Infinitely many elliptic curves of rank exactly two II

By Keunyoung JEONG

Department of Mathematical Sciences, Ulsan National Institute of Science and Technology, UNIST-gil 50, Ulsan 44919, Korea

(Communicated by Shigefumi MORI, M.J.A., May 13, 2019)

Abstract: Under the parity conjecture, an infinite family of elliptic curves of rank 2 with a torsion subgroup of order 2 or 3 is constructed.

Key words: Elliptic curves; Mordell–Weil groups.

1. Introduction. There are numerous results on the construction of an infinite family of elliptic curves of rank at least r and given torsion subgroups. For example, Dujella and Peral [DP15] proved that there are infinitely many elliptic curves $E/\mathbf{Q}$ such that

$$\begin{cases} \mathrm{rank}_{\mathbf{Z}}(E(\mathbf{Q})) \geq 3, & E(\mathbf{Q})_{\mathrm{tor}} = \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}, \\ \mathrm{rank}_{\mathbf{Z}}(E(\mathbf{Q})) \geq 3, & E(\mathbf{Q})_{\mathrm{tor}} = \mathbf{Z}/8\mathbf{Z}. \end{cases}$$

For other torsion groups, analogous results are listed in [Duj].

However, less is known regarding the construction of an infinite family of elliptic curves over the rational numbers whose rank is *exactly* r. The only known cases are $r = 0$ and 1. We recall the parity conjecture for elliptic curves over the rationals: For any elliptic curve $E/\mathbf{Q}$,

$$\mathrm{ord}_{s=1} L(s, E) \equiv \mathrm{rank}_{\mathbf{Z}}(E(\mathbf{Q})) \pmod 2.$$

Byeon and the author [BJ16] constructed an infinite family of elliptic curves over the rationals whose Mordell–Weil group is exactly $\mathbf{Z} \times \mathbf{Z}$. In this study, we will prove the analogous results for other torsion subgroups, namely, $\mathbf{Z}/2\mathbf{Z}$ and $\mathbf{Z}/3\mathbf{Z}$.

Theorem 1.1. *Under the parity conjecture, there are infinitely many elliptic curves E such that $E(\mathbf{Q}) \cong \mathbf{Z} \times \mathbf{Z} \times T$ for $T = \mathbf{Z}/2\mathbf{Z}$, $\mathbf{Z}/3\mathbf{Z}$.*

For an integer m, we denote by E_m the elliptic curve defined by $y^2 = x^3 - mx$, and by A_m the elliptic curve defined by $y^2 = x^3 + m^2$. Let p and q represent prime numbers. We will show that there are infinitely many elliptic curves of the form E_{pq} and A_{pq}, such that each has root number $+1$ and a nontrivial rational point. In other words, we show that there are infinitely many pairs of prime numbers (p, q) such that

$$(1) \quad \begin{cases} \mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \leq E_{pq}(\mathbf{Q}), & w_{E_{pq}} = +1, \\ \mathbf{Z} \times \mathbf{Z}/3\mathbf{Z} \leq A_{pq}(\mathbf{Q}), & w_{A_{pq}} = +1. \end{cases}$$

To do so, we use following lemma:

Lemma 1.2 ([BJ17, Lemma 2.2]). *Let $f(x) \in \mathbf{Z}[x]$ be a polynomial of degree k with positive leading coefficient. Let A, B be relatively prime odd integers, g be an integer, and i, j be positive integers with $0 < i, j < g$ and $(i, g) = (j, g) = 1$. We assume that there is at least one integer m such that*

$$2f(m) \equiv Ai + Bj \pmod g \text{ and } (AB, 2f(m)) = 1.$$

Then, there are infinitely many integers n such that

$$2f(n) = Ap_1 + Bp_2,$$

for some primes $p_1 \equiv i$ and $p_2 \equiv j \pmod g$.

Subsequently, the upper bound of size of Selmer groups of E_{pq} and A_{pq} will be calculated. The size of the Selmer groups of E_{-p} and A_p is determined by the residue class of p modulo 16 and 9, respectively (see [Sil09, Proposition X.6.2], and [CP09, Corollary 7.7]). In the case of E_{pq} and A_{pq}, the Selmer groups are not determined only by the residue classes of p and q modulo 16 and 9. However it will be shown that the upper bound of the size of Selmer groups can be calculated in certain cases (see Proposition 2.2, 3.4). Combining these with (1), we have Theorem 1.1.

2. 2-Torsion case. We recall that an elliptic curve E_m is defined by the equation $y^2 = x^3 - mx$, where $m \in \mathbf{Z}$. The torsion subgroup of $E_m(\mathbf{Q})$ is $\mathbf{Z}/2\mathbf{Z}$ when $m \neq -4$ and m is not square [Sil09, Proposition X.6.1].

Lemma 2.1. (i) *If m is not divisible by any square of integers, then*

2010 Mathematics Subject Classification. Primary 11G05.

doi: 10.3792/pjaa.95.53

$$w_{E_m} = w_\infty w_2,$$

where $w_\infty = \mathrm{sgn}(-m)$*, whereas* $w_2 = -1$ *if* $m \equiv 1, 3, 11, 13 \pmod{16}$*, and* $w_2 = +1$ *otherwise.*
(ii) *Let* a, b *be integers satisfying* $b^2(b^2 - a^2) \neq 0$*. Then, the elliptic curve* $E_{b^2(b^2-a^2)} : y^2 = x^3 - b^2(b^2 - a^2)x$ *has an integral point* $(b^2, \pm ab^2)$*.*

Proof. (i) It follows from [BS66, (10), (13)], and (ii) can be verified by a direct calculation. □

We recall the method of descent via two-isogeny [Sil09, Theorem X.4.9]. Let M_K^0 and M_K^∞ be the set of finite places and infinite places of a number field K, E'_m be an elliptic curve defined by the equation $y^2 = x^3 + 4mx$, $\phi : E_m \to E'_m$ be a 2-isogeny defined by

$$\phi(x, y) \longrightarrow \left(\frac{y^2}{x^2}, \frac{-y(m + x^2)}{x^2}\right),$$

and ϕ' be its dual isogeny. Then, for $S = M_{\mathbf{Q}}^\infty \cup \{v \in M_{\mathbf{Q}}^0 : v \mid 2m\}$, we have

$$\mathrm{Sel}_\phi(E_m/\mathbf{Q}) \subset H^1(\mathbf{Q}, E_m[\phi], S),$$

where $H^1(\mathbf{Q}, E_m[\phi], S) \subset H^1(\mathbf{Q}, E_m[\phi])$ is the set of cocycles unramified outside S. For

$$\mathbf{Q}(S, 2) := \left\{ x \in \frac{\mathbf{Q}^\times}{(\mathbf{Q}^\times)^2} : \mathrm{ord}_v(x) = 0 \text{ for all } v \notin S \right\},$$

there is an isomorphism $\iota : \mathbf{Q}(S, 2) \to H^1(\mathbf{Q}, E_m[\phi], S)$ defined by $\iota(d)(\sigma) := d^\sigma / d$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. We note that $E_m[\phi] \cong \mathbf{Z}/2\mathbf{Z}$ as a $G_{\mathbf{Q}}$-module. Let $\mathrm{WC}(E/\mathbf{Q})$ be the Weil–Châtelet group of the elliptic curve $E/\mathbf{Q}$. Then there is a map

$$\begin{aligned} &\mathbf{Q}(S, 2) \overset{\iota}{\cong} H^1(\mathbf{Q}, E_m[\phi], S) \to \mathrm{WC}(E_m/\mathbf{Q}), \\ &d \to C_d(w, z) : dw^2 = d^2 + 4mz^4, \end{aligned}$$

and for $d \in \mathbf{Q}(S, 2)$, $\iota(d) \in \mathrm{Sel}_\phi(E_m/\mathbf{Q})$ if and only if the homogeneous space C_d is locally trivial for all $p \in S$. That is,

$$\begin{aligned} &\{d \in \mathbf{Q}(S, 2) : C_d(\mathbf{Q}_p) \neq \varnothing \text{ for all } p \in S\} \\ &\quad \overset{\iota}{\cong} \mathrm{Sel}_\phi(E_m/\mathbf{Q}). \end{aligned}$$

We simply write $d \in \mathrm{Sel}_\phi(E_m/\mathbf{Q})$ for $\iota(d) \in \mathrm{Sel}_\phi(E_m/\mathbf{Q})$, and denote by C'_d the homogeneous space of E'_m for $d \in \mathbf{Q}(S, 2)$.

Proposition 2.2. *Let* $E = E_{pq}$ *and* $E' = E'_{pq}$ *for some primes* p *and* q*.*
(i) *If* $pq \not\equiv \pm 1 \pmod 8$*, then* $\mathbf{Z}/2\mathbf{Z} \leq \mathrm{Sel}_\phi(E/\mathbf{Q}) \leq (\mathbf{Z}/2\mathbf{Z})^2$*.*
(ii) *If one of* p *and* q *is not equivalent to* 1 *modulo* 4*, then* $\mathbf{Z}/2\mathbf{Z} \leq \mathrm{Sel}_{\phi'}(E'/\mathbf{Q}) \leq (\mathbf{Z}/2\mathbf{Z})^2$*.*

Proof. (i) By previous arguments, we know that

$$\mathbf{Q}(S, 2) = \{\pm 1, \pm 2, \pm p, \pm q, \pm 2p, \pm 2q, \pm pq, \pm 2pq\},$$

and $C_d : dw^2 = d^2 + 4pqz^4$. By [Sil09, Proposition X.4.9], we have $pq \in \mathrm{Sel}_\phi(E/\mathbf{Q})$. The negative $d \in \mathbf{Q}(S, 2)$ is not in $\mathrm{Sel}_\phi(E/\mathbf{Q})$ because $C_d(\mathbf{R})$ is empty.

Let (W, Z) be a $\mathbf{Q}_2$-point of $C_2 : w^2 = 2 + 2pqz^4$. We may assume that $W \in 2\mathbf{Z}_2$ and $Z \in \mathbf{Z}_2$. If $pq \not\equiv \pm 1 \pmod 8$, then $W^2 \equiv 2 + 2pqZ^4 \pmod 8$ does not have a solution. Hence, if $pq \not\equiv \pm 1 \pmod 8$, then $2 \notin \mathrm{Sel}_\phi(E/\mathbf{Q})$. Consequently, $\langle pq \rangle \leq \mathrm{Sel}_\phi(E/\mathbf{Q}) \leq \{1, p, q, pq, 2p, 2q\}$ which proves (i).

(ii) We note that the homogeneous space C'_d of E' is defined by the equation $dw^2 = d^2 - pqz^4$. As in (i), we have $-pq \in \mathrm{Sel}_{\phi'}(E'_{pq}/\mathbf{Q})$. We consider $C'_{-1} : w^2 + 1 = pqz^4$, and let (W, Z) be a $\mathbf{Z}_p$-point of C'_{-1}. As $W^2 + 1 \equiv 0 \pmod p$, there is no $\mathbf{Q}_p$-point in C'_{-1} when $p \not\equiv 1 \pmod 4$. Similarly, if $q \not\equiv 1 \pmod 4$, then $C'_{-1}(\mathbf{Q}_q) = \varnothing$. Hence, $-1 \notin \mathrm{Sel}_{\phi'}(E'/\mathbf{Q})$ if one of p, q is not equivalent to 1 modulo 4.

We consider $C'_{-2} : 2w^2 + 4 = pqz^4$. We may assume that a $\mathbf{Q}_2$-point (Z, W) of C'_{-2} satisfies $W \in \mathbf{Z}_2$ and $Z \in 2\mathbf{Z}_2$. As the equation $2W^2 + 4 \equiv 0 \pmod{16}$ does not have a solution, $-2 \notin \mathrm{Sel}_{\phi'}(E'/\mathbf{Q})$. Similarly, $C'_2(\mathbf{Q}_2)$ does not have a solution because $2W^2 - 4 \not\equiv 0 \pmod{16}$. Therefore, $2 \notin \mathrm{Sel}_{\phi'}(E'/\mathbf{Q})$.

Consequently, if one of p and q is not equivalent to 1 modulo 4,

$$\begin{aligned} \langle -pq \rangle &\leq \mathrm{Sel}_{\phi'}(E'/\mathbf{Q}) \\ &\leq \{1, \pm p, \pm q, -pq, \pm 2p, \pm 2q, \pm 2pq\}. \end{aligned}$$

Let $A = \{1, \pm p, \pm q, -pq, \pm 2p, \pm 2q, \pm 2pq\}$. Then, all the possible groups between A and $\{1, -pq\}$ as sets have order bounded by 4. □

Theorem 2.3. *There are infinitely many elliptic curves* E *such that* $w_E = +1$ *and*

$$\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \leq E(\mathbf{Q}) \leq \mathbf{Z} \times \mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}.$$

That is, under the parity conjecture, there are infinitely many elliptic curves whose Mordell–Weil groups are exactly $\mathbf{Z} \times \mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$*.*

Proof. There is a natural $\mathbf{Q}$-isomorphism between $E_{t^4 s} \cong E_s$ for $t, s \in \mathbf{Q}$, which is defined by $(x, y) \to (\frac{x}{t^2}, \frac{y}{t^3})$. When $b^4(b^4 - a^2) \neq 0$, $E_{b^4(b^4-a^2)} \cong E_{(b^4-a^2)}$ has a rational point of infinite order by Lemma 2.1 (ii). We use Lemma 1.2 with $A = B =$

1, $g = 16$, $i = 15$, $j = 3$, and $f(n) = 2n^2$. As $m = 1$ satisfies $2m^2 \equiv i + j \pmod{16}$, there are infinitely many integers b such that $2b^2 = p + q$ and $p \equiv 15, q \equiv 3 \pmod{16}$. Then for $a = \frac{p-q}{2}$,

$$b^4 - a^2 = (b^2 + a)(b^2 - a) = pq.$$

The torsion subgroup of E_{pq} is $\mathbf{Z}/2\mathbf{Z}$. As $pq \not\equiv \pm 1 \pmod 8$ and $p, q \equiv 3 \pmod 4$,

$$\begin{aligned} &2 + \mathrm{rank}_{\mathbf{Z}}(E_{pq}(\mathbf{Q})) \\ &\quad \le \dim_{\mathbf{F}_2}(\mathrm{Sel}_\phi(E_{pq}/\mathbf{Q})) + \dim_{\mathbf{F}_2}(\mathrm{Sel}_{\phi'}(E'_{pq}/\mathbf{Q})) \\ &\quad \le 4, \end{aligned}$$

by [Sil09, Proposition X.4.2, X.4.7] and Proposition 2.2. Finally $w_{E_{pq}} = +1$, by Lemma 2.1 (i). □

3. 3-Torsion case. In this section we consider elliptic curves $A_m : y^2 = x^3 + m^2$. We recall that if $m \neq 1$ is a cube-free integer, then the torsion subgroup of $A_m(\mathbf{Q})$ is $\mathbf{Z}/3\mathbf{Z}$ (see [Sil09, Exercise 10.19]). As in Section 2, we have the following lemma.

Lemma 3.1. (i) *If m is square-free and prime to 6, then $w_{A_m} = w_3 \prod_{p \mid m} w_p$, where*

$$\begin{cases} w_3 = -1 & \text{if } m^2 \equiv -2 \pmod 9, \\ w_3 = +1 & \text{otherwise.} \end{cases}$$

$$\begin{cases} w_p = -1 & \text{if } p \mid m, \text{ and } p \equiv 2 \pmod 3, \\ w_p = +1 & \text{otherwise.} \end{cases}$$

(ii) *Let a, b be nonzero integers satisfying $a(a^2 - b^2) \neq 0$. Then the elliptic curve $A_{a(a^2-b^2)} : y^2 = x^3 + a^2(a^2 - b^2)^2$ has an integral point $(-a^2 + b^2, \pm(a^2 b - b^3))$.*

Proof. The first part can be easily deduced from [Liv95, §9, Theorem]. The second part can be verified by a direct calculation. □

We recall the method of descent via 3-isogeny [CP09, Definition 1.3]. Let $K = \mathbf{Q}(\sqrt{-3})$, A'_m be the elliptic curve defined by the equation $y^2 = x^3 - 27m^2$, $\phi : A_m \to A'_m$ be an isogeny defined by

$$\phi : (x, y) \longrightarrow \left(\frac{x^3 + 4m^2}{x^2}, \frac{y(x^3 - 8m^2)}{x^3} \right),$$

and ϕ' be its dual isogeny. There are 3-descent maps

$$\frac{A_m(\mathbf{Q})}{\phi' A'_m(\mathbf{Q})} \xrightarrow{\alpha} \mathbf{Q}(S, 3) \text{ and } \frac{A'_m(\mathbf{Q})}{\phi A_m(\mathbf{Q})} \xrightarrow{\alpha'} K(S, 3),$$

where $S = M^\infty_{(\cdot)} \cup \{v \in M^0_{(\cdot)} : v \mid 6m\}$ for $(\cdot) = K$ or $\mathbf{Q}$. The map α is defined by

$$\alpha(O) = 1, \ \alpha(0, m) = \frac{1}{2m}, \text{ and } \alpha(x, y) = y - m.$$

We note that α' is defined by $\alpha'(x, y) = y - 3m\sqrt{-3}$, and the images of α' are in $K_N(S, 3) = \{\overline{u} \in K(S, 3) : \mathrm{Nm}_{K/\mathbf{Q}}(u) \in (\mathbf{Q}^\times)^3\}$. By [CP09, Proposition 2.2], we have $|\mathrm{im}\,\alpha||\mathrm{im}\,\alpha'| = 3^{\mathrm{rank}\, A_m(\mathbf{Q})+1}$. For all $d \in \mathbf{Q}(S, 3)$, d is in the image of α if and only if $C_d(\mathbf{Q}) \neq \varnothing$, however, we do not calculate homogeneous spaces C_d directly. Instead, we will find cubics C satisfying $d \in \mathrm{im}\,\alpha$ if and only if $C(\mathbf{Q}) \neq \varnothing$. After that, we will show that the cubic C does not have $\mathbf{Q}_p$-points in certain cases, which gives an upper bound of $|\mathrm{im}\,\alpha|$. Similarly, we will obtain an upper bound of $|\mathrm{im}\,\alpha'|$.

Lemma 3.2. *Let $p, q \ge 5$ be primes, and $A_{pq} : y^2 = x^3 + p^2 q^2$ be elliptic curves.*

(i) *For any $\overline{d} \in \mathbf{Q}(S, 3)$, let d be the unique cube-free representative of $\overline{d}$, and $d = d_1^2 d_2$ be the unique representation such that d_i are square-free and coprime. Then, $\overline{d}$ is in the image of α if and only if the cubic*

$$C_{d_1, d_2, \frac{2pq}{d_1 d_2}} : d_1 X^3 + d_2 Y^3 + \frac{2pq}{d_1 d_2} Z^3 = 0, \tag{2}$$

has a nontrivial rational point. We will denote $C_{d_1, d_2, \frac{2pq}{d_1 d_2}}$ by $(d_1, d_2, \frac{2pq}{d_1 d_2})$. Moreover, we have $\mathrm{im}\,\alpha \le \langle 2, p, q \rangle$.

(ii) *Let $u_1, u_2, u_3 \nmid 3$. The cubic $C : u_1 X^3 + u_2 Y^3 + u_3 Z^3 = 0$, which is denoted by (u_1, u_2, u_3), has a $\mathbf{Q}_3$-point if and only if $u_i \equiv \pm u_j \pmod 9$ for some $i \neq j$.*

Proof. By [CP09, Theorem 3.1.(1)], $\overline{d} \in \mathrm{im}\,\alpha$ if and only if the cubic

$$dX^3 + \frac{1}{d} Y^3 + 2pqZ^3 = 0$$

has a nontrivial rational solution. Replacing Y by $d_1 d_2 Y$, this cubic has a nontrivial rational solution if and only if (2) has. If $d \in \mathrm{im}\,\alpha$, then $d_1 d_2$ should divide $2pq$, by [CP09, Theorem 3.1.(3)]. Hence, (i) follows, whereas (ii) is exactly [CP09, Lemma 5.9.(1)]. □

Lemma 3.3. *Let $p, q \ge 5$ be primes, $A'_{pq} : y^2 = x^3 - 27p^2 q^2$ be elliptic curves, and τ be a unique nontrivial element in* $\mathrm{Gal}(K/\mathbf{Q})$.

(i) *For $\overline{d} \in K_N(S, 3)$, there is a $v = v_1 + v_2\sqrt{-3}$ such that $v_i \in \mathbf{Q}$ and $d = v^2 \tau(v)$. Then, $d \in \mathrm{im}\,\alpha'$ if and only if the cubic*

$$(3)\qquad 2v_2X^3 - 6v_1Y^3 + \frac{6pq}{v_1^2+3v_2^2}Z^3 + 6v_1X^2Y - 18v_2XY^2 = 0,$$

has a nontrivial rational solution.

(ii) *For* $\overline{d} \in \operatorname{im}\alpha'$, *there exists an ideal* $\mathfrak{a}, \mathfrak{q}$ *of* O_K *such that* $dO_K = \mathfrak{a}^2\tau(\mathfrak{a})\mathfrak{q}^3$ *and* $\mathrm{Nm}_{K/\mathbf{Q}}(\mathfrak{a})$ *is a cube-free divisor of* $2pq$ *divisible only by primes that are split in* $K/\mathbf{Q}$.

(iii) *The cubic defined by* (3) *has a* $\mathbf{Q}_2$*-point if and only if the class* $\tau(v)/v$ *is a cube in* $\mathbf{F}_{2^2}$.

Proof. [CP09, Proposition 4.1.(1), Corollary 4.3, Lemma 6.5], respectively. □

Proposition 3.4. *Let* $p, q \geq 5$ *be primes, and* $A_{pq} : y^2 = x^3 + p^2q^2$ *be elliptic curves.*

(i) *If* $p, q \equiv \pm 2 \pmod 9$, *then* $\mathbf{Z}/3\mathbf{Z} \leq \operatorname{im}\alpha \leq (\mathbf{Z}/3\mathbf{Z})^2$.

(ii) *If* $p \equiv 2 \pmod 3$ *and* $q \equiv 1 \pmod 3$, *then* $0 \leq \operatorname{im}\alpha' \leq \mathbf{Z}/3\mathbf{Z}$.

Proof. (i) By Lemma 3.2 (i),

$$\operatorname{im}\alpha = \left\{ d \in \mathbf{Q}(S,3) : d_1d_2 \mid 2pq \text{ and } \left(d_1, d_2, \frac{2pq}{d_1d_2}\right) \text{ has a nontrivial rational solution} \right\}.$$

As $\operatorname{im}\alpha$ is a group, the cubic $(d_1, d_2, \frac{2pq}{d_1d_2})$ has a nontrivial rational solution if and only if $(d_2, d_1, \frac{2pq}{d_1d_2})$ is. There are 14 cubics $(d_1, d_2, \frac{2pq}{d_1d_2})$, up to exchange of d_1 and d_2. Among them, $(1, 1, 2pq)$ and $(1, 2pq, 1)$ have a nontrivial rational solution, namely, $[1, -1, 0]$ and $[1, 0, -1]$, respectively. Hence, $\overline{1}, \overline{2pq} \in \operatorname{im}\alpha$. There are 4-sets of cubics, namely,

$$\{(2,1,pq), (1,pq,2), (pq,2,1)\},$$
$$\{(q,1,2p), (1,2p,q), (2p,q,1)\},$$
$$\{(p,2,q), (2,q,p), (q,p,2)\},$$
$$\{(p,1,2q), (1,2q,p), (2q,p,1)\}.$$

One cubic of the set is in $\operatorname{im}\alpha$ if and only if all cubics in the set are in $\operatorname{im}\alpha$, because $\overline{2pq} \in \operatorname{im}\alpha$. Hence, it suffices to check the solubility of one cubic for each set.

By Lemma 3.2 (ii), the cubic $(2, 1, pq)$ has a $\mathbf{Q}_3$-solution if and only if $pq \equiv \pm 1, \pm 2 \pmod 9$. Hence, $\overline{4} \notin \operatorname{im}\alpha$ if $pq \not\equiv \pm 1, \pm 2 \pmod 9$. Similarly, we can show the following, by considering cubics $(q, 1, 2p)$, $(p, 2, q)$, and $(p, 1, 2q)$:

- $\overline{q^2}$ does not lie in $\operatorname{im}\alpha$ when $q \not\equiv \pm 1$, $p \not\equiv \pm 5$, and $q \not\equiv \pm 2p \pmod 9$,
- $\overline{2p^2}$ does not lie in $\operatorname{im}\alpha$ when $p \not\equiv \pm 2$, $q \not\equiv \pm 2$, and $p \not\equiv \pm q \pmod 9$,
- $\overline{p^2}$ does not lie in $\operatorname{im}\alpha$ when $p \not\equiv \pm 1$, $q \not\equiv \pm 5$, and $p \not\equiv \pm 2q \pmod 9$.

If $p, q \equiv \pm 2 \pmod 9$, then $\overline{4}, \overline{p^2}, \overline{q^2}$ do not lie in $\operatorname{im}\alpha$. Therefore, $\mathbf{Z}/3\mathbf{Z} \leq \operatorname{im}\alpha \leq (\mathbf{Z}/3\mathbf{Z})^2$.

(ii) By Lemma 3.3 (ii), if $\overline{d} \in \operatorname{im}\alpha'$, then there exists a such that $d = \zeta_3^i a^2\tau(a)$ and $\mathrm{Nm}_{K/\mathbf{Q}}(a) \mid 2pq$ is divisible only by primes that split in $K/\mathbf{Q}$. In this case, $\mathrm{Nm}_{K/\mathbf{Q}}(a) \mid q$. Therefore, $\operatorname{im}\alpha' \leq \langle \zeta_3, q'^2\overline{q'} \rangle$, where q' is a prime element of K satisfying $\mathrm{Nm}_{K/\mathbf{Q}}(q') = q$.

We consider $d = \zeta_3$. For $v = \zeta_3$, we have $\zeta_3 = v^2\tau(v)$ and $\tau(v)/v \neq 1$ in $\mathbf{F}_{2^2}$. Therefore, the cubic (3) for $v = \zeta_3$ does not have a solution in $\mathbf{Q}_2$ by Lemma 3.3 (iii). Consequently, when $p \equiv 1$ and $q \equiv 2 \pmod 3$, $\operatorname{im}\alpha' \leq \mathbf{Z}/3\mathbf{Z}$. □

Theorem 3.5. *There are infinitely many elliptic curves* E *such that* $w_E = +1$ *and*

$$\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z} \leq E(\mathbf{Q}) \leq \mathbf{Z} \times \mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}.$$

That is, under the parity conjecture, there are infinitely many elliptic curves whose Mordell–Weil groups are exactly $\mathbf{Z} \times \mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$.

Proof. When $a^3(a^6 - b^2) \neq 0$, the elliptic curve $A_{a^3(a^6-b^2)}$ has an integral point of infinite order by Lemma 3.1. We use Lemma 1.2 with $A = 27, B = 1$, $i = 2, j = 7$, and $f(n) = 2n^3$. As $2m^3 \equiv 27i + j \pmod 9$ has a solution $m = -1$, there are infinitely many integers a such that $a^3 = \frac{27p+q}{2}$, and $p \equiv 2$, and $q \equiv 7 \pmod 9$. Then for $b = \frac{27p-q}{2}$,

$$(a^6 - b^2) = (a^3 + b)(a^3 - b) = 27pq.$$

Therefore, there are infinitely many elliptic curves $A_{a^3 3^3 pq} \cong A_{pq}$ whose rank is at least 1, and $A_{pq}(\mathbf{Q})_{\mathrm{tor}} = \mathbf{Z}/3\mathbf{Z}$. By Proposition 3.4, $|\operatorname{im}\alpha| \leq 3^2$ and $|\operatorname{im}\alpha'| \leq 3$ since $p \equiv 2$ and $q \equiv 7 \pmod 9$. By [CP09, Proposition 2.2], $|\operatorname{im}\alpha||\operatorname{im}\alpha'| = 3^{\mathrm{rank}_{\mathbf{Z}} A_{pq}(\mathbf{Q})+1}$. Hence, $1 \leq \mathrm{rank}(A_{pq}(\mathbf{Q})) \leq 2$, and $w_{A_{pq}} = +1$ by Lemma 3.1. □

Acknowledgments. Author thanks the referee for careful readings and valuable suggestions. Author is partially supported by Basic Science Research Program through National Research Foundation of Korea (NRF, 2019R1C1C1004264).

References

[BJ16] D. Byeon and K. Jeong, Infinitely many elliptic curves of rank exactly two, Proc. Japan Acad. Ser. A Math. Sci. **92** (2016), no. 5, 64–66.

[BJ17] D. Byeon and K. Jeong, Sums of two rational cubes with many prime factors, J. Number

Theory **179** (2017), 240–255.

[BS66] B. J. Birch and N. M. Stephens, The parity of the rank of the Mordell–Weil group, Topology **5** (1966), 295–299.

[CP09] H. Cohen and F. Pazuki, Elementary 3-descent with a 3-isogeny, Acta Arith. **140** (2009), no. 4, 369–404.

[DP15] A. Dujella and J. C. Peral, Elliptic curves with torsion group $\mathbf{Z}/8\mathbf{Z}$ or $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$, in *Trends in number theory*, Contemp. Math., 649, Amer. Math. Soc., Providence, RI, 2015, pp. 47–62.

[Duj] A. Dejulla, Infinite families of elliptic curves with high rank and prescribed torsion, available at `https://web.math.pmf.unizg.hr/~duje/tors/generic.html`.

[Liv95] E. Liverance, A formula for the root number of a family of elliptic curves, J. Number Theory **51** (1995), no. 2, 288–305.

[Sil09] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, 106, Springer, Dordrecht, 2009.