell^\infty} \longrightarrow 0. \quad (8)$$

If we tensor this sequence with \mathbb{Z}/ℓ^n , then we obtain (7).

We call the middle term of (8) the étale ℓ^∞ -Selmer group because the first term is isomorphic to $(\mathbb{Q}_\ell/\mathbb{Z}_\ell)^r$ and the last term differs from $\text{III}(E/K)_{\ell^\infty}$ by a finite group. More precisely, the image of $H^1(\mathcal{E}^0) \rightarrow H^1(\mathcal{E})$ in the cohomology sequence of the middle column of (6) is $\text{III}(E/K)$ (by proposition III.9.2 of [Mi]) and we have the exact sequence

$$\Phi(C) \longrightarrow H^1(\mathcal{E}^0) \longrightarrow \text{III}(E/K) \longrightarrow 0. \quad (9)$$

Putting these facts together and recalling that the corank of the (Galois) ℓ^∞ -Selmer group is equal to the analytic rank of E/K (cf. [T2]), we obtain the following lemma.

Lemma 18 *The corank of $H^1(\mathcal{E}_{\ell^\infty}^0)$ is equal to the analytic rank of E/K .*

An obvious corollary is that the analytic rank of E/K is at most the dimension of $H^1(\mathcal{E}_\ell^0)$, though one can often do a little better. Under favorable conditions one may start by explicitly computing $H^1(\mathcal{E}_\ell^0)$ using the cohomology sequence of the first column of (6), so for the remainder of this section we assume that \mathcal{E}_ℓ is isomorphic to the constant sheaf $\mathbb{Z}/\ell \oplus \mathbb{Z}/\ell$.

If we fix an isomorphism $\mu_\ell \simeq \mathbb{Z}/\ell$, then there is a short exact sequence

$$0 \longrightarrow \mathcal{E}_\ell(C) \longrightarrow H^1(\mathcal{E}_\ell) \longrightarrow \text{Jac}(C)(k)_\ell^{\oplus 2} \longrightarrow 0;$$

it arises from the Leray spectral sequence $H^i(\text{Gal}(\bar{k}/k), H^j(C \times \bar{k}, \mathcal{E}_\ell)) \Rightarrow H^{i+j}(\mathcal{E}_\ell)$. Applying Shapiro's lemma to $\Phi_\ell/k(w)$ one can show that the composite map

$$\iota_\ell : \mathcal{E}_\ell(C) \rightarrow H^1(\mathcal{E}_\ell) \rightarrow H^1(\Phi_\ell) \simeq \oplus_w \Phi_\ell(w)$$

sends P to $\oplus_w([\text{deg}(w)P])$, where $[\text{deg}(w)P]$ denotes the image in $\Phi_\ell(w)$.

Lemma 19 *If $\Lambda : C \rightarrow \mathbb{P}^1$ is an odd twin-prime cover and E/K is a quadratic twist of the pullback Legendre curve E_Λ/K , then $\text{Ker}(\iota_2) = 0$.*

PROOF. If $\{\bar{0}, \bar{1}\} \subset M$, then one easily verifies that $\mathcal{E}_2(C) \xrightarrow{\sim} \Phi_2(\bar{0}) \oplus \Phi_2(\bar{1})$.

Similarly, if $w \in \{\bar{0}, \bar{1}\} \cap A$, then $\mathcal{E}_2(C) \xrightarrow{\sim} \Phi_2(w)$. In both cases $\deg(\bar{0}) = \deg(\bar{1})$ is odd, so the lemma follows. \square

If we assume $\text{Ker}(\iota_\ell)$ is trivial, then as a corollary we obtain the exact sequence of \mathbb{Z}/ℓ -modules

$$0 \longrightarrow \Phi_\ell(C)/\mathcal{E}_\ell(C) \longrightarrow H^1(\mathcal{E}_\ell^0) \longrightarrow \text{Jac}(C)(k)_\ell^{\oplus 2}$$

and a near-optimal bound

$$\text{rk}_{\text{an}}(E/K) \leq h^0(\Phi_\ell) + 2(\delta_\ell - 1),$$

where $h^0(\Phi_\ell)$ is the dimension of $\Phi_\ell(C)$ and δ_ℓ is the dimension of $\text{Jac}(C)(k)_\ell$.

Theorem 20 *If $\text{Ker}(\iota_\ell) = 0$ and $(\ell\Phi)_\ell = 0$, then $\text{rk}_{\text{an}}(E/K) \leq h^0(\Phi_\ell) + 2(\delta_\ell - 2)$.*

PROOF. For any torsion \mathbb{Z}_ℓ -module M we write M_{div} for the divisible subgroup and M^\wedge for the quotient M/M_{div} . We let $M = H^1(\mathcal{E}^0)_{\ell^\infty}$ and show that $(M^\wedge)_\ell$ has dimension at least 2, hence so does $H^1(\mathcal{E}^0)_\ell$, implying the theorem. Let $N = H^1(\mathcal{E})_{\ell^\infty}$. There is a perfect pairing $(M^\wedge)_\ell \times N^\wedge \rightarrow \mathbb{Q}_\ell/\mathbb{Z}_\ell$ (theorem III.9.4 of [Mi]), so it suffices to prove that $(N^\wedge)_\ell$ has dimension at least 2. By assumption $\text{Ker}(\iota_\ell)$ is trivial. The kernel of the composition of ι_ℓ with $H^1(\Phi_\ell) \rightarrow H^1(\Phi)$ is also trivial: the image of the boundary map $(\ell\Phi)(C) \rightarrow H^1(\Phi_\ell)$ has order prime to ℓ because $(\ell\Phi)_\ell = 0$. Finally, the composite map $\text{Hom}(\mathbb{Z}, \mathcal{E}_\ell(C)) \rightarrow N \rightarrow N^\wedge$ has trivial kernel because $N \rightarrow H^1(\Phi)$ factors through $N \rightarrow N^\wedge$, hence $\dim(N^\wedge)_\ell \geq 2$. \square

REMARK: $(\ell\Phi)_\ell = 0$ if and only if $\Phi_{\ell^2} = \Phi_\ell$.

Corollary 21 *If $\Lambda : C \rightarrow \mathbb{P}^1$ is an odd twin-prime cover and E_f/K is a quadratic twist of the pullback Legendre curve E_Λ/K , then*

$$\text{rk}_{\text{an}}(E_f/K) \leq 2(\delta_\ell - 2) + \#M + 2\#A.$$

PROOF. Using lemma 15 one can easily show that $\Phi_2(w) = \Phi_4(w)$ is isomorphic to $\mathbb{Z}/2$ if $w \in M$ and $\mathbb{Z}/2 \oplus \mathbb{Z}/2$ if $w \in A$. \square

REMARK: It is clear that the bound in the corollary is better in general than the one in corollary 6; however, it is worth noting that the latter is the limit formula if we extend scalars to $\mathbb{F}_{q^{2^n}}$ and let n tend to ∞ : every place of degree $2d$ in $M \cup A$ will be replaced by two places of degree d after the

extension $\mathbb{F}_q \rightarrow \mathbb{F}_{q^2}$. An important part of this relationship is the fact that a quadratic scalar extension has no effect on the mod 2 reduction of $L(T, E_f/K)$. In fact, the sequence of L -functions tends to a limit in $\mathbb{Z}_2[T]$ as $n \rightarrow \infty$: it is the ‘Teichmüller lift’ of the mod 2 reduction of $L(T, E_f/K)$. Is there any interpretation of the zeros of the limit function?

REMARK: Suppose that E_Λ/K is an odd twin-prime Legendre curve. If one traces through the proof of theorem 20 and recalls (9), then one finds that $\text{III}(E_\Lambda/K)_2$ is trivial. Similarly, if E_f/K is an irreducible twist of E_Λ/K of odd degree and $M = \text{III}(E_f/K)_{2^\infty}$, then one can also show that M^\wedge is trivial. More precisely, one can show that it has at most one non-zero element of 2-torsion, hence must be trivial by well-known properties of the Cassels-Tate pairing $M^\wedge \times M^\wedge \rightarrow \mathbb{Q}_2/\mathbb{Z}_2$.

References

- [BiSt] B. J. Birch, N. M. Stephens, “The parity of the rank of the Mordell-Weil group,” *Topology* 5 (1966), 295–299.
- [D1] P. Deligne, “Les constantes des équations fonctionnelles,” *Seminaire Delange-Pisot-Poitou (Théorie des nombres)*, 11^e année, 1969/70, n^o 19 bis.
- [G] D. Goldfeld, “Conjectures on elliptic curves over quadratic fields,” *Number theory, Carbondale 1979 (Proc. Southern Illinois Conf., Southern Illinois Univ., Carbondale, Ill., 1979)*, pp. 108–118, Lecture Notes in Math., 751, Springer, Berlin, 1979.
- [K] N. Katz, *Twisted L-Functions and Monodromy*, Annals of Mathematics Studies, 150. Princeton University Press, Princeton, NJ, 2002.
- [La] S. Lang, *Algebra*, Revised third edition, Graduate Texts in Mathematics, 211, Springer-Verlag, New York, 2002.
- [Mi] J.S. Milne, *Arithmetic Duality Theorems*, Academic Press, Inc., Boston, MA, 1986.
- [R] M. Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, 210. Springer-Verlag, New York, 2002.
- [RT] H.-G. Rück, U. Tipp, “Heegner points and L -series of automorphic cusp forms of Drinfeld type,” *Doc. Math.* 5 (2000), 365–444.
- [Se] J-P Serre, *Lie algebras and Lie groups. 1964 lectures given at Harvard University*, Second edition, Lecture Notes in Mathematics, 1500. Springer-Verlag, Berlin, 1992.

- [Sh] T. Shioda, “Theory of Mordell-Weil lattices, ” *Proceedings of the International Congress of Mathematicians*, Vol. I, II (Kyoto, 1990), 473–489, Math. Soc. Japan, Tokyo, 1991.
- [Si1] J. Silverman, *Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, 106, Springer-Verlag, 1986.
- [Si2] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, 151, Springer-Verlag, 1994.
- [T1] J. Tate, “Algorithm for determining the type of a singular fiber in an elliptic pencil,” *Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pp. 33–52. Lecture Notes in Math., Vol. 476, Springer, Berlin, 1975.
- [T2] J. Tate, “On the conjectures of Birch and Swinnerton-Dyer and a geometric analog,” *Séminaire Bourbaki*, Vol. 9, Exp. No. 306, 415–440, Soc. Math. France, Paris, 1995.
- [U] D. Ulmer, “Elliptic curves and analogies between number fields and function fields,” *Heegner Points and Rankin L-Series*, MSRI 49, 2004, pp. 285–315.