Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
Vol. 24, 2018, No. 3, 27–36
DOI: 10.7546/nntdm.2018.24.3.27-36

Some new families of positive-rank elliptic curves arising from Pythagorean triples

Mehdi Baghalaghdam[1] **and Farzali Izadi**[2]

[1] Department of Mathematics, Faculty of Science
Azarbaijan Shahid Madani University, Tabriz 53751-71379, Iran
e-mail: mehdi.baghalaghdam@yahoo.com

[2] Department of Mathematics, Faculty of Science
Urmia University, Urmia 165-57153, Iran
e-mail: f.izadi@urmia.ac.ir

Received: 28 December 2017 **Revised:** 28 August 2018 **Accepted:** 17 September 2018

Abstract: In the present paper, we introduce some new families of elliptic curves with positive rank arising from Pythagorean triples. We study elliptic curves of the form $y^2 = x^3 - A^2x + B^2$, where $A, B \in \{a, b, c\}$ are two different numbers and (a, b, c) is a rational Pythagorean triple. First of all, we prove that if (a, b, c) is a primitive Pythagorean triple (PPT), then the rank of each family is positive. Furthermore, we construct subfamilies of rank at least 3 in each family but one with rank at least 2, and obtain elliptic curves of high rank in each family. Finally, we consider two other new families of elliptic curves of the forms $y^2 = x(x - a^2)(x + c^2)$ and $y^2 = x(x-b^2)(x+c^2)$, and prove that if (a, b, c) is a PPT, then the rank of each family is positive.
Keywords: Elliptic curves, Rank, Pythagorean triples.
2010 Mathematics Subject Classification: 11G05, 14H52, 14G05.

1 Introduction

An elliptic curve (EC) over the rationals is a curve E of genus 1, defined over $\mathbb{Q}$, together with a $\mathbb{Q}$-rational point, and is expressed by the generalized Weierstrass equation of the form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Q}$.

A theorem of Mordell–Weil [11] states that the rational points on E form a finitely generated Abelian group $E(\mathbb{Q})$ under a natural group law, i.e., $E(\mathbb{Q}) \cong \mathbb{Z}^r \times E(\mathbb{Q})_{\text{tors}}$, where r is a non-negative integer called the rank of E, and $E(\mathbb{Q})_{\text{tors}}$ is the subgroup of elements of finite order in $E(\mathbb{Q})$, called the torsion subgroup of $E(\mathbb{Q})$. The rank of E is the rank of the free part of this group.

By Mazur's theorem [9], the torsion subgroup $E(\mathbb{Q})_{\text{tors}}$ is one of the following 15 groups: $\mathbb{Z}/n\mathbb{Z}$ with $1 \leq n \leq 10$ or $n = 12$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$ with $1 \leq m \leq 4$.

Currently there is no general unconditional algorithm to compute the rank. It is not known which integers can occur as ranks, but a well-known conjecture says that the rank can be arbitrarily large. Elliptic curves of large rank are hard to find and the current record is a curve of rank at least 28, found by Elkies in 2006 (see [1]).

In a recent paper, J. Park et al. [7] presents a heuristic suggesting that there are only finitely many elliptic curves of rank greater than 21. Their heuristic is based on modeling the ranks and Shafarevich–Tate groups of elliptic curves simultaneously, and relies on a theorem counting alternating integer matrices of specified rank. Also B. Naskrecki [6] proved that for a generic triple the lower bound of the rank of the EC over $\mathbb{Q}$ is 1, and for some explicitly given infinite family, the rank is 2. To each family, the author attaches an elliptic surface fibred over the projective line and shows that the lower bounds for the rank are optimal, in the sense that for each generic fiber of such an elliptic surface its corresponding Mordell–Weil group over the function field $\mathbb{Q}(T)$ has rank 1 or 2, respectively.

Specialization is a significant technique for finding a lower bound of the rank of a family of elliptic curves. One can consider an EC on the rational function field $\mathbb{Q}(T)$ and then obtain elliptic curves over $\mathbb{Q}$ by specializing the variable T to suitable values $t \in \mathbb{Q}$ (see [10, Chapter III, Theorem 11.4] for more information).

Using this technique, Nagao and Kauyo [5] have found curves of rank ≥ 21, and Fermigier [2] obtained a curve of rank ≥ 22.

In order to determine r, one should find the generators of the free part of the Mordell–Weil group. Determining the *associated height matrix* is a useful technique for finding a set of generators.

If the determinant of an associated height matrix is nonzero, then the given points are linearly independent and rank $(E(\mathbb{Q})) \geq r$ (see [10, Chapter III] for more information).

In this paper, we study elliptic curves of the form $y^2 = x^3 - A^2x + B^2$, where $A, B \in \{a, b, c\}$ are two different numbers and (a, b, c) is a Pythagorean triple ($a, b, c \in \mathbb{Q}$). First of all, we prove that if (a, b, c) is a primitive Pythagorean triple (PPT), then the rank of each family is positive. By using both *specialization* and *associated height matrix* techniques, we construct subfamilies of rank at least 3 in each family but one with rank at least 2, and obtain elliptic curves of high rank in each family. Furthermore, we consider two other families of elliptic curves of the forms $y^2 = x(x - a^2)(x + c^2)$, and $y^2 = x(x - b^2)(x + c^2)$, and prove that if (a, b, c) is a PPT, then the rank of each family is positive. These familes are similar to another family of curves $y^2 = x(x - a^2)(x + b^2)$ with $a^2 + b^2 = c^2$ which is a special case of the well-known Frey family.

In [3], a subfamily of the elliptic curve $y^2 = x^3 - c^2x + a^2$, with the rank at least 4, has been introduced. In [4], it is proved that the rank of the elliptic curve $y^2 = x(x-a^2)(x-b^2)$ is positive

and also in [6] a subfamily of this elliptic curve with the rank at least 2 is obtained.

We need the following standard facts in this paper:

Lemma 1.1. *The following relations will generate all primitive integer Pythagorean triples* $(a^2+b^2=c^2,\ (a,b,c)=1)$ *:* $a=m^2-n^2$, $b=2mn$, $c=m^2+n^2$, *where* m *and* n, *are positive integers with* $m>n$, *and* m *and* n *coprime with different parities.*

Lemma 1.2. ***(Nagell–Lutz Theorem)*** *Let* $y^2=f(x)=x^3+ax^2+bx+c$, *be a non-singular cubic curve with integer coefficients* $a,b,c\in\mathbb{Z}$, *and let* D *be the discriminant of the cubic polynomial* $f(x)$, *i.e.,* $D=-4a^3c+a^2b^2+18abc-4b^3-27c^2$.

Let $P=(x,y)\in E(\mathbb{Q})$ *be a rational point of finite order. Then* x *and* y *are integers and, either* $y=0$, *in which case P has order* 2, *or else* y *divides* D *(see* [9]*, page: 56).*

2 The elliptic curve $y^2=x^3-a^2x+c^2$

In each family, let (a,b,c) be a PPT.
First, by letting $-a^2x+c^2=0$ in the above elliptic curve, we get $x=\frac{c^2}{a^2}$ and $y=\frac{c^3}{a^3}$. Then the point $(\frac{c^2}{a^2},\frac{c^3}{a^3})$ is on the aforementioned elliptic curve. Note that this point is of infinite order, because in a PPT we have $(a,c)=1$ and $c\neq 1$, i.e., the numbers $\frac{c^2}{a^2}$ and $\frac{c^3}{a^3}$ are not integers, then by Lemma 1.2, the rank of the above elliptic curve is positive.
Second, we look at

$$E: y^2=x^3-a^2x+c^2, \tag{1}$$

as a 1-parameter family by letting

$$a=t^2-1,\quad b=2t,\quad c=t^2+1, \tag{2}$$

where $t\in\mathbb{Q}$. Then instead of (1) one can take

$$E_t: y^2=x^3-(t^2-1)^2x+(t^2+1)^2,\quad t\in\mathbb{Q}. \tag{3}$$

Theorem 2.1. *There are infinitely many elliptic curves of the form* (3) *with rank* ≥ 3.

Proof. Clearly we have two points

$$P_t=(0,\ t^2+1),\quad Q_t=(t^2-1,\ t^2+1). \tag{4}$$

Now we impose a point on (3) with x-coordinate equal to 1. It implies that $1+4t^2$, is a square, say $=v^2$. Hence

$$t=\frac{\alpha^2-1}{4\alpha},\quad v=\frac{\alpha^2+1}{2\alpha}, \tag{5}$$

with $\alpha\in\mathbb{Q}$. Then instead of (3), one can take

$$E_\alpha: y^2=x^3-\left(\left(\frac{\alpha^2-1}{4\alpha}\right)^2-1\right)^2x+\left(\left(\frac{\alpha^2-1}{4\alpha}\right)^2+1\right)^2, \tag{6}$$

or

$$E_\alpha : y^2 = x^3 - (\frac{\alpha^4 - 18\alpha^2 + 1}{16\alpha^2})^2 x + (\frac{\alpha^4 + 14\alpha^2 + 1}{16\alpha^2})^2 \tag{7}$$

equipped with the three points

$$P_\alpha = \left(0, \left(\tfrac{\alpha^2-1}{4\alpha}\right)^2 + 1\right),$$

$$Q_\alpha = \left(\left(\tfrac{\alpha^2-1}{4\alpha}\right)^2 - 1, \left(\tfrac{\alpha^2-1}{4\alpha}\right)^2 + 1\right),$$

$$R_\alpha = \left(1, \tfrac{\alpha^2+1}{2\alpha}\right).$$

When we specialize to $\alpha = 2$, we obtain a set of points

$$S = \{P_2, Q_2, R_2\} = \left\{(0, \frac{73}{64}), (\frac{-55}{64}, \frac{73}{64}), (1, \frac{5}{4})\right\},$$

on

$$E_2 : y^2 = x^3 - (\frac{55}{64})^2 x + (\frac{73}{64})^2. \tag{8}$$

Using SAGE [8], one can easily check that the *associated height matrix* of S has a non-zero determinant $\approx 73.3583597733868 \neq 0$, showing that these three points are independent and so the rank $(E_2) \geq 3$ (actually the rank is 4). The *specialization* result of Silverman [10] implies that for all but finitely many rational numbers the rank of E_α is at least 3. For the values $\alpha = 4, 10$, and $\alpha = 8, 11$, the rank of E_α is equal to 5 and 6, respectively. □

3 The elliptic curve $y^2 = x^3 - a^2x + b^2$

We study the elliptic curve

$$E_t : y^2 = x^3 - (t^2 - 1)^2 x + (2t)^2, \tag{9}$$

where $t \in \mathbb{Q}$. We construct a subfamily with rank at least 3.

Theorem 3.1. *There are infinitely many elliptic curves of the form* (9) *with rank* ≥ 3.

Proof. Clearly we have two points

$$P_1 = (0, 2t), \quad P_2 = (t^2 - 1, 2t). \tag{10}$$

Letting $-(t^2 - 1)^2 x + (2t)^2 = 0$, in (9), yields $x = (\frac{2t}{t^2-1})^2$ and $y = (\frac{2t}{t^2-1})^3$. Then, the third point is $P_3 = ((\frac{2t}{t^2-1})^2, (\frac{2t}{t^2-1})^3) = (\frac{b^2}{a^2}, \frac{b^3}{a^3})$. By Lemma 1.2, if (a, b, c) is a PPT, then this point is of infinite order, because $(a, b) = 1$, $a \neq 1$, and the numbers $\frac{b^2}{a^2}$, and $\frac{b^3}{a^3}$ are not integers.

If we let $t = 4T^3$, and $x^3 + (2t)^2 = 0$, then we get $x = -4T^2$, and $y = 2T(16T^6 - 1)$. Then the point $P_4 = (-4T^2, 2T(16T^6 - 1))$ is on the elliptic curve (9).

When we specialize to $T = 1$, we obtain a set of points

$$A = \{P_1, P_2, P_3, P_4\} = \left\{(0, 8), (15, 8), ((\frac{8}{15})^2, (\frac{8}{15})^3), (-4, 30)\right\},$$

lying on

$$E_2 : y^2 = x^3 - (15^2)x + (8^2). \tag{11}$$

Using SAGE, one can easily check that the *associated height matrix* of the points $\{P_1, P_2, P_3\}$ or $\{P_2, P_3, P_4\}$ has a non-zero determinant $\approx 7.34210213314542 \neq 0$, showing that these three points are independent and so the rank of the elliptic curve (9) is at least 3 (actually the rank is 4). The *specialization* result of Silverman implies that for all but finitely many rational numbers the rank of E_T is at least 3. For the value $T = 2$, the rank E_T is equal to 5. □

4 The elliptic curve $y^2 = x^3 - b^2x + a^2$

We consider the elliptic curve

$$E_t : y^2 = x^3 - (2t)^2x + (t^2 - 1)^2, \tag{12}$$

where $t \in \mathbb{Q}$, and construct a subfamily with rank at least 3.

Theorem 4.1. *There are infinitely many elliptic curves of the form* (12) *with rank* ≥ 3.

Proof. Clearly we have two points

$$P_1 = (0, t^2 - 1), \quad P_2 = (2t, t^2 - 1). \tag{13}$$

Letting $-(2t)^2x + (t^2 - 1)^2 = 0$, in (12), yields $x = (\frac{t^2-1}{2t})^2$ and $y = (\frac{t^2-1}{2t})^3$. Then, the third point is $P_3 = ((\frac{t^2-1}{2t})^2, (\frac{t^2-1}{2t})^3) = (\frac{a^2}{b^2}, \frac{a^3}{b^3})$. Again by Lemma 1.2 , if (a, b, c) is a PPT, this point is of infinite order, because $(a, b) = 1$, $b \neq 1$, and the numbers $\frac{a^2}{b^2}$, and $\frac{a^3}{b^3}$ are not integers. Now we impose a point on (12) with x-coordinate equal to -1. Then, we have $y^2 = t^2(t^2 + 2)$. It implies that $t^2 + 2$ is a square, say $= \alpha^2$. Hence $t = \frac{1}{m} - \frac{m}{2}$, and $\alpha = \frac{m}{2} + \frac{1}{m}$, with $m \in \mathbb{Q}$. Then the point $P_4 = (-1, \frac{1}{m^2} - \frac{m^2}{4})$ is on the elliptic curve (12).

When we specialize to $m = 10 (t = \frac{-49}{10})$, we obtain a set of points

$$A = \{P_1, P_2, P_3, P_4\} = \left\{(0, \frac{2301}{100}), (\frac{-49}{5}, \frac{2301}{100}), ((\frac{2301}{980})^2, -(\frac{2301}{980})^3), (-1, \frac{-2499}{100})\right\},$$

lying on

$$E_2 : y^2 = x^3 - (\frac{49}{5})^2x + (\frac{2376}{25})^2. \tag{14}$$

Using SAGE, one can easily check that the *associated height matrix* of the points $\{P_1, P_3, P_4\}$ and $\{P_2, P_3, P_4\}$ has non-zero determinants ≈ 421.718713884796 and 105.429678471199, respectively. This shows that these three points are independent and so the rank of the elliptic curve (14) is at least 3 (actually the rank is 5). The *specialization* result of Silverman implies that for all but finitely many rational numbers the rank of E_m is at least 3. For the values $m = 3, 5, 6, 7, 8, 10, 11, 13$, and $m = 12, 14$, the rank of E_m is equal to 5, and 6, respectively. □

5 The elliptic curve $y^2 = x^3 - a^2x + b^2$

We consider the elliptic curve

$$E_t : y^2 = x^3 - (t^2 - 1)^2x + (2t)^2, \tag{15}$$

where $t \in \mathbb{Q}$, and construct a subfamily with rank at least 3.

Theorem 5.1. *There are infinitely many elliptic curves of the form* (15) *with rank* ≥ 3.

Proof. Clearly we have two points

$$P_1 = (0, 2t), \quad P_2 = (t^2 - 1, 2t). \tag{16}$$

Letting $-(t^2 - 1)^2x + (2t)^2 = 0$, in (15), yields $x = (\frac{2t}{t^2-1})^2$ and $y = (\frac{2t}{t^2-1})^3$. Then, the third point is $P_3 = ((\frac{2t}{t^2-1})^2, (\frac{2t}{t^2-1})^3) = (\frac{b^2}{a^2}, \frac{b^3}{a^3})$. This point is of infinite order, because in a PPT we have $(a, b) = 1$ and $a \neq 1$, i.e., the numbers $\frac{b^2}{a^2}$ and $\frac{b^3}{a^3}$ are not integers, then the rank of the above elliptic curve is positive.

If we let $t = 4T^3$ and $x^3 + (2t)^2 = 0$, then we get $x = -4T^2$ and $y = 2T(16T^6 - 1)$.

Then the point $P_4 = (-4T^2, 2T(16T^6 - 1))$ is on the elliptic curve (15).

When we specialize to $T = 1$, we obtain a set of points

$$A = \{P_1, P_2, P_3, P_4\} = \left\{(0, 8), (15, 8), ((\frac{8}{15})^2, (\frac{8}{15})^3), (-4, 30)\right\},$$

lying on

$$E_2 : y^2 = x^3 - (15^2)x + (8^2). \tag{17}$$

Using SAGE, one can easily check that the *associated height matrix* of the points $\{P_1, P_2, P_3\}$ or $\{P_2, P_3, P_4\}$ has a non-zero determinant $\approx 7.34210213314542 \neq 0$, showing that these three points are independent and so the rank of the elliptic curve (15) is at least 3 (actually the rank is 4). The *specialization* result of Silverman implies that for all but finitely many rational numbers, the rank of E_T is at least 3. For the value $T = 2$, the rank E_T is equal to 5. □

6 The elliptic curve $y^2 = x^3 - c^2x + b^2$

We study the elliptic curve

$$E_t : y^2 = x^3 - (t^2 + 1)^2x + (2t)^2, \tag{18}$$

where $t \in \mathbb{Q}$. We construct a subfamily with rank at least 3.

Theorem 6.1. *There are infinitely many elliptic curves of the form* (18) *with rank* ≥ 3.

Proof. Clearly we have two points

$$P_1 = (0, 2t), \quad P_2 = (t^2 + 1, 2t). \tag{19}$$

Letting $-(t^2+1)^2x+(2t)^2=0$ in (18) yields $x=(\frac{2t}{t^2+1})^2$ and $y=(\frac{2t}{t^2+1})^3$. Then the third point is $P_3=((\frac{2t}{t^2+1})^2,(\frac{2t}{t^2+1})^3)=(\frac{b^2}{c^2},\frac{b^3}{c^3})$. This point is of infinite order, because in a PPT, we have $(b,c)=1$ and $c\neq 1$, i.e., the numbers $\frac{b^2}{c^2}$ and $\frac{b^3}{c^3}$ are not integers, then the rank of the above elliptic curve is positive.

Now we impose a point on (18) with the x-coordinate equal to 1. Then we have $y^2=t^2(-t^2+2)$. It implies that $-t^2+2$ is a square, say $=\alpha^2$. Hence we can get $t=\frac{u^2-2u-1}{u^2+1}$, and $\alpha=\frac{-u^2-2u+1}{u^2+1}$, with $u\in\mathbb{Q}$. Then the point $P_4=(1,\frac{(-u^2-2u+1)(u^2-2u-1)}{(u^2+1)^2})$ is on the elliptic curve (18).

When we specialize to $u=2(t=\frac{-1}{5})$, we obtain a set of points

$$A=\{P_1,P_2,P_3,P_4\}=\left\{(0,\frac{-2}{5}),(\frac{26}{25},\frac{-2}{5}),((\frac{5}{13})^2,-(\frac{5}{13})^3),(1,\frac{7}{25})\right\},$$

lying on

$$E_{\frac{-1}{5}}: y^2=x^3-(\frac{26}{25})^2x+(\frac{2}{5})^2. \tag{20}$$

Using SAGE, one can easily check that the *associated height matrix* of the points $\{P_1,P_2,P_4\}$ or $\{P_2,P_3,P_4\}$ has a non-zero determinant $\approx$ 16.9957115044387 (the determinant of points $\{P_1,P_3,P_4\}$ is non-zero, too). This shows that these two points (in each set) are independent and so the rank of the elliptic curve (20) is at least 3 (actually the rank is 5). The *specialization* result of Silverman implies that for all but finitely many rational numbers, the rank of E_u is at least 3. □

7 The elliptic curve $y^2=x^3-b^2x+c^2$

We study the elliptic curve

$$E_t: y^2=x^3-(2t)^2x+(t^2+1)^2, \tag{21}$$

where $t\in\mathbb{Q}$. We construct a subfamily with rank at least 2.

Theorem 7.1. *There are infinitely many elliptic curves of the form* (21) *with rank* ≥ 2.

Proof. Clearly we have two points

$$P_1=(0,t^2+1),\quad P_2=(2t,t^2+1). \tag{22}$$

Letting $-(2t)^2x+(t^2+1)^2=0$, in (21), yields $x=(\frac{t^2+1}{2t})^2$ and $y=(\frac{t^2+1}{2t})^3$. Then the third point is $P_3=((\frac{t^2+1}{2t})^2,(\frac{t^2+1}{2t})^3)=(\frac{c^2}{b^2},\frac{c^3}{b^3})$. Note that this point is of infinite order, because in a PPT we have $(b,c)=1$ and $b\neq 1$, i.e., the numbers $\frac{c^2}{b^2}$ and $\frac{c^3}{b^3}$ are not integers, then the rank of the aforementioned elliptic curve is positive. If we impose a point on (21) with the x-coordinate equal to 2, then we get the point $P_4=(2,t^2-3)$.

When we specialize to $t=\frac{7}{29}$, we obtain a set of points

$$A=\{P_1,P_2,P_3,P_4\}=\left\{(0,\frac{890}{841}),(\frac{14}{29},\frac{890}{841}),((\frac{445}{203})^2,-(\frac{445}{203})^3),(2,\frac{2474}{841})\right\},$$

lying on

$$E_{\frac{7}{29}} : y^2 = x^3 - (\frac{14}{29})^2 x + (\frac{890}{841})^2. \tag{23}$$

Using SAGE, one can easily check that the *associated height matrix* of the points $\{P_3, P_4\}$ and $\{P_1, P_3\}$ have non-zero determinants ≈ 13.2385415745155, and 52.9541662980621, respectively. This shows that these two points (in each set) are independent and so the rank of the elliptic curve (23) is at least 2 (actually the rank is 4). The *specialization* result of Silverman implies that for all but finitely many rational numbers, the rank of E_t is at least 2. □

8 The elliptic curve $y^2 = x(x - a^2)(x + c^2)$

Theorem 8.1. *Let (a, b, c) be a PPT. Then the rank of the aforementioned elliptic curve is positive.*

Proof. We have
$y^2 = x(x-a^2)(x+c^2) = x(x^2 + (c^2 - a^2)x - a^2c^2) = x(x^2 + b^2x - a^2c^2) = x^3 + b^2x^2 - a^2c^2x.$

Then it suffices that we study the elliptic curve

$$y^2 = x^3 + b^2x^2 - a^2c^2x. \tag{24}$$

Note that $D = a^4c^4(b^4 + 4a^2c^2) \neq 0$. Now, if in (24) we take $b^2x^2 - a^2c^2x = 0$, then we get $x = \frac{a^2c^2}{b^2}$ and $y = \frac{a^3c^3}{b^3}$. Therefore the first point on (24) is $P_1 = (\frac{a^2c^2}{b^2}, \frac{a^3c^3}{b^3})$. Note that the order of this point is infinite, because in a PPT, the number ac is not divisible by b, and, the numbers $\frac{a^2c^2}{b^2}$ and $\frac{a^3c^3}{b^3}$ are not integers. (Otherwise, if p is a prime number that divides b, then p must divide one of a, c. Now, in view of the relation $a^2 + b^2 = c^2$, p divides a, b, and c, that is not correct, because (a, b, c) is a PPT: $(a, b, c) = 1$.) Then the rank of the elliptic curve (24) is always positive. If we let $x^3 + b^2x^2 = 0$, then we get $x = -b^2$, and $y = abc$. Then the second point on (24) is the point $P_2 = (-b^2, abc)$. Letting $x^3 - a^2c^2x = 0$, yields the third and fourth points $P_{3,4} = (\pm ac, abc)$. □

Remark 8.2. *Note that if in a PPT (a, b, c), b is odd, then we may prove by another method that the rank of the aforementioned elliptic curve is positive. We prove that in the point $P_2 = (-b^2, abc)$, the number abc does not divide D, otherwise abc must divide $4a^6c^6$. Then b divides a^6c^6, because b is odd. This is not correct, because (a, b, c) is a PPT. Then the point P_2 is of infinite order. Now the result follows.*

9 The elliptic curve $y^2 = x(x - b^2)(x + c^2)$

Theorem 9.1. *Let (a, b, c) be a PPT. Then the rank of the above elliptic curve is positive.*

Proof. We have $y^2 = x(x - b^2)(x + c^2) = x(x^2 + (c^2 - b^2)x - b^2c^2) = x(x^2 + a^2x - b^2c^2) = x^3 + a^2x^2 - b^2c^2x$. Then it suffices that we study the elliptic curve

$$y^2 = x^3 + a^2x^2 - b^2c^2x. \tag{25}$$

Note that $D = b^4c^4(a^4+4b^2c^2) \neq 0$. If in (25) we take $a^2x^2 - b^2c^2x = 0$, then we get $x = \frac{b^2c^2}{a^2}$ and $y = \frac{b^3c^3}{a^3}$. Then the first point on (25) is $P_1 = (\frac{b^2c^2}{a^2}, \frac{b^3c^3}{a^3})$. Note that the order of this point is infinite, because in a PPT the number bc is not divisible by a, and the numbers $\frac{b^2c^2}{a^2}$ and $\frac{b^3c^3}{a^3}$ are not integers, this can be similarly proven. Then we conclude that the rank of the elliptic curve (25) is always positive. By letting $x^3 + a^2x^2 = 0$, we get $x = -a^2$ and $y = abc$. Then the second point on (25) is the point $P_2 = (-a^2, abc)$. Letting $x^3 - b^2c^2x = 0$, yields the third and fourth points $P_{3,4} = (\pm bc, abc)$. □

Remark 9.2. *Note that if in a PPT (a, b, c), a is odd, then we may prove by another method that the rank of the aforementioned elliptic curve is positive. We prove that in the point $P_2 = (-a^2, abc)$, the number abc does not divide D, otherwise abc must divide $4b^6c^6$. Then a divides b^6c^6, because a is odd. This is not correct, because (a, b, c) is a PPT. Then the point P_2 is of infinite order. Now the result follows.*

Acknowledgements

We are very grateful to the unknown referees for careful reading of the paper and giving several useful comments, which improved the quality of this paper. The first author would like to present this work to his parents and his wife.

References

[1] Dujella, A. (2012) High rank elliptic curves with prescribed torsion. Available online: `http://www.maths.hr/~duje/tors.html`.

[2] Fermigier, S. (1996) Construction of high-rank elliptic curves over $\mathbb{Q}$ and $\mathbb{Q}(t)$ with non-trivial 2-torsion. In: Cohen H. (eds) Algorithmic Number Theory. ANTS 1996, 115–120. *Lecture Notes in Computer Science*, Vol: 1122. Springer, Berlin, Heidelberg.

[3] Izadi, F. & Nabardi, K. (2016) A family of elliptic curves of rank at least 4, *Involve journal of mathematics*, 9(5), 733–736.

[4] Izadi, F., Nabardi, K., & Khoshnam, F. (2011) On a family of elliptic curves with positive rank arising from Pythagorean triples. Available online: `https://arxiv.org/abs/1012.5837`.

[5] Nagao, K. & Kouya, T. (1994) An example of an elliptic curve over $\mathbb{Q}$ with Rank ≥ 21, *Proc. Japan Acad*, Ser: A, 70(4), 104–105.

[6] Naskrecki, B. (2013) Mordell–Weil ranks of families of elliptic curves associated to Pythagorean triples, *Acta Arith*, 160(2), 159–183.

[7] Park, J., Poonen, B., Voight, J., & Wood M. M. (2016) A heuristic for boundedness of ranks of elliptic curves. Available online: `http://arxiv.org/abs/1602.01431`.

[8] `SAGE` software. Available online: `http://sagemath.org`.

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

[10] Silverman, J. H. (1994) *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, New York.

[11] Washington, L. C. (2008) *Elliptic Curves: Number Theory and Cryptography*, Chapman-Hall.