August 14, 1998

ELLIPTIC CURVES SATISFYING THE BIRCH AND SWINNERTON-DYER CONJECTURE MOD 3

Kevin James

Department of Mathematics
Pennsylvania State University
218 McAllister Building
University Park, Pennsylvania 16802-6401
Phone: 814-865-7527
Fax: 814-865-3735
klj@math.psu.edu

Abstract. In this paper, we give examples of elliptic curves for which a positive proportion of the quadratic twists satisfy a weak form of the Birch and Swinnerton-Dyer conjecture modulo 3.

1. INTRODUCTION

We will consider the following weak form of the Birch and Swinnerton-Dyer conjecture.

Conjecture 1.1. *Let E be a rank zero elliptic curve over $\mathbb{Q}$. Then*

$$\frac{L(E,1)}{\Omega_E}\#E(\mathbb{Q})^2_{\text{tor}} \equiv \#Ш(E/\mathbb{Q})\prod_p c_p(E/\mathbb{Q}) \pmod 3, \tag{1}$$

where $L(E,s)$, Ω_E, $Ш(E/\mathbb{Q})$ and $c_p(E/\mathbb{Q})$ denote the L-series, real period, Tate-Shafarevic group and local Tamagawa factors of E respectively.

Combining a theorem of Frey (see [2]) with the results of [3] (see Proposition 2.2 in the next section), we are able to prove:

Theorem 1.2. *Let $E : y^2 = x^3 + x^2 + 72x - 368$. Then there is a set $S \subset \mathbb{N}$ having lower density at least 7/128 in the square-free natural numbers such that for all $d \in S$*

$$\text{ord}_3\left(\frac{L(E_{-d},1)}{\Omega_{E_{-d}}}\right) = 0 \quad \Longleftrightarrow \quad \text{ord}_3\left(\frac{\#Ш(E_{-d}/\mathbb{Q})\prod_p c_p(E_{-d}/\mathbb{Q})}{\#E_{-d}(\mathbb{Q})^2_{\text{tor}}}\right) = 0. \tag{2}$$

Similarly, one can prove for the three other elliptic curves E in the table below of conductor N_E that there exists a subset S_E of the square-free natural numbers having lower density at least δ_E such that for all $d \in S$, (2) holds.

E	N_E	δ_E
$y^2 = x^3 + 1$	36	1/8
$y^2 = x^3 + 4x^2 - 144x - 944$	19	19/640
$y^2 = x^3 + x^2 - 72x - 496$	26	13/224

2. RESULTS

For the sake of completeness we recall the following notation along with the next proposition which was proved in [3]. Suppose that Q is a positive definite ternary quadratic form. Then we will denote by d_Q^{sf} the square-free part of the discriminant of Q and by A_Q the number of automorphs of Q. We will let θ_Q denote the weight 3/2 modular form whose q-expansion is given by $\theta_Q(\tau) = \sum_{x,y,z\in\mathbb{Z}} q^{Q(x,y,z)}$ $(q = e^{2\pi i\tau})$(see [8]). Also, if $f \in S_{3/2}(N, \chi_t)$ is a Hecke-eigenform which lifts through the Shimura correspondence to a cusp form $F \in S_2(N/2)$, then we will let $S(f)$ denote the unique normalized weight 2 newform of trivial character having $\lambda_p(F) = \lambda_p(S(f))$ for all but finitely many of the primes p. If G is any modular form we will let N_G denote the level of G and if N is an integer we will define:

$$\begin{aligned} R(G,N) &= \{a \in (\mathbb{Z}/4N\mathbb{Z})^* : \text{there is a square-free } n \equiv a \pmod{4N} \text{ with } 3 \nmid a_n(G)\}, \\ \delta(G,N) &= \frac{\#R(G,N)}{8N\prod_{p|N}(1-\frac{1}{p^2})}. \end{aligned} \tag{3}$$

Then the statement of Proposition 3.1 of [3] becomes:

Proposition 2.2. *Suppose that Q_1 and Q_2 are the only even-integral primitive positive definite ternary quadratic forms in a genus of forms. Assume that $3 \nmid A_{Q_1}A_{Q_2}$ but $3 \mid A_{Q_1} + A_{Q_2}$. Suppose also that $f = (\theta_{Q_1} - \theta_{Q_2}) \in S_{3/2}(N, \chi_t)$ is a Hecke-eigenform which lifts through the Shimura correspondence to a cusp form. Then, the set of square-free natural numbers n such that $L(S(f)\cdot\chi_{-tn}, 1) \neq 0$ has lower density at least $\delta(f, d_{Q_1}^{\text{sf}})$ in the square-free natural numbers.*

Before stating the main results, we need the following definition and notation.

Definition 2.1. *Let E be an elliptic curve over $\mathbb{Q}$ and let v be an odd prime not dividing N_E. If $\text{ord}_v(j_E) < 0$, then we define $\gamma_v(E) = \left(\frac{-c_4c_6^{-1}}{v}\right)$, where c_4 and c_6 denote the usual Weierstrass coefficients for E and c_6^{-1} denotes the inverse of c_6 modulo v.*

Suppose that E is a modular elliptic curve over $\mathbb{Q}$. Then we will denote by F_E the weight 2 newform with the property that $L(E,s) = L(F_E,s)$. For any modular form f and any integer N, we will let $\mathfrak{R}(E,f,N)$ denote the set of all $a \in (\mathbb{Z}/24N\mathbb{Z})^*$ satisfying the following rather technical conditions. We must impose condition 1 in order to use Corollary 2 of [10]. Conditions 2 and 3 are rather mild and can be easily checked using Tate's algorithm. Conditions 4-6 are necessary to ensure that we may use Frey's results [2].

1. There exists a square-free natural number $n \equiv a$ modulo $24N$ such that $\text{ord}_3(a_n(f)) = \text{ord}_3\left(\frac{L(E_{-n})}{\Omega_{E_{-n}}}\right) = 0$.
2. For all square-free natural numbers $d \equiv a$ modulo $24N$, $3 \nmid \prod_p c_p(E_{-d}/\mathbb{Q})$
3. There exists an integer m_a depending only on a and E such that for all square-free natural numbers $d \equiv a$ modulo $24N$, $\Omega_{E_{-d}}\sqrt{d}/\Omega_{E_{-1}} = m_a$.

4. If $2 \mid N_E$ then $a \equiv 1$ modulo 4.
5. If $\ell \neq 2, 3$ is prime and $\ell \mid N_E$, then

$$\left(\frac{-a}{\ell}\right) = \begin{cases} -1, & \text{if } \mathrm{ord}_\ell(j_E) \geq 0 \\ -1, & \text{if } \mathrm{ord}_\ell(j_E) < 0 \text{ and } \gamma_\ell(E) = 1 \\ 1, & \text{otherwise.} \end{cases} \tag{4}$$

6. If $\mathrm{ord}_3(j_E) < 0$ then $a \equiv 1$ modulo 3.

Finally, for $M, N \in \mathbb{Z}$ put

$$W(M,N) = \mathrm{lcm}\left[\prod_{\substack{p \mid M \\ p \neq 2,3}} p, \prod_{\substack{p \mid N \\ p \neq 2,3}} p\right]. \tag{5}$$

Now, we are ready to state our main result.

Proposition 2.3. *Suppose that $f \in S_{3/2}(N)$ is as in Proposition 2.2. Let $E/\mathbb{Q}$ be the elliptic curve with $F_E = S(f)$. Suppose that E has a rational point P of order 3. Assume that either E is given by $y^2 = x^3 + 1$ or that P is not in the kernel of the reduction modulo 3 map. Further, suppose that for all odd primes $v \mid N_E$ with $v \equiv 2$ modulo 3, we have that $3 \mid \mathrm{ord}_3(\Delta_E)$. Put*

$$\delta = \frac{\#\mathfrak{R}(E, f, W(N_f, N_{S(f)}))}{32W(N_f, N_{S(f)}) \prod_{p \mid W(N_f, N_{S(f)})}(1 - \frac{1}{p^2})} \tag{6}$$

Then there exists a subset S of the square-free natural numbers having lower density at least δ such that for all $d \in S$ we have

$$\mathrm{ord}_3\left(\frac{L(E_d, 1)}{\Omega_{E_d}}\right) = 0 \quad \Longleftrightarrow \quad \mathrm{ord}_3\left(\frac{\#Ш(E_d/\mathbb{Q}) \prod_p c_p(E_d/\mathbb{Q})}{\#E_d(\mathbb{Q})^2_{\mathrm{tor}}}\right) = 0. \tag{7}$$

Proof of Proposition 2.3. Suppose that $a \in \mathfrak{R}(E, f, W(N_f, N_{S(f)}))$. Then, by condition 1, there exists $n \equiv a$ modulo $24W(N_f, N_{S(f)})$ such that $3 \nmid a_n(f)$, and hence $a_n(f) \neq 0$. By the main theorem of [10], we know that $L(S(f) \cdot \chi_{-n}, 1) \neq 0$. Thus, putting

$$\beta_a = \frac{L(S(f) \cdot \chi_{-n}, 1)\sqrt{n}}{a_n(f)^2}, \tag{8}$$

Corollary 2 in [10] gives us for all square-free $d \equiv a$ modulo $24W(N_f, N_{S(f)})$,

$$L(S(f) \cdot \chi_{-d}, 1) = \frac{a_d(f)^2}{\sqrt{d}} \beta_a. \tag{9}$$

Dividing through (9) by $\Omega_{E_{-1}}$ and using condition 3 above we have for all square-free natural numbers $d \equiv a$ modulo $24W(N_f, N_{S(f)})$:

$$\frac{L(E_{-d},1)}{\Omega_{E_{-d}}} = a_d(f)^2 \alpha_a, \tag{10}$$

where

$$\alpha_a = \frac{L(E_{-n},1)}{\Omega_{E_{-n}} a_n(f)^2}. \tag{11}$$

We note that $\alpha_a \in \mathbb{Q}$ and, from condition 1, we have that $\mathrm{ord}_3(\alpha_a) = 0$. Thus, $\mathrm{ord}_3(L(E_{-d},1)/\Omega_{E_{-d}}) = 0$ if and only if $\mathrm{ord}_3(a_d(f)) = 0$.

Arguing as in the proof of Proposition 2.2 (see [3]), we can show that for all square-free $d \equiv a$ modulo $24W(N_f, N_{S(f)})$, $3 \mid a_d(f)$ if and only if $3 \mid h(\Delta_{-d})$, where Δ_{-d} denotes the discriminant of $\mathbb{Q}(\sqrt{-d})$ and $h(\Delta_{-d})$ denotes the class number of this field. Thus, for all square-free natural numbers $d \equiv a$ modulo $24W(N_f, N_{S(f)})$,

$$\mathrm{ord}_3\left(\frac{L(E_{-d}}{\Omega_{E_{-d}}}\right) = 0 \quad \Longleftrightarrow \quad \mathrm{ord}_3\left(h(\Delta_{-d})\right) = 0. \tag{12}$$

Let S be the set of all square-free natural numbers d such that $d \equiv a$ modulo $24W(N_f, N_{S(f)})$ for some $a \in \mathfrak{R}(E, f, W(N_f, N_{S(f)}))$ and such that $a_d(f) \neq 0$. We note that by the Davenport-Heilbronn theorem (see [4]), we know that for any $a \in \mathfrak{R}(E, f, W(N_f, N_{S(f)}))$, at least half of the square free natural numbers $d \equiv a$ modulo $24W(N_f, N_{S(f)})$ have the property that $3 \nmid h(\Delta_{-d})$. For such d it follows that $3 \nmid a_d(f)$. Thus for each $a \in \mathfrak{R}(E, f, W(N_f, N_{S(f)}))$ at least half of the square-free natural numbers $d \equiv a$ modulo $24W(N_f, N_{S(f)})$ are in S. So, an argument analogous to the one given in the proof of Proposition 2.2 (see [3] in particular the proof Proposition 3.1) will yield that S has lower density at least δ in the set of all square-free natural numbers. We note also that only a finite number of the quadratic twists of E have 3-torsion. Thus, we can remove from S any d for which $E_{-d}(\mathbb{Q})$ has points or order 3 without affecting the lower density of S. Hence, we will assume for the remainder of the proof that S contains no such d.

Now, we note that for any $d \in S$, we have that $a_d(f) \neq 0$ and therefore by (9) it follows that $L(E_{-d}, 1) \neq 0$. Thus, by the work of Kolyvagin, we know that E_{-d} has rank 0. Therefore, for all $d \in S$ we have that E_{-d} has rank 0 and that $3 \nmid E_{-d}(\mathbb{Q})_{\mathrm{tor}}$. Hence, it follows from our construction of S that $Ш(E_{-d}/\mathbb{Q})_3 \cong S(E_{-d}/\mathbb{Q})$ for all $d \in S$. Now, it follows from Frey's theorem [2] that for all $d \in S$,

$$h(\Delta_{-d})_3 \quad | \quad \#Ш(E_{-d}/\mathbb{Q})_3 \quad | \quad (h(\Delta_{-d})_3)^2, \tag{13}$$

Thus for all $d \in S$ we have

$$3 \mid Ш(E_{-d}/\mathbb{Q}) \quad \Longleftrightarrow \quad 3 \mid h(\Delta_{-d}). \tag{14}$$

Now, the proposition follows from (12), (14), condition 2 and our assumption that for all $d \in S$, $3 \nmid E_{-d}(\mathbb{Q})_{\text{tor}}$.

Example 2.1 Let $E : y^2 = x^3 + x^2 + 72x - 368$ be the modular curve of conductor 14. Let

$$f = \sum_{x,y,z \in \mathbb{Z}} q^{x^2+7y^2+7z^2} - \sum_{x,y,z \in \mathbb{Z}} q^{2x^2+4y^2+7z^2-2xy}.$$

In [3, Example 3.1] it was shown that f and satisfies the hypotheses of Proposition 2.2 and that $S(f) = F_E$. Also, $P = (2, 2) \in E(\mathbb{Q})$ has order 3 and is not in the kernel of the reduction modulo 3 map. Further, we note that the only odd prime dividing N_E is 7 which is 1 modulo 3. Thus, E satisfies the hypotheses of Proposition 2.3.

In this case, we have $W(N_f, N_{S(f)}) = 7$ (and therefore $24W(N_f, N_{S(f)}) = 168$). We will let $R_0 \subset (\mathbb{Z}/168\mathbb{Z})^*$ be the set $R_0 = \{1, 25, 29, 37, 53, 65, 85, 109, 113, 121, 137, 149\}$ Next, we will check that $R_0 \subset \mathfrak{R}(E, f, 7)$.

By calculating the first 500 coefficients of f and using the APECS package with MAPLE to calculate $L(E_{-n}, 1)/\Omega_{E_{-n}}$, we were able to verify condition 1 for each $a \in R_0$. We can use Tate's Algorithm to calculate that for $d \equiv 1$ modulo 4, $c_2(E_{-d}/\mathbb{Q})$ is either 2 or 4. Similarly, we can check that for $d \equiv 1$, 2, or 4 modulo 7, $c_7(E_{-d}/\mathbb{Q}) = 1$. For any other prime p not dividing d, we have $c_p = 1$. For primes $p \mid d$ ($p \neq 2, 7$), Tate's Algorithm yields that $c_p(E_{-d}/\mathbb{Q})$ is 1, 2 or 4. Thus, all of the $a \in R_0$ satisfy condition 2 of the definition of $\mathfrak{R}(E, f, 7)$. Also, using Tate's Algorithm, we can verify that for all square-free natural numbers $d \equiv 1$ modulo 4 with $(d, 42) = 1$, we have $\Omega_{E_{-d}}\sqrt{d}/\Omega_{E_{-1}} = 1$. Thus, condition 3 is satisfied by each $a \in R_0$. Since for all $a \in R_0$, we have $a \equiv 1$ modulo 4, condition 4 is satisfied. Now, we note that $\text{ord}_7(j_E) = -3$ and that $\gamma_7(E) = 1$. Since for all $a \in R_0$, $a \equiv 1$, 2 or 4 modulo 7 we have that $\left(\frac{-a}{7}\right) = -1$, and therefore condition 5 is also satisfied. Since, $\text{ord}_3(j_E) = 0$, condition 6 is vacuous. Thus we have that $\mathfrak{R}(E, f, 7) \supset R_0$ and we calculate $\delta \geq 7/128$. The main result (Theorem 1.2) now follows from Proposition 2.3.

The proofs of the results listed in the table following the statement of Theorem 1.2 are straight forward. One simply applies Proposition 2.3. The computations needed to verify all of the conditions of this proposition are almost exactly the same as the ones outlined above and we will omit them for the sake of brevity.

References

1. H. Davenport and H. Heilbronn, *On the density of discriminant s of cubic fields II*, Proc. Roy. Soc. London ser. A **322** (1971), 405–420.
2. G. Frey, *On the Selmer group of twists of elliptic curves with $\mathbb{Q}$-rational torsion points*, Canad. J. Math. **40** (1988), 649–665.
3. K. James, *L-series with nonzero central critical value*, Journal of the American Mathematical Society **11** (1998), 635–641.
4. J. Nakagawa and K. Horie, *Elliptic curves with no torsion points*, Proc. A.M.S. **104** (1988), 20–25.
5. J. Nekovář, *Class numbers of quadratic fields and Shimura's correspondence*, Math. Ann. **287** (1990), 577–594.
6. K. Ono, *A note on a question of J. Nekovář and the Birch and Swinnerton-Dyer conjecture*, Proc. Amer. Math. Soc. (to appear).

7. B. Schoeneberg, *Das Verhalten von mehrfachen Thetareihen bei Modulsubstitutionen*, Math. Ann. **116**.
8. G. Shimura, *On modular forms of half integral weight*, Ann. of Math. (2) **97** (1973), 440–481.
9. C. Siegel, *Gesammelte Abhandlungen Bd. 3*, Springer Verlag, 1966, pp. 326–405.
10. J.L. Waldspurger, *Sur les coefficients de Fourier des formes modulaires de poids demi-entier*, J. Math. Pures. et Appl. **60** (1981), 375–484.