ON THE TATE-SHAFAREVICH GROUPS OF CERTAIN ELLIPTIC CURVES

JACK THORNE

Abstract. The Tate-Shafarevich groups of certain elliptic curves over $\mathbb{F}_q(t)$ are related, via étale cohomology, to the group of points of an elliptic curve with complex multiplication. The Cassels-Tate pairing is computed under this identification.

Contents

1. Introduction

Let k be a global field. One of the fundamental arithmetic invariants associated to an elliptic curve E over k is the Tate-Shafarevich group $Ш(k, E)$, which measures (in some sense) the failure of the Hasse principle for the curve E. Knowledge of its finiteness is the main barrier to the existence of an effective algorithm for computing the group of rational points of E [17].

When k is a number field, the Tate-Shafarevich group is very mysterious. It has been computed only in a handful of examples, although there are many curves for which the l^∞-torsion is known for some prime l. On the other hand, if k is a global field of positive characteristic p, a little more is known. For example, a curve over such a field can be interpreted as the generic member of a family of elliptic curves over another curve over a finite field, and one knows that the Tate-Shafarevich group is finite if the total space of this family is a rational surface or a K3 surface [8], [2]. Furthermore, if the l^∞-torsion of Ш is finite for some prime l, then the whole group must itself be finite [16].

The aim of this note is to exhibit a member of a family of examples of elliptic curves defined over global fields of positive characteristic, where

the Tate-Shafarevich group takes on a particularly pleasant form. We can also give an explicit formula for the Cassels-Tate pairing.

Let p be a prime congruent to 1 modulo 4, and let q be a power of p. Consider the elliptic curve

$$E : t(t-1)y^2 = x(x-1)(x-t)$$

over the field $\mathbb{F}_q(t)$. The above equation can be thought of as defining a family of elliptic curves over $\mathbb{P}^1_{/\mathbb{F}_q}$. In fact, the total space of the minimal regular model of this family is a $K3$ surface, cf. [6], chapter 8. Thus we know a priori that $Ш(\mathbb{F}_q(t), E)$ is finite. We will follow [16] in relating the Tate-Shafarevich group to the Brauer group of this surface and then applying the methods of étale cohomology.

We state our results as follows. Factor $p = \pi\overline{\pi}$ in the field of Gaussian integers, where π is chosen to be congruent to 1 modulo $(1+i)^3$.

Theorem 1. *Let $l \neq p$ be an odd prime. There is an isomorphism*

$$Ш(\mathbb{F}_q(t), E)[l^\infty] \cong (\mathbb{Z}[i] \otimes \mathbb{Q}_l/\mathbb{Z}_l)[(\pi/\overline{\pi})^f - 1],$$

where $q = p^f$.

Here we view $(\pi/\overline{\pi})^f - 1$ as an element of the ring $\mathbb{Z}[i] \otimes \mathbb{Z}_l$. The group on the right above is the kernel of multiplication by this element. Thus the order of the l-part of the Tate-Shafarevich group depends only on the valuations of $(\pi/\overline{\pi})^f - 1$ at the places of $\mathbb{Q}(i)$ lying above l.

Remark. One can show by a computation with L-functions that the p^∞-torsion of Ш is trivial. In fact, since Ш is finite, the conjecture of Birch and Swinnerton-Dyer is known to hold in this case [16], and this allows one to compute the order of Ш.

The Cassels-Tate pairing is a non-degenerate skew-symmetric pairing

$$\langle , \rangle : Ш(\mathbb{F}_q(t), E) \times Ш(\mathbb{F}_q(t), E) \to \mathbb{Q}/\mathbb{Z} = \oplus_l \mathbb{Q}_l/\mathbb{Z}_l.$$

We shall recall its definition below.

Theorem 2. *Let $l \neq p$ be an odd prime, and let x, y be elements of $Ш(\mathbb{F}_q(t), E)$ killed by l^n. Choose representatives $x = \alpha/l^n, y = \beta/l^n$, where α and β are Gaussian integers, under the above isomorphism. Then we can compute the Cassels-Tate pairing of x and y, viewed as an element of $\mathbb{Q}_l/\mathbb{Z}_l$, as*

$$\langle x, y \rangle = -\Re\alpha\Re\left(\left(\frac{\pi}{\overline{\pi}}\right)^f \frac{\beta}{l^{2n}} - \frac{\beta}{l^{2n}}\right) - \Im\alpha\Im\left(\left(\frac{\pi}{\overline{\pi}}\right)^f \frac{\beta}{l^{2n}} - \frac{\beta}{l^{2n}}\right) \ mod\ \mathbb{Z}_l.$$

Here $\Re$ and $\Im$ denote real and imaginary part, respectively.

Notations: We fix algebraic closures $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ and $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$. If X is a variety over a subfield of $\overline{\mathbb{Q}}$ or $\overline{\mathbb{F}}_p$ then we write $\overline{X}$ to denote the base change of this variety to the corresponding algebraic closure.

I would like to thank Benedict Gross for encouraging me to think about this example.

2. The computation

Consider the elliptic pencil defined by the equation

$$t(t-1)y^2 = x(x-1)(x-t),$$

considered as having coefficients in $K(t)$, where $K = \mathbb{Q}(i)$. Passing to the minimal regular model gives an elliptic K3 surface X, which is birational over K to the quotient of the product

$$A = E_1 \times E_2, \text{ where } E_i \text{ is the curve } y_i^2 = x_i^3 - x_i,$$

by the cyclic group generated by the order 4 automorphism

$$\sigma : ((x_1, y_1), (x_2, y_2)) \mapsto ((-x_1, iy_1), (-x_2, -iy_2)).$$

For an explicit description of this map, see [14]. This quotient has rational double points for singularities; there are 4 of type A_3, and 6 of type A_1, corresponding to the fixed points of σ and σ^2. Thus X can also be obtained by blowing up (infinitely near) points on the quotient to resolve the singularities [7].

Write Z for the union of the exceptional divisors, and U for its complement in X. Let Λ be the constant sheaf μ_{l^n} for a fixed odd prime l. We have an exact sequence in étale cohomology [4]

$$0 \longrightarrow H^2_c(\overline{U}, \Lambda) \longrightarrow H^2(\overline{X}, \Lambda) \longrightarrow H^2(\overline{Z}, \Lambda) \longrightarrow 0.$$

This sequence has a natural splitting: Z is a union of $\mathbb{P}^1$'s, and the images of these under the cycle map give free generators for $H^2(\overline{Z}, \Lambda)$.

Let U' denote the complement of the fixed points of σ and σ^2 in A. Since σ acts in an étale manner on U', we have isomorphisms

$$H^2_c(\overline{U}, \Lambda) \cong H^2_c(\overline{U'}, \Lambda)^{\langle\sigma\rangle} \cong H^2(\overline{A}, \Lambda)^{\langle\sigma\rangle}.$$

It follows that we have a canonical decomposition

$$H^2(\overline{X}, \Lambda) \cong H^2(\overline{A}, \Lambda)^{\langle\sigma\rangle} \oplus H^2(\overline{Z}, \Lambda).$$

In what follows, if S is a smooth surface we will write $H_S = H^2(\overline{S}, \mathbb{Z}_l(1))$ and C_S for the $\mathbb{Z}_l$ span in H_S of the image of the cycle map. Combining the above formula with the Künneth theorem gives an isomorphism

$$H_X/C_X \cong (H^1(\overline{E}_1, \mathbb{Z}_l) \otimes H^1(\overline{E}_2, \mathbb{Z}_l))^{\langle\sigma\rangle}(1)/M,$$

where M is the intersection of the $\mathbb{Z}_l$-span of the image of the cycle map with the (1,1) Künneth summand.

At this point it is helpful to note that, since X is an elliptic $K3$ surface, numerical, homological and algebraic equivalence of divisors are all equivalent. Moreover, the cycle map (viewed as a map $\mathrm{Pic}(\overline{X}) \to H^2$) is injective even after tensoring with $\mathbb{Z}_l$, and has primitive image. Finally, M can also be computed as the space of elements fixed by some open subgroup of the Galois group, since Tate's conjecture T^1 holds for $K3$ surfaces [15]. (Tate's conjecture can also be verified explicitly in this case using, for example, the theorem of Shioda quoted below).

The prime p splits in K; write $p = \pi\bar{\pi}$, where $\pi \equiv 1 \mod (1+i)^3$. We choose an extension of the place π to $\overline{\mathbb{Q}}$. We can reduce the above picture modulo π; use a subscript S_π to denote such reduction.

We begin by computing the l^∞-torsion of the cohomological Brauer group $\mathrm{Br}(\overline{X_\pi}) = H^2(\overline{X_\pi}, \mathbb{G}_m)$. Since this group is l-divisible it suffices to consider instead the l-adic Tate module $T_l \operatorname{Br} \overline{X_\pi}$. The Kummer exact sequence gives, after passing to the limit, an exact sequence of G-modules

$$0 \longrightarrow NS(\overline{X_\pi}) \otimes \mathbb{Z}_l \longrightarrow H^2(\overline{X_\pi}, \mathbb{Z}_l(1)) \longrightarrow T_l \operatorname{Br} \overline{X_\pi} \longrightarrow 0.$$

Thus we have isomorphisms of modules for Frob_π

$$T_l \operatorname{Br} \overline{X_\pi} \cong H_X/S_X \cong H_A/S_A \cong (H^1(\overline{E}_1, \mathbb{Z}_l) \otimes H^1(\overline{E}_2, \mathbb{Z}_l))^{\langle\sigma\rangle}(1)/M,$$

with M as above. Making use of the identification of $H^1(\overline{E}_i, \mathbb{Z}_l)$ as the dual of $T_l E$, we have

$$T_l \operatorname{Br} \overline{X_\pi} \cong (T_l E_1 \otimes T_l E_2)^{\langle\sigma\rangle}(-1)/M.$$

Now, the main theorem of complex multiplication [13] shows that $T_l E_1 = T_l E_2 = \mathbb{Z}[i] \otimes \mathbb{Z}_l$ as modules for Frob_π, where Frob_π now acts as multiplication by $\pi \otimes 1$. On the other hand, σ acts on $T_l E_1$ as multiplication by $i \otimes 1$ and on $T_l E_2$ as multiplication by $-i \otimes 1$. We thus have an isomorphism

$$T_l \operatorname{Br} \overline{X_\pi} \cong \mathbb{Z}[i] \otimes \mathbb{Z}_l,$$

with Frob_π acting as multiplication by $\pi/\overline{\pi} \otimes 1$.

Now, let $\mathbb{F}_q$ be a finite subfield of our fixed algebraic closure $\overline{\mathbb{F}}_p$, and set $G = \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_q)$. One knows that $Ш(\mathbb{F}_q(t), E)$ can be identified with the Brauer group $\mathrm{Br}(X_\pi \otimes \mathbb{F}_q)$ of $X_\pi \otimes \mathbb{F}_q$ [5]. We will now compute $\mathrm{Br}(X_\pi \otimes \mathbb{F}_q)[l^\infty]$.

First, the Hochschild-Serre spectral sequence gives a short exact sequence

$$0 \longrightarrow H^1(G, \mathrm{Pic}(\overline{X_\pi})) \longrightarrow \mathrm{Br}(X_\pi \otimes \mathbb{F}_q) \longrightarrow \mathrm{Br}(\overline{X_\pi})^G \longrightarrow 0.$$

At this point, we apply a theorem of Shioda.

Theorem 3 ([12])**.** *Let X be an elliptic surface with a section over an algebraically closed field. Let V be the sublattice of $NS(X)$ spanned by the zero section, a smooth fibre, and the components of the singular fibres not meeting the zero section. Then V is freely spanned by these cycles, and we have an isomorphism*

$$MW(X) \to NS(X)/V.$$

We call V the trivial lattice. Using the above theorem it is not hard to see that $H^1(G, V)$ always vanishes; in our case V even has trivial Galois action. It is easily computed (using, for example, a 2-descent) that $MW(\overline{X_\pi})$ is a 2-torsion group of order 4, and so we find that $H^1(G, \mathrm{Pic}(\overline{X_\pi}))[l^\infty] = 0$ and hence $\mathrm{Br}(X_\pi)[l^\infty] = \mathrm{Br}(\overline{X_\pi})[l^\infty]^G$.

Theorem 4. *Let $l \neq p$ be an odd prime. There is an isomorphism*

$$Ш(\mathbb{F}_q(t), E)[l^\infty] \cong (\mathbb{Z}[i] \otimes \mathbb{Q}_l/\mathbb{Z}_l)[(\pi/\overline{\pi})^f - 1],$$

where $q = p^f$.

We now compute the Cassels-Tate pairing $\langle , \rangle$ on $\mathrm{Br}(X_\pi)[l^\infty]$, following the description of [16]. To simplify notation, we now write X_π to mean $X_\pi \otimes \mathbb{F}_q$. After the Kummer exact sequence, we have for every $n \geq 1$ a surjection

$$H^2(X_\pi, \mu_{l^n}) \longrightarrow \mathrm{Br}(X_\pi)[l^n].$$

Given $x, y \in \mathrm{Br}(X_\pi)[l^n]$, we choose pre-images $\tilde{x}, \tilde{y}$ under this map. Associated to the exact sequence of sheaves

$$0 \longrightarrow \mu_{l^n} \longrightarrow \mu_{l^{2n}} \xrightarrow{\times l^n} \mu_{l^n} \longrightarrow 0$$

is a boundary map

$$H^2(X_\pi, \mu_{l^n}) \xrightarrow{\delta} H^3(X_\pi, \mu_{l^n}).$$

We then form the cup product $\tilde{x} \cup \delta\tilde{y} \in H^5(X_\pi, \mu_{l^n}^{\otimes 2})$. The image of this element under the canonical inclusion

$$H^5(X_\pi, \mu_{l^n}^{\otimes 2}) \longrightarrow H^5(X_\pi, \mathbb{Q}_l/\mathbb{Z}_l(2)) \cong \mathbb{Q}_l/\mathbb{Z}_l$$

defines $\langle x, y \rangle$. It is known that this pairing is skew-symmetric.

To compute this pairing, we again refer to the Hochschild-Serre spectral sequence for the covering $\overline{X_\pi} \to X_\pi$, in order to compute the cohomology of the sheaf μ_{l^n}. This sequence degenerates at the E_2 page, and we have isomorphisms

$$H^2(X_\pi, \mu_{l^n}) \cong H^2(\overline{X_\pi}, \mu_{l^n})^G, H^3(X_\pi, \mu_{l^n}) \cong H^2(\overline{X_\pi}, \mu_{l^n})_G,$$

compatible with the relevant cup products. The map δ above becomes the first boundary map in group cohomology associated to the exact sequence

$$0 \longrightarrow H^2(\overline{X_\pi}, \mu_{l^n}) \longrightarrow H^2(\overline{X_\pi}, \mu_{l^{2n}}) \longrightarrow H^2(\overline{X_\pi}, \mu_{l^n}) \longrightarrow 0.$$

We can always choose pre-images $\tilde{x}, \tilde{y}$ lying in the summand we have identified above with $(H^1(\overline{E}_1, \mu_{l^n}) \otimes H^1(\overline{E}_2, \mu_{l^n}))^{\langle\sigma\rangle}$. The relevant cup product is the tensor product of the cup products

$$H^1(\overline{E}_i, \mu_{l^n}) \times H^1(\overline{E}_i, \mu_{l^n}) \longrightarrow H^2(\overline{E}_i, \mu_{l^n}^{\otimes 2}).$$

With the identifications made above this is none other than the Weil pairing [3], and following [9] this is induced by the negative of the canonical polarization:

$$\begin{aligned} \mathbb{Z}[i] \times \mathbb{Z}[i] &\longrightarrow \mathbb{Z} \\ (x, y) &\longmapsto -\Im(x\overline{y}). \end{aligned}$$

Putting all this together, we obtain the following theorem.

Theorem 5. *Let $l \neq p$ be an odd prime, and let x, y be elements of*

$$Ш(\mathbb{F}_q(t), E)[l^\infty] \cong (\mathbb{Z}[i] \otimes \mathbb{Q}_l/\mathbb{Z}_l)[(\pi/\overline{\pi})^f - 1]$$

killed by l^n. Choose representatives $x = \alpha/l^n, y = \beta/l^n$, where α and β are Gaussian integers. Then we can compute the Cassels-Tate pairing as

$$\langle x, y\rangle = -\Re\alpha\Re\left(\left(\frac{\pi}{\overline{\pi}}\right)^f \frac{\beta}{l^{2n}} - \frac{\beta}{l^{2n}}\right) - \Im\alpha\Im\left(\left(\frac{\pi}{\overline{\pi}}\right)^f \frac{\beta}{l^{2n}} - \frac{\beta}{l^{2n}}\right) \ mod\ \mathbb{Z}_l.$$

3. Other examples

One can repeat the same argument with the curve

$$E' : y^2 + (1 - 3t^2)xy - t^4(t^2 - 1)y = x^3,$$

also studied in [14]. This time one replaces the curves E_i with the curve given by the equation $y^2 = x^3 + 1$, and the field K with $\mathbb{Q}(\sqrt{-3})$. One must further assume that p is an odd prime congruent to 1 modulo 3. What the curves E and E' have in common is that, working in characteristic zero, the associated minimal regular models over the projective

line are singular $K3$ surfaces; that is, their Picard numbers are equal to 20, the maximum possible. The conditions on the prime p mean that one avoids those primes at which the $K3$ surfaces are supersingular, in the sense of Artin [1]. This means that the rank of the Picard group does not grow when one reduces modulo p.

The singular $K3$ surfaces have been classified up to isomorphism over $\mathbb{C}$ by Shioda and Inose [10]; in fact, they are all essentially the Kummer surfaces of products of pairs of isogenous CM elliptic curves. (The Kummer surface of an abelian surface is the minimal desingularisation of the quotient by ± 1; it is always a $K3$ surface). In particular, they can all be defined over number fields, and they all admit pencils of elliptic curves. Taking any such pencil and enlarging the base field to trivialise the Galois action on the Néron-Severi group, one can apply similar reasoning to the above to compute the Tate-Shafarevich group (and, indeed, the L-function) of the associated mod p elliptic curves, whenever the reduction is ordinary (as opposed to supersingular).

One can ask what happens when one instead takes a prime p such that the reduction is supersingular. In fact, a cohomological computation of the Brauer group in this situation, over a sufficiently large field, already appears in [1]. Combining this with results of [11], one sees that it is a p-torsion group of order q/p^2 over the field with q elements, a computation valid whenever the action of the Galois group on the Néron-Severi group is trivial.

References

[1] M. Artin. Supersingular $K3$ surfaces. *Ann. Sci. École Norm. Sup. (4)*, 7:543–567 (1975), 1974.

[2] M. Artin and H. P. F. Swinnerton-Dyer. The Shafarevich-Tate conjecture for pencils of elliptic curves on $K3$ surfaces. *Invent. Math.*, 20:249–266, 1973.

[3] P. Deligne. *Cohomologie étale*. Lecture Notes in Mathematics, Vol. 569. Springer-Verlag, Berlin, 1977. Séminaire de Géométrie Algébrique du Bois-Marie SGA $4\frac{1}{2}$, Avec la collaboration de J. F. Boutot, A. Grothendieck, L. Illusie et J. L. Verdier.

[4] Eberhard Freitag and Reinhardt Kiehl. *Étale cohomology and the Weil conjecture*, volume 13 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1988. Translated from the German by Betty S. Waterhouse and William C. Waterhouse, With an historical introduction by J. A. Dieudonné.

[5] Alexander Grothendieck. Le groupe de Brauer. II. Théorie cohomologique. In *Dix Exposés sur la Cohomologie des Schémas*, pages 67–87. North-Holland, Amsterdam, 1968.

[6] Nicholas M. Katz. *Twisted L-functions and monodromy*, volume 150 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 2002.

[7] Joseph Lipman. Rational singularities, with applications to algebraic surfaces and unique factorization. *Inst. Hautes Études Sci. Publ. Math.*, (36):195–279, 1969.
[8] J. S. Milne. The Brauer group of a rational surface. *Invent. Math.*, 11:304–307, 1970.
[9] David Mumford. *Abelian varieties*, volume 5 of *Tata Institute of Fundamental Research Studies in Mathematics*. Published for the Tata Institute of Fundamental Research, Bombay, 2008. With appendices by C. P. Ramanujam and Yuri Manin, Corrected reprint of the second (1974) edition.
[10] T. Shioda and H. Inose. On singular $K3$ surfaces. In *Complex analysis and algebraic geometry*, pages 119–136. Iwanami Shoten, Tokyo, 1977.
[11] Tetsuji Shioda. Supersingular $K3$ surfaces. In *Algebraic geometry (Proc. Summer Meeting, Univ. Copenhagen, Copenhagen, 1978)*, volume 732 of *Lecture Notes in Math.*, pages 564–591. Springer, Berlin, 1979.
[12] Tetsuji Shioda. On the Mordell-Weil lattices. *Comment. Math. Univ. St. Paul.*, 39(2):211–240, 1990.
[13] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.
[14] Jan Stienstra and Frits Beukers. On the Picard-Fuchs equation and the formal Brauer group of certain elliptic $K3$-surfaces. *Math. Ann.*, 271(2):269–304, 1985.
[15] John Tate. Conjectures on algebraic cycles in l-adic cohomology. In *Motives (Seattle, WA, 1991)*, volume 55 of *Proc. Sympos. Pure Math.*, pages 71–83. Amer. Math. Soc., Providence, RI, 1994.
[16] John Tate. On the conjectures of Birch and Swinnerton-Dyer and a geometric analog. In *Séminaire Bourbaki, Vol. 9*, pages 415–440, Exp. No. 306. Soc. Math. France, Paris, 1995.
[17] John T. Tate. The arithmetic of elliptic curves. *Invent. Math.*, 23:179–206, 1974.

Harvard University, Department of Mathematics, 1 Oxford Street, Cambridge, MA 02138, USA
E-mail address: thorne@math.harvard.edu