Journal of Number Theory 131 (2011) 552–560

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Rational torsion on optimal curves and rank-one quadratic twists ☆

Dongho Byeon *, Donggeon Yhee

Department of Mathematics, Seoul National University, Seoul, Republic of Korea

ARTICLE INFO

Article history:
Received 25 August 2010
Revised 14 October 2010
Accepted 29 October 2010
Available online 11 December 2010
Communicated by David Goss

Keywords:
Rank
Torsion
Elliptic curves
Twists

ABSTRACT

When an elliptic curve $E'/\mathbb{Q}$ of square-free conductor N has a rational point of odd prime order $l \nmid N$, Dummigan (2005) in [Du] explicitly constructed a rational point of order l on the optimal curve E, isogenous over $\mathbb{Q}$ to E', under some conditions. In this paper, we show that his construction also works unconditionally. And applying it to Heegner points of elliptic curves, we find a family of elliptic curves $E'/\mathbb{Q}$ such that a positive proportion of quadratic twists of E' has (analytic) rank 1. This family includes the infinite family of elliptic curves of the same property in Byeon, Jeon, and Kim (2009) [B-J-K].

1. Introduction

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 works of Breuil, Conrad, Diamond, Taylor and Wiles [B-C-D-T,T-W,Wi] show that there is a surjective morphism $\phi : X_0(N) \to E'$ defined over $\mathbb{Q}$, which uniquely factors through a homomorphism $\pi : J_0(N) \to E'$. Let $\pi^* : E' \to J_0(N)$ be the dual map of π. An elliptic curve $E/\mathbb{Q}$ is said to be *optimal* if $\ker(\pi)$ is connected. We note that an elliptic curve $E/\mathbb{Q}$ is optimal if π^* is injective. There is a unique optimal elliptic curve E in any isogeny class of elliptic curves defined over $\mathbb{Q}$ of conductor N.

As representatives of the cusps of $X_0(N)$, we use the rational numbers $\frac{x}{d}$ where $d \mid N$, $d > 0$ 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

☆ This work is supported by KRF-2008-313-C00012.
* Corresponding author.
E-mail addresses: dhbyeon@snu.ac.kr (D. Byeon), dgyhee@gmail.com (D. Yhee).

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2010.10.005

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.

Let $\mathbf{r} = (r_d)$, where $d \mid N$, $d > 0$, be a family of rational integers $r_d \in \mathbb{Z}$. Let $\eta(z)$ be the Dedekind eta-function and $\eta_d(z) := \eta(dz)$. 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* $g_{\mathbf{r}} = \prod_{d|N} \eta_d^{r_d}$ which is a modular function on $X_0(N)$ defined over $\mathbb{Q}$ and satisfies $\operatorname{div} g_{\mathbf{r}} = lD_0$.

From now on, we consider the case that N is square-free. Let f be the newform associated with an elliptic curve $E'/\mathbb{Q}$ of conductor N and for each positive $d \mid N$ let $w_d = \pm 1$ be such that $W_d f = w_d f$, where W_d is the Atkin–Lehner involution. Let G be the product of those primes such that $w_p = 1$. Define a divisor Q supported on the cusps of $X_0(N)$,

$$Q := \sum_{d|(N/G)} w_d (P_{dG})$$

and the Dedekind eta-product $g_{\mathbf{r}}$,

$$g_{\mathbf{r}} := \left(\prod_{g|G} \prod_{d|(N/G)} \eta_{dg}^{w_d \mu(g) g} \right)^{24/h},$$

where $h := (r, 24)$, $r := \prod_{p|G}(p^2 - 1) \prod_{p|(N/G)}(p - 1)$, and μ is the Möbius function.

In [Du], Dummigan obtained the following proposition.

Proposition 1.1. *Let $E'/\mathbb{Q}$ be an elliptic curve of square-free conductor N with a rational point of odd prime order $l \nmid N$ and E be the optimal elliptic curve, isogenous over $\mathbb{Q}$ to E'. If $w_p = -1$ for at least one prime $p \mid N$ and $l \mid n$, where $n := r/h$, 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 $\operatorname{div}(g_{\mathbf{r}}^2) = (-1)^t w_N(2n) Q$, where 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) *E has a $\mathbb{Q}$-rational l-torsion point P such that $\pi^*(P) = R := \frac{2n}{l}[Q]$.*

In this paper, we will show the following proposition.

Proposition 1.2. *Let $E'/\mathbb{Q}$ be an elliptic curve of square-free conductor N with a rational point of odd prime order $l \nmid N$. Then $w_p = -1$ for at least one prime $p \mid N$, and $l \mid n$.*

So Proposition 1.1 is also true without the conditions that $w_p = -1$ for at least one prime $p \mid N$ and $l \mid n$.

Let $E'/\mathbb{Q} : y^2 = x^3 + a'x + b'$ be an elliptic curve over $\mathbb{Q}$ of conductor N 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 ϵ be the sign of the functional equation of $L(s, E')$. Then we have that $\epsilon = -\prod_{p|N} w_p$. 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 $E'_D : Dy^2 = x^3 + a'x + b'$ of E' is the twisted L-function $L(s, E'_D) = \sum_{n=1}^{\infty} \chi_D(n)a(n)n^{-s}$. Goldfeld [Go] conjectured that

$$\sum_{|D|<X} \operatorname{Ord}_{s=1} L\big(s, E'_D\big) \sim \frac{1}{2} \sum_{|D|<X} 1.$$

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

$$\sharp\big\{|D| < X \,\big|\, \operatorname{Ord}_{s=1} L\big(s, E'_D\big) = r\big\} \gg X,$$

i.e., that $\operatorname{Ord}_{s=1} L(s, E'_D) = r$ for a positive proportion of D.

In [V1], Vatsal proved that if $E'/\mathbb{Q}$ is a semi-stable elliptic curve with a $\mathbb{Q}$-rational point of order 3 and good reduction at 3, then for a positive proportion of D, $\operatorname{Ord}_{s=1} L(E'_D, s) = 0$. But for the case $r = 1$, less is known. Recently, we [B-J-K] proved that if $E/\mathbb{Q}$ is an optimal elliptic curve of square-free conductor N satisfying the following two conditions:

(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', isogenous over $\mathbb{Q}$ to E and having 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. And using a variant of the binary Goldbach problem for polynomials, we proved that there are infinitely many elliptic curves satisfying the conditions. In this paper, using Proposition 1.2, we will prove the following theorem.

Theorem 1.3. *Let $E'/\mathbb{Q}$ be an elliptic curve of square-free conductor N with a rational point of order $3 \nmid N$. If there is only one prime $p \mid N$ such that $\omega_p = -1$, then*

$$\sharp\big\{|D| < X \,\big|\, \operatorname{Ord}_{s=1} L\big(s, E'_D\big) = 1\big\} \gg X.$$

Examples. The elliptic curves satisfying the condition in Theorem 1.3 whose conductor is less than 100 are following: 14A1, 14A2, 14A4, 14A6, 19A1, 19A3, 26A1, 26A3, 34A1, 34A2, 35A1, 35A3, 37B1, 37B3, 38A1, 38A3, 77B1, 77B3 in Cremona's table [Cr]. This list includes Vatsal's example 19A1 in [V] and Byeon's example 37B1 in [B].

We note that the family of elliptic curves in Theorem 1.3 includes the elliptic curves satisfying the above two conditions (i) and (ii). And we point out that though Goldfeld's conjecture is about all quadratic twists, we prove Theorem 1.3 using imaginary quadratic twists.

2. Proof of Proposition 1.2

Using parameterizations of the elliptic curves for given torsion structures in [Ku, Table 3], we will show Proposition 1.2. We recall that if E' has split multiplication reduction at p, then $w_p = -1$ and if E' has non-split multiplication reduction at p, then $w_p = 1$.

Proof of Proposition 1.2.

Case I. $l = 3$.

Case I-1. $E'_{\text{tor}} = \mathbb{Z}/3\mathbb{Z}$.

In this case as a minimal Weierstrass equation for E, we can take

$$E'\colon\quad y^2 + a'xy + b'y = x^3,\quad a, b' \in \mathbb{Z},\ b' > 0.$$

Since the conductor N of E' is square-free, we can assume that

$$\left(a', b'\right) = 1,$$

where (a', b') denotes the greatest common divisor of a' and b'.

Let $\Delta' = b'^3(a'^3 - 27b')$ be the minimal discriminant of E'. For a prime $p \mid \Delta'$ $(p \neq 3)$, we have:

(1) $p \mid b' \Rightarrow w_p = -1$,
(2) $p \mid a'^3 - 27b' \Rightarrow w_p = -1$ *if* $p \equiv 1 \pmod 3$ *and* $w_p = 1$ *if* $p \equiv -1 \pmod 3$.

Thus if $a'^3 - 27b'$ has two or more prime factors, then $9 \mid r$, so $3 \mid n$.

Now we consider the case that $a'^3 - 27b'$ has only one or no prime factor. Let $b' = ts$, $t, s \in \mathbb{N}$, where for each prime $p \mid b'$, $p \mid t$ if $p \equiv 1 \pmod 3$ and $p \mid s$ if $p \equiv -1 \pmod 3$.

Lemma 2.1.

(i) *If* $a'^3 - 27b' = m^3$ *for an integer* m, *then there is at least one prime* $p \mid t$.
(ii) *If* $a'^3 - 27b' = \pm 1$ *and* $t = p^k$ *for a prime* p, *then* $p \equiv 1 \pmod 9$.

Proof. (i) If $a'^3 - 27b' = m^3$, then $a' \equiv m \pmod s$ because for all $p \mid s$, $p \equiv -1 \pmod 3$ and $3 \nmid |(\mathbb{Z}/s\mathbb{Z})^*|$. Let $a' = \alpha s + m$, $\alpha \in \mathbb{Z}$. Then

$$a'^3 = \left(\alpha^3 s^2 + 3\alpha^2 sm + 3\alpha m^2\right)s + m^3 = (27t)s + m^3.$$

This implies α is a multiple of 3, moreover, a multiple of 9, so $a' = 9\beta s + m$, $\beta \in \mathbb{Z}$. Thus

$$\beta\left(27\beta^2 s^2 + 9\beta sm + m^2\right) = t.$$

By completing the square in the second factor, we see that $t > 1$ and there is at least one prime $p \mid t$.

(ii) Suppose that $a'^3 - 27b' = \pm 1$ and $t = p^k$ for a prime p. By the same way in (i), we have that

$$\beta\left(27\beta^2 s^2 \pm 9\beta s + 1\right) = t.$$

Since $(\beta, t/\beta) = 1$ and $(t/\beta) > 1$, $\beta = 1$. Thus $27s^2 \pm 9s + 1 = p^k$. Euler's case $n = 3$ of Fermat's last theorem and the equation $(\pm 3s)^3 + (27s^2 \pm 9s + 1) = (\pm 3s + 1)^3$ imply that 3 cannot divide k. So $p \equiv \pm 1 \pmod 9$ and by the choice of t, we have that $p \equiv 1 \pmod 9$. □

If there are at least two primes $p \mid t$, then $9 \mid r$, so $3 \mid n$. Suppose that there is only one prime $p \mid t$. If $a'^3 - 27b'$ has a prime factor q, then $q - 1$ or $q^2 - 1$ is divisible by 3 and $p - 1$ is divisible by 3, so $9 \mid r$ and $3 \mid n$. If $a'^3 - 27b' = \pm 1$, then $p - 1$ is divisible by 9 by Lemma 2.1, so $9 \mid r$ and $3 \mid n$. If there is no prime $p \mid t$, then $a'^3 - 27b' = q^k$ for a prime q and $3 \nmid k$ by Lemma 2.1. This implies that $q = \pm 1 \pmod 9$. So $9 \mid r$ and $3 \mid n$. This completes the proof of $l \mid n$ for the case $E'_{\mathrm{tor}} = \mathbb{Z}/3\mathbb{Z}$.

On the other hand, if $b' \neq 1$, then there is a prime $p \mid b'$ such that $\omega_p = -1$. If $b' = 1$, then $\Delta' = a'^3 - 27 = (a' - 3)(a'^2 + 3a' + 9)$. We note that $a' - 3$ and $a'^2 + 3a' + 9$ are relatively prime. Suppose $\omega_p = 1$ for a prime $p \mid a'^3 - 27$. Since $p \equiv -1 \pmod 3$ and $a'^3 \equiv 27 \pmod p$, we have that $p \mid a' - 3$. Thus there should be another prime $q \mid a'^2 + 3a' + 9$ such that $\omega_q = -1$.

Case I-2. $E'_{\mathrm{tor}} = \mathbb{Z}/6\mathbb{Z}$ or $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

In this case as a Weierstrass equation for E', we can take

$$E': \quad y^2 + (u-v)xy - uv(v+u)y = x^3 - v(v+u)x^2,$$

with $u, v \in \mathbb{Z}$, $u > 0$, $(u, v) = 1$ and the minimal discriminant is

$$\Delta' = v^6(v+u)^3u^2(9v+u).$$

For a prime $p \mid \Delta'$ $(p \neq 3)$, we have:

(1) $p \mid v(v+u) \Rightarrow \omega_p = -1$,
(2) $p \mid u \Rightarrow \omega_p = -1$ *if* $p \equiv 1 \pmod 3$ *and* $\omega_p = 1$ *if* $p \equiv -1 \pmod 3$,
(3) $p \mid 9v+u \Rightarrow \omega_p = -1$ *if* $p \equiv 1 \pmod 3$ *and* $\omega_p = 1$ *if* $p \equiv -1 \pmod 3$.

Thus if $u(9v+u)$ has two or more prime factors, then $9 \mid r$, so $3 \mid n$.

Now we consider the case that $u = 1$ and $9v+1$ has only one prime factor. Let $v = ts$ where for each prime $p \mid v$, $p \mid t$ if $p \equiv 1 \pmod 3$ and $p \mid s$ if $p \equiv -1 \pmod 3$ (we may assume $t > 0$).

Lemma 2.2. *If* $9v + 1 = m^3$ *for an integer* m*, then there is a prime* $p \mid v$, $p \equiv 1 \pmod 3$.

Proof. If $9v + 1 = m^3$, then $m \equiv 1 \pmod s$ since for all $p \mid s$, $p \equiv -1 \bmod 3$ and $3 \nmid |(\mathbb{Z}/s\mathbb{Z})^*|$. Let $m = \alpha s + 1$ (we may assume that $\alpha > 0$). Then

$$m^3 = \big(\alpha^3 s^2 + 3\alpha^2 s + 3\alpha\big)s + 1 = 9ts + 1.$$

This implies α is a multiple of 3, so $m = 3\beta s + 1$ (we may assume that $\beta > 0$) and

$$\beta\big(3\beta^2 s^2 + 3\beta s + 1\big) = t.$$

Thus $t > 1$ and there is a prime $p \mid v$ such that $p \equiv 1 \pmod 3$. □

If there is a prime $p \mid v$ such that $p \equiv 1 \pmod 3$, then $9 \mid r$ and $3 \mid n$. If $v = \pm 1$, then $9v + 1 = q^k$ for a prime q and $3 \nmid k$ by Lemma 2.2. This implies that $q \equiv \pm 1 \pmod 9$. So $9 \mid r$ and $3 \mid n$. This completes the proof of $l \mid n$ for the case $E'_{\mathrm{tor}} = \mathbb{Z}/6\mathbb{Z}$ or $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

On the other hand, if a prime $p \mid v(v+u)$, then $w_p = -1$. So there is at least one prime $p \mid N$ such that $w_p = -1$.

Case I-3. $E'_{\mathrm{tor}} = \mathbb{Z}/9\mathbb{Z}$.

In this case as a Weierstrass equation for E', we can take

$$E': \quad y^2 + \big(u^3 - v^3 + uv^2\big)xy - u^4v^2\tilde{b}y = x^3 - uv^2\tilde{b}x^2$$

with $u, v \in \mathbb{Z}$, $(u, v) = 1$, $\tilde{b} = (v-u)(u^2 - uv + v^2)$. One may obtain the equation from $f = v/u$, [Ku, p. 12, Table 3]. The discriminant is

$$\Delta' = u^9v^9(v-u)^9\big(u^2 - uv + v^2\big)^3\big(u^3 + 3u^2v - 6uv^2 + v^3\big),$$

which is minimal at any prime p dividing $uv(v-u)(u^2 - uv + v^2)$ if $(u, v) = 1$.

So the minimal discriminant of E' is divisible by $uv(v-u)(u^2-uv+v^2)$ and we easily see that for all 9 possible cases, $u \equiv 0, 1, 2 \pmod 3$ and $v \equiv 0, 1, 2 \pmod 3$, $3 \mid uv\tilde{b}$. Thus we exclude this case by the assumption $3 \nmid N$.

Case I-4. $E'_{\mathrm{tor}} = \mathbb{Z}/12\mathbb{Z}$.

In this case as a Weierstrass equation for E', we can take

$$E'\colon \quad y^2 + \big(u(u-v)^3 - v\tilde{c}\big)xy - uv(u-v)^5\tilde{c}\tilde{d}y = x^3 - v(u-v)^2\tilde{c}\tilde{d}x^2$$

with $u, v \in \mathbb{Z}$, $(u, v) = 1$, $\tilde{c} = (2v-u)(u^2-3uv+3v^2)$, $\tilde{d} = (u^2-2uv+2v^2)$, with $\tau = v/u$ in [Ku, p. 11, Table 3]. The discriminant

$$\Delta' = u^2v^{12}(u-v)^{12}(2v-u)^6\big(u^2-2uv+2v^2\big)^3\big(u^2-6uv+6v^2\big)\big(u^2-3uv+3v^2\big)^4$$

is minimal at odd prime p dividing $uv(u-v)(2v-u)$. If u is odd, then Δ' is also minimal at 2.

So the minimal discriminant of E' is divisible by $uv(u-v)(u-2v)/2$ if u is even and $uv(u-v)(u-2v)$ if u is odd. And we easily see that for all 9 possible cases, $u \equiv 0, 1, 2 \pmod 3$ and $v \equiv 0, 1, 2 \pmod 3$, $3 \mid uv(u-v)(u-2v)$. Thus we exclude this case by the assumption $3 \nmid N$.

Case II. $l = 5$.

In this case, we need the following lemma, which follows from the proof of [V2, Proposition 5.3].

Lemma 2.3. *Let l be an odd prime. Let $E/\mathbb{Q}$ be an optimal elliptic curve of the minimal discriminant Δ and of square-free conductor N. Suppose that $l \nmid N$ and Δ be the lth-power of a rational number. Then there is a prime divisor $p \mid N$ such that $p \equiv 1 \pmod l$.*

Proof. For an odd prime l, if Δ is an lth power, then we know that $E[l] \cong (\mathbb{Z}/l\mathbb{Z}) \oplus \mu_l$ is a decomposable $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module (see [Du, Proposition 4.2]). From [V2, Theorem 1.1], we have $\mu_l \subset E \subset J_0(N)$ and $\mu_l \subset E[l]$ is contained in the Shimura subgroup V of $J_0(N)$. Since the order of V divides $\phi(N)$ by [LO, Corollary 1], there is a prime $p \mid N$, $p \equiv 1 \pmod l$ if $l^2 \nmid N$. □

Case II-1. $E'_{\mathrm{tor}} = \mathbb{Z}/5\mathbb{Z}$.

In this case as a minimal Weierstrass equation for E', we can take

$$E'\colon \quad y^2 + (u-v)xy - u^2vy = x^3 - uvx^2,$$

with $u, v \in \mathbb{Z}$, $(u, v) = 1$ and the minimal discriminant is

$$\Delta' = u^5v^5\big(v^2 - 11uv - u^2\big).$$

If $|uv| > 1$ and $p \mid uv$, then $w_p = -1$. If $|uv| = 1$, then the elliptic curve is isomorphic to $y^2 + y = x^3 - x^2$, $\Delta' = -11$, $N = 11$, and $w_{11} = -1$. So there is at least one prime $p \mid N$ such that $w_p = -1$.

Let E be the optimal elliptic curve, isogenous over $\mathbb{Q}$ to E', of the minimal discriminant Δ. We note that E and E' have the same n. If Δ is not the 5th-power of a rational number, then Dummigan [Du] proved that $5 \mid n$. If Δ is the 5th-power of a rational number, then by Lemma 2.3, there is a prime divisor $p \mid N$ such that $p \equiv 1 \pmod 5$. So $5 \mid n$.

This completes the proof of the case $E'_{\mathrm{tor}} = \mathbb{Z}/5\mathbb{Z}$.

Case II-2. $E'_{\mathrm{tor}} = \mathbb{Z}/10\mathbb{Z}$.

In this case as a Weierstrass equation for E', we can take

$$E'\colon\quad y^2 + (uS - vT)xy - u^2v^3STy = x^3 - uv^3Tx^2,$$

with $u, v \in \mathbb{Z}$, $(u, v) = 1$, $S = -(v^2 - 3uv + u^2)$, $T = (v - u)(2v - u)$ and the discriminant is

$$\Delta' = u^5v^{10}(u - v)^{10}(u - 2v)^5\big(u^2 - 3uv + v^2\big)^2\big(u^2 + 2uv - 4v^2\big),$$

which is minimal at any odd prime p dividing $uv(u - v)(u - 2v)$. If u is odd, then Δ' is minimal at all prime p dividing $uv(u - v)(u - 2v)$.

If $|uv(u - v)(u - 2v)| > 2$, then for an odd prime factor p of $uv(u - v)(u - 2v)$, $w_p = -1$. Since $\Delta' \neq 0$, $|T| = 1$ if and only if $v = \pm 2$, $u = \pm 3$, $|uv(u - v)(u - 2v)| > 2$. And $(u, v) = 1$ implies $uv(u - v)(u - 2v)$ has an odd prime factor. So there is at least one prime $p \mid N$ such that $w_p = -1$.

Let E be the optimal elliptic curve, isogenous over $\mathbb{Q}$ to E', of the minimal discriminant Δ. We note that E and E' have the same n. If Δ is not the 5th-power of a rational number, then $5 \mid n$. If Δ is the 5th-power of a rational number, then by Lemma 2.3, there is a prime divisor $p \mid N$ such that $p \equiv 1 \pmod 5$. So $5 \mid n$.

This completes the proof of the case $E'_{\mathrm{tor}} = \mathbb{Z}/10\mathbb{Z}$.

Case III. $l = 7$.

In this case as a minimal Weierstrass equation for E', we can take

$$E'\colon\quad y^2 + \big(u^2 + uv - v^2\big)xy - u^3v^2(v - u)y = x^3 - uv^2(v - u)x^3$$

with $u, v \in \mathbb{Z}$, $(u, v) = 1$ and the minimal discriminant is

$$\Delta' = v^7(v - u)^7u^7\big(v^3 - 8uv^2 + 5u^2v + u^3\big).$$

Dummigan [Du] proved that $7 \mid n$. And if $p \mid uv(v - u)$, then $w_p = -1$, so there is at least one p such that $w_p = -1$. This completes the proof of the case $l = 7$. □

3. Proof of Theorem 1.3

A Dedekind eta-product $g_{\mathbf{r}} = \prod_{d|N} \eta_d^{r_d}$ is said to be *l-power like* if $\widetilde{g_{\mathbf{r}}} := \prod_{d|N} d^{r_d}$ is the lth-power of a rational number.

Proposition 3.1. *Let $E'/\mathbb{Q}$ be an elliptic curve of square-free conductor N with a rational point of odd prime order $l \nmid N$ and E be the optimal elliptic curve, isogenous over $\mathbb{Q}$ to E'. Let P be the rational point of order l in Proposition* 1.1 *(the existence of such P is confirmed by Proposition* 1.2*). Then the Dedekind eta-product $g_{\mathbf{r}}$ corresponding to $\pi^*(P)$ is not l-power like if and only if there is only one prime p such that $w_p = -1$.*

Proof. Let $N = p_1 \cdots p_s q_1 \cdots q_t$ for primes p_i, q_j $(i = 1, \ldots, s,\ j = 1, \ldots, t)$ with Atkin–Lehner involution sign $w_{p_i} = -1$, $w_{q_j} = 1$. Let $G = q_1 \cdots q_t$. We have proven $s \geqslant 1$ in Section 2. The $g_{\mathbf{r}}$ corresponding to $\pi^*(P)$ is given by [Du]

$$g_{\mathbf{r}} := \left(\prod_{g|G} \prod_{d|(N/G)} \eta_{dg}^{w_d \mu(g) g} \right)^{24/h},$$

where $h := (r, 24)$, $r := \prod_{q_j} (q_j^2 - 1) \prod_{p_i} (p_i - 1)$, and μ is the Möbius function.

If $s \geqslant 2$, then

$$\prod_{d|p_1 \cdots p_s} dg^{w_d \mu(g) g} = \prod_{d|p_3 \cdots p_s} \left(\frac{dp_2 g}{dp_1 p_2 g} \right)^{-w_d \mu(g) g} \left(\frac{dg}{dp_1 g} \right)^{w_d \mu(g) g} = 1,$$

so $\widetilde{g_{\mathbf{r}}} = (\prod_{g|q_1 \cdots q_t} \prod_{d|p_1 \cdots p_s} (dg)^{w_d \mu(g) g})^{\frac{24}{h}} = 1$ and $g_{\mathbf{r}}$ is l-power like.

If $s = 1$, then we have

$$\widetilde{g_{\mathbf{r}}} = \left(\prod_{g|\frac{N}{p_1}} \left(\frac{g}{p_1 g} \right)^{\mu(g) g} \right)^{\frac{24}{h}} = \left(\prod_{g|\frac{N}{p_1}} \left(\frac{1}{p_1} \right)^{\mu(g) g} \right)^{\frac{24}{h}} = \left(p^{-(1-q_1) \cdots (1-q_s)} \right)^{\frac{24}{h}}.$$

If $l = 3$, then we know that r is always divisible by 9, in particular, by 3, so $l \nmid \frac{24}{h}$ and if $l = 5, 7$, then $l \nmid \frac{24}{h}$. Since $l \mid (q_j + 1)$, $\widetilde{g_{\mathbf{r}}}$ is not the lth-power of a rational number and $g_{\mathbf{r}}$ is not l-power like. □

In [B-J-K], we proved that if an elliptic curve $E'/\mathbb{Q}$ of conductor N satisfies the following conditions:

(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. So from Propositions 1.1, 1.2 and 3.1, we can have the following proposition.

Proposition 3.2. *Let $E'/\mathbb{Q}$ be an elliptic curve of square-free conductor N with a rational point of order $3 \nmid N$ and E be the optimal elliptic curve, isogenous over $\mathbb{Q}$ to E'. If there is only one prime $p \mid N$ such that $\omega_p = -1$, then*

$$\sharp\left\{ |D| < X \;\middle|\; \operatorname{Ord}_{s=1} L(s, E_D) = 1 \right\} \gg X.$$

Proof of Theorem 1.3. Let $E'/\mathbb{Q}$ be an elliptic curve of square-free conductor N with a rational point of order $3 \nmid N$. Suppose that there is only one prime $p \mid N$ such that $\omega_p = -1$. Let E be the optimal elliptic curve which is isogenous over $\mathbb{Q}$ to E'. Then by Proposition 3.2, we have that

$$\sharp\left\{ |D| < X \;\middle|\; \operatorname{Ord}_{s=1} L(s, E_D) = 1 \right\} \gg X.$$

Since the two elliptic curves E' and E are in the same isogeny class,

$$L(E', s) = L(E, s) = \sum_{n=1}^{\infty} a(n) n^{-s}.$$

So if D_F is coprime to the conductor of E', then

$$L\big(E'_{D_F}, s\big) = L(E_{D_F}, s) = \sum_{n=1}^{\infty} \chi_D(n) a(n) n^{-s}.$$

Thus we also have that

$$\sharp\big\{|D| < X \;\big|\; \mathrm{Ord}_{s=1} L\big(s, E'_D\big) = 1\big\} \gg X,$$

and this completes the proof. □

Acknowledgment

The authors would like to thank the referee for his careful reading and many valuable suggestions.

References

[B-C-D-T] C. Breuil, B. Conrad, F. Diamond, R. Taylor, On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises, J. Amer. Math. Soc. 14 (2001) 843–939.
[B] D. Byeon, Ranks of quadratic twists of an elliptic curve, Acta Arith. 114 (2004) 391–396.
[B-J-K] D. Byeon, D. Jeon, C.H. Kim, Rank-one quadratic twists of an infinite family of elliptic curves, J. Reine Angew. Math. 633 (2009) 67–76.
[Cr] J. Cremona, Algorithms for Elliptic Curves, Cambridge University Press, 1992.
[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, in: Number Theory, Carbondale, in: Springer Lecture Notes in Math., vol. 751, 1979, pp. 108–118.
[Ku] D.S. Kubert, Universal bounds on the torsion of elliptic curves, Proc. Lond. Math. Soc. 3 (33) (1976) 193–237.
[Li] G. Ligozat, Courbes modulaires de genre 1, Bull. Soc. Math. France Mém. 43 (1975).
[LO] S. Ling, J. Oesterlé, The Shimura subgroup of $J_0(N)$, Astérisque 6 (1991) 171–203.
[T-W] R. Taylor, A. Wiles, Ring-theoretic properties of certain Hecke algebras, Ann. of Math. 141 (1995) 553–572.
[V] V. Vatsal, Rank-one twists of a certain elliptic curve, Math. Ann. 311 (1998) 791–794.
[V1] V. Vatsal, Canonical periods and congruence formulae, Duke Math. J. 98 (1999) 397–419.
[V2] 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.