Ranks of quadratic twists of an elliptic curve

by

DONGHO BYEON (Seoul)

1. Introduction and statement of result. Let \( E : y^2 = x^3 + ax + b \) be an elliptic curve over \( \mathbb{Q} \) and let \( L(s, E) = \sum_{n=1}^{\infty} a(n)n^{-s} \) be its Hasse–Weil \( L \)-function. Let \( D \) be the fundamental discriminant of the quadratic field \( \mathbb{Q}(\sqrt{D}) \) and let \( \chi_D = (\frac{D}{\cdot}) \) denote the usual Kronecker character. Then the Hasse–Weil \( L \)-function of the quadratic twist \( E_D : Dy^2 = x^3 + ax + b \) of \( E \) is the twisted \( L \)-function \( L(s, E_D) = \sum_{n=1}^{\infty} \chi_D(n)a(n)n^{-s} \). Goldfeld [2] conjectured that

\[
\sum_{|D| < X} \text{Ord}_{s=1} L(s, E_D) \sim \frac{1}{2} \sum_{|D| < X} 1.
\]

This conjecture implies the weaker statement

\[
\#\{|D| < X \mid \text{Ord}_{s=1} L(s, E_D) = r\} \gg X,
\]

where \( r = 0 \) or \( 1 \). For the case \( r = 0 \), there are infinitely many special elliptic curves \( E \) satisfying the weaker statement (cf. [5], [12]) and the best known general result is due to Ono and Skinner [9], who showed that

\[
\#\{|D| < X \mid \text{Ord}_{s=1} L(s, E_D) = 0\} \gg X/\log X.
\]

For the case \( r = 1 \), the best known general result is the following [10]:

\[
\#\{|D| < X \mid \text{Ord}_{s=1} L(s, E_D) = 1\} \gg X^{1-\varepsilon}.
\]

However only one special elliptic curve \( E = X_0(19) \) satisfying the weaker statement (2) is known, due to Vatsal [11]. We note that \( X_0(19) \) is the unique modular curve \( X_0(N) \) such that the genus of \( X_0(N) \) is 1, \( N \) is prime, and 3 divides the number \( n = (N-1)/m \), where \( m = \gcd(12, N-1) \). The aim of this note is to provide another example satisfying the weaker statement (2) for the case \( r = 1 \) and give an estimate of the lower bound which supports the Goldfeld conjecture (1).

2000 Mathematics Subject Classification: 11M, 11R.

Key words and phrases: rank, quadratic twist, elliptic curve.

This work was supported by grant No. R08-2003-000-10243-0 from the Basic Research Program of the Korea Science & Engineering Foundation.

[391]
Theorem 1.1. Let $E$ be the elliptic curve 37C in Cremona’s table with the equation
\[ E : y^2 + y = x^3 + x^2 - 23x - 50. \]
Then for at least 40% of the positive fundamental discriminants $D$ and at least 24% of the negative fundamental discriminants $D$, $\text{Ord}_{s=1} L(s, E_D) = 1$.

Remark. Let $E$ be the elliptic curve 37C and $E_D(\mathbb{Q})$ be the Mordell–Weil group of $E_D$ over $\mathbb{Q}$. Then Theorem 1.1 together with a celebrated theorem of Kolyvagin implies that for at least 40% of the positive fundamental discriminants $D$ and at least 24% of the negative fundamental discriminants $D$, the rank of $E_D(\mathbb{Q})$ is equal to 1.

To prove Theorem 1.1, as in [11], we will use the result of Gross [3] on the non-triviality of Heegner points of Eisenstein curves, the results of Davenport–Heilbronn [1] and Nakagawa–Horie [8] on the 3-rank of the class groups of quadratic fields, and the Gross–Zagier theorem [4] on Heegner points and derivatives of $L$-series. A new ingredient in this note is the use of the fact that $X_0(37)$ is the unique modular curve $X_0(N)$ such that $N$ is prime, and 3 divides the number $n = (N - 1)/m$, and the minus part of its Jacobian is an elliptic curve.

2. Preliminaries. First we recall the result of Gross [3] on the non-triviality of Heegner points of Eisenstein curves. Let $N$ be a prime number, $m = \gcd(12, N - 1)$, and $p$ be an odd prime factor of $n = (N - 1)/m$. Let $X$ be the modular curve $X_0(N)$ and $J$ be the Jacobian of $X$. Let $K$ be an imaginary quadratic fields of discriminant $D_K$ in which the prime $(N) = n \cdot \overline{n}$ splits completely. Let $w_K$ denote the number of roots of unity in $K$.

Theorem 2.1 (Gross). Let $\chi$ be the quadratic ring class character of $K$ of conductor $c$ corresponding to the factorization
\[ c^2 \cdot D_K = d \cdot d', \]
where $d > 0$ is the fundamental discriminant of a real quadratic field $k$ and $d' < 0$ is the fundamental discriminant of an imaginary quadratic field $k'$. Let $L = kk'$ and $y_\chi$ be the Heegner divisor in $J(L)$. Let $h$ and $h'$ be the class numbers of $k$ and $k'$ respectively. Assume $\chi(n) = -1$ and $\text{ord}_p(hh') < \text{ord}_p(n)$. Then the projection $y_\chi^{(p)}$ of $y_\chi$ into the $p$-Eisenstein quotient $J^{(p)}(L)$ of $J(L)$ has infinite order.

Theorem 2.2 (Gross). Let $\chi = 1$ and $y_\chi$ be the Heegner divisor in $J(K)$. Let $A = \mathcal{O}_K[N^{-1}]$ and $h_A$ be the class number of $A$. Assume $(p, w_K) = 1$ and $\text{ord}_p(h_A) < \text{ord}_p(n)$. Then the projection $y_\chi^{(p)}$ of $y_\chi$ into the $p$-Eisenstein quotient $J^{(p)}(K)$ of $J(K)$ has infinite order.
Now we recall the result of Nakagawa and Horie [8] which is a refinement of the result of Davenport and Heilbronn [1]. Let \( m \) and \( N \) be two positive integers satisfying the following condition:

\[
(*) \quad \text{If an odd prime number } p \text{ is a common divisor of } m \text{ and } N, \text{ then } p^2 \text{ divides } N \text{ but not } m. \text{ Further if } N \text{ is even, then either (i) } 4 \text{ divides } N \text{ and } m \equiv 1 \pmod{4}, \text{ or (ii) } 16 \text{ divides } N \text{ and } m \equiv 8 \text{ or } 12 \pmod{16}.
\]

For any positive real number \( X > 0 \), we denote by \( S_+(X) \) the set of positive fundamental discriminants \( D < X \) and by \( S_-(X) \) the set of negative fundamental discriminants \( D > X \), and put

\[
S_+(X, m, N) := \{ D \in S_+(X) \mid D \equiv m \pmod{N} \},
\]

\[
S_-(X, m, N) := \{ D \in S_-(X) \mid D \equiv m \pmod{N} \}.
\]

**Theorem 2.3 (Nakagawa and Horie).** Let \( D \) be a fundamental discriminant and \( r_3(D) \) be the 3-rank of the quadratic field \( \mathbb{Q}(\sqrt{D}) \). Then for any two positive integers \( m, N \) satisfying \((*)\),

\[
\lim_{X \to \infty} \sum_{D \in S_+(X, m, N)} 3^{r_3(D)} / \sum_{D \in S_+(X, m, N)} 1 = \frac{4}{3},
\]

\[
\lim_{X \to \infty} \sum_{D \in S_-(X, m, N)} 3^{r_3(D)} / \sum_{D \in S_-(X, m, N)} 1 = 2.
\]

From Theorem 2.3 and the fact that

\[
\sum_{D \in S_\pm(X, m, N)} 3^{r_3(D)} + 3 \left( \sum_{D \in S_\pm(X, m, N)} 1 - \sum_{D \in S_\pm(X, m, N)} 3^{r_3(D)} \right) \leq \sum_{D \in S_\pm(X, m, N)} 3^{r_3(D)},
\]

we can easily obtain the following

**Lemma 2.4.** Let \( D \) be a fundamental discriminant and \( h(D) \) the class number of the quadratic field \( \mathbb{Q}(\sqrt{D}) \). Then for any two positive integers \( m, N \) satisfying \((*)\),

\[
\liminf_{X \to \infty} \frac{\#\{ D \in S_+(X, m, N) \mid h(D) \not\equiv 0 \pmod{3} \}}{\#S_+(X, m, N)} \geq \frac{5}{6},
\]

\[
\liminf_{X \to \infty} \frac{\#\{ D \in S_-(X, m, N) \mid h(D) \not\equiv 0 \pmod{3} \}}{\#S_-(X, m, N)} \geq \frac{1}{2}.
\]

3. **Proof of Theorem 1.1.** Let \( N = 37 \). Then \( m = 12 \) and \( n = p = 3 \). In this case \( X = X_0(37) \) is the modular curve with genus 2. Decomposing
$J = J_0(37)$ by means of the canonical involution $w$, we may consider the exact sequence

$$0 \to J_+ \to J \to J^- \to 0,$$

where $J_+ = (1 + w)J$. We note that $\dim J_+ = \dim J^- = 1$ (see [6, Table in Introduction]).

**Proposition 3.1.** $J^-$ is the elliptic curve $37C$ in Cremona’s table with the equation

$$E : \quad y^2 + y = x^3 + x^2 - 23x - 50.$$

**Proof.** See [7, Proposition 1 in §5].

Let $\tilde{J}$ be the Eisenstein quotient of $J$. We know that $\tilde{J}$ factors through $J^-$ and the $p$-Eisenstein quotient $J^{(p)}$ of $J$ is a quotient of $\tilde{J}$ (see [6, Chap. II, (10.4) and (17.10)]). Thus we have

**Proposition 3.2.** $J^{(p)}$ is a quotient of $J^- = E$.

**Proposition 3.3.** Let $k$ be a real quadratic field where the prime $37$ is inert. If the class number $h$ of $k$ is prime to $3$, then the projection of $y_\chi$ into $E(k) (= J^-(k))$ has infinite order.

**Proof.** Let $k$ be a real quadratic field of discriminant $d$ where $37$ is inert and whose class number $h$ of $k$ is prime to $3$. Let $k'$ be the imaginary quadratic field $\mathbb{Q}(\sqrt{-2})$ of discriminant $-8$. Note that $37$ is inert in $k'$ and the class number $h'$ of $k'$ is equal to $1$. Let $K$ be a third field contained in the biquadratic extension $L = kk'$. Then $K$ is imaginary and $37$ splits in $K$. Let $D_K$ be the discriminant of $K$ and $\chi$ be the quadratic ring class character of $K$ of conductor $c$ corresponding to the factoring of $c^2 \cdot D_K = d \cdot (-8)$. Then from Theorem 2.1, we know that $y_\chi^{(p)}$ has infinite order in $J^{(p)}(L)$. Since $J^{(p)}$ is a quotient of $J^- = E$ by Proposition 3.2, the projection of $y_\chi$ to $E(L)$ has infinite order. We note that $E(L) = E(k) \oplus E(k')$ and $E(k') = E(\mathbb{Q}) = \mathbb{Z}/3\mathbb{Z}$. Thus the projection of $y_\chi$ to $E(k)$ should have infinite order.

**Proposition 3.4.** Let $K (\neq \mathbb{Q}(\sqrt{-3}))$ be an imaginary quadratic field where the prime $37$ is split. If the class number $h$ of $K$ is prime to $3$, then the projection of $y_\chi$ into $E(K) (= J^-(K))$ has infinite order.

**Proof.** Let $K$ be an imaginary quadratic field where $37$ is split and whose class number $h$ of $K$ is prime to $3$. In this case, we note that $h_A$ is simply the quotient of $h_K$ by the order of $n$ in the class group of $K$. Then from Theorem 2.2, we know that $y_\chi^{(p)}$ has infinite order in $J^{(p)}(L)$. Since $J^{(p)}$ factors through $J^- = E$ by Proposition 3.2, the projection of $y_\chi$ to $E(K)$ should have infinite order.

**Proof of Theorem 1.1.** First we compute the number of quadratic fields $k$ and $K$ in Propositions 3.3 and 3.4. By a well known method in ana-
lytic number theory we have the following estimate on $S_{\pm}(X, m, N)$ (see [8, Proposition 2]):

$$
\#S_{\pm}(X, m, N) \sim \#S_{\mp}(X, m, N) \sim \frac{3X}{\pi^2 \varphi(N)} \prod_{p \mid N} \frac{q}{p + 1} \quad (X \to \infty),
$$

where $q = 4$ or $p$ according as $p = 2$ or not. Thus from Lemma 2.4, we obtain the following estimates:

$$
\liminf_{X \to \infty} \frac{\#\{D \in S_{+}(X) \mid h(D) \not\equiv 0 \pmod{3} \text{ and } \left(\frac{D}{37}\right) = -1\}}{\#S_{+}(X)} \geq \frac{5}{6} \cdot \frac{18}{37} \simeq 0.405,
$$

$$
\liminf_{X \to \infty} \frac{\#\{D \in S_{-}(X) \mid h(D) \not\equiv 0 \pmod{3} \text{ and } \left(\frac{D}{37}\right) = 1\}}{\#S_{-}(X)} \geq \frac{1}{2} \cdot \frac{18}{37} \simeq 0.243.
$$


**Remark.** Similarly we can obtain the following:

Let $E$ be the elliptic curve $X_0(19)$ in [11]. Then for at least 39% of the positive fundamental discriminants $D$ and at least 23% of the negative fundamental discriminants $D$, $\text{Ord}_{s=1} L(s, E_D) = 1$.

**References**


Department of Mathematics  
Seoul National University  
Seoul, South Korea  
E-mail: dhbyeon@math.snu.ac.kr

Received on 20.10.2003  
and in revised form on 5.2.2004