PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 146, Number 2, February 2018, Pages 541–545
http://dx.doi.org/10.1090/proc/13759
Article electronically published on September 6, 2017

ON A SPECIAL CASE OF WATKINS' CONJECTURE

MATIJA KAZALICKI AND DANIEL KOHEN

(Communicated by Kathrin Bringmann)

Abstract. Watkins' conjecture asserts that for a rational elliptic curve E the degree of the modular parametrization is divisible by 2^r, where r is the rank of E. In this paper, we prove that if the modular degree is odd, then E has rank zero. Moreover, we prove that the conjecture holds for all rank two rational elliptic curves of prime conductor and positive discriminant.

1. Introduction

Given a rational elliptic curve E of conductor N, by the modularity theorem, there exists a morphism of a minimal degree

$$\phi : X_0(N) \to E,$$

that is defined over $\mathbb{Q}$, where $X_0(N)$ is the classical modular curve. Its degree, denoted by m_E, is called the *modular degree.* While analyzing experimental data, Watkins conjectured that for an elliptic curve of rank r, m_E is divisible by 2^r [9, Conjecture 4.1]. In particular, if the modular degree is odd, the rank should be zero; the proof of this assertion is the main result of this work.

The study of elliptic curves with odd modular degree was first developed in [1] by Calegari and Emerton, where they showed that a rational elliptic curve with odd modular degree has to satisfy a series of very restrictive hypotheses. For a detailed list of conditions see [1, Theorem 1.1]. Later, building on this work, Yazdani [8] studied abelian varieties having odd modular degree. As a by-product of his work, he proves that if a rational elliptic curve has odd modular degree, then it has rank zero, except perhaps if it has prime conductor and even analytic rank (see [8, Theorem 3.8] for a more general statement). The main result of this paper is the following theorem:

Theorem 1.1. *If $E/\mathbb{Q}$ is an elliptic curve of odd modular degree, then E has rank zero.*

By the aforementioned results it is enough to restrict ourselves to the case where E has prime conductor p and even analytic rank. Moreover, it is clear that we can assume that the curve E is the strong Weil curve, that is, the kernel of the map $J_0(p) \to E$ is connected ($J_0(p)$ is the Jacobian of $X_0(p)$).

The elliptic curve E gives rise to a normalized newform $f_E \in S_2(\Gamma_0(p))$ by the modularity theorem. The main idea of the article is to associate to f_E (or E) an

Received by the editors January 20, 2017 and, in revised form, March 31, 2017.
2010 *Mathematics Subject Classification.* Primary 11G05; Secondary 11G20.
The first author's work was supported by the QuantiXLie Center of Excellence.
The second author's work was supported by a doctoral fellowship of the Consejo Nacional de Inevsitagciones Científicas y Técnicas.

element v_E of the Picard group $\mathcal{X}$ of a certain curve X (which is a disjoint union of curves of genus zero) as in [3]. More precisely, $\mathcal{X}$ can be described as the free $\mathbb{Z}$-module of divisors supported on the isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}_p}$, denoted by $e_1, e_2, \ldots, e_n$, where $n-1$ is the genus of $X_0(p)$. They are in bijection with the isomorphism classes of supersingular elliptic curves $E_i/\overline{\mathbb{F}_p}$. The action of Hecke correspondences on X induces an action on $\mathcal{X}$. There is a correspondence between modular forms of level p and weight 2 and elements of $\mathcal{X} \otimes \mathbb{C}$ that preserves the action of the Hecke operators ([3, Proposition 5.6]). Let $v_E = \sum v_E(e_i)e_i \in \mathcal{X}$ be an eigenvector for all Hecke operators t_m corresponding to f_E, i.e. $t_m v_E = a(m)v_E$, where $f_E(\tau) = \sum_{m=1}^{\infty} a(m)q^m$. We normalize v_E (up to sign) such that the greatest common divisor of all its entries is 1. We define a $\mathbb{Z}$-bilinear pairing

$$\langle -, - \rangle : \mathcal{X} \times \mathcal{X} \to \mathbb{Z},$$

by requiring $\langle e_i, e_j \rangle = w_i \delta_{i,j}$ for all $i, j \in \{1, \ldots, n\}$, where $w_i = \frac{1}{2}\#\mathrm{Aut}(E_i)$.

We have the following key result of Mestre that relates the norm of v_E to the modular degree m_E.

Proposition 1.2 ([6, Theorem 3])**.**

$$\langle v_E, v_E \rangle = m_E t,$$

where t is the size of $E(\mathbb{Q})_{tors}$.

The final ingredient we need is the Gross-Waldspurger formula on special values of L-series [3]. An alternative approach is to use the Gross-Kudla formula for the special values of triple products of L-functions [4].

In [5], while studying supersingular zeros of divisor polynomials of elliptic curves, the authors posed the following conjecture.

Conjecture 1.3. *If E is an elliptic curve of prime conductor p, root number 1, and $rank(E) > 0$, then $v_E(e_i)$ is an even number for all e_i with $j(E_i) \in \mathbb{F}_p$.*

The conclusion of the conjecture holds for any elliptic curve $E/\mathbb{Q}$ of prime conductor and root number -1, as well as for any curve of prime conductor that has positive discriminant and no rational points of order 2 (see [5, Thrms. 1.1, 1.2, 1.4]).

In the last paragraph of this paper, we will show the connection between this conjecture and Watkins' conjecture:

Theorem 1.4. *Let $E/\mathbb{Q}$ be an elliptic curve of prime conductor such that $rank(E) > 0$. If $v_E(e_i)$ is even number for all e_i with $j(E_i) \in \mathbb{F}_p$, then $4|m_E$.*

In particular, as remarked before, this verifies Watkins' conjecture if E has prime conductor, $disc(E) > 0$, and $rank(E) = 2$.

2. Proof of the main theorem

We will give a series of propositions that will allow us to prove Theorem 1.1.

Proposition 2.1. *If $E/\mathbb{Q}$ has non-zero rank, then $L(E, 1) = 0$.*

Proof. This is a classical application of the Gross-Zagier and Kolyvagin theorems. For a reference see [2, Theorem 3.22]. □

Proposition 2.2. *If $E/\mathbb{Q}$ has prime conductor and non-zero rank, then $E(\mathbb{Q})_{tors}$ is trivial.*

Proof. This is a well-known result; for example in [6] it is shown that the isogeny classes of rational elliptic curves with conductor p and non-trivial rational torsion subgroup are either $11.a$, $17.a$, $19.a$ and $37.b$, or the so-called Neumann-Setzer curves that have a 2-rational point. All these curves have rank zero [7]. □

Proposition 2.3. *Let $v_E = \sum_{i=1}^n v_E(e_i)e_i \in \mathcal{X}$ be the vector corresponding to f_E. We have that $\sum_{i=1}^n v_E(e_i) = 0$.*

Proof. The vector $e_0 = \sum_{i=1}^n \frac{e_i}{w_i}$ corresponds to the Eisenstein series ([3, Formula 4.9]). Moreover, the pairing $\langle -, - \rangle : \mathcal{X} \times \mathcal{X} \to \mathbb{Z}$ is compatible with the Hecke operators. Since the space of cuspforms is orthogonal to the Eisenstein series, we obtain

$$\langle v_E, e_0 \rangle = \sum_{i=1}^n v_E(e_i) = 0.$$

□

Proposition 2.4. *The numbers w_k are all equal to 1 unless $j(E_k) = 0$ (in which case $w_k = 3$) or $j(E_k) = 1728$ (in which case $w_k = 2$). The value $j = 0$ is a supersingular j-invariant precisely for $p \equiv 2 \pmod 3$ and $j = 1728$ is a supersingular j-invariant for $p \equiv 3 \pmod 4$.*

Proof. See [3, Table 1.3 p. 117]. □

Given $-D$ a fundamental negative discriminant, Gross defines

$$b_D = \sum_{i=1}^n \frac{h_i(-D)}{u(-D)} e_i,$$

where $h_i(-D)$ is the number of optimal embeddings of the order of discriminant $-D$ into $End(E_i)$ modulo conjugation by $End(E_i)^\times$ and $u(-D)$ is the number of units of the order. We are in position to state (a special case of) the Gross-Waldspurger formula [3, Proposition 13.5].

Proposition 2.5. *If $-D$ is a fundamental negative discriminant with $\left(\frac{-D}{p}\right) = -1$, then*

$$L(E,1)L(E \otimes \varepsilon_D, 1) = \frac{(f_E, f_E)}{\sqrt{D}} \frac{{m_D}^2}{\langle v_E, v_E \rangle},$$

where ε_D is the quadratic character associated to $-D$, (f_E, f_E) is the Petersson inner product on $\Gamma_0(p)$ and

$$m_D = \langle v_E, b_D \rangle.$$

We will use the formula in the case that $-D = -4$ (and thus $p \equiv 3 \bmod 4$). In this situation a rational elliptic curve of j-invariant equal to 1728 with complex multiplication by $\mathbb{Z}[i]$ reduces mod p to the supersingular elliptic curve E_k and this reduction induces two optimal embeddings of $\mathbb{Z}[i]$ into $End(E_k)$. On the other hand, we know that $\sum_i h_i(-4) = 2h(-4) = 2$, where $h(-4)$ is the class number of the quadratic imaginary field $\mathbb{Q}(\sqrt{-1})$ ([3, Formula 1.12]); thus $h_i = 0$ unless $i = k$ in which case $h_k(-4) = 2$. Since $u(-4) = 4$, we obtain that $b_4 = \frac{1}{2}e_k$.

Now we have the necessary ingredients in order to prove Theorem 1.1.

Proof of Theorem 1.1. As remarked in the introduction, it is enough to prove the theorem when E has prime conductor p and it is the strong Weil curve. Suppose on the contrary that E has positive rank. In consequence, by Proposition 1.2 and Proposition 2.2 we know that $\langle v_E, v_E\rangle$ must be odd. Moreover,

$$\langle v_E, v_E\rangle = \sum_{i=1}^{n} w_i v_E(e_i)^2 \equiv \sum_{i=1}^{n} w_i v_E(e_i) \pmod 2.$$

Using Propositions 2.3 and 2.4 we obtain that if $p \equiv 1 \pmod 4$ $\langle v_E, v_E\rangle$ is even and if $p \equiv 3 \pmod 4$, then $\langle v_E, v_E\rangle \equiv v_E(e_k) \pmod 2$, where k is the only index such that $w_k = 2$. In that case, since $L(E,1) = 0$ (by Proposition 2.1), Proposition 2.5 implies that

$$m_4 = \langle v_E, b_4\rangle = 0.$$

Since $b_4 = \frac{1}{2}e_k$, we get that

$$m_4 = v_E(e_k) = 0.$$

Therefore, $\langle v_E, v_E\rangle$ is even, leading to a contradiction. $\square$

Remark 2.6. Another proof along the same lines uses that if $L(E,1) = 0$, then

$$\sum_i {w_i}^2 v_E(e_i)^3 = 0.$$

This is proved in [4, Corollary 11.5], as a consequence of the Gross-Kudla formula of special values of triple product L-functions. The number $\sum_i {w_i}^2 v_E(e_i)^3$ clearly has the same parity as $\langle v_E, v_E\rangle$, leading to the desired contradiction.

3. The proof of Theorem 1.4

Proof of Theorem 1.4. For a given e_i, denote by $\bar{i} \in \{1, 2, \ldots, n\}$ the unique index such that $e_{\bar{i}}$ corresponds to the curve E_i^p. Then [3, Proposition 2.4] implies that $v(e_i) = v(e_{\bar{i}})$. By Proposition 2.4 we have that $j(E_k) \in \mathbb{F}_p$ whenever $w_k \neq 1$, and thus $v_E(e_k)$ is even. Hence Proposition 2.2 implies that

$$m_E \equiv \sum_i v_E(e_i)^2 \pmod 4.$$

If E_i is defined over $\mathbb{F}_p$ (i.e. $\bar{i} = i$), then by the assumption

$$v_E(e_i)^2 \equiv 0 \pmod 4.$$

Hence

$$m_E \equiv {\sum_i}' 2 v_E(e_i)^2 \pmod 4,$$

where we sum over the pairs $\{i, \bar{i}\}$ with $i \neq \bar{i}$. Using again Proposition 2.1 and the Gross-Kudla formula, we get that

$$\sum_i v_E(e_i)^3 \equiv {\sum_i}' 2 v_E(e_i) \equiv 0 \pmod 4,$$

where the second sum is over the pairs $\{i, \bar{i}\}$ for which $v_E(e_i)$ is odd. It follows that the number of such pairs is even, hence $m_E \equiv 0 \pmod 4$. $\square$

Acknowledgments

The authors would like to thank A. Dujella, I. Gusić, M. Mereb, F. Najman and the anonymous reviewer for their useful comments and suggestions.

References

[1] Frank Calegari and Matthew Emerton, *Elliptic curves of odd modular degree*, Israel J. Math. **169** (2009), 417–444, DOI 10.1007/s11856-009-0017-x. MR2460912

[2] Henri Darmon, *Rational points on modular elliptic curves*, CBMS Regional Conference Series in Mathematics, vol. 101, Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 2004. MR2020572

[3] Benedict H. Gross, *Heights and the special values of L-series*, Number theory (Montreal, Que., 1985), CMS Conf. Proc., vol. 7, Amer. Math. Soc., Providence, RI, 1987, pp. 115–187. MR894322

[4] Benedict H. Gross and Stephen S. Kudla, *Heights and the central critical values of triple product L-functions*, Compositio Math. **81** (1992), no. 2, 143–209. MR1145805

[5] Matija Kazalicki and Daniel Kohen, *Supersingular zeros of divisor polynomials of elliptic curves of prime conductor*, Res. Math. Sci. **4** (2017), Paper No. 10, 15, DOI 10.1186/s40687-017-0099-8. MR3647576

[6] J.-F. Mestre, *La méthode des graphes. Exemples et applications* (French), Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata, 1986), Nagoya Univ., Nagoya, 1986, pp. 217–242. MR891898

[7] William Stein and Mark Watkins, *Modular parametrizations of Neumann-Setzer elliptic curves*, Int. Math. Res. Not. **27** (2004), 1395–1405, DOI 10.1155/S1073792804133916. MR2052021

[8] Soroosh Yazdani, *Modular abelian varieties of odd modular degree*, Algebra Number Theory **5** (2011), no. 1, 37–62, DOI 10.2140/ant.2011.5.37. MR2833784

[9] Mark Watkins, *Computing the modular degree of an elliptic curve*, Experiment. Math. **11** (2002), no. 4, 487–502 (2003). MR1969641

Department of Mathematics, University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia

E-mail address: matija.kazalicki@math.hr

Departamento de Matemática, Universidad de Buenos Aires and IMAS-CONICET, Ciudad Universitaria, Buenos Aires Argentina

E-mail address: dkohen@dm.uba.ar