Functiones et Approximatio
56.1 (2017), 25–37
doi: 10.7169/facm/1585

ELLIPTIC CURVES WITH RANK 0 OVER NUMBER FIELDS

Pallab Kanti Dey

Abstract: Let $E : y^2 = x^3 + bx$ be an elliptic curve for some nonzero integer b. Also consider K be a number field with $4 \nmid [K : \mathbb{Q}]$. Then in this paper, we obtain a necessary and sufficient condition for E having rank 0 over K.

Keywords: elliptic curve, number field, Diophantine equation.

1. Introduction

Let E be an elliptic curve defined over a number field K. By Mordell-Weil's Theorem, it is well-known that the set of all K-rational points $E(K)$ is a finitely generated Abelian group. Hence, by the structure theorem of finitely generated Abelian groups, we can write

$$E(K) \cong T \oplus \mathbb{Z}^r,$$

for some non-negative integer r which is called the *rank* of E over K and T is the torsion subgroup. Sometimes we may write $T = E(K)_{tors}$.

In 1994, Merel [6] has proved that for every integer d, there is a constant $B(d)$ such that for every elliptic curve E/K with $[K : \mathbb{Q}] = d$ we have $|E(K)_{tors}| \leqslant B(d)$. The bound in Merel's proof is not effective (it relies on Falting's theorem). However he proved the following. If p is the largest prime divisor of $|E(K)_{tors}|$ for $[K : \mathbb{Q}] = d > 1$, then $p \leqslant d^{3d^2}$. This bound was later improved by Oesterle to $(1 + 3^{\frac{d}{2}})$ [1994, unpublished!].

Finding the rank of a given elliptic curve is a very difficult problem compared to that of the torsion group. If $E : y^2 = x^3 + bx$ is an elliptic curve over $\mathbb{Q}$, then, from [7], it is well-known that

$$\mathrm{Rank}(E(\mathbb{Q})) \leqslant 2\beta(2b) - 1$$

2010 Mathematics Subject Classification: primary: 14H52; secondary: 11R04

where $\beta(2b)$ denote the number of distinct primes $p|2b$. If b is a prime number, then,

$$\text{Rank}(E(\mathbb{Q})) \leqslant 2.$$

In [5], Kudo and Motose computed the rank of an elliptic curve $y^2 = x^3 - px$ over $\mathbb{Q}$ for Fermat prime p and Mersenne prime p. Also Bremner and Casssels [2] computed that for all odd prime p with $p \equiv 5 \pmod 8$, the rank of $y^2 = x^3 + px$ over $\mathbb{Q}$ is 1. In [3], for odd prime p, the rank of elliptic curves of the form $y^2 = x^3 - px$ over $\mathbb{Q}$ has been studied. Also in [4], the rank of an elliptic curve $y^2 = x^3 + pqx$ over $\mathbb{Q}$ was considered with p and q are primes. In [9], Spearman proved that the rank of an elliptic curve $y^2 = x^3 - px$ over $\mathbb{Q}$ is 2 for all primes p with $p = u^4 + v^4$ for some integers u and v. In [10], the rank has been computed for an elliptic curve of the form $y^2 = x^3 - 2px$ over $\mathbb{Q}$ with p is prime.

In this paper, we consider the rank of a class of elliptic curves of the form $y^2 = x^3 + bx$ for some nonzero integer b over a number field K with $[K : \mathbb{Q}] \not\equiv 0 \pmod 4$. More precisely, let K be a number field with its degree $[K : \mathbb{Q}]$ is not divisible by 4 and let $E : y^2 = x^3 + bx$ be an elliptic curve for some nonzero integer b. Then we give a necessary and sufficient condition for E having rank 0 over K.

Theorem 1. *Let K be a number field with $[K : \mathbb{Q}] \equiv 2 \pmod 4$ and b be a nonzero integer with $b \neq 4m^4$ for any integer m. Then the elliptic curve $E : y^2 = x^3 + bx$ has rank 0 over K if and only if the Diophantine equation $X^4 + bY^4 = Z^2$ has only trivial solutions in K.*

Theorem 2. *Let K be a number field of odd degree and b be a nonzero integer. Then the elliptic curve $E : y^2 = x^3 + bx$ has rank 0 over K if and only if the Diophantine equation $X^4 + bY^4 = Z^2$ has only trivial solutions in K.*

Remark 1. The statement of Theorem 1 is not true for $b = 4m^4$ for any integer m. In this case, the elliptic curve $E : y^2 = x^3 + 4m^4x$ is isomorphic to the curve $E_4 : y^2 = x^3 + 4x$. The rank of E_4 over $\mathbb{Q}(\sqrt{2})$ is 0. Hence the rank of E over $\mathbb{Q}(\sqrt{2})$ is 0. But the Diophantine equation $x^4 + 4m^4y^4 = z^2$ has a nontrivial solution $(\sqrt{2}m, 1, 2\sqrt{2}m^2)$ over $\mathbb{Q}(\sqrt{2})$.

In order to prove the above results, we need to compute the torsion subgroup of E over a number field K with $[K : \mathbb{Q}] \not\equiv 0 \pmod 4$. Indeed, we prove the following propositions.

Proposition 1. *Let $E : y^2 = x^3 + bx$ be an elliptic curve for some 4-th power-free integer b and let $E(K)$ be the Elliptic curve group over K, where $[K : \mathbb{Q}]$ is odd. If T is the torsion subgroup of $E(K)$, then T is isomorphic to one of the following groups.*

1. *$T \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, if $-b$ is a square.*
2. *$T \cong \mathbb{Z}/4\mathbb{Z}$, if $b = 4$.*
3. *$T \cong \mathbb{Z}/2\mathbb{Z}$, otherwise.*

Proposition 2. *Let $E: y^2 = x^3 + bx$ be an elliptic curve for some 4-th powerfree integer b and let $E(K)$ be the Elliptic curve group over K, where $[K:\mathbb{Q}] \equiv 2 \pmod 4$. If T is the torsion subgroup of $E(K)$, then T is isomorphic to one of the following groups.*

1. $T \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \begin{cases} \textit{if } b = 4 \textit{ and } i \in K, \\ \textit{or } b = -1 \textit{ and } i \in K. \end{cases}$
2. $T \cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}, \begin{cases} \textit{if } b = -1 \textit{ and } i \notin K, \\ \textit{or } b = t^2 \textit{ for some nonzero integer } t(\neq \pm 2) \textit{ and } i \in K, \\ \textit{or } -b \textit{ is a square}, \\ \textit{or } \sqrt{-b} \in K. \end{cases}$
3. $T \cong \mathbb{Z}/4\mathbb{Z}, \begin{cases} \textit{if } b = 4 \textit{ and } i \notin K, \\ \textit{or } b = t^2 \textit{ for some nonzero integer } t(\neq \pm 2) \\ \textit{and } \sqrt{2t} \in K. \end{cases}$
4. $T \cong \mathbb{Z}/2\mathbb{Z}$, *otherwise.*

Remark 2. From Propositon 1 and Propositon 2, it is clear that the largest prime divisor of $|E(K)_{tors}|$ is 2 for all elliptic curves $E: y^2 = x^3 + bx$ and for all number field K with $4 \nmid [K:\mathbb{Q}]$.

2. Preliminaries

To prove Theorem 1 we need to build up some tools.

Throughout this article by an elliptic curve E we mean $E: y^2 = x^3 + bx$ for some nonzero integer b. For any given prime p, $\bar{E}(\mathbb{F}_p)$ denote the elliptic curve over $\mathbb{F}_p$ after reducing modulo p on E.

Proposition 3 ([11]). *For any prime p, let $|\bar{E}(\mathbb{F}_p)| = p + 1 - a$ with $|a| \leqslant 2\sqrt{p}$. Let the quadratic equation $X^2 - aX + p = (X - \alpha)(X - \beta)$ for some complex numbers α, β. Then,*

$$|\bar{E}(\mathbb{F}_{p^n})| = p^n + 1 - (\alpha^n + \beta^n)$$

for all $n \geqslant 1$.

Corollary 1. *Let $E: y^2 = x^3 + bx$ be an elliptic curve, where b is a nonzero integer. Let $p \equiv 3 \pmod 4$ be an odd prime such that $p \nmid \Delta$ where Δ is the discriminant of E. Then, we have*

$$|\bar{E}(\mathbb{F}_{p^n})| = \begin{cases} (p^n + 1), & \textit{if } n \textit{ is odd} \\ (p^{\frac{n}{2}} + 1)^2, & \textit{if } n \equiv 2 \pmod 4. \end{cases}$$

Proof. By Hasse's theorem [11], $|\bar{E}(\mathbb{F}_p)| = p + 1 - a$, where $|a| \leqslant 2\sqrt{p}$. In this case, $a = 0$ as $p \equiv 3 \pmod 4$. Consider,

$$X^2 + p = (X - i\sqrt{p})(X + i\sqrt{p}).$$

If we set $\alpha = i\sqrt{p}$ and $\beta = -i\sqrt{p}$, then, by Proposition 3, we have,

$$|\bar{E}(\mathbb{F}_{p^n})| = \begin{cases} (p^n + 1), & \text{if } n \text{ is odd} \\ (p^{\frac{n}{2}} + 1)^2, & \text{if } n \equiv 2 \pmod 4). \end{cases} \blacksquare$$

Proposition 4. *Let $E : y^2 = x^3 + bx + c$ be an elliptic curve for some integers b and c. Let T be the torsion subgroup of $E(K)$ for some number field K. Let $\mathcal{O}_K$ be the ring of integers in K. Also let $\mathcal{P}$ be a prime ideal lying above p in $\mathcal{O}_K$ for an odd prime p. If E has good reduction at $\mathcal{P}$, then let ϕ be the reduction modulo $\mathcal{P}$ map on T. That is, the reduction map $\phi : T \longrightarrow \bar{E}(\mathcal{O}_K/\mathcal{P})$ is defined as $P = (x, y) \to \bar{P} = (\bar{x}, \bar{y})$ if $P \neq \mathcal{O}$ and $\mathcal{O} \to \bar{\mathcal{O}}$. Then, the reduction map ϕ is an injective homomorphism except finitely many prime ideals $\mathcal{P}$.*

Proof. Any elment in K can be wriiten as $t^{-1}x$, where $t \in \mathbb{Z}$ and $x \in \mathcal{O}_K$. Now we have only finitely many prime ideals containing t. Since by Merel's theorem [6] T is finite, we have only finite collection of prime ideals which contains denominators of coordinates of any nontrivial point in T. Except these finitely many prime ideals we consider here reduction modulo $\mathcal{P}$ homomorphism whenever E has good reduction at $\mathcal{P}$.

It is given that ϕ is a reduction modulo $\mathcal{P}$ map. We need to prove that ϕ is an injective homomorphism. First we note that for a point Q on $E(K)$, we have,

$$\overline{-Q} = \phi(-Q) = \phi(x, -y) = \overline{(x, -y)} = (\overline{x}, -\overline{y}) = -\overline{Q}.$$

To show ϕ is a homomorphism, it is enough to prove that for the points Q_1, Q_2 and Q_3 in T,

$$\text{if } Q_1 \oplus Q_2 \oplus Q_3 = \mathcal{O}, \text{ then } \bar{Q_1} \oplus \bar{Q_2} \oplus \bar{Q_3} = \bar{\mathcal{O}},$$

since it implies that

$$\phi(Q_1 \oplus Q_2) = \phi(-Q_3) = -\bar{Q_3} = \bar{Q_1} \oplus \bar{Q_2} = \phi(Q_1) \oplus \phi(Q_2).$$

If any of Q_1, Q_2 or Q_3 equals $\mathcal{O}$, then the result follows from the fact that negatives goes to negatives. So we may assume that Q_1, Q_2 and Q_3 are not equal to $\mathcal{O}$. Let $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ and $P_3 = (x_3, y_3)$, where x_i, y_i's are in K.

From the definition of the group law on E, the condition $Q_1 \oplus Q_2 \oplus Q_3 = \mathcal{O}$ is equivalent to saying that Q_1, Q_2 and Q_3 lie on a line. Let

$$y = \lambda x + k$$

be the line passing through Q_1, Q_2 and Q_3 (If two or three of the points coincide, then the line has to satisfy certain tangency conditions).

From the addition formula [8], we get

$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = \lambda x_3 + k.$$

Since x_1, x_2, x_3 and y_3 are elements of K, we have $\lambda, k \in K$. Therefore, except for finitely many prime ideals $\mathcal{P}$, we can reduce λ and k modulo $\mathcal{P}$.

Substituting the equation of the line into the equation of the cubic, we know that the equation

$$x^3 + bx + c - (\lambda x + k)^2 = 0$$

has x_1, x_2 and x_3 as its roots. In other words, we have the factorization

$$x^3 + bx + c - (\lambda x + k)^2 = (x - x_1)(x - x_2)(x - x_3).$$

This is the relation that ensures that $Q_1 \oplus Q_2 \oplus Q_3 = \mathcal{O}$, regardless of whether or not the points are distinct.

Reducing this last equation modulo $\mathcal{P}$, we obtain

$$x^3 + \bar{b}x + \bar{c} - (\bar{\lambda}x + \bar{k})^2 = (x - \bar{x_1})(x - \bar{x_2})(x - \bar{x_3}).$$

Also, we can reduce the equations $y_i = \lambda x_i + k$ to get

$$\bar{y_i} = \bar{\lambda}\bar{x_i} + \bar{k}, \quad i = 1, 2, 3.$$

This means that the line $y = \bar{\lambda}x + \bar{k}$ intersects the curve $\bar{E} : y^2 = x^3 + \bar{b}x$ at the three points $\bar{Q_1}, \bar{Q_2}$ and $\bar{Q_3}$. Further if two of the points among $\bar{Q_1}, \bar{Q_2}$ and $\bar{Q_3}$ are the same, say, $\bar{Q_1} = \bar{Q_2}$, then the line is tangent to $\bar{E}$ at $\bar{Q_1}$; and similarly, if all three points coincide, then the line has a triple order contact with $\bar{E}$. Therefore,

$$\bar{Q_1} \oplus \bar{Q_2} \oplus \bar{Q_3} = \bar{\mathcal{O}},$$

which completes the proof that ϕ is a homomorphism.

A nonzero point $(x, y) \in T$ is sent to the reduced point $(\bar{x}, \bar{y}) \in \bar{E}(\mathcal{O}_K/\mathcal{P})$, and that reduced point is not $\bar{\mathcal{O}}$. So the kernel of the reduction map consists only of $\mathcal{O}$. Hence the map is injective. ∎

Now consider $E : y^2 = x^3 + bx$ be an elliptic curve with discriminant Δ, where b is a nonzero integer. Let T denote the torsion subgroup in $E(K)$ where $[K : \mathbb{Q}] = n$ for some integer n with $n \not\equiv 0 \pmod 4$. Then we have the following lemmas.

Lemma 1. *For any odd prime q, q does not divide $|T|$.*

Proof. Since $4 \nmid n$, we seperate two cases as n is odd and $n \equiv 2 \pmod 4$.

Case 1: n is odd. Suppose q divides $|T|$. Then, by Dirichlet's theorem on primes in arithmetic progression [1], we can choose a prime p with $p \nmid \Delta$ and $p \equiv 2q(q+2) + 1 \pmod{4q}$ as $(2q(q+2)+1, 4q) = 1$. Let $p\mathcal{O}_K = \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2} \ldots \mathcal{P}_r^{e_r}$ be the ideal decomposition in $\mathcal{O}_K$ where $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_r$ are prime ideals in $\mathcal{O}_K$ lying above p and e_i's are ramification index for $\mathcal{P}_i$'s. Also, we have $\sum_{i=1}^{r} e_i f_i = n$ where f_i's are residual degree for $\mathcal{P}_i$'s.

Since n is odd, there exists a f_i which is an odd integer for some i. Let $\mathcal{P}_i$ be the corresponding prime ideal and consider the reduction map modulo $\mathcal{P}_i$. Since $|\mathcal{O}_K/\mathcal{P}_i| = p^{f_i}$ and f_i is odd, we have $|\bar{E}(\mathcal{O}_K/\mathcal{P}_i)| = p^{f_i} + 1$ by Corollary 1, as $p \equiv 3 \pmod 4$. Hence by Proposition 4, we conclude that $q \mid (p^{f_i} + 1)$. But we also have $p \equiv 1 \pmod q$ which implies $p^{f_i} + 1 \equiv 2 \pmod q$, which is a contradiction as $q \nmid 2$. Therefore, any odd prime q does not divide $|T|$.

Case 2: $n \equiv 2 \pmod 4$. Suppose q divides $|T|$. Then, by Dirichlet's theorem on primes in arithmetic progression [1], we can choose a prime p with $p \nmid \Delta$ and $p \equiv 2q(q+2)+1 \pmod{4q}$ as $(2q(q+2)+1, 4q) = 1$. Let $p\mathcal{O}_K = \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2}\dots\mathcal{P}_r^{e_r}$ be the ideal decomposition in $\mathcal{O}_K$ where $\mathcal{P}_1, \mathcal{P}_2, \dots, \mathcal{P}_r$ are prime ideals in $\mathcal{O}_K$ lying above p and e_i's are ramification index for $\mathcal{P}_i$'s. Also, we have $\sum_{i=1}^r e_i f_i = n$ where f_i's are residual degree for $\mathcal{P}_i$'s.

Since $n \equiv 2 \pmod 4$, we see that one of f_i's is either odd or $f_i \equiv 2 \pmod 4$. We consider the corresponding prime ideal $\mathcal{P}_i$ and the reduction map modulo $\mathcal{P}_i$. Since $|\mathcal{O}_K/\mathcal{P}_i| = p^{f_i}$, by Corollary 1, we have $|\bar{E}(\mathcal{O}_K/\mathcal{P}_i)| = p^{f_i}+1$ if f_i is odd and $|\bar{E}(\mathcal{O}_K/\mathcal{P}_i)| = (p^{\frac{f_i}{2}+1})^2$ if $f_i \equiv 2 \pmod 4$, as $p \equiv 3 \pmod 4$. Hence by Proposition 4, we conclude that $q \mid (p^t+1)$ for some integer t. But we also have $p \equiv 1 \pmod q$ which implies $p^t + 1 \equiv 2 \pmod q$, which is a contradiction as $q \nmid 2$. Therefore, any odd prime q does not divide $|T|$. ■

Lemma 2. *T does not have an element of order 8.*

Proof. As before, we have two cases.

Case 1: n is odd. Suppose T has an element of order 8. Then 8 divides $|T|$. By Dirichlet's theorem on primes in arithmetic progression [1], we can choose a prime p with $p \nmid \Delta$ and $p \equiv 3 \pmod 8$. Let $p\mathcal{O}_K = \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2}\dots\mathcal{P}_r^{e_r}$ be the ideal decomposition in $\mathcal{O}_K$ where $\mathcal{P}_1, \mathcal{P}_2, \dots, \mathcal{P}_r$ are prime ideals in $\mathcal{O}_K$ lying above p and e_i's are ramification index for $\mathcal{P}_i$'s. Also, we have $\sum_{i=1}^r e_i f_i = n$ where f_i's are residual degree for $\mathcal{P}_i$'s.

Since n is odd, we see that one of f_i's is odd. We consider the corresponding prime ideal $\mathcal{P}_i$ and the reduction map modulo $\mathcal{P}_i$. Since $|\mathcal{O}_K/\mathcal{P}_i| = p^{f_i}$ and f_i is odd, we have $|\bar{E}(\mathcal{O}_K/\mathcal{P}_i)| = p^{f_i}+1$ by Corollary 1, as $p \equiv 3 \pmod 4$. Hence by Proposition 4, we conclude that $8 \mid (p^{f_i}+1)$. But we also have $p \equiv 3 \pmod 8$ which implies $p^{f_i}+1 \equiv 4 \pmod 8$, which is a contradiction as $8 \nmid 4$. Therefore, T does not have any element of order 8.

Case 2: $n \equiv 2 \pmod 4$. First we want to understand the points of order 4 in T. Indeed, we have the following claim.

Claim 1. *If $P = (x, y)$ is a point of order 4 in T, then we have $x^2 = b$.*

By the duplication formula [8], we have

$$x(2P) = \frac{(x^2-b)^2}{4y^2}$$

and

$$y(2P) = \frac{(x^2-b)(x^4-4bx^2+b^2)}{8y^3}.$$

Since $P = (x, y)$ is of order 4 in T, we have $y(2P) = 0$ and hence we get,

$$(x^2-b)(x^4-4bx^2+b^2) = 0.$$

If $x^4 - 4bx^2 + b^2 = 0$, then $[\mathbb{Q}(x) : \mathbb{Q}] = 4$, as the polynomial $x^4 - 4bx^2 + b^2$ is an irreducible polynomial over $\mathbb{Q}$. Further since $n \equiv 2 \pmod 4$, we conclude that $x \notin K$. Hence if $P = (x, y)$ is a point of order 4 in T, then $x^2 - b = 0$. This proves Claim 1.

If possible, we assume that T has an element of order 8. Therefore T must have an element, say, $P = (x, y)$ of order 4. Hence by Claim 1, we get $x^2 = b$.

Subcase 1: b is not a square. In this case, $x = \pm\sqrt{b} \in \mathbb{Z}[\sqrt{d}]$ where d is a square-free part of b. Since b is 4-th power free integer, we let $b = t^2 d$ for some square-free integer t. Then $x = \pm t\sqrt{d}$ and $y^2 = \pm 2t^3 d\sqrt{d}$. Since $y \in K$ and $y^2 \in \mathbb{Z}[\sqrt{d}]$, we have $y \in \mathbb{Z}[\sqrt{d}]$. Now let $y = y_1 + y_2\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$. Therefore, the two relations $y_1^2 + dy_2^2 = 0$ and $y_1 y_2 = \pm t^3 d$ together imply that $dt^6 = -y_2^4$. Since t is square-free, $d = -1$ and $t = \pm 1$. Therefore we get $b = -1$. This implies that $K \supseteq \mathbb{Q}(i)$.

Let $Q = (x_1, y_1)$ be a point of order 8 in T and let $P = 2Q$. Then P is of order 4 in T where $x(P) = \pm i$. So, $8Q = \mathcal{O} \Rightarrow 4(2Q) = \mathcal{O} \Rightarrow x(2Q) = \pm i$. That is, if $Q = (x_1, y_1)$, then

$$\Rightarrow \frac{(x_1^2 + 1)^2}{4x_1(x_1^2 - 1)} = \pm i \quad \Longleftrightarrow \quad x_1^4 + 2x_1^2 + 1 = \pm(4ix_1^3 - 4ix_1).$$

By putting $r = ix_1 \in K$, we get

$$r^4 - 2r^2 + 1 = \pm(4r^3 + 4r) \quad \Longleftrightarrow \quad r^4 \pm 4r^3 - 2r^2 \pm 4r + 1 = 0.$$

Now consider the polynomials $f(X) = X^4 - 4X^3 - 2X^2 - 4X + 1$ and $g(X) = X^4 + 4X^3 - 2X^2 + 4X + 1$. We claim that $f(X)$ and $g(X)$ are irreducible polynomials in $\mathbb{Z}[X]$.

It is clear that $f(X)$ does not have any integer root. Suppose $f(X)$ is reducible in $\mathbb{Z}[X]$. Then, $f(X) = (X^2 + aX + a_1)(X^2 + bX + b_1)$ for some integers a, b, a_1 and b_1. Since the constant term in $f(X)$ is 1, either $a_1 = b_1 = 1$ or $a_1 = b_1 = -1$. If $f(X) = (X^2 + aX + 1)(X^2 + bX + 1)$, then we have relations: $a + b = -4$ and $ab = -4$, which is a contradiction to a and b are integers. If $f(X) = (X^2 + aX - 1)(X^2 + bX - 1)$, then we have relations: $a + b = -4$ and $a + b = 4$, which is impossible. Hence, $f(X)$ is irreducible in $\mathbb{Z}[X]$. Similarly, we can prove that $g(X)$ is also irreducible in $\mathbb{Z}[X]$.

Now, by Gauss lemma, $f(X)$ and $g(X)$ are irreducible polynomials over $\mathbb{Q}$. As a result, we see that $[\mathbb{Q}(r) : \mathbb{Q}] = 4$, which is a contradiction as $K \supseteq \mathbb{Q}(r)$ and $[K : \mathbb{Q}] = n \equiv 2 \pmod 4$.

Subcase 2: b is a square. Since b is 4-th power free, we can write $b = t^2$ for some nonzero square-free integer t. Let $Q = (x_1, y_1)$ be a point of order 8 in T. In this subcase, the elements of order 4 in T has x-coordinates $\pm t$. Hence $8Q = \mathcal{O} \Rightarrow 4(2Q) = \mathcal{O} \Rightarrow x(2Q) = \pm t$. That is,

$$\Rightarrow \frac{(x_1^2 - t^2)^2}{4x_1(x_1^2 + t^2)} = \pm t \quad \Longleftrightarrow \quad x_1^4 - 2t^2x_1^2 + t^4 = \pm(4tx_1^3 + 4t^3x_1).$$

By putting $r = x_1/t \in K$, we get

$$r^4 - 2r^2 + 1 = \pm(4r^3 + 4r) \iff r^4 \pm 4r^3 - 2r^2 \pm 4r + 1 = 0.$$

Now consider the polynomials $f(X) = X^4 - 4X^3 - 2X^2 - 4X + 1$ and $g(X) = X^4 + 4X^3 - 2X^2 + 4X + 1$. As in the previous case, we see that $f(X)$ and $g(X)$ are irreducible polynomials over $\mathbb{Q}$ and hence $[\mathbb{Q}(r) : \mathbb{Q}] = 4$, which is a contradiction as $K \supseteq \mathbb{Q}(r)$ and $[K : \mathbb{Q}] = n \equiv 2 \pmod 4$. This proves the lemma. ■

Proof of Proposition 1. Note that $P = (x, y)$ is a point of order 2 in $T \iff 2P = \mathcal{O} \iff P = -P \iff 2y = 0 \iff x(x^2 + b) = 0$. Therefore, either $x = 0$ or $x^2 + b = 0$. If $x = 0$, then the point $(0, 0)$ is a point of order 2. If $x \neq 0$, then $x = \pm\sqrt{-b}$.

Note that $-b$ must be a square of an integer. For otherwise, if $-b$ is not a square, then $x \notin K$, since K and $\mathbb{Q}(\sqrt{-b})$ are linearly disjoint number fields over $\mathbb{Q}$ (as $[K : \mathbb{Q}]$ is odd), which is a contradiction to $P \in E(K)$. Thus, as $-b$ is a square, $x \in \mathbb{Z} \subset K$. Thus, if (x, y) is a point of order 2 in T, then $(x, y) = (0, 0)$ or $(\pm\sqrt{-b}, 0)$ with $-b$ is a square of an integer.

Now, let $P = (x, y)$ be an element of order 4 in T. Then by Claim 1 in Lemma 2, we have $x^2 - b = 0 \iff x = \pm\sqrt{b}$.

Again note that b is a square. If not, then $x = \sqrt{b}$, which is impossible because K and $\mathbb{Q}(\sqrt{b})$ are linearly disjoint over $\mathbb{Q}$. If b is a square, then $x \in \mathbb{Z} \subseteq K$. Let $b = a^2$ for some square-free integer a. Thus if $P = (x, y)$ is a point of order 4 in T, then $x = \pm a$. Then $y^2 = \pm 2a^3 \Rightarrow y = \pm 2a\sqrt{\pm\frac{a}{2}}$. Since $y \in K$, we have $\pm\frac{a}{2}$ must be a square. Since a is square-free, we conclude that $a = \pm 2$. Hence the only elements of order 4 are $(2, \pm 4)$ with $b = 4$.

In Lemma 1 and Lemma 2, we have seen that there are no points of order 8 or of order q for any odd prime q. Therefore, by combining all the cases, we get the desired result. ■

Proof of Proposition 2. First we compute all the points of order 2 in T. If $P = (x, y)$ is a point of order 2, then $2P = \mathcal{O} \iff P = -P \iff 2y = 0 \iff x(x^2 + b) = 0$. Therefore, if $P = (x, y) \in T$ is a point of order 2, then $x = 0$ or $x = \pm\sqrt{-b}$. If $x = 0$, then the point $(0, 0)$ is a point of order 2. If $x \neq 0$, then $x = \pm\sqrt{-b} \in K$.

Now, let $P = (x, y)$ be an element of order 4 in T. Then by Claim 1 in Lemma 2, we have $x^2 - b = 0 \iff x = \pm\sqrt{b}$.

Again note that b is a square. If not, then $x = \pm\sqrt{b} \Rightarrow y^2 = \pm 2b\sqrt{b}$, which is impossible because $y \in K$ and $[K : \mathbb{Q}] \equiv 2 \pmod 4$. Therefore, write $b = t^2$ for some square-free integer t. Thus, $x = \pm t \Rightarrow y^2 = \pm 2t^3$. Hence $y = \pm t\sqrt{\pm 2t}$.

If $\pm 2t$ is a square, then $t = \pm 2$, because t is square-free. Hence $b = 4$. In this case the possible elements of order 4 are $(2, \pm 4)$ and $(-2, \pm 4i)$.

If $\pm 2t$ is not a square, then $(t, \pm t\sqrt{2t})$ are the only points of order 4 in T, when $\sqrt{2t} \in K$ and $(-t, \pm t\sqrt{-2t})$ are the only points of order 4 in T, when $\sqrt{-2t} \in K$.

In Lemma 1 and Lemma 2, we have seen that there are no points of order 8 or of order q for any odd prime q.

Combining all the above cases, we get the desired result. ∎

3. Proof of Theorem 1 and Theorem 2

First we prove two claims and we deduce Theorem 1 and 2.

Claim 1.

1. *Let K be a number field with $[K:\mathbb{Q}] \equiv 2 \pmod 4$ and $E: Y^2 = X^3 + bX$ be a given elliptic curve for some 4-th power free integer $b \neq 4$. If the rank of E over K is 0, then the equation $x^4 + by^4 = z^2$ has only trivial solutions over K.*
2. *Let K be a number field of odd degree and $E: Y^2 = X^3 + bX$ be a given elliptic curve for some 4-th power free integer b. If the rank of E over K is 0, then the equation $x^4 + by^4 = z^2$ has only trivial solutions over K.*

Suppose $(x, y, z) \in K^3$ with $xyz \neq 0$ is a nontrivial solution of the equation $x^4 + by^4 = z^2$. Dividing the equation by y^4 and by the change of variable

$$s \mapsto \frac{x}{y} \text{ and } t \mapsto \frac{z}{y^2},$$

we obtain the equation $s^4 + b = t^2$ for some $s, t \in K$. We can rewrite this equation as

$$r = s^2 \text{ and } r^2 + b = t^2.$$

Now, we multiply the last equation by r and using the relation $r = s^2$, we get

$$r^3 + br = (st)^2.$$

Then, by applying another change of variable $X = r$ and $Y = st$, we obtain an elliptic curve

$$E: Y^2 = X^3 + bX.$$

Since x, y and z are nonzero, we have r, s and t are nonzero. This implies that the corresponding X and Y are nonzero.

Case 1: $[K:\mathbb{Q}] \equiv 2 \pmod 4$. By the assumption, the elliptic curve $E: Y^2 = X^3 + bX$ has rank 0 over K. Therefore, by Proposition 2, if $b \neq -1$ and b is not a square, we have

$$E(K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \qquad \text{or} \qquad E(K) \cong \mathbb{Z}/2\mathbb{Z}.$$

That is, every nontrivial element of this group is of order 2 and hence $Y = 0$, which forces that either $x = 0$ or $z = 0$, which is a contradiction. Hence, the equation $x^4 + by^4 = z^2$ has only trivial solutions over K if b is not a square and $b \neq -1$.

Suppose $b = -1$.

Subcase 1: $i \notin K$. If $b = -1$ and $i \notin K$, as E has rank 0 over K by Proposition 2, we have

$$E(K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

That is, every nontrivial element of this group is of order 2 and hence $Y = 0$ which forces that either $x = 0$ or $z = 0$, which is a contradiction. Hence, the equation $x^4 + by^4 = z^2$ has only trivial solutions over K, if $b = -1$ and $i \notin K$.

Subcase 2: $i \in K$. If $b = -1$ and $i \in K$, as rank of E is 0 over K by Proposition 2, we have

$$E(K) \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

Here $(0, 0)$ and $(\pm 1, 0)$ are elements of order 2 and $(i, \pm(1 - i)), (-i, \pm(1 + i))$ are elements of order 4. The points of order 2 will lead to trivial solution for the equation $x^4 + by^4 = z^2$ over K. Corresponding to the points of order 4, we have $r = s^2 = \pm i$, which is a contradiction because $s \in K$ and $[K : \mathbb{Q}] \not\equiv 0 \pmod 4$. Therefore, the equation $x^4 + by^4 = z^2$ has only trivial solutions for $b = -1$ and $i \in K$.

Now, we assume that b is a square and let $b = t^2$ for some nonzero integer t with $t \neq \pm 2$ as $b \neq 4$.

If $\sqrt{2t} \in K$, as E has rank 0 over K by Proposition 2, we have

$$E(K) \cong \mathbb{Z}/4\mathbb{Z}.$$

Here, $(0, 0)$ is the only element of order 2 and $(t, \pm t\sqrt{2t})$ are elements of order 4. The point $(0, 0)$ will lead to trivial solution for the equation $x^4 + by^4 = z^2$ over K. Corresponding to the point $(t, \pm t\sqrt{2t})$, we have $r = s^2 = t$, which is a contradiction as $s \in K$ and $\sqrt{2t} \in K$. Therefore, the equation $x^4 + by^4 = z^2$ has only trivial solutions in this case.

If $\sqrt{2t} \notin K$, as E has rank 0 over K and $b \neq 4$, by Proposition 2, we have

$$E(K) \cong \mathbb{Z}/2\mathbb{Z}.$$

Here, $(0, 0)$ is the only element of order 2. Since the point $(0, 0)$ leads to trivial solution for the equation $x^4 + by^4 = z^2$ over K, we are done.

Combining all the cases, we see that the equation $x^4 + by^4 = z^2$ has only trivial solutions over K for any nonzero 4-th power free integer $b \neq 4$ whenever E has rank 0 over K.

Case 2: $[K : \mathbb{Q}]$ is odd. By the assumption, the elliptic curve $E : Y^2 = X^3 + bX$ has rank 0 over K. Therefore, by Proposition 1, if $b \neq 4$, we have

$$E(K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \qquad \text{or} \qquad E(K) \cong \mathbb{Z}/2\mathbb{Z}.$$

That is, every nontrivial element of $E(K)$ is of order 2 and hence $Y = 0$ which forces that either $x = 0$ or $z = 0$, which is a contradiction. Hence, the equation $x^4 + by^4 = z^2$ has only trivial solutions over K if $b \neq 4$.

When $b = 4$, by Proposition 1 and the assumption that the rank of $E(K)$ is 0, we have

$$E(K) \cong \mathbb{Z}/4\mathbb{Z}.$$

Here, $(0, 0)$ is the only element of order 2 and $(2, \pm 4)$ are the only elements of order 4. Note that $(0, 0)$ will lead to trivial solution for the equation $x^4 + by^4 = z^2$

over K. Corresponding to the point $(2, \pm 4)$, we have $r = s^2 = 2 \iff s = \pm\sqrt{2}$. Since $s \in K$, we see that $\sqrt{2} \in K$, which is a contradiction because K and $\mathbb{Q}(\sqrt{2})$ are linearly disjoint over $\mathbb{Q}$. Therefore the equation $x^4 + by^4 = z^2$ has only trivial solutions in this case also.

Combining all the cases, we see that the equation $x^4+by^4 = z^2$ has only trivial solutions over K for any nonzero 4-th power free integer b whenever E has rank 0 over K. This proves the Claim 1.

Claim 2. *Let $E : Y^2 = X^3 + bX$ be an elliptic curve over K, where K is any field with characteristic* 0*. If the equation $x^4 + by^4 = z^2$ has only trivial solutions over K, then E has rank* 0 *over K.*

Suppose E has positive rank over K. Then there exists a point $P = (X, Y)$ of infinite order in $E(K)$. Therefore, $XY \neq 0$.

By the duplication formula, we have

$$X(2P) = \frac{(X^4 - 2bX^2 + b^2)}{4Y^2} = \frac{(X^2 - b)^2}{(2Y)^2}.$$

Note that, $X(2P)$ is a square in K. Since P is of infinite order, so is $2P$.

Therefore there exists a point $Q = (x', y')$ on E such that $x' = s^2$ and $y' = st$ for some nonzero $s, t \in K$.

So we have,

$$s^2t^2 = s^6 + bs^2 \Rightarrow t^2 = s^4 + b.$$

Thus $(s, 1, t)$ is a nontrivial solution for the equation $x^4 + by^4 = z^2$ over K, which is a contradiction to the assumption. Hence we conclude that if $x^4 + by^4 = z^2$ has only trivial solutions over K, then E has rank 0 over K, which proves the Claim 2.

To prove Theorem 1 and Theorem 2, it is enough to assume that b is a 4-th power free integer. If not, let $b = at^4$ for some 4-th power free integer a and nonzero integer t. Then (t^2x, t^3y) is a point on the elliptic curve $E : y^2 = x^3 + bx$ if and only if (x, y) is a point on $E_1 = y^2 = x^3 + ax$. Also (x, y, z) is a solution of the Diophantine equation $x^4 + by^4 = z^2$ if and only if (x, ty, z) is a solution of the Diophantine equation $x^4 + ay^4 = z^2$. Thus, it is enough to assume that b is a 4-th power-free integer. Then theorems follow from Claim 1 and Claim 2. ■

4. Applications

As an application we have following results.

Corollary 2. *For any nonzero integer b the Diophantine equation $x^4 + by^4 = z^2$ has only trivial solutions over $\mathbb{Q}$ iff it has only trivial solutions over $\mathbb{Q}(i)$.*

Proof. If $x^4 + by^4 = z^2$ has only trivial solutions over $\mathbb{Q}(i)$ then obviously it has trivial solutions over $\mathbb{Q}$.

Conversely, assume that the equation $x^4 + by^4 = z^2$ has only trivial solutions over $\mathbb{Q}$. Then by Theorem 1, the elliptic curve $E : y^2 = x^3 + bx$ has rank 0 over $\mathbb{Q}$.

Now, note that -1-quadratic twist of E is $E^{(-1)}: y^2 = x^3 + x$, which is E itself. Now from [7], it is well-known that if E^D be the D-quadratic twist of E for some rational D, then

$$\text{Rank } E(\mathbb{Q}(\sqrt{D})) = \text{ Rank } E(\mathbb{Q}) + \text{ Rank } E^D(\mathbb{Q}).$$

For $D = -1$ we have, $E^{(-1)}(\mathbb{Q}) = E(\mathbb{Q})$. Since Rank $E(\mathbb{Q})$ is 0, we have Rank $E(\mathbb{Q}(i)) = 0$. Then again by Theorem 1, $x^4 + by^4 = z^2$ has only trivial solutions over $\mathbb{Q}(i)$. ■

Corollary 3. *A positive square-free integer n is a congruent number iff $x^4 - y^4 = z^2$ has a non-trivial solution in $\mathbb{Q}(\sqrt{n})$.*

Proof. We know that a positive square-free integer n is a congruent number iff $E_n : y^2 = x^3 - n^2x$ has positive rank over $\mathbb{Q}$. Now E_n is n-quadratic twist of $E : y^2 = x^3 - x$. Since E has rank 0 over $\mathbb{Q}$, we have Rank $E_n(\mathbb{Q})$ = Rank $E(\mathbb{Q}(\sqrt{n}))$. Hence n is a congruent number iff Rank $E(\mathbb{Q}(\sqrt{n})) > 0$. Then, by Theorem 1, we get, n is a congruent number iff $x^4 - y^4 = z^2$ has a non-tivial solution in $\mathbb{Q}(\sqrt{n})$. ■

References

[1] R. Ayoub, *An introduction to the analytic theory of numbers*, American Mathematical Society, Providence, RI, (1963).

[2] A. Bremner and J.W.S. Cassels, *On the equation $Y^2 = X(X^2 + p)$*, Math. Comp. **42** (1984), 257–264.

[3] A.J. Hollier, B.K. Spearman and Q. Yang, *On the rank and integral points of ellipitc curves $y^2 = x^3 - px$*, Int. J. of Algebra **3** (2009), 401–406.

[4] A.J. Hollier, B.K. Spearman and Q. Yang, *Elliptic Curves $y^2 = x^3 + pqx$ with maximal rank*, Int. Math. Forum **5** (2010), 1105–1110.

[5] T. Kudo and K. Motose, *On group structures of some special elliptic curves*, Math J. Okayam Univ. **47** (2005), 81–84.

[6] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Inventiones Mathematicae **124** (1996), 437–449.

[7] J.H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, (1992).

[8] J.H. Silverman and J.Tate, *Rational points on elliptic curves*, Springer-Verlag, New York, (1992).

[9] B.K. Spearman, *Elliptic curves $y^2 = x^3 - px$ of rank two*, Math. J. Okayama Univ. **49** (2007), 183–184.

[10] B.K. Spearman, *On the group structure of elliptic curves $y^2 = x^3 - 2px$*, Int. J. of Algebra **1** (2007), 247–250.

[11] L.C. Washington, *Elliptic curves number theory and cryptography*, Chapman and Hall/CRC, Florida, (2003).

Address: Pallab Kanti Dey: Harish-Chandra Research Institute, Chhatnag Road, Jhunsi, Allahabad, 211019, India.

E-mail: pallabkantidey@gmail.com

Received: 6 October 2015; **revised:** 25 August 2016