**Notes on Number Theory and Discrete Mathematics**
**Print ISSN 1310–5132, Online ISSN 2367–8275**
**Vol. 27, 2021, No. 3, 130–142**
**DOI: 10.7546/nntdm.2021.27.3.130-142**

# On the rational solutions of $y^2 = x^3 + k^{6n+3}$

**Richa Sharma**[1] **and Sanjay Bhatter**[2]

[1] Department of Mathematics, Malaviya National Institute of Technology
Jawahar Lal Nehru Marg, Jhalana Gram, Malviya Nagar, Jaipur, Rajasthan 302017, India
e-mail: richasharma582@gmail.com

[2] Department of Mathematics, Malaviya National Institute of Technology
Jawahar Lal Nehru Marg, Jhalana Gram, Malviya Nagar, Jaipur, Rajasthan 302017, India
e-mail: Sbhatter.maths@mnit.ac.in

**Received:** 25 October 2020 **Revised:** 12 August 2021 **Accepted:** 17 August 2021

**Abstract:** We consider a family of elliptic curves $E(k^{6n+3}):\ y^2 = x^3 + k^{6n+3}$ for some integers $k$ and $n \geq 0$ and prove that their rank is zero and the torsion part is isomorphic to $\mathbb{Z}_2$. This is an extension of a recent work of Wu and Qin [14].

**Keywords:** Diophantine equation, Lebesgue–Nagell type equation, Integer solution, Lucas sequences, Primitive divisors.
**2020 Mathematics Subject Classification:** 11G05, 14G05, 11R29.

## 1 Introduction

The Diophantine equation $y^2 = x^3 + k$ has played a fundamental role in the development of number theory. The earliest recorded result was given in 1621 by Bachet, who noted that when $k = -2; x = 3$ is a solution and other rational solutions can be found by the usual tangent method. Then Fermat posed a problem for the English mathematicians to show that the only integer solutions of $y^2 = x^3 - 2$ are given by $x = 3$.

The first proof of the existence of an infinity of rational solutions was given by Fueter [8] in 1930 and this work was extended by Brunner in his doctorate thesis [4]. Cassels [5] studied the equation $y^2 = x^3 - d$ in cubic number-fields and Baker [2,3] proved that all the integral solutions of $y^2 + k = x^3$ satisfy the following inequality:

$$\max\{|\ x\ |, |\ y\ |\} \leq \exp\left\{10^{10} \cdot |k|^{10^4}\right\},$$

where $|k|$ denotes the absolute value of $k$.

Ellison et al. [6] found all integral solutions of $y^2 + k = x^3$ when $k = 28$. Ljunggren [9] gave a list of all the unsolved equations with $\mid k \mid \leq 100$. The complete solutions for $k = 18, 25, 100$ was claimed by London and Finkelstein [7].

Mordell [10] considered some variants of $y^2 = x^3 + k$ and showed that this equation does not have any rational solution provided some conditions on the integer $k$, the class number of real and imaginary quadratic field and on the fundamental solution of Pell's equation. He showed that there is no finite algorithm known for finding solutions if they exist, except for special values of $k$.

Later in 2018, Wu and Qin [14] considered $E(k^3) : y^2 = x^3 + k^3$ and showed that the rank of this elliptic curve is zero for certain values of $k$ and also found out explicitly the torsion points. They used the class number of quadratic field and Pell equation to describe these square-free integers $k$ such that $E(k^3)(\mathbb{Q})$ has rank zero.

Wu and Qin followed the method of Mordell to derive their results. Extending the study further, we consider $E(k^{6n+3}) : \ y^2 = x^3 + k^{6n+3}$ another variant of the Mordell curve $y^2 = x^3 + k$ and with some conditions on the integer $k$, similar conditions on the class numbers prove our results. Wu and Qin's result is the special case corresponding to $n = 0$ of this paper's results.

In this paper, we consider a family of elliptic curves $E(k^{6n+3}) : \ y^2 = x^3 + k^{6n+3}$ for some integers $k$ and $n$ and show that their rank is zero and the torsion part is isomorphic to $\mathbb{Z}_2$.

# 2 Main result

The following results will be required in the subsequent study.

**Lemma 2.1** ([13], Exercise 4.11.)**.** *Let $\mathcal{G} \neq 0$ be an integer that is $6^{th}$ power free. Suppose $C$ be an elliptic curve, defined by*

$$C : y^2 = x^3 + \mathcal{G},$$

*and let $\psi$ be a subgroup of $C(\mathbb{Q})$ which consists of all points of finite order. Then*

*(a) $\#\psi$ divides 6.*

*(b) More accurately, $\psi$ can be defined as:*

$$\psi \cong \begin{cases} \mathbb{Z}/6\mathbb{Z} \ \textit{if} \ \mathcal{G} = 1, \\ \mathbb{Z}/3\mathbb{Z} \ \textit{if} \ \mathcal{G} \neq 1 \ \textit{is a square, or if} \ \mathcal{G} = -432, \\ \mathbb{Z}/2\mathbb{Z} \ \textit{if} \ \mathcal{G} \neq 1 \ \textit{is a cube}, \\ 1 \qquad \textit{otherwise} \ . \end{cases}$$

**Lemma 2.2.** *Let $P = (x, y)$ be a point on the curve $y^2 = x^3 + c$. Then the $x$-coordinate of the point $2P$ would be (using [13], Exercise 1.19),*

$$x([2]P) = \frac{9x^4 - 8xy^2}{4y^2}.$$

*Similarly,*

$$y([2]P) = \frac{-27x^6 + 36y^2x^3 - 8y^4}{8y^3}.$$

The following reflection Theorem of Scholz [11] will be required.

**Theorem 2.1.** *Let $l$ be the 3 rank of the ideal class group of $\mathbb{Q}(\sqrt{D})$ and $m$ be the 3 rank of the ideal class group of $\mathbb{Q}(\sqrt{-3D})(=\mathbb{Q}(\sqrt{-D/3}$ if $3 \mid D)$. Then $l \leq m \leq l+1$. Here $D$ is a square-free integer.*

A simplified version of Scholz theorem states that if 3 divides the class number of a real quadratic field $\mathbb{Q}(\sqrt{d})$, then 3 also divides the class number of the imaginary quadratic field $\mathbb{Q}\left(\sqrt{-3d}\right)$.

**Remark 1.** *The $j$-invariant $j(E(k^{6n+3}))=0$ and so there exists a unique $6^{th}$ power free integer $k$ such that $E$ is defined by the Weierstrass equation $E(k^{6n+3}): y^2=x^3+k^{6n+3}$ (using [12], Exercise 10.19).*

Let $h_D$ be the class number of $\mathbb{Q}(\sqrt{D})$. The following two theorems are our main results:

**Theorem 2.2.** *Let $E(k^{6n+3}): \ y^2=x^3+k^{6n+3}$ be an elliptic curve, where $k$ is a square-free negative integer and $n$ a non negative integer. Suppose that*

$(\mathbb{A})$ $k \equiv 11, 23, 35 \pmod{36}$,

$(\mathbb{B})$ $3 \nmid h_k$.

*Then*

$$\left\{(x,y) \in E(k^{6n+3})(\mathbb{Q}) : \mathrm{ord}_p(y) \leq 0 \ \forall \textit{ prime factors } p \mid 3k\right\} = \varnothing,$$

*and*

$$\left\{(x,y) \in E((-3k)^{6n+3})(\mathbb{Q}) : \mathrm{ord}_p(y) \leq 0 \ \forall \textit{ prime factors } p \mid 3k\right\} = \varnothing.$$

Here as usual $\varnothing$ denotes an empty set.

**Theorem 2.3.** *Let $k$ be a negative integer which is also square-free and satisfies $(\mathbb{A})$ and $(\mathbb{B})$ in Theorem 2.2. Then*

*(I)* $E(k^{6n+3})(\mathbb{Q}) = \mathrm{Tors}\, E(k^{6n+3})(\mathbb{Q}) = \{\mathcal{O}, (-k^{2n+1}, 0)\}$,

*(II)* $E((-3k)^{6n+3})(\mathbb{Q}) = \mathrm{Tors}\, E((-3k)^{6n+3})(\mathbb{Q}) = \{\mathcal{O}, ((3k)^{2n+1}, 0)\}$.

## 2.1 Proof of Theorem 2.2

*Proof.* The equation is

$$y^2 = x^3 + k^{6n+3} \tag{1}$$

with $k$ being as stated in the theorem.

We make a change of variable in (1) by substituting $y = \frac{Y}{Z'}$, where $(Y, Z') = 1$ and get

$$Z'(Y^2 - k^{6n+3}{Z'}^2) = x^3{Z'}^3. \tag{2}$$

Now each of the factors $Z'$ and $(Y^2 - k^{6n+3}{Z'}^2)$ has to be a perfect cube as $(Z', Y^2 - k^{6n+3}{Z'}^2) = 1$. Thus substituting $Z' = Z^3$ in (2), we have

$$Y^2 - k^{6n+3}Z^6 = (Z^2x)^3.$$

Let us replace $Z^2x = X$ for simplicity,

$$Y^2 - k^{6n+3}Z^6 = X^3, \tag{3}$$

where $(X, Y, Z) = 1$.

Now (3) is the homogenized version of (1) and we are looking for integer solutions $(X, Y, Z)$ of (3).

First we show that (3) has no integer solutions with $(Y, 3k) = 1$ and $(Y, Z) \neq (0, 0)$. To this end, let $(X, Y, Z)$ be an integral solution of (3) such that $Z > 0, Y > 0, (Y, 3k) = 1$ with $Z$ is minimal.

Clearly $(Y, Z) = 1$ as $(Y, Z^{'}) = 1$ in (3). Thus $(Z, X) = 1$. Also $(Y, k) = 1$, for if a prime $p$ divides both $Y$ and $k$, then it will be a prime divisor of both $Y$ and $3k$ which contradicts the fact that $(Y, 3k) = 1$.

Now we claim that $X$ is odd. If possible let $X \equiv 0 \pmod 2$. That would imply that $Z \equiv 1 \pmod 2$ and hence

$$Y^2 \equiv k^{6n+3} \pmod 4.$$

As $Y^2 \equiv 0, 1 \pmod 4$, this would imply that $k^{6n+3} \equiv 0, 1 \pmod 4$ and thus we get a contradiction to the fact that $k \equiv 11 \pmod{36}$. Thus $X$ is odd and also $(X, k) = 1$ as $k$ is square-free. Further the left-hand side of (3) can be split as:

$$(Y + k^{3n+1}Z^3\sqrt{k})(Y - k^{3n+1}Z^3\sqrt{k}) = X^3 \tag{4}$$

and this factorization is happening in $\mathbb{Q}(\sqrt{k})$ with $k < 0$. It is easy to see that both the ideals $(Y + k^{3n+1}Z^3\sqrt{k})$ and $(Y - k^{3n+1}Z^3\sqrt{k})$ are co-prime in $\mathcal{O}_K$ as $(X, 2k) = 1$ and $(X, Y, Z) = 1$.

By assuming condition $(\mathbb{B})$, the class number $h_k$ of $\mathbb{Q}(\sqrt{k})$ is not divisible by 3. Therefore by the unique factorization of ideals, $(Y + k^{3n+1}Z^3\sqrt{k})$ can be expressed as a cube of some ideal in $\mathcal{O}_K$. Therefore

$$Y + k^{3n+1}Z^3\sqrt{k} = \eta^3$$

for some algebraic integer $\eta \in \mathbb{Q}(\sqrt{k})$. Let $\eta = A + B\sqrt{k}$ where $A$ and $B$ are integers. Thus

$$Y + k^{3n+1}Z^3\sqrt{k} = (A + B\sqrt{k})^3, \tag{5}$$

where $X = A^2 - kB^2$ and $(A, B) = 1$.

Further equating the real and imaginary parts of (5), we get

$$Y = A^3 + 3AB^2k \tag{6}$$

and

$$Z^3k^{3n+1} = B(3A^2 + kB^2). \tag{7}$$

Now from (7) we get that $k \mid 3A^2B$ (since $(3, k) = 1$ and $k$ is square-free) and hence $k \mid AB$.

Now we show that $(k, A) = 1$. If possible, let a prime $p$ divides both $k$ and $A$. Then (6) will show that $p \mid Y$ and that would imply $p \mid (k, Y)$, which is in contrary to the assumption $(k, Y) = 1$. Thus $k \mid B$.

Let $B = B_1 k$ and with this (7) is changed to

$$Z^3 k^{3n} = B_1(3A^2 + B_1^2 k^3).$$

A similar analysis would show that $B_1 = kB_2$ and we get

$$Z^3 k^{3n-1} = B_2(3A^2 + k^5 B_2^2).$$

Continuing this process, we have

$$Z^3 = B_{3n+1}(3A^2 + k^{6n+3} B_{3n+1}^2), \tag{8}$$

where $B = B_{3n+1} k^{3n+1}$. Two cases are to be considered:

Case I: When $(B_{3n+1}, 3) = 1$. Then $B_{3n+1} = B_{3n+1'}^3$ and $Z = B_{3n+1'} Z_1$. Thus

$$Z_1^3 = 3A^2 + k^{6n+3} B_{3n+1'}^6. \tag{9}$$

If $A \equiv 0 \pmod 3$, then (6) implies that $Y$ is also a multiple of 3 and this contradicts $(Y, 3) = 1$. Hence $A \not\equiv 0 \pmod 3$.

Now if $Z_1 \equiv 0 \pmod 3$, then from (9) either $k$ or $B_{3n+1'}$ is also a multiple of 3 but by assumption $(B_{3n+1}, 3) = 1$ and $(k, 3) = 1$, which implies $Z_1 \not\equiv 0 \pmod 3$.

Further reducing (9) modulo 9, we get

$$B_{3n+1'}^6 \equiv 1 \pmod 9.$$

(Here we use Euler's theorem

$$a^{\phi(m)} \equiv 1 \pmod m$$

when $(a, m) = 1$ with $\phi$ denotes the Euler's $\phi$-function.)

Therefore, from (9)

$$Z_1^3 \equiv 3A^2 + k^{6n+3} \pmod 9. \tag{10}$$

This is not feasible if:

$$k \equiv 11, 23, 35 \pmod{36}, A \not\equiv 0 \pmod 3 \text{ and } Z_1 \not\equiv 0 \pmod 3.$$

Hence (3) does not have any integer solution when $(B_{3n+1}, 3) = 1$.

Case II: When $(B_{3n+1}, 3) \neq 1$. Then $B_{3n+1} = 9B_{3n+1'}^3$ and $Z = 3B_{3n+1'} Z_1$. This implies (from (8)) that

$$Z_1^3 = A^2 + 27k^{6n+3} B_{3n+1'}^6. \tag{11}$$

Clearly $Z_1 \not\equiv 0 \pmod 3$ as $(A, B) = 1$.

Further we claim $Z_1$ is odd.

If possible let $Z_1$ is even. Then the right-hand side of (11) is also even. Hence either both the terms are odd or both are even. Now $(A, 9k^{3n+1} B_{3n+1'}^3) = 1$ as $(A, B) = 1$. Suppose $9k^{3n+1} B_{3n+1'}^3$ is even and then from (11), $A$ must also be even which is a contradiction to the fact that $(A, 9k^{3n+1} B_{3n+1'}^3) = 1$. Thus $A, B_{3n+1'}$ and $k$ are all odd. Hence we get ( by (6) ) that $Y$ is even and thus $X$ is also even, which contradicts $(X, Y, Z) = 1$.

So far we have shown $Z_1$ is odd, it is not a multiple of 3 and also that $A$ is not a multiple of 3.

Now (11) can be re-written as

$$(A + 3B_{3n+1'}^3 k^{3n+1}\sqrt{-3k})(A - 3B_{3n+1'}^3 k^{3n+1}\sqrt{-3k}) = Z_1^3. \tag{12}$$

The two factors on the left-hand side of (12) are co-prime to each other. Thus by using Theorem 2.1, we can further conclude that $(h_{-3k}, 3) = 1$. Thus as before we have,

$$(A + 3B_{3n+1'}^3 k^{3n+1}\sqrt{-3k}) = \eta(C + D\sqrt{-3k})^3,$$

where $\eta$ is a unit in $\mathbb{Q}(\sqrt{-3k})$ $(k < 0)$ and that $(C, D) = 1$.

Now $\eta = \epsilon^n$, where $n = 0, \pm 1, \pm 2, \ldots$ and $\epsilon = T + U\sqrt{-3k}$ is the fundamental unit. Here $(X, Y) = (U, T)$ is the fundamental solution of

$$Y^2 + 3kX^2 = 1.$$

If $n \equiv 0 \pmod 3$, then $\eta$ can be absorbed in $(C + D\sqrt{-3k})^3$, and thus

$$(A + 3B_{3n+1'}^3 k^{3n+1}\sqrt{-3k}) = (C + D\sqrt{-3k})^3 \ . \tag{13}$$

As before equating the real and imaginary parts of (13)

$$A = C^3 - 9kCD^2 \tag{14}$$

and

$$B_{3n+1'}^3 k^{3n+1} = D(C^2 - kD^2). \tag{15}$$

Now $k \mid C^2D$ (from (15)) and thus $k \mid CD$.

If $k \mid C$ then from (14) we get $k \mid A$. Then from (11) we have $k \mid Z_1$ and together we conclude $k \mid Z$. Now from $X = A^2 - kB^2$ we get that $k \mid X$ (as we have already shown that $k|A$) and that contradicts $(X, Z) = 1$.

Thus $k \mid D$ and set $D = D_1 k$. The from (15)

$$B_{3n+1'}^3 k^{3n} = D_1(C^2 - D_1^2 k^3).$$

Similarly $D_1 = D_2 k$ and

$$B_{3n+1'}^3 k^{3n-1} = D_2(C^2 - k^5 D_2^2).$$

Continuing this process,

$$(B_{3n+1'})^3 = D_{3n+1}(C^2 - k^{6n+3} D_{3n+1}^2),$$

where $D = D_{3n+1}k^{3n+1}$. As before

$$D_{3n+1} = D_{3n+1'}^3, B_{3n+1'} = D_{3n+1'} B_{3n+1''}$$

and

$$B_{3n+1''}^3 = C^2 - k^{6n+3} D_{3n+1'}^6.$$

Thus $(B_{3n+1''}, C, D_{3n+1'})$ is another solution of (3) with $D_{3n+1'} \neq 0$ (since $B_{3n+1''} > 0$). Also,

$$|D_{3n+1'}| \leq |D_{3n+1}|^{\frac{1}{3}} \leq |B_{3n+1'}| \leq \frac{|Z|}{3}.$$

This is a contradiction to the fact that $Z$ is minimal. Hence (3) doesn't have any integer solution.

If $n \equiv \pm 1 \pmod 3$ then $\eta^{n\pm 1}$ can be absorbed in $(C + D\sqrt{-3k})^3$. In this case $\eta = T \pm U\sqrt{(-3k)}$ and

$$(A + 3B^3_{3n+1'}k^{3n+1}\sqrt{-3k}) = \eta(C + D\sqrt{-3k})^3.$$

Hence,

$$(A + 3B^3_{3n+1'}k^{3n+1}\sqrt{-3k}) = (T \pm U\sqrt{-3k})(C + D\sqrt{-3k})^3.$$

Again equating real and imaginary parts, we have

$$A = TC^3 - 9kTCD^2 \pm (9k^2UD^3 - 9kUC^2D) \tag{16}$$

and

$$3B_3^{3n+1'}k^{3n+1} = -3kTD^3 + 3TC^2D \pm (UC^3 - 9kCD^2U). \tag{17}$$

Now reducing (16) modulo 3,

$$A \equiv TC^3 \pmod 3.$$

Since $A \not\equiv 0 \pmod 3$, (shown already!) this implies that $C, T \not\equiv 0 \pmod 3$.
Now we claim that the solution $(X, Y) = (U, T)$ (the fundamental solution) of $Y^2 + 3kX^2 = 1$ in Theorem 2.2 satisfies $3 \nmid U$. Clearly $-k \equiv 1 \pmod 3$. This is so because:

- $k$ is a negative as well as square-free integer,
- $k \equiv 11, 23, 35 \pmod{36}$.

Recall $\epsilon = T + U(\sqrt{-3k})$ is the fundamental unit of $\mathbb{Q}(\sqrt{-3k})$. As both $h_k, h_{-3k}$ are not divisible by 3, using [1, Theorem II], we get

$$Th_k + Uh_{-3k} \equiv 0 \pmod 3. \tag{18}$$

Since $T, h \not\equiv 0 \pmod 3$ in (18), we conclude that $U \not\equiv 0 \pmod 3$.

Now reducing (17) modulo 3 gives $UC^3 \equiv 0 \pmod 3$. As $C \not\equiv 0 \pmod 3$, we have that $U \equiv 0 \pmod 3$. This contradicts the previous conclusion. Hence (3) does not have any integer solution when $(B_{3n+1}, 3) \neq 1$.

Thus (3) has no integer solutions and that in turn implies (1) has no rational solutions. Hence

$$\{(x, y) \in E(k^n)(\mathbb{Q}) : \mathrm{ord}_p(y) \leq 0 \,\forall \text{ prime factors } p \mid 3k\} = \varnothing.$$

If $(x, y)$ is such a solution, then (1) should always have rational solutions.

Now we prove

$$\{(x, y) \in E((-3k)^n)(\mathbb{Q}) : \mathrm{ord}_p(y) \leq 0 \,\forall \text{ prime factors } p \mid 3k\} = \varnothing.$$

It is sufficient to show that

$$Y^2 + (3k)^{6n+3}Z^6 = X^3 \tag{19}$$

has no rational solutions with $(X, Y, Z) = 1$, $(Y, Z) = 1$, $Y \neq 0$, $Z \neq 0$, $(Y, 3k) = 1$ with $Z$ is the least possible (as in the previous case).

Recall that $Y$ and $Z$ cannot be both even. We show that $X$ must be odd. If possible let $X \equiv 0 \pmod 2$, then $Z \equiv 1 \pmod 2$. Therefore

$$Y^2 + (3k)^{6n+3} \equiv 0 \pmod 4.$$

Thus $Y^2 \equiv k^{6n+3} \pmod 4$ (since $Y^2 \equiv 0, 1 \pmod 4$) and this gives that $k^{6n+3} \equiv 0, 1 \pmod 4$.

This is inconsistent with the condition on $k$ (since $k \equiv 11, 23, 35 \pmod{36}$). Therefore $X$ is odd.

Further (19) can be written as:

$$\left(Y + 3^{3n+1}k^{3n+1}Z^3\sqrt{-3k}\right)\left(Y - 3^{3n+1}k^{3n+1}Z^3\sqrt{-3k}\right) = X^3.$$

The above factors on the left-hand side have no common divisors as $(X, 2k) = 1$ and $(X, Y, Z) = 1$. As $3 \nmid h_{-3k}$ (using assumption in Theorem 2.1),

$$\left(Y + 3^{3n+1}k^{3n+1}Z^3\sqrt{-3k}\right) = \left(T + U\sqrt{-3k}\right)^{\alpha}\left(A + B\sqrt{-3k}\right)^3 \tag{20}$$

with $(A, B) = 1$ and $(U, T)$ is the smallest solution to $Y^2 + 3kX^2 = 1$.

If $\alpha \not\equiv 0 \pmod 3$, then $\left(T + U\sqrt{-3k}\right)^{\alpha\pm1}$ can be absorbed in $\left(A + B\sqrt{-3k}\right)^3$ leading to

$$\left(Y + 3^{3n+1}k^{3n+1}Z^3\sqrt{-3k}\right) = \left(T \pm U\sqrt{-3k}\right)\left(A + B\sqrt{-3k}\right)^3.$$

Again equating real and imaginary parts as before, we get

$$Y = A^3T - 9kTAB^2 \pm (9k^2UB^3 - 9kUA^2B) \tag{21}$$

and

$$3^{3n+1}k^{3n+1}Z^3 = -3kTB^3 + 3TA^2B \pm (A^3U - 9kUAB^2). \tag{22}$$

As before we prove that the solution $(X, Y) = (U, T)$ (the fundamental solution) of $Y^2 + 3kX^2 = 1$ in Theorem 2.2 satisfies $3 \nmid U$. Now reducing (22) modulo 3 entails

$$A^3U \equiv 0 \pmod 3. \tag{23}$$

If $3 \mid A$, then via (21) we get $3 \mid Y$ and that contradicts $(Y, 3) = 1$. Hence $A \not\equiv 0 \pmod 3$. Therefore from (23) we must have $U \equiv 0 \pmod 3$, which is a contradiction. Thus in this case no solution of (19) can exist.

If $\alpha \equiv 0 \pmod 3$, then $\left(T + U\sqrt{-3k}\right)^{\alpha}$ can be absorbed in $\left(A + B\sqrt{-3k}\right)^3$ and from (20) we get

$$\left(Y + 3^{3n+1}k^{3n+1}Z^3\sqrt{-3k}\right) = \left(A + B\sqrt{-3k}\right)^3.$$

Equating real and imaginary parts in this case gives,

$$Y = A^3 - 9kAB^2 \tag{24}$$

and

$$3^{3n}k^{3n+1}Z^3 = -kB^3 + A^2B, \tag{25}$$

where $X = A^2 + 3kB^2$. Further (25) implies that $k \mid AB$. Suppose $k \mid A$, then there exists a prime $p$ such that $p \mid k$ and $p \mid A$. Therefore (24) gives that $p \mid y$. This implies that $p \mid (k, Y)$, which contradicts $(k, Y) = 1$. Therefore $k \mid B$ and let $B = kB_1$. Then from (25)

$$3^{3n}k^{3n}Z^3 = B_1(A^2 - k^3B_1^2). \tag{26}$$

Again (26) implies $k \mid B_1$ and write $B_1 = kB_2$. Thus (26) is converted to

$$3^{3n}k^{3n-1}Z^3 = B_2(A^2 - k^5B_2^2) \text{ with } (A, B_2) = 1.$$

Hence on continuing this process

$$Z^3 3^{3n} = B_{3n+1}(A^2 - k^{6n+3}B_{3n+1}^2) \text{ with } (A, B_{3n+1}) = 1. \tag{27}$$

Thus (27) implies that either $B_{3n+1}$ divides $3^{3n}$ or $Z$.

Case I: Let $(B_{3n+1}, 3^{3n}) \neq 1$. Then the possible values of $B_{3n+1}$ are $\pm 1,\ \pm 3^t$ and $\pm 3^{3n}$ for some integer $1 < t < 3n$.

Let $B_{3n+1} = \pm 1$. Then (27) would imply

$$3^{3n}Z^3 = \pm(-k^{6n+3} + A^2).$$

Reducing this equation modulo 3, we get

$$0 = \pm(-k^{6n+3} + A^2) \pmod 3.$$

As $A \not\equiv 0 \pmod 3$ and $k^{6n+3} \equiv 2 \pmod 3$, this would imply

$$0 \equiv \pm(-1) \pmod 3,$$

which is not possible.

Further let $B_{3n+1} = \pm 3^t$ where $1 < t < 3n$. In these cases (27) would imply

$$3^{3n-t}Z^3 = \pm(-3^{2t}k^{6n+3} + A^2). \tag{28}$$

If we reduce (28) modulo 3 it would give$A \equiv 0 \pmod 3$ which is a contradiction.

Similarly one treats the case $B_{3n+1} = \pm 3^{3n}$.

Case II: Let $(B_{3n+1}, Z) \neq 1$ and $Z = B_{3n+1}Z_1$. Then from (27), we get

$$3^{3n}B_{3n+1}^2Z_1^3 = A^2 - k^{6n+3}B_{3n+1}^2.$$

This contradicts the assumption that $(A, B_{3n+1}) = 1$.
Therefore for all the cases when $\alpha \equiv 0 \pmod 3$ and $\alpha \not\equiv 0 \pmod 3$ equation (19) does not have any integer solution. This completes the proof of Theorem 2.2. □

We use Theorem 2.2 to prove Theorem 2.3.

## 2.2 Proof of Theorem 2.3

*Proof.* Let $\mathcal{G} = k^{6n+3}$ or $(-3k)^{6n+3}$, where $n$ is a positive integer. By Lemma 2.1,

$$\operatorname{Tors} E(k^{6n+3})(\mathbb{Q}) = \left\{\mathcal{O}, (-k^{2n+1}, 0)\right\}$$

and

$$\operatorname{Tors} E((-3k)^{6n+3})(\mathbb{Q}) = \left\{\mathcal{O}, \left((3k)^{2n+1}, 0\right)\right\}.$$

On the other hand, by Theorem 2.2, we get

$$E(\mathcal{G})(\mathbb{Q}) = \left\{(x, y) \in Q^2 : y^2 = x^3 + \mathcal{G}, p|3\mathcal{G},\ \operatorname{ord}_p(y) \geq 1\right\}.$$

Thus to prove Theorem 2.3, it suffices to prove the finiteness of the above set.

Let $p$ be a prime such that $p \mid 3\mathcal{G}$ and so making use of the equation $E(\mathcal{G})$, we obtain the following facts.

(i) If $p \neq 3$, then $\operatorname{ord}_p(y) \geq 1$ iff $\operatorname{ord}_p(x) = 1$.

The fact that $p \neq 3$ and $p \mid 3\mathcal{G}$ would give $p \mid \mathcal{G}$. Thus $\operatorname{ord}_p(\mathcal{G}) \geq 1$. Now if $\operatorname{ord}_p(y) \geq 1$, we show that $\operatorname{ord}_p(x) = 1$. Since $\operatorname{ord}_p(y) \geq 1$ gives $p \mid y$ and hence $p \mid x$. Thus $\operatorname{ord}_p(x) \geq 1$. Suppose if $(x, y) \in E(\mathcal{G})(\mathbb{Q})$, with $\operatorname{ord}_p(x) > 1$ and $\operatorname{ord}_p(y) \geq 1$.

Here we consider two sub-cases:

(c1) Suppose $\operatorname{ord}_p(x) = 2$ and $\operatorname{ord}_p(y) = 1$. Then $\operatorname{ord}_p(\mathcal{G}) = -4$ so we arrive at a contradiction by $\operatorname{ord}_p(\mathcal{G}) \geq 1$.

(c2) Suppose $\operatorname{ord}_p(x) = 2$ and $\operatorname{ord}_p(y) = 2$. Then $\operatorname{ord}_p(\mathcal{G}) = -2$ so again we arrive at a contradiction by $\operatorname{ord}_p(\mathcal{G}) \geq 1$.

Hence $\operatorname{ord}_p(x) = 1$. The other side can be proved similarly.

(ii) $\operatorname{ord}_3(y) \geq 1$ if and only if

$$\operatorname{ord}_3(x) = \begin{cases} 1 \text{ if } 3 \mid \mathcal{G}, \\ 0 \text{ if } 3 \nmid \mathcal{G}. \end{cases}$$

If possible let

$$E(\mathcal{G})(\mathbb{Q}) \neq E(\mathcal{G})(\mathbb{Q})_{\text{Tors}}.$$

Thus there is at least one $P = (x, y) \in E(\mathcal{G})(\mathbb{Q}) \setminus \operatorname{Tors} E(\mathcal{G})(\mathbb{Q})$ and a prime $p$ with $p \mid 3\mathcal{G}$ and $\operatorname{ord}_p(y) \geq 1$. We appeal to Lemma 2.2 and using this the following can be proven by induction.

(i) $p \neq 3$. Then $\forall\ n \geq 1$ we have $\operatorname{ord}_p(y([2^n]P)) \leq 0$.

(ii) $p = 3$. Then $\forall\ n \geq 2$ we have $\operatorname{ord}_3(y([2^n]P)) \leq 0$.

These imply that for any prime $p \mid 3\mathcal{G}$ we must have $\operatorname{ord}_p(y([2^n]P)) \leq 0$, which is a contradiction to the assumption that $\operatorname{ord}_p(y) \geq 1$. This completes the proof of Theorem 2.3. □

We consider a few examples before winding up.

**Example 1.** *Let $k = -37$. Consider the elliptic curves*

$$\begin{aligned} E((-37)^{6n+3}) &: y^2 = x^3 - 37^{6n+3} \\ E(111^{6n+3}) &: y^2 = x^3 + 111^{6n+3}. \end{aligned}$$

*Here $h_{-37} = 2$.*

*Applying Theorem 2.3, we get,*

*(i)* $E(-37^{6n+3})(\mathbb{Q}) = \operatorname{Tors} E(-37^{6n+3})(\mathbb{Q}) = \{\mathcal{O}, (37^{2n+1}, 0)\}$.

*(ii)* $E((111)^{6n+3})(\mathbb{Q}) = \operatorname{Tors} E((111)^{6n+3})(\mathbb{Q}) = \{\mathcal{O}, (-111^{2n+1}, 0)\}$.

**Example 2.** *Let $k = -97$. Consider the elliptic curves*

$$E((-97)^{6n+3}) : y^2 = x^3 - 97^{6n+3}$$

$$E(291^{6n+3}) : y^2 = x^3 + 291^{6n+3}.$$

*Here $h_{-97} = 4$.*

*Applying Theorem 2.3, we obtain,*

*(i)* $E((-97)^{6n+3})(\mathbb{Q}) = \operatorname{Tors} E((-97)^{6n+3})(\mathbb{Q}) = \{\mathcal{O}, (97^{2n+1}, 0)\}$.

*(ii)* $E((291)^{6n+3})(\mathbb{Q}) = \operatorname{Tors} E((291)^{6n+3})(\mathbb{Q}) = \{\mathcal{O}, (-291^{2n+1}, 0)\}$.

# 3 Concluding remarks

Here we have showed that the family of elliptic curves $E(k^{6n+3}) : y^2 = x^3 + k^{6n+3}$ with some additional conditions on $k$, the torsion part is always isomorphic to $\mathbb{Z}_2$ and the rank of each member of this family is zero.

In the other case when the exponent of $k$ is not divisible by 3 and with some conditions on $k$, we proved/noticed:

- The torsion part is always isomorphic either to $\mathbb{Z}_3$ or it is trivial. This follows directly from Lemma 2.1 and here is an explanation.

  If $K^l$ is a cube, then it would imply that $3 \mid l$. Which is not possible in our case as we have taken $k$ to be square-free and $l$ not a multiple of 3. Thus, the torsion part cannot be isomorphic to $\mathbb{Z}_2$.

  Now $l$ cannot be zero by the given condition on $l$ and $k \neq 1$ as $k$ is a square-free integer. Therefore $k^n \neq 1$. This implies that the torsion part cannot be isomorphic to $\mathbb{Z}_6$.

- The rank part is not consistent in the sense that for some exponents of $k$ it is coming out to be zero, for other exponents of $k$ it is coming out to be positive. Suppose $k \equiv 61 \pmod{88}$, then

| $k$ | $l$ | Rank | Torsion |
|---|---|---|---|
| $-115$ | 5 | 0 | Trivial |
| $-203$ | 5 | 0 | Trivial |
| $-291$ | 5 | 1 | Trivial |
| $-115$ | 7 | 1 | Trivial |
| $-203$ | 7 | 1 | Trivial |
| $-291$ | 7 | 2 | Trivial |

Table 1. Rank and torsion part of $E(k^l) : y^2 = x^3 + k^l$ with certain conditions on $k$ and $l$.

When $k \equiv 23 \pmod{37}$, then

| $k$ | $l$ | Rank | Torsion |
|---|---|---|---|
| $-14$ | 5 | 1 | Trivial |
| $-51$ | 5 | 0 | Trivial |
| $-273$ | 7 | 1 | Trivial |
| $-310$ | 7 | 1 | Trivial |
| $-347$ | 7 | 1 | Trivial |

Table 2. Rank and torsion part of $E(k^l) : y^2 = x^3 + k^l$ with certain conditions on $k$ and $l$.

It would of considerable interest to characterize those $l$'s for which the rank turns out to be trivial or for which the rank is positive.

# Acknowledgements

The authors are grateful to Prof. Kalyan Chakraborty for his careful reading, helpful comments and suggestions. The authors are indebted to the anonymous referee for his/her valuable suggestions which has helped improving the presentation of this manuscript.

# References

[1] Ankeny, N. C., Artin, E., & Chowla, S. (1952). The class-number of real quadratic number fields. *Annals of Mathematics* Second Series, 56(3), 479–493.

[2] Baker, A. (1968). Contributions to the theory of Diophantine equations, I. On the representation of integers by binary quadratic forms. *Philosophical Transactions of the Royal Society of London. Series A, Mathematical and Physical Sciences*, 263, 173–191.

[3] Baker, A. (1968). Contributions to the theory of Diophantine equations, II. The Diophantine equation $y^2 = x^3 + k$. *Philosophical Transactions of the Royal Society of London. Series A, Mathematical and Physical Sciences*, 263, 193–208.

[4] Brunner, O. (1933). *Losungseigenschaften der kubischen diophantischen Gleichung* $Z^3 - y^2 = D$. Inauguraldissertation, Zurich.

[5] Cassels, J. W. S. (1950). The rational solutions of the Diophantine equation $y^2 = x^3 - d$. *Acta Mathematica*, 82, 243–273.

[6] Ellison, W. J., Ellison, F., Pesek, J., Stahl, C. E., & Stall, D. S. (1972). The Diophantine equation $y^2 + k = x^3$. *Journal of Number Theory*, 4, 107–117.

[7] Finkelstein, R., & London, H. (1970). On Mordell's equation $y^2 - k = x^3$: An interesting case of Sierpinski. *Journal of Number Theory*, 2, 310–321.

[8] Fueter, R. (1930). Uber kubische diophantische Gleichungen. *Commentarii Mathematici Helvetici*, 2, 69–89.

[9] Ljunggren, W. (1961). The Diophantine equation $y^2 = x^3 - k$. *Acta Arithmetica*, 8, 451–465.

[10] Mordell, L. J. (1969). On some Diophantine equations $y^2 = x^3 + k$ with no rational solutions (II). In: *Number Theory and Analysis*, Springer, Boston, MA, pp. 224–232.

[11] Scholz, A. (1932). Über die Beziehung der Klassenzahl enquadratischer Körper zueinander. *Journal für die reine und angewandte Mathematik*, 166, 201–203.

[12] Silverman, J. H. (1986). *The Arithmetic of Elliptic Curves*. Springer-Verlag.

[13] Silverman, J. H., & Tate, J .T. (1992). *Rational Points on Elliptic Curves*, *Undergraduate Texts in Mathematics*, Springer-Verlag, New York.

[14] Wu, X. & Qin, Y. (2018). Rational points of Elliptic Curve $y^2 = x^3 + k^3$. *Algebra Colloquium*, 25, 133–138.