ELLIPTIC CURVES WITH CONDUCTOR HAVING n PRIME FACTORS

DONGHO BYEON

Abstract. In this paper, we prove that for any integer $n \geq 2$, there are infinitely many elliptic curves over $\mathbb{Q}$ with a rational point of order two (resp. three) whose conductor is a square-free integer having n prime factors.

1. Introduction

For $n = 1$ or 2, there are many studies on elliptic curves over $\mathbb{Q}$ with conductor having n prime factors. For an example (see [DJ] for more examples), Setzer [Se] prove that there is an elliptic curve over $\mathbb{Q}$ of prime conductor p with a rational point of order two if and only if $p = 17$ or $p = u^2 + 64$ for some integer u. But we do not know that there are infinitely many such curves.

In [DJ], Dąbrowski and Jędrzejak classify elliptic curves over $\mathbb{Q}$ with a rational point of order two whose conductor is a product of two odd prime powers and conjecture that there are infinitely many elliptic curves over $\mathbb{Q}$ with a rational point of order two whose conductor is a square-free integer having two odd prime factors. (cf. [DJ, p. 258, Remark]).

In [BJK], using a variant of the binary Goldbach problem for polynomials, we construct infinitely many elliptic curves over $\mathbb{Q}$ with a rational point of order three whose conductor is a square-free integer having two odd prime factors and whose root number is $+1$ (cf. [BJK, Section 5, Proof of Theorem 1.1).

In this paper, using a similar method, we prove that the conjecture of Dąbrowski and Jędrzejak is true by proving the following theorem.

The author was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2020R1F1A1A01053449).

Theorem 1.1. *For any integer $n \geq 2$ (resp. $n \geq 3$), there are infinitely many elliptic curves over $\mathbb{Q}$ with a rational point of order two whose conductor is a square-free integer having n odd prime factors and whose root number is equal to -1 (resp. $+1$).*

Further, we prove the following theorem.

Theorem 1.2. *For any integer $n \geq 2$, there are infinitely many elliptic curves over $\mathbb{Q}$ with a rational point of order three whose conductor is a square-free integer having n odd prime factors and whose root number is equal to -1 (resp. $+1$).*

Remark. There are no elliptic curves over $\mathbb{Q}$ with a rational point of order ≥ 6 whose conductor is a product of two odd prime powers except only two elliptic curves over $\mathbb{Q}$ with a rational point of order 8 (cf. [Sa] and [DJ]).

2. Preliminaries

To prove Theorem 1.1 and Theorem 1.2, we need the following lemmas.

Lemma 2.1. ([BJ, Lemma 2.2]) *Let $f(x) \in \mathbb{Z}[x]$ be a polynomial which has a positive leading coefficient. Let A, B be relatively prime odd integers and u, v positive integers with $0 < u, v < 9$ and $(u, 9) = (v, 9) = 1$. Suppose there is at least one integer m' such that*

$$2f(m') \equiv Au + Bv \pmod 9 \text{ and } (AB, 2f(m')) = 1.$$

Then there are infinitely many integers m such that

$$2f(m) = Ap + Bq$$

for some primes $p \equiv u$ and $q \equiv v \pmod 9$.

Lemma 2.2. *Let $f(x) \in \mathbb{Z}[x]$ be a polynomial which has a positive leading coefficient. Let A be an even integer and B an odd integer which is relatively prime to A. Let u and v be positive integers with $0 < u, v < 8$ and $(u, 8) = (v, 8) = 1$. Suppose there is at least one integer m' such that*

$$2f(m') + 1 \equiv Au + Bv \pmod 8 \text{ and } (AB, 2f(m') + 1) = 1.$$

Then there are infinitely many integers m such that

$$2f(m)+1 = Ap + Bq$$

for some primes $p \equiv u$ and $q \equiv v \pmod 8$.

Proof. Proof of Lemma 2.2 is exactly same to [BJ, Proof of Lemma 2.2] if $2f(m)$ is changed by $2f(m)+1$ and 9 is changed by 8. □

3. Proof of Theorem 1.1

Let E be an elliptic curve over $\mathbb{Q}$ with a rational point of order two. As a minimal model outside 2 for E, we can take

$$E : y^2 = x^3 + ax^2 + bx \tag{1}$$

with $a, b \in \mathbb{Z}$ such that neither $p^2 \mid a$ nor $p^4 \mid b$ for any prime p (cf. [Mu, Section 2.1]). The discriminant of Δ of E is

$$\Delta = 2^4 b^2 (a^2 - 4b).$$

We note that if $a \equiv 1 \pmod 4$ and $2^4 \mid b$, then

$$y^2 + xy = x^3 + (\frac{a-1}{4})x^2 + (\frac{b}{16})x$$

is a minimal model for (1) at every prime p (cf. [Mu, Corollary 2.2]), so the minimal discriminant $\Delta_{\min}$ for (1) is

$$\Delta_{\min} = 2^{-8} b^2 (a^2 - 4b).$$

To prove Theorem 1.1, we need the following lemma.

Lemma 3.1. *Let E be an elliptic curve given by the equation (1). Suppose that $(a,b) = 1$. Let p be an odd prime such that $p \,|\, \Delta = 2^4 b^2 (a^2 - 4b)$ and w_p the local root number of E at p. Then E has multiplicative reduction at p and*
(i) If $p \mid b$ and $(\frac{a}{p}) = \pm 1$, then $w_p = \mp 1$,
(ii) If $p \mid a^2 - 4b$ and $(\frac{-2a}{p}) = \pm 1$, then $w_p = \mp 1$.

Proof. For the definition of split or non-split multiplicative reduction at p, see [Si] and for the corresponding value of w_p, see [Ro].

Since $c_4 = 2^4(a^2 - 3b)$, E has multiplicative reduction at p for every odd prime factor p of Δ. For every odd prime factor p of b such that $(\frac{a}{p}) = +1$ (resp. -1), E has split (resp. non-split) multiplicative reduction at p because the slopes of the tangent lines at the node $(0,0) \in E(\mathbb{F}_p)$ are $\pm\sqrt{a}$, so we have $w_p = -1$ (resp. $+1$). For every odd prime factor p of $a^2 - 4b$ such that $(\frac{-2a}{p}) = +1$ (resp. -1), E has split (resp. non-split) multiplicative reduction at p because the slopes of the tangent lines at the node $(\frac{-a}{2}, 0) \in E(\mathbb{F}_p)$ are $\pm\sqrt{\frac{-a}{2}}$, so we have $w_p = -1$ (resp. $+1$). □

Now we can prove Theorem 1.1.

Proof of Theorem 1.1. First we assume that $n = 2$. Let $f(x) = \frac{(2x+1)^4-1}{2}$, $A = 2^6$, $B = 1$, $u = 1$, $v = 1$ and $m' = 0$. By Lemma 2.2, there are infinitely many integers m such that

$$(2m+1)^4 = 2^6 p + q$$

for some odd primes $p \equiv 1$ and $q \equiv 1 \pmod 8$. Let $a = (2m+1)^2$, $b = 2^4 p$ and E be an elliptic curve over $\mathbb{Q}$ with a rational point of order two given by the equation

$$y^2 = x^3 + ax^2 + bx.$$

Then we have

$$\Delta = 2^{12}p^2(2^6 p + q - 2^6 p) = 2^{12}p^2 q.$$

Since $a \equiv 1 \pmod 4$ and $2^4 \mid b$, we have

$$\Delta_{\min} = p^2 q.$$

We note that $(a, b) = 1$. By Lemma 3.1, we have

$$N = pq$$

and $w_p = -1$, $w_q = -1$ because a is square and $q \equiv 1 \pmod 8$, so the root number $w(E)$ of E is

$$w(E) = -w_p w_q = -1.$$

Now we assume that $n \geq 3$ and let p_i $(1 \leq i \leq n-2)$ be fixed distinct odd primes such that $p_1 \equiv 1$ (resp. $p_1 \equiv 5$) (mod 8) and $p_i \equiv 1$ (mod 8) $(i \geq 2)$. Let $f(x) = \frac{(2x+1)^4-1}{2}$, $A = 2^6$, $B = p_1 \cdots p_{n-2}$ (resp. $B = p_1^2 \cdots p_{n-2}$), $u = 1$, $v = 1$ and $m' = 0$. By Lemma 2.2, there are infinitely many integers m such that

$$(2m+1)^4 = 2^6 p + p_1 \cdots p_{n-2} q \quad (resp.\ (2m+1)^4 = 2^6 p + p_1^2 \cdots p_{n-2} q)$$

for some odd primes $p \equiv 1$ and $q \equiv 1$ (mod 8).

Let $a = (2m+1)^2$, $b = 2^4 p$ and E be an elliptic curve over $\mathbb{Q}$ with a rational point of order two given by the equation

$$y^2 = x^3 + ax^2 + bx.$$

Then we have

$$\Delta = 2^{12} p^2 p_1 \cdots p_{n-2} q \quad (resp.\ \Delta = 2^{12} p^2 p_1^2 \cdots p_{n-2} q).$$

Since $a \equiv 1$ (mod 4) and $2^4 \mid b$, we have

$$\Delta_{\min} = p^2 p_1 \cdots p_{n-2} q \quad (resp.\ \Delta_{\min} = p^2 p_1^2 \cdots p_{n-2} q).$$

We may assume that $(a, b) = 1$. By Lemma 3.1, we have

$$N = p p_1 \cdots p_{n-2} q.$$

and $w_p = -1$, $w_{p_1} = -1$ (resp. $w_{p_1} = +1$), $w_{p_i} = -1$ $(i \geq 2)$ and $w_q = -1$, so

$$w(E) = -w_p w_q \prod_{i=1}^{n-2} w_{p_i} = (-1)^{n+1} \quad (resp.\ w(E) = (-1)^n).$$

Therefore we proved the theorem. □

Remark. The family of elliptic curves of conductor pq in the proof of Theorem 1.1 is a subfamily of the family (iid) in [DJ, Theorem 2].

4. Proof of Theorem 1.2

Let E be an elliptic curve over $\mathbb{Q}$ with a rational point of order three. As a minimal model for E, we can take

$$E : y^2 + axy + by = x^3 \tag{2}$$

with $a, b \in \mathbb{Z}$, $b > 0$ such that neither $p \mid a$ nor $p^3 \mid b$ for any prime p (cf. [Ha, Section 1]). The discriminant of $\Delta(= \Delta_{\min})$ of E is

$$\Delta = b^3(a^3 - 27b).$$

To prove Theorem 1.2, we need the following lemma.

Lemma 4.1. *Let E be an elliptic curve given by the equation (2). Suppose that $(a, b) = 1$. Let $p \neq 3$ be a prime such that $p \,|\, \Delta = b^3(a^3 - 27b)$ and w_p the local root number at p. Then E has multiplicative reduction at p and*
(i) If $p \,|\, b$, then $w_p = -1$,
(ii) If $p \,|\, a^3 - 27b$ and $p \equiv \pm 1 \pmod 3$, then $w_p = \mp 1$.

Proof. Since $c_4 = a(a^3 - 24b)$, E has multiplicative reduction at p for every prime factor $p \neq 3$ of Δ. For every prime factor p of b, E has split multiplicative reduction at p because the slopes of the tangent lines at the node $(0, 0) \in E(\mathbb{F}_p)$ are 0 or $-a$, so we have $w_p = -1$. For every odd prime factor $p \equiv -1$ (resp. $+1$) (mod 3) of $a^3 - 27b$, E has non-split (resp. split) multiplicative reduction at p because the slopes of the tangent lines at the node $(-a^2/9, a^3/27) \in E(\mathbb{F}_p)$ are $(-3a \pm a\sqrt{-3})/6$, so we have $w_p = +1$ (resp. -1). Similarly we can show that $w_2 = +1$ if $2 \mid a^3 - 27b$. □

Now we can prove Theorem 1.2.

Proof of Theorem 1.2. Let $n \geq 2$ be an integer and p_i $(1 \leq i \leq n-2)$ be fixed distinct odd primes such that $p_i \equiv 1 \pmod 9$. Let $f(x) = 2^2x^3$, $A = 27$, $B = p_1 \cdots p_{n-2}$, $u = 1$, $v = 1$ (resp. $v = -1$) and $m' = 2$ (resp. $m' = 1$). By Lemma 2.1, there are infinitely many integers m such that

$$2^3m^3 = 27p + p_1 \cdots p_{n-2}q$$

for some odd primes $p \equiv 1$ and $q \equiv 1$ (resp. $q \equiv -1$) (mod 9).

Let $a = 2m$, $b = p$ and E be an elliptic curve over $\mathbb{Q}$ with a rational point of order three given by the equation

$$y^2 + axy + by = x^3.$$

Then we have

$$\Delta_{\min} = p^3(27p + p_1 \cdots p_{n-2}q - 27p) = p^3 p_1 \cdots p_{n-2}q.$$

We may assume that $(a, b) = 1$. By Lemma 4.1, we have

$$N = pp_1 \cdots p_{n-2}q.$$

and $w_p = -1$, $w_{p_i} = -1$ $(i \geq 1)$ and $w_q = -1$ (resp. $w_q = +1$), so

$$w(E) = -w_p w_q \prod_{i=1}^{n-2} w_{p_i} = (-1)^{n+1} \quad (resp.\ w(E) = (-1)^n).$$

Therefore we proved the theorem. □

Acknowledgment. The author thanks the referee for valuable comments.

References

[BJ] D. Byeon and K. Jeong, *Sums of two rational cubes with many prime factors*, J. Number Theory **179** (2017), 240–255.

[BJK] D. Byeon, D. Jeon and C.H. Kim, *Rank-one quadratic twists of an infinite family of elliptic curves*, J. Reine Angew. Math. **633** (2009), 67-76.

[DJ] A. Dąbrowski and T. Jędrzejak, *Elliptic curves over the rationals with good reduction outside two odd primes,* J. Number Theory **202** (2019), 254-277.

[Ha] T. Hadano, *Elliptic curves with torsion point,* Nagoya Math. J. **66** (1977), 99–108.

[Mu] J. T. Mulholland, *Elliptic curves with rational 2-torsion and related ternary Diophantine equations,* Thesis (Ph.D.), University of British Columbia (2006).

[Ro] D. Rohrlich, *Variation of the root number in families of elliptic curves*, Compositio Math. **87** (1993) 119-151.

[Se] B. Setzer, *Elliptic curves of prime conductor*, J. Lond. Math. Soc. **10** (1975) 367-378.

[Si] J. H. Silverman, *The arithmetic of Elliptic Curves*, 2nd ed., Grad. Texts in Math. **106**, Springer 2009.

[Sa] M. Sadek, *On elliptic curves whose conductor is a product of two prime powers,* Math. Comp. **83** (2014) 447-460.

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