Rank-one Twists of a Certain Elliptic Curve

V. Vatsal
University of Toronto
100 St. George Street
Toronto M5S 1A1, Canada
vatsal@math.toronto.edu

June 18, 1999

Abstract

The purpose of this note is to give the first known example for a conjecture of Goldfeld on the number of rank-one curves appearing in a family of quadratic twists. We show unconditionally that the curve $X_0(19)$ has the property that a positive proportion of its quadratic twists have analytic rank one. This amounts to a strong nonvanishing statement for the *derivatives* of certain L-functions when the sign of the functional equation is -1. We simultaneously obtain the fact that a positive proportion of twists have analytic rank zero when the sign of the functional equation is $+1$.

Let E be a modular elliptic curve over $\mathbf{Q}$, with corresponding newform $F(z) = \sum a_n q^n \in S_2(\Gamma_0(N))$. Let $L(s, F) = L(s, E) = \sum a_n n^{-s}$ be the usual L-series. Then $L(s, F)$ satisfies a functional equation under $s \mapsto 2 - s$, with sign $\epsilon = \pm 1 = \epsilon(E)$. Let D be the fundamental discriminant of a quadratic field $K = K(\sqrt{D})$ and write χ_D for the associated quadratic character. In this setting we define the twisted L-function $L(s, F_D) = \sum \chi_D(n) \cdot a_n n^{-s}$. If E is given by the equation $Y^2 = P(X)$, then $L(s, F_D)$ is the L-function attached to the twisted elliptic curve E_D given by $DY^2 = P(X)$. Therefore $L(s, F_D)$ also satisfies a functional equation and, if $(D, N) = 1$, then the sign is given by $\epsilon_D = \epsilon \cdot \chi_D(-N)$. For $r = 0, 1$, and a positive real number X, define

$$M_F^r(X) = \#\{D : |D| < X : \mathrm{Ord}_{s=1} L(s, F_D) = r\}.$$

The following conjecture of Goldfeld [Gol79] is well-known:

Conjecture I. If $r = 0, 1$, then the following asymptotic formulae hold, as $X \to \infty$:

$$M_F^r(X) \sim X/2. \tag{1}$$

A weaker version of this conjecture would require that

$$M_F^r(X) \gg X, \tag{2}$$

for $r = 0, 1$, as $X \to \infty$. The essence of the conjecture is that the elliptic curves obtained by taking quadratic twists of E should usually have rank 0 or 1, and that this rank should be dictated by the sign in the functional equation. It follows from work of Kolyvagin, Gross, and Zagier, that $L(1, F_D) \neq 0 \implies \mathrm{Rank}(E_D(\mathbf{Q})) = 0$, and that, if $\epsilon_D = -1$, then $L'(1, F_D) \neq 0 \implies \mathrm{Rank}(E_D(\mathbf{Q})) = 1$. This is in accordance with the conjecture of Birch and Swinnerton-Dyer. One could also conjecture the estimates (1), (2), for the L-series attached to arbitrary modular forms of weight 2 on $\Gamma_0(N)$.

To the best of our knowledge, there is no known example of an elliptic curve E for which both estimates in (2) are valid, still less the equality of (1). While a recent preprint of Iwaniec and Sarnak [IS97] shows the estimates in (2) hold under assumption of the Riemann hypothesis, all unconditional results are rather weak. The best known general estimate for $M_F^0(X)$ is due to Ono and Skinner [OS], who prove that

$$M_F^0(X) \gg X/\log(X).$$

Even less is known about $M_F^1(X)$; the current record seems to be due to Perelli and Pomykala [PP97], who show that

$$M_F^1(X) \gg_\varepsilon X^{1-\varepsilon}.$$

However, more is known for special curves E. The first example in which part of (2) holds was given by K. James [Jam], who showed that $M_E^0(X) \gg X$ when E is the curve 14B in Cremona's tables [Cre92]. James' method was subsequently extended to different situations by W. Kohnen [Koh97] and the present author [Vat97]. Indeed, Theorem 0.3 of [Vat97] showed that the estimate $M_F^0(X) \gg (X)$ holds for any semistable elliptic curve with a rational point of order 3 and good reduction at 3. The purpose of this note is to provide what appears to be the first example of a modular form where the complementary estimate for the rank one situation $M_F^1(X) \gg X$ is valid. The precise statement of our result is as follows:

Theorem II. *Let E be the curve $X_0(19)$ (or 19B in Cremona's tables). Then we have the estimate*

$$M_F^r(X) \gg X,$$

as $X \to \infty$, for $r = 0, 1$.

As in James' original method, a key ingredient in the proof is a theorem of Davenport and Heilbronn [DH71] on the 3-primary part of the class groups of quadratic fields. The other major ingredient is a theorem of Gross, which relates 3-torsion in the class groups to the (non)triviality of certain twisted Heegner divisors. We will also need the celebrated Gross-Zagier theorem [GZ86], which relates the heights of these Heegner divisors to the derivative of a certain L-function. We remark here that the relationship between class groups and the arithmetic of the Eisenstein quotients of certain Jacobian varieties may be traced back to fundamental work of B. Mazur [Maz79], where the relationships between class groups and the Mordell-Weil rank are rendered quite explicit. However, the theorems of Gross provide some extra information, and are more convenient for the present application.

III. To prove our result we need some notation concerning Heegner points and quadratic fields (we refer the reader to [Gro84], Ch. I, for a more detailed discussion). Let N be a prime number, and let $m = \text{g.c.d.}(12, N-1)$. Let $n = (N-1)/m$. We will let X denote the modular curve $X_0(N)$. Let K be a complex quadratic field of discriminant D_K in which the prime N splits completely. If c is a square-free positive integer, we let $\mathcal{O}$ denote the order in K with conductor c and conductor $D = c^2 D_K$. If the equation $D^2 = B^2 - 4NC$ has a solution in integers with $(N, B, C) = 1$, then we may define Heegner points with endomorphism ring $\mathcal{O}$ as in [Gro84], I.2. Let χ be a quadratic Galois character of the ring-class-field of K with conductor c; then χ determines and is determined by a factorization

$$D = D_K \cdot c^2 = d \cdot d',$$

where d and d' are fundamental discriminants of quadratic fields k and k', with $d > 0$ (see [Gro84], page 93). Thus k is real and k' is imaginary. In this paper we will only use the case where $c > 0, c \equiv 1 \pmod 4, (c, ND) = 1$, and

$$d = c, d' = D_K \cdot c.$$

With these assumptions we set $L = k \cdot k'$. We let y_χ denote the Heegner divisor in the Jacobian $J = J_0(N)$ defined in [Gro84], I.8. Then this point will be rational over the field L. We let h and h' be the class numbers of k and k' respectively. Let $\mathfrak{n}$ denote a degree-one factor of N in K; we assume that $\chi(\mathfrak{n}) = -1$. Finally, we will let p be an odd prime factor of the number $n = (N-1)/m$.

Then the result of Gross that we will need is the following (see [Gro84], Prop. 15.1):

Theorem IV. *If $ord_p(h \cdot h') < ord_p(n)$, then the Heegner point y_χ is of infinite order in the p-th Eisenstein quotient $J^p(L)$ of J.*

V. We may now prove our main result. We take $N = 19$, $K = \mathbf{Q}(\sqrt{-3})$, $D_K = -3$, and $p = 3$ (observe that the prime 19 splits in $\mathbf{Q}(\sqrt{-3})$). Our conditions on c and χ are as follows:

- $c > 0$ is squarefree, $c \equiv 1 \pmod 4$, $(c, 3 \cdot 19) = 1$;
- $-3c^2 = B^2 - 4 \cdot 19C$ has an integer solution with $(19, B, C) = 1$;
- $\chi(\mathfrak{n}) = -1$, for a degree-one factor $\mathfrak{n}$ of 19 in K.

Then one checks that the second condition above is empty because the given equation is solvable for any choice of c with $(19 \cdot 4 \cdot 3, c) = 1$. The point is that -3 is a square modulo both 4 as well as 19. The third condition can be obtained by choosing c so that 19 is inert in $\mathbf{Q}(\sqrt{c})$. We find that all three conditions are satisfied if c is positive, and lies in the appropriate congruence class modulo $3 \cdot 4 \cdot 19$. Gross' theorem then applies, and gives a criterion for the Heegner point to have infinite order in the Jacobian $J_0(19) = X_0(19) = E$.

Let ψ and and ψ' denote the quadratic Galois characters associated to k and k' respectively. Then $\rho = \mathrm{Ind}_{\mathbf{Q}}^{L}(\chi) = \psi \oplus \psi'$. Note that our hypotheses imply that the twisted L-series $L(s, F \otimes \psi)$ has a functional equation with sign -1, whereas $L(s, F \otimes \psi')$ has sign $+1$. Let g_χ denote the weight-one Eisenstein series with associated Galois representation $\psi \oplus \psi'$. We find that the Rankin-Selberg convolution $L(s, F \otimes g_\chi)$ has a functional equation with sign -1 and vanishes at $s = 1$. But now we may apply the Gross-Zagier theorem [GZ86] to compute the derivative: a convenient form of this result is in given in [Gro84], Theorem 24.1, and we find that the derivative is nonzero precisely when the Heegner point y_χ is of infinite order. In this case, we may conclude that the product

$$L(s, F \otimes \psi) \cdot L(s, F \otimes \psi')$$

has a simple zero at $s = 1$, and in view of the functional equations satisfied by each of the factors, we find that $L(s, F \otimes \psi)$ has a simple zero, and $L(s, F \otimes \psi')$ is non-zero. Gross' theorem states that this happens if the class numbers of k and k' are both 3-adic units.

According to the Davenport-Heilbronn theorem and a subsequent refinement by Nakagawa and Horie (see [NH88], Prop. 2; a convenient statement is also given in [Jam]), we see that the number of $0 < c < X$ satisfying our conditions such that the class number $h' = h(-3c)$ of $k = \mathbf{Q}(\sqrt{-3c})$ is prime to 3 is $\gg X$ as $X \to \infty$. On the other hand, a classical reflection theorem due to Scholz (see [Sch32], or [Wsh80], Thm. 10.10) states that if the class number of $\mathbf{Q}(\sqrt{-3c})$ is prime to 3, then the same is true for the class number of $\mathbf{Q}(\sqrt{c})$. Thus we find that the class numbers of k and k' are prime to three for a positive proportion of c, and this implies our theorem.

References

[Cre92] J. Cremona, *Algorithms for elliptic curves*, Cambridge University Press, 1992.

[DH71] H. Davenport and H. Heilbronn, *On the density of discriminants of a cubic fields II*, Proc. Roy. Soc. London, Ser. A **322**, 1971, 405–420.

[Gol79] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, Number Theory, Carbondale, Springer Lecture Notes, vol. 751, Springer Verlag, 1979, pp. 108–118.

[Gro84] B. Gross, *Heegner points on $X_0(N)$*, Modular forms (R. Rankin, ed.), Chichester, Ellis Horwood Company, 1984.

[GZ86] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84**, (1986), 225–320.

[IS97] H. Iwaniec and P. Sarnak, *The non-vanishing of central values of automorphic L-functions and Siegel's zeros*, preprint, 1997.

[Jam] K. James, *L-series with nonzero central critical value*, to appear in the Journal of the A.M.S.

[Koh97] W. Kohnen, *On the proportion of quadratic twists of modular forms nonvanishing at the central critical point*, preprint, 1997.

[Maz79] B. Mazur, *On the arithmetic of special values of L-functions*, Invent. Math. **55** (1979), 207–240.

[NH88] J. Nakagawa and K. Horie, *Elliptic curves with no torsion points*, Proc. A.M.S. **104** (1988), 20–25.

[OS] K. Ono and C. Skinner, *Nonvanishing of quadratic twists of modular L-functions*, to appear in Invent. Math.

[PP97] A. Perelli and J. Pomykala, *Averages of twisted L-functions*, Acta Arithmetica (1997), 149–163.

[Sch32] A. Scholz, *Über die Beziehung der Klassenzahlen quadratischer Zahlkörper zueinander*, J. reine angew. Math., **166**, 1932, 201–203

[Vat97] V. Vatsal, *Canonical periods and congruence formulae*, to appear, 1997.

[Wsh80] L. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Math. 83, Springer-Verlag, 1980.