

**A NOTE ON A QUESTION OF J. NEKOVÁŘ  
 AND THE BIRCH AND SWINNERTON-DYER CONJECTURE**

KEN ONO

(Communicated by David E. Rohrlich)

ABSTRACT. If  $D$  is a square-free integer, then let  $E(D)$  denote the elliptic curve over  $\mathbb{Q}$  given by the equation

$$(1) \quad E(D) : \quad Dy^2 = 4x^3 - 27.$$

Let  $L(E(D), s)$  denote the Hasse-Weil  $L$ -function of  $E(D)$ , and let  $L^*(E(D), 1)$  denote the ‘algebraic part’ of the central critical value  $L(E(D), 1)$ . Using a theorem of Sturm, we verify a congruence conjectured by J. Nekovář. By his work, if  $S(3, E(D))$  denotes the 3-Selmer group of  $E(D)$  and  $D \neq 1$  is a square-free integer with  $|D| \equiv 1 \pmod{3}$ , then we find that

$$L^*(E(D), 1) \not\equiv 0 \pmod{3} \iff S(3, E(D)) = 0.$$

If  $D \neq 1$  is a square-free integer, then  $E(D)$  is the  $D$ -quadratic twist of the Fermat cubic  $x^3 + y^3 = 1$ . J. Nekovář explicitly computed the 3-Selmer ranks of these elliptic curves, and verified the ‘mod 3’ part of the Birch and Swinnerton-Dyer Conjecture for most of these curves when  $|D| \equiv 1 \pmod{3}$  using Waldspurger’s theorem on the Shimura correspondence.

If  $q := e^{2\pi iz}$ , and  $\eta(z)$  and  $\Theta(z)$  denote the usual weight  $1/2$  modular forms

$$\eta(z) := q^{1/24} \prod_{n=1}^{\infty} (1 - q^n) \quad \text{and} \quad \Theta(z) := 1 + 2 \sum_{n=1}^{\infty} q^{n^2},$$

then define  $a(n)$  by  $\sum_{n=1}^{\infty} a(n)q^n := \eta^2(3z)\eta^2(9z) \in S_2(\Gamma_0(27))$ . The Hasse-Weil  $L$ -function  $L(E(D), s)$  is given by

$$(2) \quad L(E(D), s) := \sum_{n=1}^{\infty} \frac{a(n) \left(\frac{D}{n}\right)}{n^s}.$$

Also let  $L^*(E(D), 1)$  denote the ‘algebraic part’ of the critical value  $L(E(D), 1)$ . In particular, it is given by

$$(3) \quad L^*(E(D), 1) := \frac{L(E(D), 1)}{\Omega(E(D)) \prod_p c_p},$$

where  $\Omega(E(D))$  is the real period of  $E(D)$ , and  $\prod_p c_p$  is the ‘Tamagawa factor.’ In particular if  $p$  is an odd prime and  $S(p, E(D))$  denotes the  $p$ -Selmer group of  $E(D)$ ,

Received by the editors March 13, 1997.

1991 *Mathematics Subject Classification*. Primary 11G40; Secondary 14G10.

*Key words and phrases*. Elliptic curves, modular forms.

The author is supported by National Science Foundation grants DMS-9304580 and DMS-9508976, and NSA grant MSPR-YO12.

then the Birch and Swinnerton-Dyer Conjecture predicts that

$$(4) \quad L^*(E(D), 1) \not\equiv 0 \pmod{p} \Rightarrow S(p, E(D)) = 0.$$

Since the  $E(D)$  are curves with complex multiplication by  $\mathbb{Q}(\sqrt{-3})$ , a theorem of Rubin [R] implies that

$$L^*(E(D), 1) \not\equiv 0 \pmod{p} \Rightarrow S(p, E(D)) = 0$$

for primes  $p \geq 5$ .

If  $D$  is square-free and  $|D| \equiv 2 \pmod{3}$ , then  $L(E(D), 1) = L^*(E(D), 1) = 0$ , and so we restrict our attention to those square-free  $D$  where  $|D| \equiv 1 \pmod{3}$ . J. Nekovář computed the 3-Selmer ranks of  $E(D)$  and verified (4) when  $p = 3$  [N, Cor. 7.5] for all such  $D$  except when

$$(5) \quad 0 > D \equiv 5 \pmod{8} \quad \text{and} \quad 1 < D \equiv 1 \pmod{8}.$$

He explicitly computed 3-Selmer ranks using ideal class groups of suitable quadratic fields, and employed elementary congruences between certain Fourier coefficients of weight  $3/2$  cusp forms and class numbers.

To prove (4) when  $p = 3$  for the remaining cases (5), Nekovář noted that it suffices to prove:

**Conjecture** ([N, (7.1)]). Define  $a_1(n)$  and  $a_2(n)$  by

$$\begin{aligned} \sum_{n=1}^{\infty} a_1(n)q^n &:= \eta(6z)\eta(18z)\Theta(3z), \\ \sum_{n=1}^{\infty} a_2(n)q^n &:= \eta(6z)\eta(18z)\Theta(9z). \end{aligned}$$

If  $h(-n)$  denotes the class number of the quadratic field  $\mathbb{Q}(\sqrt{-n})$ , then

- (i)  $\frac{a_1(D)}{3} \equiv -h(-D) \pmod{3}$  if  $D \equiv 19 \pmod{24}$  is square-free,
- (ii)  $\frac{a_2(D)}{3} \equiv -h(-3D) \pmod{3}$  if  $1 < D \equiv 1 \pmod{24}$  is square-free.

**Theorem.** Conjecture (7.1) is true.

**Corollary.** If  $D \neq 1$  is a square-free integer for which  $|D| \equiv 1 \pmod{3}$ , then

$$L^*(E(D), 1) \not\equiv 0 \pmod{3} \iff S(3, E(D)) = 0.$$

*Proof of Corollary.* This follows immediately from Theorem 4.6, Proposition 7.1, and Proposition 7.2 in [N]. □

*Proof of Theorem.* Throughout,  $k$  denotes a non-negative integer. We begin with a well known fact. If  $g(z) := \sum_{n=1}^{\infty} c(n)q^n \in M_{k+\frac{1}{2}}(\Gamma_1(N))$ , then

$$(6) \quad g_{r,t}(z) := \sum_{n \equiv r \pmod{t}} c(n)q^n \in M_{k+\frac{1}{2}}\left(\Gamma_1\left(\frac{Nt^2}{\gcd(r,t)}\right)\right).$$

We recall a special case of a theorem of Sturm [S]. Suppose that  $h(z) := \sum_{n=0}^{\infty} d(n)q^n \in M_k(\Gamma_1(M))$  has integer Fourier coefficients. Sturm proved that

$$(7) \quad h(z) \equiv 0 \pmod{S} \iff \text{Ord}_S(h(z)) > \frac{k}{12}M^2 \prod_{p|M} \left(1 - \frac{1}{p^2}\right),$$

where

$$\text{Ord}_S(h(z)) := \min_n(d(n)) \not\equiv 0 \pmod{S}.$$

If  $i(z) := \sum_{n=0}^\infty e(n)q^n \in M_{k+\frac{1}{2}}(\Gamma_1(M))$  has integer coefficients, then by applying (7) to  $i(z)\Theta(z)$  we find that

$$(8) \quad i(z) \equiv 0 \pmod{S} \iff \text{Ord}_S(i(z)) > \frac{k+1}{12}M^2 \prod_{p|M} \left(1 - \frac{1}{p^2}\right).$$

Case (i). The form  $\sum_{n=1}^\infty a_1(n)q^n$  is in  $S_{\frac{3}{2}}(\Gamma_0(108), \chi_0)$ , where  $\chi_0$  is the trivial character, and has the property that  $a_1(n) = 0$  if  $n \not\equiv 1 \pmod{3}$ . Therefore by (6) we find that

$$\begin{aligned} f_1(z) &:= \sum_{n \equiv 3 \pmod{8}} a_1(n)q^n \\ &= \sum_{n \equiv 19 \pmod{24}} a_1(n)q^n = -3q^{19} + 6q^{43} - \dots \in S_{\frac{3}{2}}(\Gamma_1(108 \cdot 8^2)). \end{aligned}$$

Similarly if  $\Theta^3(z) := \sum_{n=0}^\infty r_1(n)q^n \in M_{\frac{3}{2}}(4)$ , then by (6)

$$\begin{aligned} t_1(z) &:= \sum_{n \equiv 19 \pmod{24}} r_1(n)q^n \\ &= 24q^{19} + 24q^{43} + 24q^{67} + 48q^{91} + \dots \in M_{\frac{3}{2}}(4 \cdot 24^2). \end{aligned}$$

It is easy to verify that  $f_1(z) \equiv 0 \pmod{3}$  and  $t_1(z) \equiv 0 \pmod{24}$ , and with these observations define  $i_1(z)$  by

$$i_1(z) := \frac{f_1(z)}{3} + \frac{t_1(z)}{24} = 3q^{43} + 3q^{91} + 6q^{139} + \dots \in M_{\frac{3}{2}}(\Gamma_1(6912)).$$

A computation verified the congruence  $i_1(z) \equiv 0 \pmod{3}$  for the first 5,400,000 terms, and so by (8)

$$\frac{a_1(n)}{3} \equiv -\frac{r_1(n)}{24} \pmod{3}$$

for every integer  $n \equiv 19 \pmod{24}$ . Conjecture 7.1 (i) follows immediately by Gauss' theorem that if  $n \equiv 19 \pmod{24}$  is square-free, then  $r_1(n) = 24h(-n)$  (see [J]).

Case (ii). The form  $\sum_{n=1}^\infty a_2(n)q^n \in S_{\frac{3}{2}}(\Gamma_0(108), \chi_{-3})$  has the property that  $a_2(n) = 0$  if  $n \not\equiv 1 \pmod{3}$ . Therefore by (6) it turns out that

$$\begin{aligned} f_2(z) &:= \sum_{n \equiv 1 \pmod{8}} a_2(n)q^n \\ &= \sum_{n \equiv 1 \pmod{24}} a_2(n)q^n = q + q^{25} - 2q^{49} - \dots \in S_{\frac{3}{2}}(\Gamma_1(108 \cdot 8^2)). \end{aligned}$$

Similarly if  $\sum_{n=0}^\infty r_2(n)q^n := \Theta^2(z)\Theta(3z) \in M_{\frac{3}{2}}(\Gamma_1(12))$ , then by (6)

$$\begin{aligned} t_2(z) &:= \sum_{n \equiv 1 \pmod{24}} r_2(n)q^n \\ &= 4q + 28q^{25} + 28q^{49} + 48q^{73} + \dots \in M_{\frac{3}{2}}(\Gamma_1(12 \cdot 24^2)). \end{aligned}$$

It is easy to see that  $t_2(z) \equiv 0 \pmod{4}$ , and so the modular form

$$f_2(z) + \frac{t_2(z)}{4} = 2q + 8q^{25} + 5q^{49} + 9q^{73} + 9q^{97} + \dots \in M_{\frac{3}{2}}(\Gamma_1(12 \cdot 24^2)),$$

and modulo 9 its first few terms are

$$f_2(z) + \frac{t_2(z)}{4} \equiv 2q + 8q^{25} + 5q^{49} + 5q^{121} + \dots \pmod{9}.$$

Although it is unnecessary, we recall the following eta-function identity:

$$\frac{\eta^5(6z)}{\eta^2(3z)} = \sum_{1 \leq n \equiv 1,2 \pmod{6}} nq^{n^2} - \sum_{0 < n \equiv 4,5 \pmod{6}} nq^{n^2} \in S_{\frac{3}{2}}(\Gamma_1(144)).$$

By (6) it is easy to see that

$$j_2(z) := \sum_{1 \leq n \equiv 1 \pmod{6}} nq^{n^2} - \sum_{0 < n \equiv 5 \pmod{6}} nq^{n^2} \in S_{\frac{3}{2}}(\Gamma_1(144 \cdot 4)).$$

Define the form  $i_2(z) \in M_{\frac{3}{2}}(\Gamma_1(6912))$  by

$$i_2(z) := f_2(z) + \frac{t_2(z)}{4} - 2j_2(z) = 18q^{25} - 9q^{49} + 9q^{73} + 9q^{97} + \dots.$$

After computing the first 5,400,000 terms, by (8) we find that  $i_2(z) \equiv 0 \pmod{9}$ . In particular if  $1 < n \equiv 1 \pmod{24}$  is square-free, then

$$(9) \quad a_2(n) + \frac{r_2(n)}{4} \equiv 0 \pmod{9}.$$

Since  $r_2(n) = \#\{x^2 + y^2 + 3z^2 = n \mid x, y, z \in \mathbb{Z}\}$ , and the ternary form  $x^2 + y^2 + 3z^2$  is in a genus with a single class, by [J, Th. 86] it turns out that  $r_2(n) = 12h(-3n)$  if  $1 < n \equiv 1 \pmod{24}$  is square-free. Therefore for such  $n$  it is easy to see by (9) that

$$\frac{a_2(n)}{3} \equiv -h(-3n) \pmod{3}.$$

□

*Remark.* Using a theorem of Davenport and Heilbronn, as refined by Horie and Nakagawa (see [D-H], [H-N]), it is easy to deduce that

$$\liminf_{x \rightarrow \infty} \frac{\#\{|D| < x \mid \text{square-free } |D| \equiv 1 \pmod{3}, \text{ with } S(3, E(D)) = 0\}}{\#\{|D| < x \mid \text{square-free } |D| \equiv 1 \pmod{3}\}} \geq \frac{1}{2}.$$

In particular, for such  $D$  the curves  $E(D)$  have rank zero at least half the time. These ideas have been employed by James [Ja], Horie and Nakagawa [H-N], and Wong [W] to deduce that a positive proportion of certain families of twists of fixed elliptic curves have rank zero.

ACKNOWLEDGEMENTS

The author is indebted to W. Galway whose computations verified the conjectured congruences.

## REFERENCES

- [D-H] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields. II.*, Proc. Roy. Soc. London, Ser. A. **322** (1971), 405-420. MR **58**:10816
- [Ja] K. James, *L-series with non-zero central critical value*, Ph.D. Thesis, Univ. Georgia, 1997.
- [J] B. Jones, *The arithmetic theory of quadratic forms*, Math. Assoc. Amer., 1950. MR **12**:244a
- [H-N] K. Horie and J. Nakagawa, *Elliptic curves with no rational points*, Proc. Amer. Math. Soc. **104** (1988), 20-24. MR **89k**:11113
- [N] J. Nekovář, *Class numbers of quadratic fields and Shimura's correspondence*, Math. Ann. **287** (1990), 577-594. MR **91k**:11051
- [R] K. Rubin, *Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication*, Invent. Math. **89** (1987), 527-559. MR **89a**:11065
- [S] J. Sturm, *On the congruence of modular forms*, Number Theory (New York, 1984-1985) Ed. D. C. Chudnovsky, G. V. Chudnovsky, M. B. Nathanson, Springer Lect. Notes. Math. **1240** (1984), 275-280. MR **88h**:11031
- [W] S. Wong, *Rank zero twists of elliptic curves*, preprint, Brown University.

SCHOOL OF MATHEMATICS, INSTITUTE FOR ADVANCED STUDY, PRINCETON, NEW JERSEY 08540  
*E-mail address:* [ono@math.ias.edu](mailto:ono@math.ias.edu)

DEPARTMENT OF MATHEMATICS, PENN STATE UNIVERSITY, UNIVERSITY PARK, PENNSYLVANIA 16802  
*E-mail address:* [ono@math.psu.edu](mailto:ono@math.psu.edu)