Astérisque

TETSUJI SHIODA

Some remarks on elliptic curves over function fields

Astérisque, tome 209 (1992), p. 99-114

<http://www.numdam.org/item?id=AST_1992__209__99_0>

SOME REMARKS ON ELLIPTIC CURVES OVER FUNCTION FIELDS

Tetsuji SHIODA

In my lecture at the Journées Arithmétiques in Geneva (entitled "Mordell-Weil lattices and sphere packings"), I talked on
1) a brief survey on lattices and sphere packings,
2) basic results on Mordell-Weil lattices, and
3) application to sphere packings via supersingular surfaces.
For these topics, the following references are available: 1) [CS,Ch.1], 2) [S3], [S4] and 3) [E], [Oe], [S5].

In this note, instead of reporting on these, I would like to treat some related topics on elliptic curves over a function field, especially some results on the L-function of an elliptic curve over a function field with a finite constant field. Most of them must be known to experts, but the approach based on surface theory and Mordell-Weil lattices seems to provide a natural setting for this subject (cf. [T2],[G],[Mc]). In particular, this method enables one to write down explicit examples of such an L-function in some nontrivial cases.

The contents of this paper are as follows:

The present work has been done during my visit to Max-Planck-Institut, Bonn and the University of Geneva. I would like to thank Professor F. Hirzebruch and Professor D. Coray for their kind invitation.

1 Elliptic surfaces

Let us review first some basic results on elliptic surfaces, fixing the notation. Let k be an algebraically closed field of arbitrary characteristic and let K/k be a function field of one variable over k, i.e., $K = k(C)$ for some smooth projective curve C over k. Let E/K be an elliptic curve with a K-rational point O, and let $f : S \longrightarrow C$ denote the elliptic surface associated with E/K (the Kodaira-Néron model). The elliptic curve E is recovered from f as its generic fibre and, as is well known, the K-rational points of E can be identified with the sections of f; for each $P \in E(K)$, (P) denotes the image curve in S of the section $P : C \longrightarrow S$. We always assume the condition $(*)$ that f has at least one singular fibre.

Now let $N = \mathrm{NS}(S)$ be the Néron-Severi group of S; it is a free module of finite rank ρ (=the Picard number of S), which is an (indefinite) integral lattice with respect to the intersection pairing. We denote by T or L the trivial or essential sublattice of N; by definition, T is the sublattice generated by the zero-section (O), a fibre and all components of reducible fibres of f, and L is the orthogonal complement of T in N. In particular, we have

$$N \otimes \mathbf{Q} = (T \otimes \mathbf{Q}) \oplus (L \otimes \mathbf{Q}) \tag{1.1}$$

and

$$\rho = \mathrm{rk}\, T + \mathrm{rk}\, L. \tag{1.2}$$

Further we have

$$\mathrm{rk}\, T = 2 + \sum_{v \in C} (m_v - 1) \tag{1.3}$$

where m_v is the number of irreducible components of the fibre $f^{-1}(v)$, and $\mathrm{rk}\, L$ is equal to the Mordell-Weil rank of E/K:

$$r := \mathrm{rk}\, L = \mathrm{rk}\, E(K). \tag{1.4}$$

Actually there is a natural isomorphism

$$L \otimes \mathbf{Q} \simeq E(K) \otimes \mathbf{Q}, \tag{1.5}$$

which takes the intersection pairing on L to the height pairing on the Mordell-Weil group (up to the sign change); indeed this is essentially how we defined the structure of Mordell-Weil lattices (see [S4]).

Next we consider the cycle map

$$\gamma : N \longrightarrow H = H^2(S, \mathbf{Q}_l(1)) \tag{1.6}$$

where H stands for the l-adic cohomology group with a fixed prime number $l \neq \mathrm{char}(k)$ (cf. [T1]). It is injective and takes the intersection pairing of N into the cup-product pairing in H. Let us denote by $\mathrm{Trans}(S)$ the orthogonal complement of $\mathrm{Im}(\gamma)$ in H, whose elements are called transcendental cycles on S, and by W the orthogonal complement of $\gamma(T)$ in H. The space W corresponds to what Weil called the *essential part* in the second homology of S (cf. his comments to the paper [1967a] in [W, III]). Then we have

$$H \simeq (N \otimes \mathbf{Q}_l) \oplus \mathrm{Trans}(S) \simeq (T \otimes \mathbf{Q}_l) \oplus W \tag{1.7}$$

and

$$W \simeq (L \otimes \mathbf{Q}_l) \oplus \mathrm{Trans}(S) \tag{1.8}$$

The Lefschetz number of S is defined as

$$\lambda := \dim \mathrm{Trans}(S) = b_2 - \rho \qquad (b_2 = \dim H^2(S)) \tag{1.9}$$

which is known to be a birational invariant of S.

Proposition 1 *The dimension w of the vector space W is given by*

$$w = r + \lambda = b_2 - \mathrm{rk}\, T. \tag{1.10}$$

If $\mathrm{char}(k) \neq 2, 3$, *then*

$$w = 4g - 4 + \mu + 2\alpha \tag{1.11}$$

where g is the genus of C (or of K) and μ (resp. α) is the number of singular fibres of multiplicative (resp. additive) type.

Proof. The first part is immediate from (1.7) and (1.8). The second part is also well-known (cf.[R],[S1]). Let us briefly recall the idea of the proof. From the standard facts in surface theory, we have

$$b_2 = c_2 + 2b_1 - 2 \qquad (c_2 = \text{ Euler number of } S)$$

where $b_1 = 2g$ since we are assuming the condition $(*)$. On the other hand, we have the following formula for $\mathrm{char}(k) \neq 2, 3$:

$$c_2 = \sum_v e_v \qquad (e_v = \text{ Euler number of } f^{-1}(v)) \tag{1.12}$$

(cf. [K],[Ogg],[Ogu]). Then, by (1.9) and (1.3), we have

$$w = 4g - 4 + \sum_v (e_v - m_v + 1).$$

It remains to check that

$$e_v = m_v \quad \text{or} \quad m_v + 1$$

according as the fibre $f^{-1}(v)$ is of multiplicative or additive type, which can be done using the classification of singular fibres([K],[N],[T3]). *q.e.d.*

It may be worthwhile to mention the following direct consequence. Simply note that we have $\lambda \geq 0$ in general and $\lambda \geq 2p_g$ (p_g: geometric genus of S) in characteristic 0.

Corollary 2 *If* $\mathrm{char}(k) \neq 2, 3$, *then*

(1.13). $$r \leq w = 4g - 4 + \mu + 2\alpha.$$

Corollary 3 *Assume* $\mathrm{char}(k) = 0$. *Then*

(1.14) $$p_g \leq \frac{1}{2}w = 2g - 2 + \frac{1}{2}\mu + \alpha$$

(1.15) $$c_2 = 12(p_g - g + 1) \leq 6(2g - 2 + \mu + 2\alpha)$$

and

(1.13′). $$r \leq 4g - 4 + \mu + 2\alpha - 2p_g.$$

Remark. (a) In case $\mathrm{char}(k) = 2$ or 3, (1.10) is still valid, but (1.11) should be modified by adding an extra term caused by wild ramifications (cf. [Ogg],[R],[Sa]). In other words, each e_v in (1.12) should be replaced by $e_v + \delta_v$ with a well-defined non-negative integer δ_v so that the right hand side of (1.11) should have the term $\sum_v \delta_v$.
(b) The idea behind equality of expressions in (1.10) and (1.11) was first used by Igusa [I] to define a correct Betti number b_2 of an algebraic surface, and later it was formulated in a more general situation as the so-called Ogg-Shafarevich formula (cf. [R]).
(c) The above (1.14) or its equivalent (1.15) seems to have been proved by many authors again and again, though it was explicitly stated in [S1,Cor.2.7] in 1972. In particular, (1.15) is sometimes called Szpiro's conjecture (cf. [Sz,p.10]); note that we make no assumption of semi-stability ($\alpha = 0$) in the above argument.

2 The L-function of an elliptic curve

From now on, we consider the following situation. Let $k_0 = \mathbf{F}_q$ be a finite field with q elements and let k be its algebraic closure. Let $K_0 = k_0(C)$ be the function field of a curve C defined over k_0, and let E be an elliptic curve defined over K_0.

In this section, we shall show that the L-function of E/K_0 is essentially the characteristic polynomial of the Frobenius on the space W introduced above.

The L-function $L(E/K_0, s)$ is defined by the eulerian product

$$L(E/K_0, s) = \prod_v P_v(s)^{-1} \tag{2.1}$$

where v runs over the closed points of C/k_0 (equivalently, over the places of K_0/k_0) whose residue field $\mathbf{F}_v$ is a finite field with q_v elements and where

(2.2)
$$P_v(s) = \begin{cases} 1 - (q_v + 1 - N_v)q_v^{-s} + q_v^{1-2s} & \text{if } f^{-1}(v) \text{ is smooth} \\ 1 - \epsilon_v q_v^{-s} & \text{if } f^{-1}(v) \text{ is of multiplicative type} \\ 1 & \text{if } f^{-1}(v) \text{ is of additive type.} \end{cases}$$

Here N_v is the number of $\mathbf{F}_v$-rational points of the elliptic curve $f^{-1}(v)$, and $\epsilon_v = 1$ or -1 is determined as follows: in the multiplicative reduction case, the minimal Weierstrass model of E at v reduces to a rational curve with a node, and $\epsilon_v = 1$ or -1 according as the tangents at the node are $\mathbf{F}_v$-rational or not (cf. [T3,(5.2)], [Se2]).

On the other hand, regarding E as an elliptic curve over $K = k(C)$, we consider the associated elliptic surface

$$f : S \longrightarrow C$$

as in Section 1. We use the same notation as there unless otherwise mentioned; an exception is that v denotes a closed point of C/k_0 rather than a geometric point.

Note that, in the present situation, the surface S is defined over k_0; namely there is a smooth projective surface, say S_0, over k_0 such that S is equal to the base extension $S_0 \otimes k$.

Now the Galois group $G = \mathrm{Gal}(k/k_0)$ naturally acts on $N = \mathrm{NS}(S)$ and $H = H^2(S, \mathbf{Q}_l(1))$ ($l \neq \mathrm{char}(k)$) and their subspaces T, L, W, etc. appearing in Section 1. It is easy to see that all the maps or the direct sum decompositions there are compatible with the G-action. Letting $\sigma \in G$ be the Frobenius

automorphism of k:

$$\sigma : x \longrightarrow x^q,$$

we can consider the characteristic polynomial of σ or σ^{-1} (called the geometric Frobenius) on these vector spaces.

Theorem 4 *The L-function $L(E/K_0, s)$ of E/K_0 is a polynomial in $x = q^{1-s}$ of degree $w = \dim(W)$ and it is equal to the characteristic polynomial of σ^{-1} on W:*

$$L(E/K_0, s) = \det(1 - x\sigma^{-1} \mid W) \tag{2.3}$$

It satisfies the functional equation (corresponding to $x \to 1/x$):

$$L(E/K_0, 2 - s) = (-1)^w \det(\sigma|W) q^{(s-1)w} L(E/K_0, s).$$

Proof. This is implicit in [T2] where a more general situation is treated. For the convenience of the reader, let us give a complete proof in the case under consideration. First recall that the zeta function of the curve C (or the surface S) over the finite field k_0 is given as follows: letting $u = q^{-s}$, we have

$$\zeta(C/k_0, s) = \frac{P_1(u)}{(1-u)(1-qu)} \tag{2.4}$$

and

$$\zeta(S/k_0, s) = \frac{P_1(u)P_1(qu)}{(1-u)P_2(u)(1-q^2u)} \tag{2.5}$$

where $P_i(u)$ is the characteristic polynomial of the Frobenius endomorphism φ acting on $H^i(S, \mathbf{Q}_l)$. That the same $P_1(u)$ appears both for C and S is a consequence of the fact that the Picard variety of S is isomorphic to the Jacobian of C (cf. [S4,Sect.4]). Now, by a general property of zeta-functions (cf. [Se1]), we have

$$\zeta(C/k_0, s) = \prod_v \frac{1}{1 - q_v^{-s}} \tag{2.6}$$

and

$$\zeta(S/k_0, s) = \prod_v \zeta(f^{-1}(v)/\mathbf{F}_v, s) \tag{2.7}$$

where v runs over the closed points of C/k_0. Note that a closed point v determines and is determined by a G-orbit in $C(k)$, say $\{\bar{v}_1, \ldots, \bar{v}_d\}$ where $d = \deg(v), q_v = q^d$. We put

$$T_v = \sum_{i=1}^{d} T_{\bar{v}_i} \subset N$$

where $T_{\bar{v}_i}$ is the sublattice of N generated by the (k-)irreducible components of $f^{-1}(\bar{v}_i)$ other than the component meeting the zero section. Writing m_v for the common value of $m_{\bar{v}_i}$ (= the number of irreducible components of $f^{-1}(\bar{v}_i)$), we have $\mathrm{rk}\, T_v = \deg(v)(m_v - 1)$.

Lemma 5 *With the above notation, we have*

$$\zeta(f^{-1}(v)/\mathbf{F}_v, s) = \frac{P_v(s)}{(1 - q_v^{-s})(1 - q_v^{1-s})} \frac{1}{\det(1 - u\varphi \mid T_v)} \tag{2.8}$$

where $P_v(s)$ is as defined by (2.2).

Assume this for a moment. By (2.7), (2.6), (2.1) and (2.2), we have

$$\zeta(S/k_0, s) = \frac{\zeta(C/k_0, s)\zeta(C/k_0, s-1)}{L(E/K_0, s) \prod_v \det(1 - u\varphi \mid T_v)} \tag{2.9}$$

In view of (2.4) and (2.5), this implies

$$L(E/K_0, s) = \frac{P_2(u)}{(1 - qu)^2 \prod_v \det(1 - u\varphi \mid T_v)}. \tag{2.10}$$

Since the numerator (resp. denominator) in the right hand side is the characteristic polynomial of φ on $H' = H^2(S, \mathbf{Q}_l)$ (resp. T), the quotient is equal to the characteristic polynomial of φ on the space $W' \subset H'$ corresponding to $W \subset H$. Further, noting that

$$\begin{aligned} P_2(s) &= \det(1 - u\varphi \mid H^2(S, \mathbf{Q}_l)) \\ &= \det(1 - qu\sigma^{-1} \mid H^2(S, \mathbf{Q}_l(1))), \end{aligned} \tag{2.11}$$

(cf. [T1,Sect.3]), we have proven (2.3) by setting $x = qu = q^{1-s}$.

The functional equation for L follows from that of P_2 (which is a consequence of the Poincaré duality for S), since the denominator in (2.10) also satisfies a similar equation (see Lemma 6 below).

To prove Lemma 5, we need

Lemma 6 *Let $m = m_v, d = \deg(v)$ and $x = (qu)^d$. Then*

$$\det(1 - u\varphi \mid T_v) = (1 - x)^{m-1} \tag{2.12}$$

if every irreducible component of $f^{-1}(\bar{v}_i)$ is rational over $\mathbf{F}_v$. Otherwise, let e be the degree of the smallest extension of $\mathbf{F}_v$, say k_1, over which the condition

holds. Then e is either 2 or 3, and the characteristic polynomial of φ on T_v is equal to one of the following :

$$
\begin{array}{lll}
(1-x^2)^{\frac{m-1}{2}} & I_m\ (m:\text{odd}) & e=2 \\
(1-x)(1-x^2)^{\frac{m-2}{2}} & I_m\ (m:\text{even}) & \\
(1-x)^{m-3}(1-x^2) & I_b^*\ (m=b+5) & \\
(1-x^2) & IV\ (m=3) & \\
(1-x)^2(1-x^2)^2 & IV^*\ (m=7) & \\
(1-x)(1-x^3) & I_0^*\ (m=5) & e=3
\end{array} \tag{2.13}
$$

Proof of Lemma 6. By an easy argument (linear algebra), we can reduce the proof to the case $d=1$. Assume $d=1$ (i.e. $v \in C(k_0)$) so that $\mathbf{F}_v = k_0$. Then the first assertion is obvious because then the Frobenius endomorphism φ acts by multiplication by q on T_v. To see the other assertion, recall that the dual graph of a singular fibre (vertices correspond to $m-1$ irreducible components) is a Dynkin diagram of type A_{m-1}, D_{m-1} or E_{m-1}. The Galois group G induces a cyclic automorphism group of this graph, which can be nontrivial only for type A, D or E_6 (cf. [B, Ch.6]), i.e., only for the singular fibre of type I_m, I_b^* or IV^* $(e=2)$ or I_0^* $(e=3)$. If the number of the vertices fixed by G is a, then the characteristic polynomial is equal to $(1-x)^a(1-x^e)^b$ where $b=(m-1-a)/e$. Then, checking case by case, we can verify the above formulas. *q.e.d.*

Proof of Lemma 5. In case $f^{-1}(v)$ is smooth (an elliptic curve), this is well-known. Assume that $f^{-1}(v)$ is a singular fibre. By using Lemma 6, we can assume that v has degree 1 (replace $\mathbf{F}_v$ by k_0 and q_v by q). Let D denote the support of $f^{-1}(v)$ and $\tilde{D}$ its normalization. The latter is a disjoint union of m smooth rational curves, of which $a+1$ are rational over k_0 and the rest are rational over k_1, grouped into e curves conjugate over k_0. (We use the same notation as above.) Therefore we have (cf. (2.6))

$$\zeta(f^{-1}(v)/k_0, s) = \zeta(\mathbf{P}^1/k_0, s)^{a+1}\zeta(\mathbf{P}^1/k_1, es)^b(1-u)^n(1-u^e)^{n'}$$

where n (or n') is the number of closed points of degree 1 (or e) on $\tilde{D}$ which are mapped to singular points of D minus the number of singular closed points of degree 1 (or e) on D. It is easy to count these numbers using the classification of singular fibres, and we can verify the required formula (2.8) by noting that the sign $\epsilon_v = -1$ occurs precisely when we have either $I_m(m>1), e=2$ or I_1 (a rational curve with a node) having irrational tangent lines at the node. *q.e.d.*

This completes the proof of Theorem 4.

Theorem 7 *The L-function of E/K_0 is the product of the characteristic polynomials of σ^{-1} (the geometric Frobenius) on the Mordell-Weil group $E(K)$ and on the space of transcendental cycles* $\mathrm{Trans}(S)$*:*

$$L(E/K_0, s) = \det(1 - x\sigma^{-1} \mid E(K) \otimes \mathbf{Q}) \det(1 - x\sigma^{-1} \mid \mathrm{Trans}(S)). \tag{2.14}$$

The first factor is a polynomial of degree $r = \mathrm{rk}\, E(K)$ in x which is a product of cyclotomic polynomials and whose order of zero at $x = 1$ is equal to the Mordell-Weil rank $r_0 := \mathrm{rk}\, E(K_0)$.

Proof. The first assertion follows from Theorem 4 in view of (1.5) and (1.8). As for the second, let $k_1 \supset k_0$ be the smallest extension such that $E(K) = E(k_1(C))$ (the "splitting field" of $E(K)$). Then the action of $G = \mathrm{Gal}(k/k_0)$ on $E(K)$ factors through the finite cyclic group $\mathrm{Gal}(k_1/k_0)$. Hence the action of σ on $E(K) \otimes \mathbf{C}$ is diagonalizable, and the multiplicity of the eigenvalue 1 is precisely the rank of $E(K_0) = E(K)^G$.

Remark. From the above, one can easily deduce the equivalence of the Birch-Swinnerton-Dyer conjecture for E/K_0:

$$\mathrm{ord}_{s=1} L(E/K_0, s) = r_0 \tag{2.15}$$

and the Tate conjecture for S/k_0:

$$\mathrm{ord}_{u=1/q} P_2(u) = \rho_0 := \mathrm{rk} N_0, \tag{2.16}$$

where we denote by

$$N_0 := \mathrm{NS}(S/k_0) = \mathrm{NS}(S)^G$$

the subgroup of $\mathrm{NS}(S)$ generated by k_0-rational divisors. Indeed, both are equivalent to asserting that the second factor in (2.14) has no zero at $x = 1$, i.e., to the claim $\mathrm{Trans}(S)^G = 0$.

Furthermore the other part of the Birch-Swinnerton-Dyer conjecture involving the Shafarevich-Tate group is equivalent to the Artin-Tate formula for S/k_0 involving the Brauer group, i.e., the statement (d) of [T2] is true in the present case. In fact, in view of Theorem 3.1 in [T2] saying that

$$Ш(E/K_0) \simeq \mathrm{Br}(S/k_0), \tag{2.17}$$

the equivalence reduces to verifying the equality (cf. [T2,(4.4)])

$$\det \mathrm{NS}(S) = \frac{\det(E(K)/(tor))}{[E(K)_{tor}]^2} \det T. \tag{2.18}$$

This can be seen easily from the formalism of Mordell-Weil lattices based on a new definition of the height pairing on $E(K)$ (cf. [S4]).

Finally it is known that the Artin-Tate formula is true provided the Tate conjecture (2.16) holds (see [T2, Th.5.2], [Milne]). Noting that $\mathrm{NS}(S)$ is torsionfree (cf. [S4]), we can state the result as follows:

Theorem 8 *Assume that (2.15) or (2.16) is true and write* $L(E/K_0, s) = (1-x)^{r_0}h(x)$. *Then the value* $h(1)$ *is given by*

$$h(1) = \frac{[\mathrm{Br}(S/k_0)] \det \mathrm{NS}(S/k_0)}{q^{\alpha(S)}} \tag{2.19}$$

or, equivalently,

$$h(1) = \frac{[Ш(E/K_0)] \det(E(K_0)/(tor))}{q^{\alpha(S)}[E(K_0)_{tor}]^2} \det T_0 \ (T_0 = T^G) \tag{2.20}$$

where $\alpha(S) = \chi - 1 + g$, χ *being the arithmetic genus of* S.

3 Supersingular case

A surface S over k is called *supersingular* if

$$\mathrm{Trans}(S) = 0 \tag{3.1}$$

or equivalently if $\lambda = 0$ or $\rho = b_2$. For example, rational surfaces and more generally unirational surfaces are known to be supersingular ([S2, Lem.2]).

(N.B. This notion has nothing to do with that of a "supersingular" elliptic curve.)

Keeping the same notation as before, we first note:

Proposition 9 *Given an elliptic curve* E/K_0, *the L-function is trivial:*

$$L(E/K_0, s) = 1$$

if and only if the associated elliptic surface S *is supersingular and the Mordell-Weil group* $E(K)$ *is finite.*

Proof. By Theorem 4, the L-function is trivial if and only if W is a vector space of dimension 0. By Proposition 1, $w = 0$ is equivalent to $r = 0$ and $\lambda = 0$. *q.e.d.*

(Note that the above condition is a "geometric" one: both S and K are considered over the algebraically closed field k.)

Theorem 10 *For an elliptic curve E/K_0 such that the associated elliptic surface S is supersingular, the L-function $L(E/K_0, s)$ is equal to the characteristic polynomial of the geometric Frobenius on $E(K)/(tor)$, which is a polynomial in $x = q^{1-s}$ of degree $r = \mathrm{rk}\, E(K)$ of the form*

$$L(E/K_0, s) = (1-x)^{r_0} h(x), \quad h(1) \neq 0 \tag{3.2}$$

where $r_0 = \mathrm{rk}\, E(K_0)$ and $h(x)$ is a product of cyclotomic polynomials. The rank r is equal to w given by (1.10) or (1.11), and $h(1)$ satisfies the formula (2.20).

This is obvious from Proposition 1 and Theorems 7, 8.

Thus the Birch-Swinnerton-Dyer conjecture and the Tate conjecture are true for this class of elliptic curves E/K_0 and elliptic surfaces S/k_0. Also it is evident from (3.2) that the sign of the functional equation of the L-function is $(-1)^{r_0}$.

The above theorem applies for instance to unirational (in particular, rational) elliptic surfaces.

Example 1 Consider the elliptic curve

$$E : Y^2 = X^3 + t^m + 1 \tag{3.3}$$

over $K_0 = k_0(t), k_0 = \mathbf{F}_q$, m being a natural number not divisible by $p = \mathrm{char}(k_0)$. Assume for simplicity that $m \equiv 0 \pmod 6$. Then the elliptic surface S has no reducible fibre so that $\mathrm{rk}\, T = 2, \det T = 1$. In this case, we have

$$w = r + \lambda = 2m - 4 \tag{3.4}$$

(cf. [S5, Prop.3.4]).

Now S is unirational (hence supersingular) if $p^e \equiv -1 \pmod m$ for some $e > 0$ (Prop.4.1, *loc.cit.*). Take $q = p^{2e}$. Then we have $E(K) = E(K_0)$ is of rank $r = 2m - 4$ and torsionfree. By (2.20), we have

$$[Ш(E/K_0)] \det(E(K_0)) = (p^e)^{2p_g}, \tag{3.5}$$

since $\alpha(S) = p_g$. This fact was used in Remark 4.5 of [S5].

In general, it is hard to separate the first factor from the second one (called the regulator), but in this case it can be achieved by means of a crystalline method; see Proposition 4.3, *loc.cit.*.

Remark. In characteristic 0, we can show that the rank of the elliptic curve (3.3) over $\mathbf{C}(t)$ for any m is universally bounded by 68 and that the rank is equal to 68 if m is a multiple of 360. As far as we know, this is the largest rank of an elliptic curve over $\mathbf{C}(t)$ at the moment.

Also, in characteristic $p > 0$ not satisfying the condition $p^e \equiv -1 \pmod{m}$, the surface S is not supersingular in general; for example, for p ordinary (i.e. $p \equiv 1 \pmod{m}$), the rank has the same bound as in characteristic 0.

In any case, the L-function of (3.3) can be expressed in terms of certain Jacobi sums. We hope to discuss these elsewhere.

4 Rational elliptic surfaces

Suppose that S is a rational elliptic surface over k. This means that the function field $k(S)$ of S is a purely transcendental extension of dimension 2 over k. Then $K = k(C)$ is also purely transcendental over k, i.e. $K = k(t)$ (a rational function field) and $g = 0$. Further we have $\rho = b_2 = 10$ and $\lambda = 0$ so that S is supersingular. In the statement of Theorem 10, the formula (2.20) reduces to

$$\frac{[Ш(E/K_0)]\det(E(K_0)/(tor))}{[E(K_0)_{tor}]^2} = \frac{h(1)}{\det T_0} \tag{4.1}$$

since $\alpha(S) = p_g = 0$ for a rational elliptic surface S .

On the other hand, by (1.10), we have

$$r = 8 - \sum_v \deg(v)(m_v - 1) \leq 8. \tag{4.2}$$

The structure of $E(K)$ is well understood by the theory of Mordell-Weil lattices (cf. [S4], [OS]). It is especially interesting for relatively large r. For $r = 8, 7$ or 6, it is isomorphic to E_8, E_7^* or E_6^* or D_6^*, where E_r and D_r are the root lattices and $*$ indicates the dual lattices.

The Galois group of k/k_0 preserves the lattice structure in general. Hence, by Theorem 8, the L-function $L(E/k_0(t), s)$ is equal to the characteristic polynomial of some automorphism of these lattices (in fact, of some element in the Weyl group $W(E_r)$, etc.), and it is a product of some cyclotomic polynomials. Can we determine them more explicitly?

Yes! It can be done with the aid of "algebraic equations arising from Mordell-Weil lattices" (cf. [S6], [S7]). Here are some examples.

Example 2 Let us consider the elliptic curve E defined by

$$Y^2 = X^3 + (1 + t^2)X + (1 + t + t^2 + t^4) \tag{4.3}$$

over $K_0 = \mathbf{F}_p(t)$. We have studied this curve over $\mathbf{Q}(t)$ in [S7, Ex.7.4]) and the information below has been obtained in the course of it. The Mordell-Weil group $E(k(t))$ (k:algebraic closure of $\mathbf{F}_p$) is of rank 6 and isomorphic to E_6^* for any $p \neq 2$, 137, 15784603.

In the following table, we determine the L-function $L(E/\mathbf{F}_p(t), s)$ as a product of cyclotomic polynomials in $x = p^{1-s}$ for $2 < p < 137$. We denote by h_n the n-th cyclotomic polynomial; thus

$$h_2 = 1 + x, h_3 = 1 + x + x^2, \ldots, h_9 = 1 + x^3 + x^6, \ldots$$

p	L-function	cycle type	M_1	No.
3,29,41,67,97	h_9	$(9)^3$		14
5,11,23,37,71,73	$(1-x)^2h_5$	$(1)^2(5)^5$		15
7,127	$(1-x)h_2h_3h_6$	$(3)(6)^4$	+1	23
13	$(1-x)^3h_2h_4$	$(1)^5(2)(4)^5$		18
17,61,79	h_3h_{12}	$(3)(12)^2$		13
19,103,109	$(1-x)h_2h_5$	$(2)(5)^3(10)$		25
31	$(1-x)h_2^3h_4$	$(1)(2)^3(4)^5$	-1	19
43,47	$(1-x)h_2h_4h_6$	$(1)(4)^2(6)(12)$		24
53,89	$(1-x)h_2h_8$	$(1)(2)(8)^3$		20
59	$h_2^2h_3h_6$	$(3)(6)^4$	-1	10
83	$(1-x)^2h_2^2h_4$	$(1)(2)^3(4)^5$	+1	5
101	$(1-x)^4h_2^2$	$(1)^7(2)^9$		2
107	$(1-x)^2h_2^2h_6$	$(1)^3(2)^3(6)^3$	+1	7
113	$(1-x)h_2h_3^2$	$(3)^5(6)^2$		22
131	$(1-x)^2h_2^2h_3$	$(1)(2)^4(3)^2(6)^2$		8

To verify this table, we need to determine the Frobenius element σ_p in the Weyl group $W(E_6)$, up to conjugation.

This group, say G, acts naturally on the dual lattice E_6^*, hence on the set of 54 minimal vectors, forming two orbits of 27 elements. In this way, G embeds into the symmetric group S_{27}. It is known that G has 25 conjugacy classes, and they are determined by the cycle type of an element $g \in G$ viewed as an element of S_{27}, plus the knowledge of $tr(g)$ (trace of g on E_6) (in case the cycle type does not uniquely determine the class); see [Sw, Table 1]. In the above table, the 3rd column gives the cycle type of σ_p, the 4th the value of $M_1 = tr(\sigma_p) + 1$ (when necessary) and the 5th the numbering of conjugacy

classes following Swinnerton-Dyer. The characteristic roots for each conjugacy class can be found in his table (*loc.cit.*).

On the other hand, we have an algebraic equation of degree 27 whose roots describe the minimal vectors of $E(K) \simeq E_6^*$, which in the case under consideration is given by Eq. (7.3) of [S7]:

$$F(X) = X^{27} + 12X^{25} + 60X^{23} + \cdots + 5888X - 4096. \tag{4.4}$$

For each p, decomposing $F(X) \bmod p$ into irreducible factors, we get the cycle type of σ_p; for instance, for $p = 3$, $F(X) \bmod p$ splits into a product of 3 irreducible polynomials of degree 9; we denote the corresponding cycle type by $(9)^3$, and similarly for other cases. Further M_1 can be computed by counting the number a_p of $\mathbf{F}_p$-rational points of the surface S:

$$tr(\sigma_p) = (p^2 + 4p + 1 - a_p)/p. \tag{4.5}$$

Once the conjugacy class is determined, we can apply the result of Swinnerton-Dyer to get the characteristic polynomial. In this way, we can verify the table.

Let us derive some consequence from the above table. First observe that the formula (4.1) becomes

$$[Ш(E/K_0)] \det(E(K_0)) = \frac{h(1)}{3} \tag{4.6}$$

since $\det T_0 = \det T = 3$ and $E(K)$ is torsionfree in our case. Also note that $3\det(E(K_0))$ is an integer (=$\det N_0$).

Now, for $p = 3, 29, 41, \cdots$, we have $r_0 = 0$ and $h(1) = 3$. Thus the Mordell-Weil group $E(\mathbf{F}_p(t))$ is trivial. Further, using the general fact that the order of Ш is a square or twice a square (cf. [T2]), we conclude that the Shafarevich-Tate group is also trivial:

$$Ш(E/\mathbf{F}_p(t)) = 0.$$

Also we can see that $N_0 = \mathrm{NS}(S/k_0)$ is an indefinite lattice of rank 4 with $\det = 3$.

Similarly, for $p = 5, 11, 23, \cdots$, we have $r_0 = 2$ and $h(1) = 5$. By the same argument as above, we see

$$Ш(E/\mathbf{F}_p(t)) = 0, \quad \det(E(\mathbf{F}_p(t))) = \frac{5}{3}.$$

We can also give generators of the Mordell-Weil group $E(\mathbf{F}_p(t))$ explicitly. Namely, in this case, the algebraic equation (4.4) has exactly 2 roots in $\mathbf{F}_p$

(look at the cycle type). For example, for $p = 5$, they are given by $X = -1, -2 \bmod p$; by the theory of Mordell-Weil lattices of type E_6 (cf. [S7], [S6]), we see that there are 2 rational points A, B in $E(\mathbf{F}_p(t))$ of the form

$$A = (-t + b, t^2 + dt + e), B = (-2t + b', t^2 + d't + e').$$

To show that these points generate the full Mordell-Weil group $E(\mathbf{F}_p(t))$, we have only to check the Gram matrix to be

$$\begin{pmatrix} < A, A > & < A, B > \\ < A, B > & < B, B > \end{pmatrix} = \begin{pmatrix} 4/3 & -1/3 \\ -1/3 & 4/3 \end{pmatrix},$$

which is an easy exercise in computing the height pairing (cf. [S4]).

In my original plan, this paper should also have included some other type of examples (not necessarily supersingular), for instance, those related to elliptic modular surfaces or to Jacobi sums. Because of space and time limitation, however, I hope to treat them in some other occasion.

References

[B] Bourbaki, N.: Groupes et Algèbres de Lie, Chap. 4,5 et 6, Hermann, Paris (1968).

[CS] Conway, J., Sloane, N.: Sphere Packings, Lattices and Groups, Springer-Verlag (1988).

[E] Elkies, N.: On Mordell-Weil lattices, Arbeitstagung Bonn (1990).

[G] Gordon, W.J.: Linking the conjectures of Artin-Tate and Birch-Swinnerton-Dyer, Compos. Math. 38, 163-199(1979).

[I] Igusa, J.: Betti and Picard numbers of abstract algebraic surfaces, Proc. N.A.S. 46, 724-726(1960).

[K] Kodaira, K.: On compact analytic surfaces II-III, Ann. of Math. 77, 563-626(1963); 78, 1-40(1963); Collected Works, III, 1269-1372, Iwamami and Princeton Univ. Press (1975).

[Mc] McGuinness, O.: The explicit formula for elliptic curves over function fields, Appendix to A. Brumer, Preprint.

[Mi] Milne, J.: On a conjecture of Artin and Tate, Ann. of Math.102, 517-533(1975).

[N] Néron, A. : Modèles minimaux des variétés abéliennes sur les corps locaux et globaux, Publ. Math. IHES **21** (1964).

[Oe] Oesterlé, J.: Empilements de sphères, Sém. Bourbaki 1990, $n^0$727.

[Ogg] Ogg, A.P.: Elliptic curves and wild ramification, Am. J. Math. 89, 1-21(1967).

[Ogu] Oguiso, K.: An elementary proof of the topological Euler characteristic formula for an elliptic surface, Comment. Math. Univ. St. Pauli 39, 81-86(1990).

[OS] Oguiso, K., Shioda, T.: The Mordell-Weil lattice of a rational elliptic surface, Comment. Math. Univ. St. Pauli 40, 83-99(1991).

[R] Raynaud, M.: Caractéristique d'Euler-Poincaré d'un faisceau et cohomologie des variétés abéliennes, Sém. Bourbaki 1964/65, $n^0$286; In: Dix Exposés ..., 12-30(1968).

[Sa] Saito, T.: Conductor, discriminant, and the Noether formula of arithmetic surfaces, Duke Math. J. 57, 151-173(1988).

[Se1] Serre, J-P.: Zeta and L functions, In: Arithmetical Algebraic Geometry, Harper and Row, New York, 93-110 (1965); Collected Papers, II, 249-259.

[Se2] — : Facteurs locaux des fonctions zêta des variétés algébriques, Sém. DPP 1969/70 $n^0$19; Collected Papers, II, 581-592.

[S1] Shioda, T.: On elliptic modular surfaces, J. Math. Soc. Japan 24, 20-59(1972).

[S2] — : An example of unirational surfaces in characteristic p, Math. Ann. 211, 233-236(1974).

[S3] — : Mordell-Weil lattices and Galois representation, I,II,III. Proc. Japan Acad. **65A**, 268-271; 296-299; 300-303 (1989).

[S4] — : On the Mordell-Weil lattices, Comment. Math. Univ. St. Pauli 39, 211- 240(1990).

[S5] — : Mordell-Weil lattices and sphere packings, Am. J. Math. 113, 931-948(1991).

[S6] — : Construction of elliptic curves with high rank via the invariants of the Weyl groups, J. Math. Soc. Japan 43, 673-719 (1991).

[S7] — : Theory of Mordell-Weil lattices, Proc. ICM Kyoto 1990, Springer, vol.I, 473-489 (1991).

[Sw] Swinnerton-Dyer, H.P.F.: The zeta function of a cubic surface over a finite field, Proc.Cambridge Phil.Soc. 63, 55-71(1967).

[Sz] Szpiro, L.: Discriminant et conducteur des courbes elliptiques, Astérisque 183, 7-18(1990).

[T1] Tate, J.: Algebraic cycles and the pole of zeta functions, In: Arithmetical Algebraic Geometry, 93-110, Harper and Row, New York (1965).

[T2] — : On the conjectures of Birch and Swinnerton-Dyer and a geometric analog, Sém. Bourbaki 1965/66, $n^0$306.; In: Dix Exposés ..., 189-214(1968).

[T3] — : Algorithm for determining the type of a singular fiber in an elliptic pencil, LNM 476, 33-52(1975).

[W] Weil, A. : Collected Papers I, II, III, Springer-Verlag (1980).

Department of Mathematics
Rikkyo University
Nishi-Ikebukuro, Tokyo 171
Japan