AN EXAMPLE OF AN ELLIPTIC CURVE WITH A POSITIVE DENSITY OF PRIME QUADRATIC TWISTS WHICH HAVE RANK ZERO

Kevin James

Abstract. If p is prime, then let E_p denote the elliptic curve over the rationals given by

$$E_p : y^2 = x^3 - 32p^3.$$

We prove that E_p has only the trivial point (at infinity) for at least $\frac{1}{3}$ of the primes p. In fact, we will show that for 1/3 of the primes p, $L(E_p, 1) \neq 0$.

1. INTRODUCTION

Given an elliptic curve $E : y^2 = x^3+Ax^2+Bx+C \quad (A, B, C \in \mathbb{Z})$ defined over $\mathbb{Q}$ and having minimal discriminant Δ_E, we define $a_p = p+1-\#E(\mathbb{F}_p)$. Then we associate to E its L-series:

$$L(E, s) = \prod_{p|\Delta_E} \frac{1}{1 - a_p p^{-s}} \prod_{p\nmid\Delta_E} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} = \sum_{n\geq 1} \frac{a_n}{n^s}. \tag{1}$$

This product converges for $Re(s) > 3/2$. In the case that E has complex multiplication, it is known that $L(E, s)$ has analytic continuation to the whole complex plane. The Coates-Wiles theorem [3] then tells us that if $L(E, 1) \neq 0$ then E has only a finite number of rational points.

Given an elliptic curve E as above and an integer D, we define the D^{th} quadratic twist of E to be the curve $E_D : y^2 = x^3 + ADx^2 + BD^2x + CD^3$. If we let $L(E_D, s)$ denote the L-function associated to E_D, then we have

$$\begin{aligned} L(E_D, s) &= \prod_{p|\Delta_{E_D}} \frac{1}{1 - \chi_D(p)a_p p^{-s}} \prod_{p\nmid\Delta_{E_D}} \frac{1}{1 - \chi_D(p)a_p p^{-s} + p^{1-2s}} \\ &= \sum_{n\geq 1} \chi_D(n)\frac{a_n}{n^s}. \end{aligned} \tag{1}$$

where $\chi_D(n)$ denotes the Kronecker symbol $(\frac{D}{n})$. We will sometimes refer to $L(E_D, s)$ as the D^{th} quadratic twist of $L(E, s)$. In this paper, we will be

interested in determining how often we have $L(E_D, 1) \neq 0$ as D varies over all square-free numbers.

There have been many papers which have investigated this question. For a historical account, particularly of the works of Lucas and Sylvester, see chapter XXI of [4]. In the more recent papers of Bump, Friedberg and Hoffstein [1, 2], Murty and Murty [8], Iwaniec [7], Friedberg and Hoffstein [6] and Ono [9], one can find general theorems on the vanishing and non-vanishing of the quadratic twists of the L-function associated to a given elliptic curve. These theorems ensure that an infinite number of the quadratic twists of such an L-function will have nonzero central critical value.

In the case of an elliptic curve E having rational 2-torsion, one can often say much more. For example in the papers of Frey [5] and Tunnell [17] it is proved for certain elliptic curves E having rational 2-torsion that $L(E_p, 1) \neq 0$ for a positive proportion of primes p.

In the general case, the situation was much less satisfactory until recently. In [10], Ono has shown several examples of elliptic curves E such that $L(E_p, 1) \neq 0$ for a set of primes p of density $1/3$. Ono also proves a Theorem which gives sufficient conditions under which the L-function associated to an elliptic curve will have this property. In order to understand the proof of this theorem however, one must have some understanding of the Galois representations attached to modular forms. Using this theory of Galois representations, Ono and Skinner (see [11] and [12]) have recently extended this theorem.

In this paper, we will show:

Theorem 1. *Let $E : y^2 = x^3 - 32p^3$. Then $L(E_p, 1) \neq 0$ for at least $\frac{1}{3}$ of the primes p.*

Although this theorem follows from the more general theorems of Ono and Skinner mentioned above, it is not included in the specific examples worked out in [10]. We would like to discuss a simpler proof of this result that does not explicitly involve the theory of Galois representations.

Using the Coates-Wiles theorem, we can then deduce the following:

Corollary 2. *The curve*

$$y^2 = x^3 - 32p^3$$

has only the trivial point (at infinity) for at least $\frac{1}{3}$ of the primes p.

2. RESULTS

Denote by E_D the elliptic curve

$$E_D : y^2 = x^3 + 4D^3$$

where D is any 6^{th} power free integer, and let

$$L(E_1, s) = \sum_{n \geq 1} \frac{a_n}{n^s}.$$

Now, we note that E_D has complex multiplication by $\mathbb{Z}[\omega]$, where ω is a cube root of unity. Thus,

$$f_D(z) = \sum_{n=1}^{\infty} a_n \chi_D(n) q^n \in S_2(N_D) \quad (q = e^{2\pi i z})$$

where N_D is the conductor of E_D. Also, f_D is an eigenform for all of the Hecke operators.

Let,

$$g(z) = \frac{1}{2}\left(\sum_{x,y,z \in \mathbb{Z}} q^{x^2+27y^2+6z^2} - \sum_{x,y,z \in \mathbb{Z}} q^{4x^2+2xy+7y^2+6z^2} \right) = \sum_{n=1}^{\infty} b_n q^n.$$

Then by theorems of Schoenberg [13] and Siegel [15], we have that $g(z) \in S_{\frac{3}{2}}(216, \chi_2)$. We can check computationally that $g(z)$ is an eigenform for all of the Hecke operators, and that g lifts through the Shimura correspondence [14] to f_1. Now we can apply a theorem of Waldspurger [18 Corollary 2] to gain information about the values $L(E_D, 1)$. In our case Waldspurger's theorem specializes to the following.

Theorem 2.1. *For $t \equiv 1$ modulo 6,*

$$L(E_{-2t}, 1) = \frac{b_t^2}{\sqrt{t}} \beta,$$

where $\beta \approx 1.363$ (the value of β was computed using the Apecs package with MAPLE).

Thus, $L(E_{-2t}, 1) = 0$ if and only if $b_t = 0$.

Now, by a theorem of Sturm [16] we know that if we have two cusp forms in $S_k(N, \chi)$ that are congruent modulo some prime q up to the first $\frac{k}{12} N \prod_{p|N}(1 + \frac{1}{p})$ coefficients, then the two forms are all congruent modulo q. Now, $f_1 \in S_2(108) \subseteq S_2(216)$, and $g(z)\theta(2z) \in S_2(216)$. Thus by Sturm's theorem, we can check computationally that $g(z)\theta(2z) \equiv f_1(z)$ modulo 2. Now, we notice that $\theta(2z) \equiv 1$ modulo 2. Hence $g(z) \equiv f_1(z)$ modulo 2.

Now, we note that if $x^3 + 4$ has no root modulo p for p, a prime then $a_p \equiv 1$ modulo 2. This is because $E_1(\mathbb{F}_p)$ has no point of order 2 in this case. This implies that $b_p \equiv 1$ modulo 2. In particular $b_p \neq 0$. Thus from Theorem 2.1, $L(E_{-2p}, 1) \neq 0$ for such primes. So, Theorem 1 follows from the following lemma.

Lemma 2.2. *x^3+4 has no root modulo p for $\frac{1}{3}$ of the primes p.*

Proof. Note that for $p \equiv 2$ modulo 3, cubing is an automorphism of $\mathbb{F}_p$. So, x^3+4 always has a root modulo p when $p \equiv 2$ modulo 3. Thus we restrict our attention to $p \equiv 1(3)$ from now on. Hence, we have $\left(\frac{-3}{p}\right) = 1$. Now, we note that $\left(\frac{p}{3}\right) = \left(\frac{-3}{p}\right) = 1$, which implies that p splits in $\mathbb{Z}[\omega]$.

We have

$$\begin{array}{ccc} \mathbb{Q}(\omega) & & \mathfrak{p}_1\mathfrak{p}_2 \\ | & & | \\ \mathbb{Q} & & p \equiv 1 \pmod 3 \end{array}$$

Now, x^3+4 is irreducible over $\mathbb{Z}[\omega]$ (ω is a cube root of unity). Also, x^3+4 has a root in $\mathbb{Z}[\omega]/\mathfrak{p}_i$ $(i=1,2)$ if and only if it has a root modulo p. (In fact $\mathbb{Z}[\omega]/\mathfrak{p}_i \cong \mathbb{F}_p$.) The splitting of x^3+4 modulo $\mathfrak{p}_i$ determines the splitting of $\mathfrak{p}_i$ in $\mathbb{Z}[\omega, 4^{\frac{1}{3}}]$. In particular, if x^3+4 has no root modulo p, then the $\mathfrak{p}_i$'s remain inert in $\mathcal{O}_{\mathbb{Q}(\omega,4^{\frac{1}{3}})}$. Thus p splits into exactly two primes in $\mathcal{O}_{\mathbb{Q}(\omega,4^{\frac{1}{3}})}$

$$\begin{array}{ccc} \mathbb{Q}(\omega, 4^{\frac{1}{3}}) & & \mathfrak{P}_1\mathfrak{P}_2 \\ | & & | \\ \mathbb{Q} & & p \equiv 1 \pmod 3 \end{array}$$

Now, $\mathbb{Q}(\omega, 4^{\frac{1}{3}})/\mathbb{Q}$ is a Galois extension with Galois group S_3. So, the residual degrees $f(\mathfrak{P}_1)$ and $f(\mathfrak{P}_2)$ are the same, and the ramification indices of $\mathfrak{P}_1$ and $\mathfrak{P}_2$ are the same namely 1. Thus $f(\mathfrak{P}_1) = f(\mathfrak{P}_2) = 3$. This tells us that the order of the Frobenius $\sigma_{\mathfrak{P}_i}$ is 3. So, the size of the conjugacy class of $\sigma_{\mathfrak{P}_i}$ on S_3 is 2. The Lemma now follows from the Chebetorev Density Theorem.

Since f is an eigenform for all of the Hecke operators, it follows that the a_n's are multiplicative, that is if $\gcd m, n = 1$ then $a_{mn} = a_n a_n$. Thus we can deduce the following corollary form Theorem 1:

Corollary 2.3. *If D is a square free natural number with only prime factors $p \equiv 1$ modulo 3 such that x^3+4 has no root modulo p, $L(E_D, 1) \neq 0$.*

ACKNOWLEDGEMENTS

The author would like to thank Alice Silverberg for her helpful comments during the preparation of this manuscript.

References

1. D. Bump, S. Friedberg, and J. Hoffstein, *Eisenstein series on the metaplectic group and nonvanishing theorems for automorphic L-functions and their derivatives*, Ann. of Math. **131** (1990), 53–127.
2. D. Bump, S. Friedberg, and J. Hoffstein, *Nonvanishing theorems for L-functions of modular forms and their derivatives*, Inventiones Math. **102** (1990), 543–618.
3. J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. **39** (1977), no. 3, 223–251.
4. L. E. Dickson, *Theory of Numbers*, vol. 2, Chelsea Publishing Co., 1966.
5. G. Frey, *Der Rang der Lsungen von* $Y^2 = X^3 \pm p^3$ *uber* $\mathbb{Q}$., Manuscripta Math. **48** (1984), no. 1–3, 71–101.
6. S. Friedberg and J. Hoffstein, *Nonvanishing theorems for automorphic L-functions on* $GL(2)$, Ann. of Math. **142** (1995), no. 2, 385–423.
7. H. Iwaniec, *On the order of vanishing of modular L-series at the critical point*, Sém. de Théor. Nombres, Bordeaux **2** (1990), no. 2, 365–376.
8. M.R. Murty and V.K. Murty, *Mean values of derivatives of modular L-series*, Ann. of Math. **133** (1991), 447–475.
9. K. Ono, *Rank zero quadratic twists of modular elliptic curves*, Compositio Math. **104** (1996), 293-304.
10. K. Ono, *Twists of elliptic curves*, Compositio Math. **106** (1997), 349-360.
11. K. Ono and C. Skinner, *Fourier coefficients of half-integral weight modular forms modulo* ℓ, Annals of Math. (to appear).
12. K. Ono and C. Skinner, *Non-vanishing of quadratic twists of modular L-functions*, Inventiones Math. (to appear).
13. B. Schoeneberg, *Das Verhalten von mehrfachen Thetareihen bei Modulsubstitutionen*, Math. Ann. **116**.
14. G. Shimura, *On modular forms of half integral weight*, Ann. of Math. (2) **97** (1973), 440–481.
15. C. Siegel, *Gesammelte Abhandlungen Bd. 3*, Springer Verlag, 1966, pp. 326–405.
16. J. Sturm, *On the congruence of modular forms*, Springer Lect. Notes **1240** (1984), Springer-Verlag, 275–280.
17. J. Tunnell, *A classical Diophantine problem and modular forms of weight* 3/2, Invent. Math. **72** (1983), no. 2, 323–334.
18. J.L. Waldspurger, *Sur les coefficients de Fourier des formes modulaires de poids demi-entier*, J. Math. Pures. et Appl. **60** (1981), 375–484.

Department of Mathematics, Penn State University, University Park, Pennsylvania 16802

E-mail address: klj@math.psu.edu