ZETA FUNCTIONS OF A CLASS OF ELLIPTIC CURVES OVER A RATIONAL FUNCTION FIELD OF CHARACTERISTIC TWO

ERNST-ULRICH GEKELER, RITA LEITL, AND BODO WACK

ABSTRACT. We show how to calculate the zeta functions and the orders $|\text{Ш}|$ of Tate-Shafarevich groups of the elliptic curves with equation $Y^2 + XY = X^3 + \alpha X^2 + \text{const} \cdot T^{-k}$ over the rational function field $\mathbf{F}_q(T)$, where q is a power of 2. In the range $q = 2$, $k \leq 37$, $\alpha \in \mathbf{F}_2[T^{-1}]$ odd of degree ≤ 19, the largest values obtained for $|\text{Ш}|$ are 47^2 (one case), 39^2 (one case) and 27^2 (three cases).

We observe and discuss a remarkable pattern for the distributions of signs in the functional equation and of fudge factors at places of bad reduction. These imply strong restrictions on the precise form of the Langlands correspondence for GL(2) over local or global fields of characteristic two.

INTRODUCTION

The behavior of elliptic curves in characteristic two deviates significantly from that of elliptic curves in other characteristics. The main difference (except that, for some questions, the multiplicative group of the ground field has to be replaced by its additive group) stems from the facts that pencils of elliptic curves in characteristic two admit arbitrarily high ramification (a property shared by elliptic curves in characteristic three), and that quadratic twists may arbitrarily enlarge conductors (a property peculiar to characteristic two). The aim of the present paper is to provide some empirical material about the simplest case of such a situation, namely, that of an elliptic curve E over $K = \mathbf{F}_q(T)$ (q is a power of 2) with its ramification essentially concentrated in the place v that corresponds to $T = 0$. In order to have a non-constant j-invariant, we further assume that E has (split) multiplicative reduction at yet another place w. We deal with the case where w is the place at infinity. These curves and their conductors have been classified in [4], which led to a certain normal form $E = E_{\alpha,\beta}$. We first express the ingredients of the Birch/Swinnerton-Dyer conjecture for E/K through quantities that may be computed mechanically from this normal form (formula (2.12)). Then we sketch (section 3) an algorithm that allows fast calculation of the zeta functions of $E_{\alpha,\beta}$ in a wide range of the parameters α and β. We finally present numerical results ($\approx 20\,000$ curves) over $K = \mathbf{F}_2(T)$ and comment on the observed distribution of fudge factors at the place v, signs in the functional equation and zero orders at

the critical point. The calculations were performed on a SGI Challenge L with 120 MIPS. The marginal computer time needed to determine the zeta function of an elliptic curve E/K with total degree 41 of its conductor was about 300 seconds.

1. THE CURVES $E_{\alpha,\beta}$

We let $\mathbf{F}_q$ be a finite field with $q = 2^e$ elements, $A = \mathbf{F}_q[T]$ the polynomial ring and $K = \mathbf{F}_q(T)$ the rational function field in an indeterminate T over $\mathbf{F}_q$. Places v of K are identified in the usual way with elements of the set $\{x \in A \mid x \text{ monic, prime}\} \cup \{\infty\}$. We briefly write "$v = T$" (or also "$v = 0$") and "$v = \infty$" for the places corresponding to $x = T$ and ∞, respectively.

Let E/K be an elliptic curve. If its invariant $j(E)$ is non-zero, an equation for E may be written in short Weierstraß form (SWF):

$$(1.1) \qquad\qquad Y^2 + XY = X^3 + a_2 X^2 + a_6$$

with discriminant $\Delta = a_6$ and $j(E) = a_6^{-1}$. We are interested in such E/K whose conductor $\operatorname{cond}(E)$ is essentially concentrated in one rational place v of K, where, without loss of generality, $v = 0$. Since this assumption, by an easy argument ([4], Prop. 2.1), implies that E is a twisted constant curve (i.e., $j(E) \in \mathbf{F}_q$), we admit one further rational place $w \neq v$ of K (without loss of generality, $w = \infty$) where E has split multiplicative reduction. Our objects of study are therefore elliptic curves E/K subject to the condition:

1.2. E has good reduction off $\{0, \infty\}$ and split multiplicative reduction at $v = \infty$. The conductor $\operatorname{cond}(E)$ has then the form

$$(1.3) \qquad\qquad \operatorname{cond}(E) = (0)^f \cdot (\infty).$$

But note that, unlike the common cases of "good" characteristics, the exponential conductor $f = f(E/K_0)$ of E over $K_0 = \mathbf{F}_q((T))$ may be arbitrarily large. Some of the features to follow are therefore peculiar to characteristic two (with some analogous phenomena in characteristic three), and do not have a counterpart in other characteristics.

The next two results are proved in [4]. Here and in the sequel, an "odd" polynomial is a polynomial all of whose exponents are odd.

1.4. Theorem. *Condition* (1.2) *on E/K is equivalent to the following:*
(1.2′) *E may be written in SWF*

$$E_{\alpha,\beta} : Y^2 + XY = X^3 + \alpha X^2 + \beta,$$

where $\alpha \in \mathbf{F}_q[T^{-1}]$ is an odd polynomial and $\beta = c \cdot T^{-k}$ with $c \in \mathbf{F}_q^*$ and $k \in \mathbf{N}$. Moreover, up to K-isogeny, the exponent k may be chosen odd.   □

1.5. Theorem. *Let $E_{\alpha,\beta}/K$ be an elliptic curve as above. Suppose that $\alpha \in \mathbf{F}_q[T^{-1}]$ is an odd polynomial and $\beta = c \cdot T^{-k}$ with $c \in \mathbf{F}_q^*$ and $k \in \mathbf{N}$ odd. Then $f = f(E_{\alpha,\beta}/K_0)$ is given by*

$$f = \begin{cases} k + 2, & 2 \cdot \deg \alpha < k, \\ 2 \cdot \deg \alpha + 2, & 2 \cdot \deg \alpha > k. \end{cases} \quad \square$$

1.6.   Next, let L be any field of characteristic two. The following sets correspond bijectively to each other:

(a) Separable extensions L'/L of degree ≤ 2;
(b) Characters χ of $\mathrm{Gal}(L^{\mathrm{sep}}/L)$ with $\chi^2 = 1$;
(c) $L/\wp(L)$, where $\wp : L \longrightarrow L$ is the additive map $x \longmapsto x^2 + x$.

1.7.   Let $L_\alpha = L(s)$ with $\wp(s) = \alpha \in L$ be a separable quadratic extension. If E/L is given in SWF

$$E : Y^2 + XY = X^3 + a_2 X^2 + a_6 \,,$$

then its twist by L_α (or by the associated character χ, or by α) is

$$E_\alpha : Y^2 + XY = X^3 + (a_2 + \alpha)X^2 + a_6 \,.$$

In particular, the curve $E_{\alpha,\beta} = (E_{0,\beta})_\alpha$ of (1.4) is the twist of $E_{0,\beta}$ by α or K_α.

2. The zeta function and the Birch/Swinnerton-Dyer conjecture

Let S be an indeterminate, and for a place v of K, put $S_v = S^{\deg v}$ and $q_v = q^{\deg v} = $ cardinality $|\mathbf{F}_v|$ of the residue class field $\mathbf{F}_v$. The Euler factor of $E = E_{\alpha,\beta}$ (subject always to $(1.2')$) at v is

$$P_v(S) = \begin{cases} 1 \,, & v = 0, \\ (1 - S)^{-1} \,, & v = \infty, \\ (1 - c(v)S_v + q_v S_v^2)^{-1} \,, & v \neq 0, \infty \,, \end{cases}$$

where $c(v) = q_v + 1 - a(v)$, and $a(v)$ is the number $|E(\mathbf{F}_v)|$ of rational points of the reduction of E at v. The Z-function $Z(E/K, S)$ is

$$(2.1) \qquad\qquad Z(E/K, S) = \prod_{v \text{ a place of } K} P_v(S) \,,$$

a priori a formal power series in S. Finally, the complex-valued zeta function of E is $\zeta(E/K, s) := Z(E/K, q^{-s})$. The following is the specialization of well-known facts to our case (see [3] and [10], Thm. 4):

2.2. Theorem. *$Z(E/K, S)$ is actually a polynomial of degree $g = f - 3$ in S and, with a suitable sign $w = w(E/K) \in \{\pm 1\}$, satisfies the functional equation*

$$Z(E/K, S) = w(qS)^g \, Z(E/K, q^{-2}S^{-1}) \,. \quad \square$$

(Here f is the exponent of $\mathrm{cond}(E)$ at $v = 0$ given by (1.5), and $g = f - 3 = \deg \mathrm{cond}(E) - 4$ as in [10].)

Let $r = r(E/K)$ be the rank of the finitely generated abelian group $E(K)$ and $r_{an} = r_{an}(E/K)$ the zero order of $Z(E/K, S)$ at $S = q^{-1}$ (or of $\zeta(E/K, s)$ at $s = 1$). It has been proven in [11]that always

$$(2.3) \qquad\qquad r \leq r_{an} \,.$$

The Birch/Swinnerton-Dyer conjecture (or Artin/Tate conjecture: [11], conjectures B, C; [7], p. 117; the two are equivalent in our case: [7], p. 371) states that we have in fact equality and, moreover, the leading term of $\zeta(E/K, s)$ at $s = 1$ is given by

$$(2.4) \qquad\qquad \gamma(E/K) \lim_{s \to 1} \frac{\zeta(E/K, s)}{(s - 1)^r} = \frac{|\Sha(E/K)| \, |\det \langle \, . \, \rangle|}{|E(K)_{\mathrm{tor}}|^2} \,.$$

The ingredients of (2.4) are as follows: $E(K)_{\mathrm{tor}}$ is the torsion subgroup of $E(K)$, $\det\langle \, . \, \rangle$ is the determinant (well-defined up to sign) of the height pairing on $E(K)$

mod torsion, $\mathrm{III}(E/K)$ is the Tate-Shafarevich group, and $\gamma(E/K)$ is a comparison factor described in [7], p. 115 (essentially, the quotient L_S^*/L_S of *loc. cit.*). It will be determined below.

The comparison factor. By definition, $\gamma(E/K)$ results from integrating Néron differentials on E against normalized Haar measures at the v-adic ($v = 0, \infty$) completions of K. Recall that, as $A = \mathbf{F}_q[T]$ is principal, E has a globally minimal model $\mathcal{E}$ over A. Let ω be the Néron differential associated to $\mathcal{E}$ and ω' the Néron differential associated to a minimal model $\mathcal{E}'$ at ∞. Then $\omega' = u\omega$ with some $u \in K_\infty$ with normalized absolute value $|u|_\infty > 1$. We call $|u|_\infty$ the *discrepancy* of E. Note that u is just the parameter of the coordinate change between $\mathcal{E}$ and $\mathcal{E}'$ (see [12], 2.1).

Going through the definitions of [7], p. 115, we get

2.5. Proposition. *Let E/K be an elliptic curve subject to* (1.2). *The comparison factor in formula* (2.4) *is*

$$\gamma(E/K) = \frac{|u|_\infty}{q \cdot c_0 \cdot c_\infty},$$

where $|u|_\infty$ is the discrepancy and the $c_v = c_v(E/K)$ are the fudge factors at the two places $v = 0, \infty$ of bad reduction of E. $\square$

The c_v are discussed in [12]. They are determined by applying Tate's algorithm.

Now let E again be one of the curves $E_{\alpha,\beta}$, where α and $\beta = c \cdot T^{-k}$ are as in (1.2'). Then we know a priori that:

(2.6) $c_\infty = k$, since E/K_∞ is a Tate curve with $v_\infty(j(E)) = -k$.

(2.7) $c_0 \in \{1, 2, 3, 4\}$, since E has additive reduction at $v = 0$.

The next result follows from a detailed analysis of Tate's algorithm applied to $E_{\alpha,\beta}$.

2.8. Theorem ([6]). *Let $\alpha \in \mathbf{F}_q[T^{-1}]$ be an odd polynomial of degree d and $\beta = c \cdot T^{-k}$ with k odd, and write $k = 6l - m$ with $l \in \mathbf{N}$ and $m \in \{1, 3, 5\}$. Put $\bar{l} := \max\{l, \frac{d+1}{2}\}$. Then*

(i) $$Y^2 + T^{\bar{l}}XY = X^3 + T^{2\bar{l}}\alpha X^2 + T^{6\bar{l}}\beta$$

is a globally minimal equation for $E = E_{\alpha,\beta}$ over $A = \mathbf{F}_q[T]$.

(ii) *The Kodaira type of E at $v = 0$ is II, I_0^*, I_ν^* (some $\nu \in \mathbf{N}$) or II^*.* $\square$

2.9. *Remark.* The precise description of the Kodaira types, irrelevant for our present purposes, depends on complicated case considerations on (m, α, β). It is carried out in detail in [6]. We also have some so far incomplete results on c_0, but in general we need to calculate it through the algorithm. The results for $q = 2$ are tabulated in (4.8).

2.10. Corollary. *With the above notation, the discrepancy of E is $q^{\bar{l}}$.*

Proof. We have $u = T^{\bar{l}}$ and $|u|_\infty = q^{\bar{l}}$. $\square$

2.11. Corollary. *The fudge factor is 1, 2 or 4.*

Proof. These are the only fudge factors admitted by our Kodaira types. $\square$

Combining the preceding results, the BSD conjecture (2.4) for our curves $E_{\alpha,\beta}$ with $k = v_\infty(\beta)$ odd reads

$$(2.12) \qquad \frac{q^{\bar{l}-1}}{c_0 \cdot k} \lim_{s \to 1} \frac{\zeta(E/K, s)}{(s-1)^r} = \frac{|\text{Ш}(E/K)| \, |\det \langle \, . \, \rangle|}{|E(K)_{\text{tor}}|^2}.$$

We should mention that its truth in full strength would be a consequence of the conjectured equality $r = r_{an}$ in (2.3) ([7], Cor. 9.7, p. 371). Hence if $\zeta(E/K, s)$ doesn't vanish at $s = 1$, the formula

$$(2.13) \qquad \frac{q^{\bar{l}-1}}{c_0 \cdot k} \zeta(E/K, 1) = \frac{|\text{Ш}(E/K)|}{|E(K)_{\text{tor}}|^2}$$

is valid unconditionally, and yields an efficient method to calculate $|\text{Ш}(E/K)|$.

3. Computation of $Z(E/K, S)$

Here we describe how to efficiently calculate $Z(E/K, S)$ for all the curves $E = E_{\alpha,\beta}$ over K with conductor $\text{cond}(E) = (0)^f \cdot (\infty)$ and f less than or equal to some bound $f_{\max}$ depending on the size of the machine available.

Without restriction (1.4), we assume that $k = v_\infty(\beta)$ is odd. Let $g = f - 3$ be the degree of $Z(E/K, S) = \sum c_n S^n$.

First step. From the functional equation, we have

$$(3.1) \qquad c_{g-n} = w(E/K) q^{g-2n} c_n.$$

It therefore suffices to calculate the c_n for $n \leq \bar{g} := [g/2] + 1$, provided that $c_{\bar{g}}$ doesn't vanish. Otherwise (which in practice occurs very rarely), we have to calculate the first non-vanishing c_n with $n > \bar{g}$, or use some other method (see (4.2)) to determine the sign $w(E/K)$.

Second step. For a prime $v \neq 0$ of $A = \mathbf{F}_q[T]$ (i.e., an irreducible monic polynomial $v \neq T$) and $i \in \mathbf{N}$, put

$$(3.2) \qquad a(v, i) := |E(\mathbf{F}_{v^i})| = \text{number of rational points of } E \text{ over}$$
$$\text{the extension of degree } i \text{ of } \mathbf{F}_v = A/(v).$$

We finally let c be the multiplicative function on monics in A vanishing on multiples of T and given on prime powers v^i $(v \neq T)$ by

$$(3.3) \qquad c(v^i) = q_v^i + 1 - a(v, i).$$

The c_n of (3.1) are then given by

$$(3.4) \qquad c_n = \sum_{x \in A \text{ monic, } \deg x = n} c(x).$$

From the theory of elliptic curves over finite fields, we have the well-known recursions ($v \neq T$ prime, $i \geq 3$)

$$(3.5) \qquad \begin{aligned} c(v^2) &= c(v)^2 - 2q_v, \\ c(v^i) &= c(v)c(v^{i-1}) - q_v c(v^{i-2}), \end{aligned}$$

from which the $a(v, i)$ may be determined. Let D be the logarithmic derivative operator $f(S) \longmapsto Df(S) = S \cdot \frac{f'(S)}{f(S)}$ on $\mathbf{Z}[[S]]$. After a quick calculation, (2.1) translates to

$$(3.6) \qquad DZ(E/K, S) = \sum_{n \geq 1} [q^{2n} - \sum_{d \mid n} d \sum_{\substack{v \in A \text{ monic, prime} \\ \text{of degree } d, \ v \neq T}} a(v, n/d)] S^n \ ,$$

which is considerably simpler to evaluate than (2.1) combined directly with (3.3)–(3.5). The coefficients $\tilde{c}_n$ of $DZ(E/K, S)$ yield the c_n through

$$(3.7) \qquad c_n = \frac{1}{n} \sum_{0 \leq i < n} c_i \tilde{c}_{n-i} \quad (n \geq 1), \quad c_0 = 1 \, .$$

(We are confident that the present $c_0 = 1$ is not confused with the local fudge factor at $v = 0$ discussed in section two.)

Third step. We are now reduced to calculating the $a(v) = a(v, 1)$ (or equivalently the $c(v)$) for places $v \neq T$ of degree up to $\overline{g}$. Let $E = E_{0,\beta}$ and $E' = E_{\alpha,\beta}$ with α, β subject to (1.2'). If $c(x)$, $c'(x)$ denote the Fourier coefficients (3.3) associated with E and E', respectively, then

$$(3.8) \qquad c'(x) = \chi_\alpha(x) c(x) \, ,$$

where $\chi_\alpha : A \longrightarrow \mathbf{C}$ is the Dirichlet character attached to the quadratic extension K_α/K. It may be described as follows: If α has odd degree d, then K_α/K has conductor (T^{d+1}) and splits at ∞ (e.g., [4], sect. 1). Hence $\mathrm{Gal}(K_\alpha/K)$ is a quotient of $(A/(T^{d+1}))^*/\mathbf{F}_q^*$ and χ_α is the composition $(A/(T^{d+1}))^* \longrightarrow \mathrm{Gal}(K_\alpha/K) \cong \{\pm 1\}$, considered as a function on A in the usual fashion. For a monic prime $v \neq T$ in A, we have

$$(3.9) \qquad \chi_\alpha(v) = (-1)^{[\alpha, v]},$$

where $[\alpha, v] = \mathrm{Tr}_{\mathbf{F}_2}^{\mathbf{F}_q} \mathrm{Res}_0(\alpha \frac{dv}{v}) \in \mathbf{F}_2$ is the Artin-Schreier symbol ([8], p. 221) at the place $w = 0 = (T)$.

3.10. Example. Let $q = 2$, $v = \sum v_i T^i$ prime. Then $[T^{-1}, v] = v_1$, $[T^{-3}, v] = v_1 + v_1 v_2 + v_3$.

Since $[.,.)$ is bilinear, it suffices to evaluate and store the Fourier coefficients $c(v)$ (v prime) for $E = E_{0,\beta}$ and the values $\chi_\alpha(v)$ for $\alpha = \mathrm{const} \cdot T^{-i}$ (i odd) instead of the coefficients $c'(v)$ for $E' = E_{\alpha,\beta}$ and all the v and α. Moreover, the defining equation for $E_{0,\beta}$ is particularly simple to handle (see step five).

Fourth step. We still have to determine $a(v) = |E_{0,\beta}(\mathbf{F}_v)|$ for all the places $v \neq (T)$ of degree $d \leq \overline{g} = [g/2] + 1$, which involves calculations in $\approx q^{\overline{g}}/\overline{g}$ fields of size up to $q^{\overline{g}}$. We therefore eliminate the quantity v from our considerations. For each $d \leq \overline{g}$, we choose, by means of a minimal equation, a standard field L_d of degree d over $\mathbf{F}_q$. The different v's of degree d then correspond to the orbits of length d under the Galois action in L_d. If $b \in L_d$ is the image of $\beta \in A[T^{-1}]$ under $A[T^{-1}] \longrightarrow \mathbf{F}_v = A/(v) \cong L_d$, then

$$(3.11) \qquad \begin{aligned} a(v) \ &= \ \text{number of solutions over } L_d \\ & \quad \text{(including the infinite one) of } Y^2 + XY = X^3 + b \\ &= \ |E_{0,b}(L_d)| \, . \end{aligned}$$

Fifth step. The following simple lemma allows to separate variables when computing $|E_{0,b}(L_d)|$.

3.12. Lemma. $|E_{0,b}(L_d)| = 2 + 2\,|\{x \in L_d^* \mid x + bx^{-2} \in \wp(L_d)\}|.$

Proof. For $x \in L_d^*$ we have $\wp(L_d) = \{y^2 + y \mid y \in L_d\} = x^{-2}\{y^2 + xy \mid y \in L_d\}$. Hence $\{y^2 + xy \mid y \in L_d\} = x^2\{y^2 + y \mid y \in L_d\}$ and $x^3 + b \in \{y^2 + xy \mid y \in L_d\} \Leftrightarrow x + bx^{-2} \in \wp(L_d)$ whenever $0 \neq x \in L_d$. For each such x, there exist two L_d-rational points (x,y) of $E_{0,b}$, and $E_{0,b}(L_d) = \{(x,y) \mid x \neq 0\} \cup \{(0, \sqrt{b}), \infty\}$. $\qquad\square$

The above suggests that we should mark and store for each L_d the $q^d/2$ elements of the form $y^2 + y$. The remaining determination of $|E_{0,b}(L_d)|$ is then achieved with $q^d - 1$ evaluations of $f(x) = x + bx^{-2}$.

Let $d_{\max}$ be the largest integer d such that we can efficiently perform the necessary calculations in L_d (which, in our approach, requires the storage of a discrete logarithm and of the value set of the $\wp$-function on L_d). Except for a very small number of curves $E_{\alpha,\beta}$ with lacunary Z-function (see (3.1)), our algorithm will determine $Z(E/K, S)$ for all the curves $E = E_{\alpha,\beta}$ with $g = \deg Z(E/K,S) \leq 2d_{\max} - 1$, i.e., $f \leq f_{\max} = 2d_{\max} + 2$, or finally with

(3.13) $$\max\{k, 2\,\deg_{T^{-1}} \alpha\} \leq 2d_{\max} \quad \text{(see (1.5))}.$$

The computer time needed to perform steps one to four is small compared to step five, i.e., the calculation of all the $|E_{0,b}(L_d)|$ for $b \in L_d$, $1 \leq d \leq d_{\max}$. Hence, for practical purposes, the total computer time to determine $Z(E/K,S)$ for all the $E = E_{\alpha,\beta}$ in the above range is $O(q^{2d_{\max}})$.

4. NUMERICAL RESULTS

We list the results on $Z(E/K,S)$ obtained from our algorithm, for $q = 2$ and $d_{\max} = 19$. Hence $E = E_{\alpha,\beta}$, where $\alpha \in \mathbf{F}_2[T^{-1}]$ is an odd polynomial of degree ≤ 19 and $\beta = T^{-k}$ with $k \leq 37$, where by Theorem 1.4, we suppose without loss of generality that k is odd. By [4], 5.4 and 5.5, we have

4.1. The resulting curves $E_{\alpha,k} := E_{\alpha,T^{-k}}$ are all non-isogeneous, and
$$E_{\alpha,k}(\mathbf{F}_2(T))_{\text{tor}} = 0\,.$$

The algorithm as described delivered $Z(E/K,S)$ in $19\,448$ cases from a total number of $19 \times 2^{10} = 19\,456$ pairs (α, k), i.e., in these cases, the sign $w(E/K)$ in the functional equation came out. Of the remaining 8 cases, we could decide $w(E/K)$ for 7 pairs (α, k), mainly through arguments based on the next observation, which follows from (2.13) and (4.1):

4.2. If $\zeta(E/K, 1) = Z(E/K, 1/2) \neq 0$, then
$$\frac{2^{\bar{l}-1}}{c_0 \cdot k} Z(E/K, 1/2) = |\text{Ш}(E/K)|$$
is the square of a natural number.

The case $(\alpha, k) = (0, 25)$ resisted and needs a more detailed analysis. Based on (4.7), we suspect here the "+" sign, which gives the order of zero 2 at the critical point $S = q^{-1} = 1/2$. That case is counted in Table 4.3 and Observation 4.7 with the proposed sign and zero order. The four curves with $r_{an} = 4$ have parameters $(\alpha, k) = (T^{-11} + T^{-7} + T^{-3} + T^{-1}, 31), (0, 33), (T^{-13} + T^{-11} + T^{-7} + T^{-3} + T^{-1}, 35)$ and $(T^{-15} + T^{-7}, 37)$.

TABLE 4.3. (zero orders r_{an} of $Z(E/K, S)$ at $S = 1/2$)

# cases	r_{an}
5 799	0
13 325	1
288	2
40	3
4	4
0	≥ 5
19 456	

We further observed empirically:

4.4. $Z(E/K, 1/2) \neq 0$, i.e., $r_{an} = r = 0$ whenever $\deg \alpha = k$, and $r_{an} = 1$ whenever $\deg \alpha > k$.

TABLE 4.5. (values of $|\text{III}(E/K)|$ if $Z(E/K, 1/2) \neq 0$)

# cases	$|\text{III}(E/K)|$	# cases	$|\text{III}(E/K)|$
2 658	1^2	91	11^2
154	2^2	44	13^2
1 494	3^2	28	15^2
50	4^2	18	17^2
648	5^2	11	19^2
11	6^2	9	21^2
367	7^2	5	25^2
2	8^2	3	27^2
202	9^2	1	39^2
2	10^2	1	47^2
		5 799	

The value $|\text{III}| = 39^2$ is obtained for

$$(\alpha, k) = (T^{-19} + T^{-17} + T^{-15} + T^{-9} + T^{-7} + T^{-5} + T^{-1}, 21),$$

the value 47^2 for

$$(\alpha, k) = (T^{-19} + T^{-17} + T^{-15} + T^{-13} + T^{-7} + T^{-5} + T^{-3}, 21).$$

The prime $l = 47$ seems to be the largest prime divisor of some $|\text{III}(E/K)|$ documented in the literature which is unequal to the characteristic p. For $l = p$, see e.g., [9].

The Z-function for the curve $E = E_{0,25}$ with so far undetermined sign $w = w(E/K)$ is

(4.6) $$Z(E_{0,25}/K, S) = (1 - R)(1 - wR^5)$$

with $R := (2S)^4$, which has $r_{an} = 2$ if $w = 1$, as we suspect, and $r_{an} = 1$ if $w = -1$.

The respective behaviors of signs $w(E/K)$ in the functional equation and of the fudge factors $c_0(E/K)$ at $v = 0$ (see (2.7)) seem to coincide in some sense. Define for pairs (α, k) as above the following segments (where "deg" is the degree of α in T^{-1}):

$$\begin{array}{ll}
\text{(segment 1)} & \alpha = 0, \\
\text{(segment 2)} & 1 \leq \deg \alpha \leq k/3, \\
\text{(segment 3)} & k/3 < \deg \alpha \leq k/2, \\
\text{(segment 4)} & k/2 < \deg \alpha < k, \\
\text{(segment 5)} & \deg \alpha = k, \\
\text{(segment 6)} & \deg \alpha > k.
\end{array}$$

Depending on the different segments, we made the empirical observations listed below.

4.7 Observations. $(E = E_{\alpha,k},\ w = w(E/K),\ r_{an} = r_{an}(E/K))$:

(1)

$$(\alpha, k) \text{ in segment } 1 \Rightarrow w = \begin{cases} 1 \text{ if } k \equiv 1, 7 \,(\text{mod } 8) \\ -1 \text{ if } k \equiv 3, 5 \,(\text{mod } 8) \end{cases}$$

(2)

$$(\alpha, k) \text{ in segment } 2 \Rightarrow w(E/K) = \begin{cases} w(E_{0,k}/K) \text{ if } k \equiv 1, 5 \,(\text{mod } 6) \\ \quad \text{or } k \equiv 3 \,(\text{mod } 6) \text{ and } \deg \alpha < k/3 \\ -w(E_{0,k}/K), \text{ if } k \equiv 3 \,(\text{mod } 6) \\ \quad \text{and } \deg \alpha = k/3 \end{cases}$$

(3) (α, k) in segment 3. The fudge factor $c_0(E_{\alpha,k}/K)$ is 2 or 4. For each pair (d, k) with $k/3 < d \leq k/2$ there exists a permutation $\sigma_{d,k}$ of $\{\pm 1\}$ such that for all the α with $\deg \alpha = d$, we have

$$w(E_{\alpha,k}/K) = \sigma_{d,k}(1) \Leftrightarrow c_0(E_{\alpha,k}/K) = 2\,.$$

In other words: The distribution of signs w follows the same pattern as c_0, as long as $(\deg \alpha, k)$ is constant.

(4) (α, k) in segment 4. Then $c_0 = c_0(E/K) \in \{2, 4\}$ and

$$\begin{array}{lcl lcl}
c_0 = 2 & \Leftrightarrow & w = 1 & \Rightarrow & r_{an} = 0, \\
c_0 = 4 & \Leftrightarrow & w = -1 & \Rightarrow & r_{an} = 1.
\end{array}$$

(5) (α, k) in segment $5 \Rightarrow w = 1,\ r_{an} = 0$.

(6) (α, k) in segment $6 \Rightarrow w = -1,\ r_{an} = 1$.

These should be contrasted with the following *proved facts* on Kodaira types and fudge factors.

4.8. Proposition. *Let* (α, k) *be an odd polynomial in* $\mathbf{F}_2[T^{-1}]$, *an odd natural number, respectively. The Kodaira type and fudge factor c_0 of $E_{\alpha,k}$ at $v = 0$ are given by:*

(α, k) in			Kodaira type	$c_0(E_{\alpha,k}/K)$
segments $1, 2$,	$k \equiv 1 \,(\text{mod } 6)$		II^*	1
	$k \equiv 3 \,(\text{mod } 6)$,	$\deg \alpha < k/3$	I_0^*	2
		$\deg \alpha = k/3$	I_0^*	1
	$k \equiv 5 \,(\text{mod } 6)$		II	1
segments $3, 4$			$I_\nu^*\ (\nu > 0)$	$2, 4$
segment 5			$I_\nu^*\ (\nu > 0)$	2
segment 6			$I_\nu^*\ (\nu > 0)$	4

Proof. Analysis of Tate's algorithm. We omit the details.   □

5. Comments

Observations (4.4) and (4.7) suggest, in view of (4.1), that for $E = E_{\alpha,k}$, $K = \mathbf{F}_2(T)$ we have

$$
\begin{array}{lllll}
(5.1) & E(K) & = & 0 & \text{if } (\alpha, k) \text{ in segment 5, i.e., } \deg \alpha = k, \\
& E(K) & \cong & \mathbf{Z} & \text{if } (\alpha, k) \text{ in segment 6, i.e., } \deg \alpha > k.
\end{array}
$$

Is there a uniform proof for these "facts"? In particular, can we prescribe rational points on E if $\deg \alpha > k$, and show that E has none if $\deg \alpha = k$?

5.2.   The missing sign $w(E/K)$ in the functional equation is an essentially local invariant of E in $v = 0$; see below. Though we see no connection *a priori* between $w(E/K)$ and $c_0(E/K)$, there must be a link, which has to be revealed. We sketch how this problem could be approached. Let $K_0 = \mathbf{F}_q((T))$ be the completion of K at $v = 0$. To E/K_0 there correspond an automorphic representation σ_E of $\mathrm{GL}(2, K_0)$ and also a representation σ'_E of H^*, where H/K_0 is the central division algebra of dimension 4 (see [5], [2], [13]). E being defined over $K = \mathbf{F}_q(T)$ and subject to (1.2), the sign $w(E/K)$ is nothing else than the root number (e.g., [1], p. 22) of σ'_E. Since $E \rightsquigarrow \sigma'_E$ is compatible with twists (1.7) and the behavior of root numbers under twists is easy to describe ([1], p. 28), we are reduced to determining the representation σ'_E of H^* attached to $E = E_{0,k}$ (if $q = 2$), or, more generally, of $E_{0,\beta}$, $\beta = \mathrm{const} \cdot T^{-k}$. Thus we propose to study for arbitrary local fields K_0 of characteristic two the Langlands-Shimura map

$$
\mathrm{LS}: \quad \{j \in K_0^* \mid 0 < |j| < 1\} \quad \longrightarrow \quad \left\{ \begin{array}{l} \text{irreducible admissible} \\ \text{representations of } H^* \text{ with} \\ \text{trivial central character} \end{array} \right\},
$$
$$
j \quad \longmapsto \quad \sigma'_E, \text{ where } E = E_{0,j^{-1}}.
$$

Note that the Langlands and Langlands-Shimura correspondences don't give more than the mere existence of LS, whose properties seem to be largely unknown. Our empirical results (4.7) imply certain restrictions for LS; among others, they suggest that the representations σ'_E with $E = E_{0,\beta}$ (or rather $E = E_{\alpha,\beta}$ with (α, β) "in segments 1 or 2") are distinguished among all the representations σ'_E.

References

[1] Bushnell, C., Fröhlich, A.: Gauss sums and *p*-adic division algebras. Lect. Notes Math. **987**, Springer-Verlag 1983. MR **84m:**12017

[2] Deligne, P.: Formes modulaires et représentations de GL(2). In Lect. Notes Math. **349**, Springer-Verlag 1973, 55-105. MR **50:**240

[3] Deligne, P.: Les constantes des équations fonctionnelles des fonctions L. In Lect. Notes Math. **349**, Springer-Verlag 1973, 501-597. MR **50:**2128

[4] Gekeler, E.-U.: Highly ramified pencils of elliptic curves in characteristic two. Duke Math. J. **89** (1997), 95–107. CMP 97:15

[5] Jacquet, H., Langlands, R.P.: Automorphic forms on GL(2). Lect. Notes Math. **114**, Springer-Verlag 1970. MR **53:**5481

[6] Leitl, R.: Elliptische Kurven über $\mathbf{F}_q(T)$ mit kleinem Führer, Diplomarbeit Saarbrücken 1995.

[7] Milne, J.S.: Arithmetic duality theorems. Academic Press, Boston-Orlando 1986. MR **88e:**14028

[8] Serre, J.P.: Corps locaux, 2nd ed., Hermann, Paris 1968. MR **50:**7096

[9] Shioda, T.: Mordell-Weil lattices and sphere packings, Am. J. Math. **113** (1991), 931-948. MR **92m:**11066
[10] Shioda, T.: Some remarks on elliptic curves over function fields, Astérisque **209** (1992), 99-114. MR **94d:**11046
[11] Tate, J.: On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. In Dix exposés sur la cohomologie des schémas, North Holland, Amsterdam 1968. CMP 98:09; MR **39:**2777
[12] Tate, J.: Algorithm for determining the type of a singular fiber in an elliptic pencil. In Lect. Notes Math. **476**, Springer-Verlag 1975, 33-52. MR **52:**13850
[13] Tunnell, J.: On the local Langlands conjecture for GL(2), Invent. Math. **46** (1978), 179-200. MR **57:**16262

Fachbereich 9 Mathematik, Universität des Saarlandes, Postfach 15 11 50, D-66041 Saarbrücken

E-mail address: `gekeler@math.uni-sb.de`

E-mail address: `rita@math.uni-sb.de`

E-mail address: `bodo@math.uni-sb.de`