Infinitely many elliptic curves of rank exactly two

By Dongho BYEON and Keunyoung JEONG

Department of Mathematics, Seoul National University, Seoul 151-747, Korea

(Communicated by Shigefumi MORI, M.J.A., April 12, 2016)

Abstract: In this note, we construct an infinite family of elliptic curves E defined over $\mathbf{Q}$ whose Mordell-Weil group $E(\mathbf{Q})$ has rank exactly two under the parity conjecture.

Key words: Elliptic curve; rank.

1. Introduction. Let E be an elliptic curve defined over $\mathbf{Q}$. By the *rank* of E we mean the rank of the Mordell-Weil group $E(\mathbf{Q})$. For a small positive integer r, there are many results on the existence of infinitely many elliptic curves of rank $\geq r$. For examples, see [GM] or [RS]. However less is known for the existence of infinitely many elliptic curves of rank exactly r.

In [BJK], infinitely many elliptic curves of rank exactly one were constructed and in [M], Mai proved that under the parity conjecture if p and q are two primes such that $p - q = 24$, then the elliptic curves $E_{3pq} : x^3 + y^3 = 3pq$ have rank exactly two. But we don't know that there are infinitely many such primes, though the celebrated work [Z] made a breakthrough.

In this note, we prove the following theorem.

Theorem 1.1. *There are infinitely many elliptic curves whose rank is exactly two under the parity conjecture.*

The main tools are Mai's work on cubic twists of elliptic curves [M], a variant of the binary Goldbach problem for polynomials [BKW] and a computation of Selmer groups of cubic twists [S].

2. Preliminaries. Let n be a cube free integer and $E_n : y^2 = x^3 - 2^4 3^3 n^2$ the elliptic curve. We note that E_n is isomorphic to the curve $x^3 + y^3 = n$. In [M, Lemma 2.1], Mai proved the following lemma.

Lemma 2.1. *E_n has integral points if and only if n has one of the following six forms*:

$$n = \pm \frac{b(a^2 - b^2)}{4} \quad \text{or} \quad n = \pm \frac{3a^2 b - 3b^3}{24} \pm \frac{a^3 - 9ab^2}{24}$$

for some $a, b \in \mathbf{Z}$.

In [BJ, Lemma 2.2], we slightly modified the result of Brüdern, Kawada and Wooley [BKW, Theorem 1] and obtained the following lemma.

Lemma 2.2. *Let $f(x) \in \mathbf{Z}[x]$ be a polynomial which has a positive leading coefficient. Let A, B be relatively prime odd integers, and $0 \leq i, j \leq 8$ integers. If there is at least one integer m such that*

$$2f(m) \equiv Ap + Bq \pmod 9$$

for some primes $p \equiv i$ and $q \equiv j \pmod 9$, then there are infinitely many integers m such that

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

for some primes $p \equiv i$ and $q \equiv j \pmod 9$.

Let $n = 3^s \prod_{i=1}^{a} l_i^{u_i} \prod_{j=1}^{c} r_j^{v_j}$ be the prime decomposition of n such that $l_i \equiv 1 \pmod 3$ and $r_j \equiv 2 \pmod 3$. Let

$$\lambda : E_n \longrightarrow E_n/\langle(0, \pm 12m\sqrt{-3})\rangle \cong E'_n$$

be the 3-isogeny and λ' be its dual. Let S_n be a Selmer group defined by λ and S'_n be the dual Selmer group defined by λ'. From [S, Théorème 2.9], we have the following lemma.

Lemma 2.3. *If $n \equiv \pm 1 \pmod 9$ $(s = 0)$, $l_i \equiv 1 \pmod 9$ for all $i = 1, \cdots, a$, $r_j \equiv -1 \pmod 9$ for all $j = 1, \cdots, c$, and for all $i = 1, \cdots, a$, l_k for $k = 1, \cdots, i-1, i+1, \cdots, a$ and r_j for $j = 1, \cdots, c$ are cubes modulo l_i, then $S_n \simeq (\mathbf{Z}/3\mathbf{Z})^{a+c}$ and $S'_n \simeq (\mathbf{Z}/3\mathbf{Z})^{a+1}$.*

3. Proof of Theorem 1.1.

Proposition 3.1. *There are infinitely many primes p, q such that $p, q \equiv 8 \pmod 9$ and the elliptic curve $E_{pq} : y^2 = x^3 - 2^4 3^3 p^2 q^2$ has a nontrivial rational point.*

Proof. By Lemma 2.1, $E_{b^3 n}$ has integral points if

2010 Mathematics Subject Classification. Primary 11G05; Secondary 11G40.

doi: 10.3792/pjaa.92.64

$$b^3 n = b^3(16b^6 - a^2) = -\frac{(4b^3)(a^2 - (4b^3)^2)}{4}$$
for some $a, b \in \mathbf{Z}$.

On the other hand, by Lemma 2.2 there are infinitely many b, $p \equiv 8$ and $q \equiv 8 \pmod 9$ satisfying $4b^3 = \frac{p+27q}{2}$ because $8b^3 \equiv p + 27q \pmod 9$ has a solution. For such infinitely many primes p, q set $a = \frac{p-27q}{2}$, then

$$n = 16b^6 - a^2 = 27pq.$$

So $E_{b^3 3^3 pq}$ has an integral point. Since $E_{b^3 3^3 pq}$ is isomorphic to E_{pq} over $\mathbf{Q}$, E_{pq} has a rational point for infinitely many primes p, q such that $p, q \equiv 8 \pmod 9$. $\square$

Proof of Theorem 1.1. Let $L_{E_n}(s)$ be the Hasse-Weil L-function of E_n and $w_n \in \{1, -1\}$ its root number. Then $L_{E_n}(s)$ satisfies the functional equation

$$\begin{aligned} &N^{s/2}(2\pi)^{-s}\Gamma(s)L_{E_n}(s) \\ &\quad = w_n N^{(2-s)/2}(2\pi)^{-(2-s)}\Gamma(2-s)L_{E_n}(2-s), \end{aligned}$$

where N is the conductor of E_n whose divisors are 3 and primes $p \mid n$. The *analytic rank* of E_n is the order of vanishing at the central point $s = 1$ of $L_{E_n}(s)$. The functional equation implies that $w_n = 1$ if and only if the analytic rank of E_n is even. The *parity conjecture* predicts that $w_n = 1$ if and only if the rank of E_n is even.

The root number w_n can be computed by the following way, due to Birch and Stephens [BS],

$$w_n = \prod_{p \,\mathrm{prime}} w_n(p),$$

where for $p \neq 3$,

$$w_n(p) = \begin{cases} -1 & \text{if } p \mid n \text{ and } p \equiv 2 \pmod 3 \\ 1 & \text{otherwise} \end{cases}$$

and for $p = 3$,

$$w_n(p) = \begin{cases} -1 & \text{if } n \equiv 0, \pm 2, \pm 4, \pmod 9 \\ 1 & \text{otherwise.} \end{cases}$$

Consider E_{pq} constructed in Proposition 3.1. Then the root number w_{pq} of E_{pq} in Proposition 3.1 is equal to one. So the parity conjecture implies that the rank of $E_{pq}(\mathbf{Q})$ in Proposition 3.1 is at least 2.

Since $pq > 17$, $E_{pq}(\mathbf{Q})$ has no torsion points. So from the following exact sequences

$$\begin{aligned} 0 &\longrightarrow \frac{E'_{pq}(\mathbf{Q})[\lambda']}{\lambda(E_{pq}(\mathbf{Q}))[3]} \longrightarrow \frac{E'_{pq}(\mathbf{Q})}{\lambda(E_{pq}(\mathbf{Q}))} \longrightarrow \frac{E_{pq}(\mathbf{Q})}{3E_{pq}(\mathbf{Q})} \\ &\longrightarrow \frac{E_{pq}(\mathbf{Q})}{\lambda'(E'_{pq}(\mathbf{Q}))} \longrightarrow 0, \end{aligned}$$

and

$$0 \longrightarrow \frac{E'_{pq}(\mathbf{Q})}{\lambda(E_{pq}(\mathbf{Q}))} \longrightarrow S_{pq} \longrightarrow \text{Ш}(E_{pq}/\mathbf{Q})[\lambda] \longrightarrow 0,$$

$$0 \longrightarrow \frac{E_{pq}(\mathbf{Q})}{\lambda'(E'_{pq}(\mathbf{Q}))} \longrightarrow S'_{pq} \longrightarrow \text{Ш}(E'_{pq}/\mathbf{Q})[\lambda'] \longrightarrow 0,$$

we have that

$$\begin{aligned} \operatorname{rank} E_{pq}(\mathbf{Q}) &= \dim_{\mathbf{F}_3} \frac{E'_{pq}(\mathbf{Q})}{\lambda(E_{pq}(\mathbf{Q}))} \\ &\quad + \dim_{\mathbf{F}_3} \frac{E_{pq}(\mathbf{Q})}{\lambda'(E'_{pq}(\mathbf{Q}))} - 1 \\ &\leq \dim_{\mathbf{F}_3} S_{pq} + \dim_{\mathbf{F}_3} S'_{pq} - 1. \end{aligned}$$

Here we may assume $p \neq q$ for p, q in Proposition 3.1 since there is no b, p which satisfy $8b^3 = 28p$. By Lemma 2.3, E_{pq} in Proposition 3.1 has $S_{pq} \simeq (\mathbf{Z}/3\mathbf{Z})^2$ and $S'_{pq} \simeq (\mathbf{Z}/3\mathbf{Z})$, so the rank of $E_{pq}(\mathbf{Q})$ in Proposition 3.1 is at most 2.

Thus the elliptic curves E_{pq} in Proposition 3.1 have ranks exactly two under the parity conjecture and the theorem follows. $\square$

Acknowledgement. This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2013R1A1A2007694).

References

[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.

[BJ] D. Byeon and K. Jeong, Sums of two rational number with many prime factors. (Preprint).

[BKW] J. Brüdern, K. Kawada and T. D. Wooley, Additive representation in thin sequences. II. The binary Goldbach problem, Mathematika **47** (2000), no. 1–2, 117–125.

[BS] B. J. Birch and N. M. Stephens, The parity of the rank of the Mordell-Weil group, Topology **5** (1966), 295–299.

[GM] F. Gouvêa and B. Mazur, The square-free sieve and the rank of elliptic curves, J. Amer. Math. Soc. **4** (1991), no. 1, 1–23.

[M] L. Mai, The analytic rank of a family of elliptic curves, Canad. J. Math. **45** (1993), no. 4, 847–862.

[RS] K. Rubin and A. Silverberg, Ranks of elliptic curves, Bull. Amer. Math. Soc. (N.S.) **39**

(2002), no. 4, 455–474 (electronic).
[S] P. Satgé, Groupes de Selmer et corps cubiques, J. Number Theory **23** (1986), no. 3, 294–317.
[Z] Y. Zhang, Bounded gaps between primes, Ann. of Math. (2) **179** (2014), no. 3, 1121–1174.