Rank-one quadratic twists of an infinite family of elliptic curves

[*][†][‡]Dongho Byeon, Daeyeol Jeon and Chang Heon Kim

Abstract. A conjecture of Goldfeld implies that a positive proportion of quadratic twists of an elliptic curve $E/\mathbb{Q}$ has (analytic) rank 1. This assertion has been confirmed by Vatsal [V1] and the first author [By] for only two elliptic curves. Here we confirm this assertion for infinitely many elliptic curves $E/\mathbb{Q}$ using the Heegner divisors, the 3-part of the class groups of quadratic fields, and a variant of the binary Goldbach problem for polynomials.

1 Introduction

Let $E/\mathbb{Q} : y^2 = x^3 + ax + b$ 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 defined for $\Re(s) > \frac{3}{2}$. The work of Breuil, Conrad, Diamond, Taylor and Wiles [B-C-D-T] [T-W] [Wi] implies that $L(s, E)$ has an analytic continuation to $\mathbb{C}$ and satisfies a functional equation relating the values at s and $2 - s$. 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. For D coprime to the conductor of E, the Hasse-Weil L-function of the quadratic twist $E_D : Dy^2 = x^3 + ax + b$ of E is the twisted L-function $L(s, E_D) = \sum_{n=1}^{\infty} \chi_D(n)a(n)n^{-s}$ which also has an analytic continuation to $\mathbb{C}$ and satisfies a functional equation relating the values at s and $2-s$. Goldfeld [Go] conjectured that

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

---

[*]2000 *Mathematics Subject Classification*: 11G, 11M.

[†]This work is supported by KRF-2005-070-C00004.

[‡]The first author also holds joint appointment in the Research Institute of Mathematics, Seoul National University.

A weaker version of this conjecture is that for $r = 0$ or 1,

$$\sharp\{|D| < X| \ \mathrm{Ord}_{s=1} L(s, E_D) = r\} \gg X. \tag{1}$$

For the case $r = 0$, there is remarkable progress [J] [O] [O-S] [V2]. In particular, it is known that there are infinitely many E such that (1) holds with $r = 0$ [V2]. But for the case $r = 1$, we know only two elliptic curves satisfying (1) [By] [V1]. For more results on Goldfeld's conjecture, see Chapter 9 of [O1]. In this direction, we shall show the following theorem.

Theorem 1.1 *There are infinitely many elliptic curves $E/\mathbb{Q}$ such that* $\mathrm{Ord}_{s=1}$ $L(s, E_D) = 1$ *for a positive proportion of fundamental discriminants D.*

Remark 1. By "infinitely many elliptic curves $E/\mathbb{Q}$", we mean infinitely many $E/\mathbb{Q}$ with distinct j-invariants.

Remark 2. Theorem 1.1 answers Problem 9.33 in [O1].

In Section 3, as in [By] [V1], using a theorem of Davenport and Heilbronn [D-H] on the 3-parts of the class groups of quadratic fields, a theorem of Gross [Gr] on the non-triviality of Heegner points, and Gross and Zagier's theorem [G-Z] on Heegner points and derivatives of L-series, we shall prove the following Theorem 1.2. A new ingredient in this theorem is the relation between Dedekind eta-products and cuspidal divisors, which will be stated in Section 2 and used to show the non-triviality of Heegner points.

Before stating Theorem 1.2, we shall briefly explain some notions and facts. Let $E/\mathbb{Q}$ be an elliptic curve of conductor N and $X_0(N)$ the modular curve of level N with Jacobian $J_0(N)$. The work of Breuil, Conrad, Diamond, Taylor and Wiles [B-C-D-T] [T-W] [Wi] shows that there is a surjective morphism $\phi : X_0(N) \to E$ defined over $\mathbb{Q}$, which uniquely factors in $J_0(N)$ through a homomorphism π : $J_0(N) \to E$. An elliptic curve $E/\mathbb{Q}$ is said be *optimal* if $\ker(\pi)$ is connected. There is a unique optimal elliptic curve E in any isogeny class of elliptic curves defined over $\mathbb{Q}$ of conductor N. Let δ denote a positive divisor of N and let $\mathbf{r} = (r_\delta)$ a family of rational integers $r_\delta \in \mathbb{Z}$. Let $\eta(z)$ be the Dedekind eta-function and $\eta_\delta(z) := \eta(\delta z)$. It is known [Li] that if D_0 is a $\mathbb{Q}$-rational cuspidal divisor of order l in $J_0(N)$, then there is a *Dedekind eta-product* $g_{\mathbf{r}} = \prod_{\delta|N} \eta_\delta^{r_\delta}$ which is a modular function on $X_0(N)$ defined over $\mathbb{Q}$ and satisfies $\mathrm{div}\, g_{\mathbf{r}} = lD_0$. The Dedekind eta-product $g_{\mathbf{r}}$ is said to be *l-power like* if $\prod_{\delta|N} \delta^{r_\delta}$ is the lth-power of a rational number.
For more details on Dedekind eta-products, see Section 2.

Theorem 1.2 *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N. Let $X_0(N)$ be the modular curve of level N with Jacobian $J_0(N)$, $\phi : X_0(N) \to E$ a surjective morphism, which factors in $J_0(N)$ through $\pi : J_0(N) \to E$, and $\pi^* : E \to J_0(N)$ its dual map. Suppose that*

(i) the sign ϵ of the functional equation of $L(s, E)$ is equal to $+1$,
(ii) E has a $\mathbb{Q}$-rational 3-torsion point P,
(iii) $\pi^*(P)$ is a $\mathbb{Q}$-rational cuspidal divisor of order 3 in $J_0(N)$,
(iv) the Dedekind eta-product $g_{\mathbf{r}}$ such that $\operatorname{div} g_{\mathbf{r}} = 3\pi^*(P)$ is not 3-power like.

Then $\operatorname{Ord}_{s=1} L(s, E_D) = 1$, for a positive proportion of fundamental discriminants D.

In Section 4, we shall find a family of elliptic curves which satisfy the conditions in Theorem 1.2. The most expected family would come from the following result [Theorem 1.2, Du] [V3];

> *Let l be a prime number. Let $E'/\mathbb{Q}$ be an elliptic curve of conductor N such that $l^2 \not| N$, and let E be the optimal elliptic curve in the isogeny class of E'. If E' has a $\mathbb{Q}$-rational l-torsion, then E has a $\mathbb{Q}$-rational l-torsion point P such that $\pi^*(P)$ is a $\mathbb{Q}$-rational cuspidal divisor of order l in $J_0(N)$.*

But we do not know whether these elliptic curves also satisfy the condition (iv) in Theorem 1.2 or not. In fact, some of these elliptic curves have the corresponding $g_{\mathbf{r}}$ which is l-power like. So, instead of using this result, we will use the more explicit result of Dummigan [Du], which will be stated in Proposition 4.1. And we shall show the following theorem.

Theorem 1.3 *Let $E/\mathbb{Q}$ be an optimal elliptic curve of square-free conductor N. Let F be the associated newform, and for $d|N$ let $\omega_d = \pm 1$ be such that $W_d F = \omega_d F$, where W_d is the Atkin-Lehner involution. Suppose that*

(i) $N = pq$, where p, q are different primes such that $\omega_p = -1$, $\omega_q = 1$ and $p \neq 3$, $q \equiv -1 \pmod 9$,
(ii) there is an elliptic curve $E'/\mathbb{Q}$ which is isogenous over $\mathbb{Q}$ to E and has a $\mathbb{Q}$-rational 3-torsion point.

Then $\operatorname{Ord}_{s=1} L(s, E_D) = 1$, for a positive proportion of fundamental discriminants D.

Finally, in Section 5, using some results [B-K-W] [Pe] on the binary Goldbach problem for polynomials, we shall show that there are infinitely many elliptic curves satisfying the conditions in Theorem 1.3 and complete the proof of Theorem 1.1.

2 Dedekind eta-products and cuspidal divisors

Let N be a positive integer and let δ denote a positive divisor of N. Let $\mathbf{r} = (r_\delta)$ be a family of rational integers $r_\delta \in \mathbb{Z}$ indexed by all the positive divisors δ of N. Let

$$g_{\mathbf{r}} = \prod_{\delta|N} \eta_\delta^{r_\delta},$$

where $\eta(z)$ is the Dedekind eta-function and $\eta_\delta(z) := \eta(\delta z)$. Then we have the following Proposition.

Proposition 2.1 ([Proposition 3.2.1, Li]) *The Dedekind eta-product $g_{\mathbf{r}}$ is a modular function on $X_0(N)$ defined over $\mathbb{Q}$, i.e., $g_{\mathbf{r}} \in \mathbb{Q}(X_0(N))$ if and only if the following conditions are satisfied:*

(i) $\sum_{\delta|N} r_\delta = 0,$

(ii) $\sum_{\delta|N} \delta\, r_\delta \equiv 0 \pmod{24},$

(iii) $\sum_{\delta|N} \frac{N}{d} r_\delta \equiv 0 \pmod{24},$

(iv) $\prod_{\delta|N} \delta^{r_\delta} \in \mathbb{Q}^2.$

To state Theorem 1.2, we need the following definition.

Definition 2.2 *For an odd prime l, the Dedekind eta-product $g_{\mathbf{r}} = \prod_{\delta|N} \eta_\delta^{r_\delta}$ is said to be l-power like if $\prod_{\delta|N} \delta^{r_\delta}$ is the lth-power of a rational number.*

As representatives of the cusps of $X_0(N)$, we use the rational numbers $\frac{x}{d}$ where $d|N$, $d > 0$ and $(x, d) = 1$ with x taken modulo $(d, N/d)$. We say that such a cusp $\frac{x}{d}$ is of level d and it is defined over $\mathbb{Q}(\zeta_m)$, where $m = (d, N/d)$. Let (P_d) denote the divisor on $X_0(N)$ defined as the sum of all the cusps of level d (each with multiplicity one). Then (P_d) is invariant under $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ and the $\mathbb{Q}$-rational cuspidal subgroup $C(N)$ of $J_0(N)$ is generated by divisor classes of divisors of the kind

$$\phi((d, N/d))P_1 - (P_d),$$

as d runs through the positive divisors of N. And we have the following relation between $\mathbb{Q}$-rational cuspidal divisors of degree 0 and Dedekind eta-products.

Proposition 2.3 ([Proposition 3.2.10, Li]) *Let $D_0 = \sum_{d|N} m_d(P_d)$ be a $\mathbb{Q}$-rational cuspidal divisor of degree 0 of $X_0(N)$, i.e.,*

$$\sum_{d|N} \phi((d, N/d))m_d = 0.$$

Then there exists a Dedekind eta-product $g_{\mathbf{r}} \in \mathbb{Q}(X_0(N))$ such that $\operatorname{div} g_{\mathbf{r}} = lD_0$ and l is the order of D_0.

The following proposition is needed to state and prove Theorem 1.2.

Proposition 2.4 *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N. Let $X_0(N)$ be the modular curve of level N with Jacobian $J_0(N)$, $\phi : X_0(N) \to E$ a surjective morphism, which factors in $J_0(N)$ through $\pi : J_0(N) \to E$, and $\pi^* : E \to J_0(N)$ its dual map. Suppose that E has a $\mathbb{Q}$-rational l-torsion divisor point $P = [A]$, where A is a $\mathbb{Q}$-rational divisor of degree 0 of E, and $\pi^*(A) = [B]$ where B is a $\mathbb{Q}$-rational cuspidal divisor of degree 0 with order l of $X_0(N)$. Let $f \in \mathbb{Q}(E)$ such that $\operatorname{div} f = lA$. Then $f \circ \phi = \alpha g_{\mathbf{r}} \cdot g^l \in \mathbb{Q}(X_0(N))$ for some constant $\alpha \in \mathbb{Q}$, Dedekind eta-product $g_{\mathbf{r}}$ and g in $\mathbb{Q}(X_0(N))$.*

Proof: Let $\phi^* : \mathrm{Div}^0(E) \to \mathrm{Div}^0(X_0(N))$ be the homomorphism corresponding to $\phi : X_0(N) \to E$. Since $\pi^*(P) = [B]$, we can write $\phi^*(A) = B + \operatorname{div} g$, for some $g \in \mathbb{Q}(X_0(N))$. By Proposition 2.3, there exists a Dedekind eta-product $g_{\mathbf{r}} \in \mathbb{Q}(X_0(N))$ such that $\operatorname{div} g_{\mathbf{r}} = lB$. But

$$\operatorname{div}(f \circ \phi) = \phi^*(\operatorname{div} f) = \phi^*(lA) = l\phi^*(A) = lB + l\operatorname{div} g.$$

(Cf. [p. 33 Proposition 3.6, Si].) Thus $\operatorname{div}(f \circ \phi) = \operatorname{div}(g_{\mathbf{r}} \cdot g^l)$ and we have $f \circ \phi = \alpha g_{\mathbf{r}} \cdot g^l$ for some constant $\alpha \in \mathbb{Q}$. (Cf. [p. 32 Proposition 3.1, Si].) □

3 Proof of Theorem 1.2

To prove Theorem 1.2, we need the following proposition.

Proposition 3.1 *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N. Let $X_0(N)$ be the modular curve of level N with Jacobian $J_0(N)$, $\phi : X_0(N) \to E$ a surjective morphism, which factors in $J_0(N)$ through $\pi : J_0(N) \to E$, and $\pi^* : E \to J_0(N)$ its dual map. Suppose that*

(i) the sign ϵ of the functional equation of $L(s, E)$ is equal to $+1$,
(ii) E has a $\mathbb{Q}$-rational l-torsion point P,
(iii) $\pi^*(P)$ is a $\mathbb{Q}$-rational cuspidal divisor of order l in $J_0(N)$,
(iv) the corresponding $g_{\mathbf{r}}$ to $\pi^*(P)$ in Proposition 2.4 is not l-power like.

Let K be an imaginary quadratic field with the discriminant $D_K(\neq -3)$. Suppose that

(v) every prime factor of N splits completely in K,
(vi) E_{D_k} has no Q-rational l-torsion point,
(vii) l does not divide the class number $h(D_K)$ of K.

Then we have

$$\mathrm{Ord}_{s=1} L(s, E_{D_K}) = 1.$$

Proof: Let O_K be the ring of integers of K and $\mathbf{a}$ an ideal of O_K. By the condition (v), we can define the *Heegner point* on $X_0(N)$ with coordinates $j(\mathbf{a})$, $j(\mathbf{n}^\tau \mathbf{a})$, where $(N) = \mathbf{n} \cdot \mathbf{n}^\tau$ in K and τ is the complex conjugation. We denote it by

$$(O_K, \mathbf{n}, [\mathbf{a}]),$$

where $[\mathbf{a}]$ denotes the ideal class of K containing $\mathbf{a}$. Following Birch, Stephens [B-S] and Gross [Gr], let

$$P_E^*(D_K, 1, 1) := \sum_{\mathbf{a} \in \mathrm{Pic}(O_K)} \phi((O_K, \mathbf{n}, [\mathbf{a}])) \; - \sum_{\mathbf{a} \in \mathrm{Pic}(O_K)} \phi((O_K, \mathbf{n}, [\mathbf{a}])^\tau).$$

Then by the condition (i),

$$P_E^*(D_K, 1, 1) \in E_{D_K}(\mathbb{Q}).$$

By the condition (ii), there is $f \in \mathbb{Q}(E)$ such that $\mathrm{div} f = lA$, where $P = [A]$ and $A \in \mathrm{Div}^0(E)$. Then by Weil's reciprocity law, f induces a homomorphism

$$\delta : E(K)/lE(K) \to K^*/(K^*)^l,$$

in particular, which gives

$$\delta(P_E^*(D_K,1,1)) = \prod_{\mathbf{a}\in \mathrm{Pic}(O_K)} \frac{f(\phi((O_K,\mathbf{n},[\mathbf{a}])))}{f(\phi((O_K,\mathbf{n},[\mathbf{a}])^\tau))}.$$

By the condition (iii) and Proposition 2.4, $f\circ\phi = \alpha g_{\mathbf{r}}\cdot g^l$ for some constant $\alpha\in\mathbb{Q}$, Dedekind eta-product $g_{\mathbf{r}}$ and $g\in\mathbb{Q}(X_0(N))$. Thus

$$\begin{aligned}\delta(P_E^*(D_K,1,1)) &= \prod_{\mathbf{a}\in \mathrm{Pic}(O_K)} \frac{\alpha g_{\mathbf{r}}((O_K,\mathbf{n},[\mathbf{a}]))}{\alpha g_{\mathbf{r}}((O_K,\mathbf{n},[\mathbf{a}])^\tau)}\cdot\Big(\prod_{\mathbf{a}\in \mathrm{Pic}(O_K)} \frac{g((O_K,\mathbf{n},[\mathbf{a}]))}{g((O_K,\mathbf{n},[\mathbf{a}])^\tau)}\Big)^l \\ &= \beta^l\cdot \prod_{\mathbf{a}\in \mathrm{Pic}(O_K)} \frac{g_{\mathbf{r}}((O_K,\mathbf{n},[\mathbf{a}]))}{g_{\mathbf{r}}((O_K,\mathbf{n},[\mathbf{a}])^\tau)},\end{aligned}$$

for some $\beta\in K$.

For each positive divisor d of N, we denote by $\mathbf{n}_d$ the unique O_K-ideal of norm d with $\mathbf{n}_d|\mathbf{n}$. From the definition of $g_{\mathbf{r}}$ and the condition (i) in Proposition 2.1, we have that

$$g_{\mathbf{r}}((O_K,\mathbf{n},[\mathbf{a}]))^{24} = \prod_{d|N}\Delta(\mathbf{n}_d\mathbf{a})^{r_d} = \prod_{d|N}\left(\frac{\Delta(\mathbf{n}_d\mathbf{a})}{\Delta(\mathbf{a})}\right)^{r_d}.$$

And we know that $\Delta(\mathbf{a})/\Delta(\mathbf{n}_d\mathbf{a})$ is an integer in the Hilbert class field H of K which generates the ideal $\mathbf{n}_d^{12}$ and from the condition (iv) in Proposition 2.1, we have

$$\prod_{d|N}\mathbf{n}_d^{r_d} = \mathbf{m}^{-2},$$

for some fractional O_K-ideal $\mathbf{m}$. Thus $\delta(P_E^*(D_K,1,1))$ is an element in K^* which generates the ideal $(\beta^l)\cdot(\mathbf{m}/\mathbf{m}^\tau)^{h(D_K)}$ and

$$\delta(P_E^*(D_K,1,1)) = \zeta\cdot\beta^l\cdot\gamma^{h(D_K)/O(\mathbf{m})},$$

where ζ is a root of unity in K^*, γ is a generator of the principal ideal $(\mathbf{m}/\mathbf{m}^\tau)^{O(\mathbf{m})}$ and $O(\mathbf{m})$ is the order of $\mathbf{m}$ in $\mathrm{Pic}(O_K)$. Hence by the conditions (iv),(vii), $\delta(P_E^*(D_K,1,1))$ is not an lth-power and by the condition (vi), $\delta(P_E^*(D_K,1,1))$ has infinite order in $E_{D_K}(\mathbb{Q})$.

Finally Gross and Zagier's theorem [G-Z] on Heegner points and derivatives of L-series implies that $\mathrm{Ord}_{s=1}L(s,E_{D_K}) = 1$ and we completed the proof. □

Now we can prove Theorem 1.2.

Proof of Theorem 1.2; For any elliptic curve $E/\mathbb{Q}$, there are only finitely many fundamental discriminants D such that E_D has a $\mathbb{Q}$-rational 3-torsion point. A theorem of Davenport and Heilbronn [D-H] (as refined by Nakagawa and Horie [N-H]) on the 3-parts of the class groups of quadratic fields implies that for a positive proporion of negative fundamental discriminants D, every prime factor of N splits in the imginary quadratic fields $\mathbb{Q}(\sqrt{D})$ and 3 does not divide the class number of $\mathbb{Q}(\sqrt{D})$. Thus Theorem 1.2 follows from Proposition 3.1 for the case of $l = 3$. □

4 Proof of Theorem 1.3

Let $E/\mathbb{Q}$ be an optimal elliptic curve of square-free conductor N. Let l be an odd prime such that $l \not| N$. Under some conditions, Dummigan [Theorem 4.1, Du] shows that if an elliptic curve $E'/\mathbb{Q}$ in the isogeny class of E has a $\mathbb{Q}$-rational point of order l then so has E. To prove it, he [Proposition 3.2 and Corollary 3.3, Du] use Dedekind eta-products and explicitly construct a $\mathbb{Q}$-rational cuspidal divisor of degree 0 in $J_0(N)$ whose order is divisible by l. In order to apply Dummigan's result to prove Theorem 1.3, we combine Proposition 3.2, Corollary 3.3, Theorem 4.1 in [Du] and obtain the following proposition.

Proposition 4.1 ([Du]) *Let $E/\mathbb{Q}$ be an optimal elliptic curve of square-free conductor N. Let $X_0(N)$ be the modular curve of level N with Jacobian $J_0(N)$, $\phi : X_0(N) \to E$ a surjective morphism, which factors in $J_0(N)$ through $\pi : J_0(N) \to E$, and $\pi^* : E \to J_0(N)$ its injective dual map. Let F be the associated newform, and for $d|N$ let $\omega_d = \pm 1$ be such that $W_d F = \omega_d F$, where W_d is the Atkin-Lehner involution. Let G be the product of those primes such that $\omega_p = 1$. Define a divisor Q supported on the cusps of $X_0(N)$ and the Dedekind eta-product $g_{\mathbf{r}}$;*

$$Q := \sum_{\delta|(N/G)} \omega_\delta(P_{\delta G}) \quad \textit{and} \quad g_{\mathbf{r}} := \Big(\prod_{g|G} \prod_{d|(N/G)} \eta_{dg}^{\omega_d \mu(g) g}\Big)^{24/h},$$

where $h := (r, 24)$, $r := \prod_{p|G}(p^2-1) \prod_{p|(N/G)}(p-1)$, and μ is the Möbius function. If $\omega_p = -1$ for at least one prime $p|N$, then

(i) Q is a $\mathbb{Q}$-rational cuspidal divisor of degree 0,
(ii) $g_{\mathbf{r}}^2 \in \mathbb{Q}(X_0(N))$ and $\mathrm{div}\,(g_{\mathbf{r}}^2) = (-1)^t \omega_N(2n) Q$, where $n := r/h$ and t is the number of prime divisors of N,
(iii) the exact order of the rational point $[Q]$ in $J_0(N)$ is either n or $2n$,

(iv) if there is an elliptic curve $E'/\mathbb{Q}$ which is isogenous over $\mathbb{Q}$ to E and has a $\mathbb{Q}$-rational l-torsion point, where l is an odd prime such that $l \not| N$ and $l|n$, then E has a $\mathbb{Q}$-rational l-torsion point P such that $\pi^*(P) = R := \frac{2n}{l}[Q]$.

Now we can prove Theorem 1.3.

Proof of Theorem 1.3; We will show that if E is an optimal elliptic curve which satisfies the conditions in Theorem 1.3, E satisfies the conditions in Theorem 1.2.

By the condition (i) in Theorem 1.3, we have $\epsilon = -\omega_N = -\omega_p \cdot \omega_q = +1$; the condition (i) in Theorem 1.2. And by Proposition 4.1, we can construct $\mathbb{Q}$-rational cuspidal divisor Q of degree 0;

$$Q = \sum_{\delta|p} \omega_\delta (P_{\delta q}) = (P_q) - (P_{pq}),$$

and the Dedekind eta-product $g_{\mathbf{r}} \in \mathbb{Q}(X_0(N))$;

$$g_{\mathbf{r}} = (\prod_{g|q} \prod_{d|p} \eta_{dg}^{\omega_d \mu(g) g})^{24/h} = (\frac{\eta_1 \eta_{pq}^q}{\eta_p \eta_q^q})^{24/h},$$

where $h = ((q^2-1)(p-1), 24)$. And

$$\mathrm{div}(g_{\mathbf{r}}^2) = -(2n)Q,$$

where $n = (q^2-1)(p-1)/((q^2-1)(p-1), 24)$. We note that $3 \not| N = pq$ and $3|n$. Thus by the condition (ii) in Theorem 1.3 and Proposition 4.1 (iv), we easily see that E satisfies the conditions (ii),(iii) in Theorem 1.2.

Finally the corresponding eta-product $g_{\mathbf{r}}^{-2}$ to $R = \frac{2n}{3}[Q]$ is not a cubic because $p^{(q-1)\cdot \frac{24}{((q^2-1)(p-1),24)}}$ is not a cubic. Thus E satisfies the condition (iv) in Theorem 1.2 and we completed the proof. □

5 Proof of Theorem 1.1

Let $G(x) \in \mathbb{Z}[x]$ be a polynomial of degree k with positive leading coefficient. Perelli [Pe] and Brüdern, Kawada and Wooley [B-K-W] proved that almost all values of the polynomial $2G(m)$ are the sum of two primes. We slightly modify the result to show that there are infinitely many elliptic curves satisfying the conditions in Theorem 1.3.

Proposition 5.1 ([B-K-W]) *Let $G(x) \in \mathbb{Z}[x]$ be a polynomial of degree k with positive leading coefficient and A, B be positive integers such that $(A, B) = 1$. Let $S_k(M, G)$ denote the number of natural numbers m with $1 \leq m \leq M$, for which the equation*

$$2G(m) = Ap_1 + Bp_2$$

has no solution in primes p_1, p_2. Then there is an absolute constant $c > 0$ such that

$$S_k(M, G) \ll_G M^{1-c/k}.$$

Proof: We define $S(A\alpha) := \sum_{p \leq X} (\log p) e(A\alpha p)$, $e(\alpha) := e^{2\pi i \alpha}$, where the summation is over prime numbers and define

$$r(m) := \int_0^1 S(A\alpha) S(B\alpha) e(-\alpha m) d\alpha.$$

Then $r(2G(m))$ counts the solutions of $2G(m) = Ap_1 + Bp_2$ with weight $(\log p_1)(\log p_2)$. If we directly follow the proof of Theorem 1 in [B-K-W], we obtain $r(2G(m)) > 0$ for each integer m with $1 \leq m \leq M$, with at most $O(M^{1-c/k})$ possible exceptions for a constant $c > 0$, which does not depend on A, B and $G(x)$. □

Now we can prove Theorem 1.1.

Proof of Theorem 1.1; Let $E'/\mathbb{Q} : y^2 + a_1 xy + a_3 y = x^3$, $a_1, a_3 \in \mathbb{Z}$. Then the point $(0, 0) \in E'(\mathbb{Q})$ is a 3-torsion point. The discriminant Δ of E' is

$$\Delta = a_3^3 (a_1^3 - 27 a_3).$$

Now we assume that $2, 3 \not| \Delta$ and $(a_1, a_3) = 1$. Then since $c_4 := a_1 (a_1^3 - 24 a_3)$, we easily see that for every prime factor t of Δ, $E'/\mathbb{Q}$ has multiplicative reductions at t. Thus the conductor N of E' is square-free. Furthermore, for every prime factors t of a_3, clearly E' has a *split* multiplicative reduction at t. On the other hand, for every prime factor $t \equiv -1 \pmod 3$ of $(a_1^3 - 27 a_3)$ has a *non-split* multiplicative reduction at t and for every prime factor $t \equiv 1 \pmod 3$ of $(a_1^3 - 27 a_3)$ has a *split* multiplicative reduction at t because the slopes of the tangent lines at the node $(-a_1^2/9, a_1^3/27) \in E'(\mathbb{F}_t)$ are $(-3a_1 \pm a_1 \sqrt{-3})/6$.

Let $G(x) := (9(2x + 1) - 1)^3/2$. Then by Proposition 5.1, we know that there are infinitely many m such that

$$2G(m) = (9(2m + 1) - 1)^3 = 27p + q,$$

for some primes p, q. For such m, p, q, let $a_1 := (9(2m+1)-1)$ and $a_3 := p\,(\neq 3)$. Then we have

$$\Delta = p^3 q \quad \text{and} \quad N = pq,$$

where $p \neq 3$ and $q \equiv -1 \pmod 9$. So E' has a *split* multiplicative reduction at p and has a *non-split* multiplicative reduction at q. Since the signs of Atkin-Lehner involutions $\omega_t = -1$ or $+1$ according as the multiplicative reduction at primes t is *split* or *non-split*, respectively, we have $\omega_p = -1$ and $\omega_q = +1$. Thus if we let $E/\mathbb{Q}$ be the optimal elliptic curve of the isogeny class of $E'/\mathbb{Q}$, then E satisfies all the conditions in Theorem 1.3.

Hence we proved that there are infinitely many elliptic curves E satisfying the conditions in Theorem 1.3. And we easily see that these elliptic curves E have different j-invariants by the form of the conductors of E. Finally Theorem 1.1 immediately follows from Theorem 1.3. □

Acknowledgement This paper was completed when the first author stayed at University of Wisconsin, Madison from March 2006 to February 2007. The author greatly thank Ken Ono for his careful reading this paper and suggesting many valuable suggestions. And the authors also thank the referee for some helpful suggestions.

References

[B-C-D-T] C. Breuil, B. Conrad, F. Diamond and R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$; wild 3-adic exercises,* J. Amer. Math. Soc. **14** (2001), 843-939.

[B-S] B. J. Birch and N. M. Stephens, *Computation of Heegner points,* in: Modular forms (Durham, 1983), 13–41, Ellis Horwood Ser. Math. Appl., Statist. Oper. Res., Horwood, Chichester, 1984.

[B-K-W] J. Brüdern, K. Kawada and T. D. Wooley, *Additive reprensentation in thin sequences, II: The binary Goldbach problem,* Mathematica **47** (2000), 117-125.

[By] D. Byeon, *Ranks of of quadratic twists of an elliptic curve,* Acta Arith. **114** (2004), 391-396.

[D-H] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields II,* Proc. Roy. Soc. London A, **322** (1971), 405–420.

[Du] N. Dummigan, *Rational torsion on optimal curves,* Int. J. Number Theory, **1** (2005), 513–531.

[Go] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields,* Number Theory, Carbondale, Springer Lect. Notes **751** (1979), 108-118.

[Gr] B. H. Gross, *Heegner points on $X_0(N)$,* in: Modular forms (Durham, 1983), 87–105, Ellis Horwood Ser. Math. Appl., Statist. Oper. Res., Horwood, Chichester, 1984.

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

[J] K. James, *L-series with nonzero central critical value,* J. Amer. Math. Soc. **11** (1998), 635–641.

[Li] G. Ligozat, *Courbes modulaires de genre* 1, Bull. Soc. Math. France Mém. **43** (1975).

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

[O-S] K. Ono and C. Skinner, *Non-vanishing of quadratic twists of modular L-functions,* Invent. Math. **134** (1998), 651–660.

[O] K. Ono, *Nonvanishing of quadratic twists of modular L-functions and applications to elliptic curves,* J. Reine Angew. Math. **533** (2001), 81–97.

[O1] K. Ono, *The web of modularity: Arithmetic of the coefficients of modular forms and q-series,* CBMS Regional Conference Series **102**, Amer. Math. Soc. Providence, R. I., 2004.

[Pe] A. Perelli, *Goldbach numbers represented by polynomials,* Rev. Mat. Iberoamericana, **12** (1996), 477-490.

[Si] J. H. Silverman, *The arithmetic of ellipitic curves,* Grad. Texts in Math. **106**, Springer-Verlag, New York, 1986.

[T-W] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras,* Ann. of Math. **141** (1995), 553–572.

[V1] V. Vatsal, *Rank-one twists of a certain elliptic curve,* Math. Ann. **311** (1998), 791–794.

[V2] V. Vatsal, *Canonical periods and congruence formulae,* Duke Math. J. **98** (1999), 397–419.

[V3] V. Vatsal, *Multiplicative subgroups of $J_0(N)$ and applications to elliptic curves,* J. Inst. Math. Jussieu **4** (2005), 281–316.

[Wi] A. Wiles, *Modular elliptic curves and Fermat's last theorem,* Ann. of Math. **141** (1995), 443–551.

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

Department of Mathematics Education, Kongju National University, Kongju, Korea
E-mail: dyjeon@kongju.ac.kr

Department of mathematics, Seoul Women's university, Seoul, Korea
E-mail: chkim@swu.ac.kr