A CONJECTURE OF WATKINS FOR QUADRATIC TWISTS

JOSE A. ESPARZA-LOZANO AND HECTOR PASTEN

Abstract. Watkins conjectured that for an elliptic curve E over $\mathbb{Q}$ of Mordell-Weil rank r, the modular degree of E is divisible by 2^r. If E has non-trivial rational 2-torsion, we prove the conjecture for all the quadratic twists of E by squarefree integers with sufficiently many prime factors.

1. Ranks and modular degree

For an elliptic curve E over $\mathbb{Q}$ of conductor N, the modularity theorem [25, 22, 4] gives a non-constant morphism $\phi_E : X_0(N) \to E$ defined over $\mathbb{Q}$ where $X_0(N)$ is the modular curve associated to the congruence subgroup $\Gamma_0(N) \subseteq SL_2(\mathbb{Z})$. We assume that ϕ_E has minimal degree and that it maps the cusp $i\infty$ to the neutral point of E. These requirements uniquely determine ϕ_E up to sign. The *modular degree* of E is $m_E = \deg \phi_E$ and it has profound arithmetic relevance; for instance, polynomial bounds for its size in terms of N are essentially equivalent to the *abc* conjecture [11, 17].

The 2-adic valuation is denoted by v_2. Motivated by numerical data, Watkins [24] conjectured that $v_2(m_E)$ for an elliptic curve E is closely related to the Mordell-Weil rank of E over $\mathbb{Q}$.

Conjecture 1.1 (Watkins)**.** *For every elliptic curve E over $\mathbb{Q}$ we have* $\operatorname{rank} E(\mathbb{Q}) \leq v_2(m_E)$.

Dummigan [8] showed that part of the conjecture would follow from strong $R = \mathbb{T}$ conjectures. Also, large part of Watkins' conjecture is proved for elliptic curves of odd modular degree [5, 26, 12, 13], although it is not known whether there exist infinitely many elliptic curves of this kind [20].

The goal of this note is to prove Watkins' conjecture unconditionally in several new cases. Let us introduce some notation. For an elliptic curve E and a fundamental (quadratic) discriminant D, the quadratic twist of E by D is denoted by $E^{(D)}$. The Manin constant of E is denoted by c_E (cf. Section 2.3). The number of distinct prime factors of an integer n is $\omega(n)$.

Theorem 1.2. *Let E be an elliptic curve over $\mathbb{Q}$ of conductor N with non-trivial rational* 2*-torsion. Assume that E has minimal conductor among its quadratic twists. If D is a fundamental discriminant with $\omega(D) \geq 6 + 5\omega(N) - v_2(m_E/c_E^2)$, then Watkins' conjecture holds for $E^{(D)}$.*

The quantity $6 + 5\omega(N) - v_2(m_E/c_E^2)$ is effectively computable and it can be read from existing tables of elliptic curves when N is not too large, see for instance [14].

For a positive integer A, it is a standard result of analytic number theory that the number of positive integers n up to x having $\omega(n) \leq A$ is $O(x(\log\log x)^{A-1}/\log x)$. We deduce:

Corollary 1.3. *Let E be an elliptic curve over $\mathbb{Q}$ with non-trivial rational* 2*-torsion. There is an effective constant $\kappa(E)$ depending only on E such that the number of fundamental discriminants D with $|D| \leq x$ such that Watkins' conjecture fails for $E^{(D)}$ is bounded by $O\left(x(\log\log x)^{\kappa(E)}/\log x\right)$.*

Let us remark that in the cases where we prove Watkins' conjecture our argument actually shows that $v_2(m_{E^{(D)}})$ bounds the 2-Selmer rank, which is a stronger version of Watkins' conjecture.

Date: January 21, 2020.

2010 *Mathematics Subject Classification.* Primary 11G05; Secondary 11F11, 11G18.

Key words and phrases. Elliptic curve, rank, modularity.

J. E.-L. was supported by a Carroll L. Wilson Award and the MIT International Science and Technology Initiatives (MISTI). H. P. was supported by FONDECYT Regular grant 1190442.

2. Preliminaries

2.1. **Faltings height.** Let E be an elliptic curve over $\mathbb{Q}$. We denote by ω_E a global Neron differential for E; it is unique up to sign. The Faltings height of E (over $\mathbb{Q}$) is defined as certain Arakelov degree [10], which in our case takes the simpler form [18]

$$h(E) = -\frac{1}{2}\log\left(\frac{i}{2}\int_{E(\mathbb{C})}\omega_E\wedge\overline{\omega_E}\right). \tag{2.1}$$

Ramanujan's cusp form is $\Delta(z) = q\prod_{n=1}^{\infty}(1-q^n)^{24}$ where $q=\exp(2\pi iz)$, defined on the upper half plane $\mathfrak{h}=\{z\in\mathbb{C}:\Im(z)>0\}$. The modular j-function is normalized as $j(z)=q^{-1}+744+...$

The global minimal discriminant of E is denoted by Δ_E. If $\tau_E\in\mathfrak{h}$ satisfies that $j(\tau_E)$ is the j-invariant of E, then the Faltings height admits the expression [21, 18]

$$h(E) = \frac{1}{12}\left(\log|\Delta_E| - \log\left|\Delta(\tau_E)\Im(\tau_E)^6\right|\right) - \log(2\pi). \tag{2.2}$$

Given elliptic curves E_1, E_2 over $\mathbb{Q}$, let us define $\delta(E_1,E_2)=\exp(2h(E_1)-2h(E_2))$.

Lemma 2.1 (Variation of $h(E)$ under quadratic twist)**.** *Let E_1 be an elliptic curve over $\mathbb{Q}$ and let E_2 be a quadratic twist of E_1. Then $\delta(E_1,E_2)$ is a rational number and it satisfies $|v_2(\delta(E_1,E_2))|\le 3$.*

Proof. We use (2.2) for both E_1 and E_2. The elliptic curves are isomorphic over $\mathbb{C}$, so we can take $\tau_{E_1}=\tau_{E_2}$ which gives $\delta(E_1,E_2)=|\Delta_{E_1}/\Delta_{E_2}|^{1/6}$. The result follows from explicit formulas for the variation of the minimal discriminant under quadratic twists, cf. Proposition 2.4 in [23]. □

2.2. **Petersson norm.** For a positive integer N, let $S_2(N)$ be the space of weight 2 cuspidal holomorphic modular forms for the congruence subgroup $\Gamma_0(N)$ acting on $\mathfrak{h}$. Given $f\in S_2(N)$, its Fourier expansion is $f(z)=a_1(f)q+a_2(f)q^2+...$ where $q=\exp(2\pi iz)$ and the numbers $a_n(f)$ are the Fourier coefficients of f. The Petersson norm of f relative to $\Gamma_0(N)$ is defined by

$$\|f\|_N = \left(\int_{\Gamma_0(N)\backslash\mathfrak{h}}|f(z)|^2dx\wedge dy\right)^{1/2}, \quad z=x+iy\in\mathfrak{h}.$$

The norm depends on the choice of N in the following sense: If $N|M$ and $f\in S_2(N)$, then we certainly have $f\in S_2(M)$, and $\|f\|_M^2=[\Gamma_0(N):\Gamma_0(M)]\cdot\|f\|_N^2$.

We need some additional notation. For an elliptic curve E over $\mathbb{Q}$ of conductor N we denote by $f_E\in S_2(N)$ the Hecke newform attached to E by the modularity theorem, normalized by $a_1(f_E)=1$. The modular form f_E is characterized by the following property: If p is a prime of good reduction for E and we define $a_p(E)=p+1-\#E(\mathbb{F}_p)$, then $a_p(f_E)=a_p(E)$. For a fundamental discriminant D, let $\mathscr{P}(D,N)$ be the set of primes p with $p|D$ and $p\nmid 2N$.

Lemma 2.2 (Variation of the Petersson norm under quadratic twist)**.** *Let E be an elliptic curve over $\mathbb{Q}$ and let D be a fundamental discriminant. Let N and $N^{(D)}$ be the conductors of E and $E^{(D)}$ respectively, and assume that $N|N^{(D)}$. Then $\|f_{E^{(D)}}\|^2_{N^{(D)}}/\|f_E\|^2_N\in\mathbb{Q}^\times$ and we have*

$$v_2(\|f_{E^{(D)}}\|^2_{N^{(D)}}/\|f_E\|^2_N)+1\ge\sum_{p\in\mathscr{P}(D,N)}v_2\left((p-1)(p+1-a_p(E))(p+1+a_p(E))\right).$$

Proof. The quadratic Dirichlet character attached to D has conductor $|D|$. The result follows from the precise formula given in Theorem 1 of [7] when one only keeps the contribution of $p=2$ and the primes $p\in\mathscr{P}(D,N)$ —the product of the latter primes is denoted by D_1 in *loc. cit.* □

We remark that the terms $(p-1)(p+1-a_p(E))(p+1+a_p(E))$ have a clear conceptual origin; they come from Euler factors of the imprimitive symmetric square L-function $L(\mathrm{Sym}^2 f_E,s)$ that are removed by twisting, and $L(\mathrm{Sym}^2 f_E,2)$ is (up to a mild factor) equal to $\|f_E\|^2_N$. See [27, 7, 24].

2.3. **Manin constant.** Given an elliptic curve E over $\mathbb{Q}$ of conductor N, we have that $\phi_E^*\omega_E$ is a regular differential on $X_0(N) = \Gamma_0(N)\backslash\mathfrak{h} \cup \{\text{cusps}\}$. More precisely

$$\phi_E^*\omega_E = 2\pi i c_E f_E(z)dz \tag{2.3}$$

where c_E is a rational number uniquely defined up to sign. We assume that the signs of ϕ_E and ω_E are chosen such that $c_E > 0$. It follows from (2.1) and (2.3) that (cf. [21, 18])

$$m_E = 4\pi^2 c_E^2 \|f_E\|_N^2 \exp(2h(E)). \tag{2.4}$$

The quantity c_E is called the Manin constant, and a fundamental fact is

Lemma 2.3 (cf. [9])**.** *The Manin constant c_E is an integer.*

We recall that Manin [15] conjectured that if E is a strong Weil curve in the sense that m_E is minimal within the isogeny class of E, then $c_E = 1$. See [16, 3, 2, 6] and the references therein.

3. Consequences for Watkins' conjecture

Lemma 3.1. *Let E be an elliptic curve over $\mathbb{Q}$ of conductor N and suppose that E has minimal conductor among its quadratic twists. Let D be a fundamental discriminant. Then*

$$v_2(m_{E^{(D)}}) \geq v_2(m_E/c_E^2) - 4 + \sum_{p\in\mathscr{P}(D,N)} v_2\left((p-1)(p+1-a_p(E))(p+1+a_p(E))\right).$$

Proof. Applying (2.4) to E and $E^{(D)}$ we find

$$\frac{m_{E^{(D)}}}{m_E} = \frac{c_{E^{(D)}}^2}{c_E^2} \cdot \frac{\|f_{E^{(D)}}\|_{N^{(D)}}^2}{\|f_E\|_N^2} \cdot \delta(E^{(D)}, E).$$

The result follows from lemmas 2.1, 2.2, and 2.3. □

Proposition 3.2. *Let E be an elliptic curve over $\mathbb{Q}$ of conductor N with non-trivial rational 2-torsion and suppose that E has minimal conductor among its quadratic twists. Let D be a fundamental discriminant. We have $v_2(m_{E^{(D)}}) \geq 3\omega(D) + v_2(m_E/c_E^2) - (7 + 3\omega(N))$.*

Proof. As $E(\mathbb{Q})[2]$ is non-trivial and it maps injectively into $E(\mathbb{F}_p)$ for every prime $p \nmid 2N$, we have $p + 1 \equiv a_p(E) \bmod 2$ for these primes. We get $v_2(m_{E^{(D)}}) \geq v_2(m_E/c_E^2) - 4 + 3 \cdot \#\mathscr{P}(D, N)$ from Lemma 3.1, and the result follows from $\#\mathscr{P}(D, N) \geq \omega(D) - \omega(2N) \geq \omega(D) - \omega(N) - 1$. □

The following upper bound for the Mordell-Weil rank is standard and it comes from a bound for a 2-isogeny Selmer rank (cf. Section X.4 in [19]; see also [1]).

Lemma 3.3. *Let E be an elliptic curve over $\mathbb{Q}$ of conductor N with non-trivial rational 2-torsion. Then* $\operatorname{rank} E(\mathbb{Q}) \leq 2\omega(N) - 1$.

Proof of Theorem 1.2. Since $E^{(D)}[2] \simeq E[2]$ as Galois modules and E has non-trivial rational 2-torsion, we can use Lemma 3.3 for $E^{(D)}$, which gives

$$\operatorname{rank} E^{(D)}(\mathbb{Q}) \leq 2\omega(N^{(D)}) - 1 \leq 2(\omega(D) + \omega(N)) - 1.$$

If Watkins' conjecture fails for $E^{(D)}$, then Proposition 3.2 would give

$$2(\omega(D) + \omega(N)) - 1 \geq v_2(m_{E^{(D)}}) + 1 \geq 3\omega(D) + v_2(m_E/c_E^2) - 6 - 3\omega(N).$$

This is not possible when $\omega(D) \geq 6 + 5\omega(N) - v_2(m_E/c_E^2)$. □

4. Acknowledgments

The first author was supported by a Carroll L. Wilson Award and the MIT International Science and Technology Initiatives (MISTI) during an academic visit to Pontificia Universidad Católica de Chile. The second author was supported by FONDECYT Regular grant 1190442.

References

[1] J. Aguirre, A. Lozano-Robledo, J. Peral, *Elliptic curves of maximal rank.* Proceedings of the "Segundas Jornadas de Teoría de Números", 1-28, Bibl. Rev. Mat. Iberoamericana, Rev. Mat. Iberoamericana, Madrid, 2008.

[2] A. Agashe, K. Ribet, W. Stein, *The Manin constant.* Pure Appl. Math. Q. 2 (2006), no. 2, Special Issue: In honor of John H. Coates. Part 2, 617-636.

[3] A. Abbes, E. Ullmo, *À propos de la conjecture de Manin pour les courbes elliptiques modulaires.* Compositio Math. 103 (1996), no. 3, 269-286.

[4] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over Q: wild 3-adic exercises.* J. Amer. Math. Soc. 14 (2001), no. 4, 843-939.

[5] F. Calegari, M. Emerton, *Elliptic curves of odd modular degree.* Israel J. Math. 169 (2009), 417-444.

[6] K. Cesnavicius, *The Manin constant in the semistable case.* Compos. Math. 154 (2018), no. 9, 1889-1920.

[7] C. Delaunay, *Computing modular degrees using L-functions.* J. Théor. Nombres Bordeaux 15 (2003), no. 3, 673-682.

[8] N. Dummigan, *On a conjecture of Watkins.* J. Théor. Nombres Bordeaux 18 (2006), no. 2, 345-355.

[9] B. Edixhoven, *On the Manin constants of modular elliptic curves.* Arithmetic algebraic geometry (Texel, 1989), 25-39, Progr. Math., 89, Birkhäuser Boston, Boston, MA, 1991.

[10] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern.* Invent. Math. 73 (1983), no. 3, 349-366.

[11] G. Frey, *Links between solutions of A-B=C and elliptic curves.* Number theory (Ulm, 1987), 31-62, Lecture Notes in Math., 1380, Springer, New York, 1989.

[12] M. Kazalicki, D. Kohen, *On a special case of Watkins' conjecture.* Proc. Amer. Math. Soc. 146 (2018), no. 2, 541-545.

[13] M. Kazalicki, D. Kohen, *Corrigendum to "On a special case of Watkins' conjecture".* Proc. Amer. Math. Soc. 147 (2019), no. 10, 4563.

[14] The LMFDB Collaboration, *The L-functions and Modular Forms Database.* (2020) `www.lmfdb.org`

[15] J. Manin, *Cyclotomic fields and modular curves.* (Russian) Uspehi Mat. Nauk 26 (1971), no. 6(162), 7-71.

[16] B. Mazur, *Rational isogenies of prime degree* (with an appendix by D. Goldfeld). Invent. Math. 44 (1978), no. 2, 129-162.

[17] R. Murty, *Bounds for congruence primes.* Automorphic forms, automorphic representations, and arithmetic (Fort Worth, TX, 1996), 177-192, Proc. Sympos. Pure Math., 66, Part 1, Amer. Math. Soc., Providence, RI, 1999.

[18] J Silverman, *Heights and elliptic curves.* Arithmetic geometry (Storrs, Conn., 1984), 253-265, Springer, New York, 1986.

[19] J. Silverman, *The arithmetic of elliptic curves.* Second edition. Graduate Texts in Mathematics, 106. Springer, Dordrecht, 2009. xx+513 pp. ISBN: 978-0-387-09493-9.

[20] W. Stein, M. Watkins, *Modular parametrizations of Neumann-Setzer elliptic curves.* Int. Math. Res. Not. 2004, no. 27, 1395-1405.

[21] L. Szpiro, *Discriminant et conducteur des courbes elliptiques.* Séminaire sur les Pinceaux de Courbes Elliptiques (Paris, 1988). Astérisque No. 183 (1990), 7-18.

[22] R. Taylor, A. Wiles, *Ring-theoretic properties of certain Hecke algebras.* Ann. of Math. (2) 141 (1995), no. 3, 553-572.

[23] V. Pal, *Periods of quadratic twists of elliptic curves.* With an appendix by Amod Agashe. Proc. Amer. Math. Soc. 140 (2012), no. 5, 1513-1525.

[24] M. Watkins, *Computing the modular degree of an elliptic curve.* Experiment. Math. 11 (2002), no. 4, 487-502.

[25] A. Wiles, *Modular elliptic curves and Fermat's last theorem.* Ann. of Math. (2) 141 (1995), no. 3, 443-551.

[26] S. Yazdani, *Modular abelian varieties of odd modular degree.* Algebra Number Theory 5 (2011), no. 1, 37-62.

[27] D. Zagier, *Modular parametrizations of elliptic curves.* Canad. Math. Bull. 28 (1985), no. 3, 372-384.

African Institute for Mathematical Sciences
Rue KG590 ST, Kigali, Rwanda
Email address, J. Esparza-Lozano: `josealanesparza@gmail.com`

Pontificia Universidad Católica de Chile
Facultad de Matemáticas
4860 Av. Vicuña Mackenna, Macul, RM, Chile
Email address, H. Pasten: `hector.pasten@mat.uc.cl`