EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
Vol. 7, No. 2, 2014, 131-139
ISSN 1307-5543 – www.ejpam.com

Elliptic Curves and Pythagorean Triples

Farzali Izadi, Kamran Nabardi*

Department of Pure Mathematics, Azarbaijan Shahid Madani University, Tabriz, Iran

Abstract. The aim of this paper is to study the family of elliptic curves of the form

$$y^2 = x(x-a^2)(x-b^2),$$

where (a,b,c) is a primitive Pythagorean triple. First we show that the rank is positive. Then we construct some subfamilies with rank ≥ 2 by different methods.

2010 Mathematics Subject Classifications: 11G05, 14H52, 14G05
Key Words and Phrases: Elliptic curves, Rank, Pythagorean triples

1. Introduction

An elliptic curve E over the rational field $\mathbb{Q}$ is a curve that is given by

$$Y^2 = X^3 + aX^2 + bX + c, \quad a,b,c \in \mathbb{Q}, \tag{1}$$

with the condition that the polynomial $X^3 + aX^2 + bX + c$ has no multiple zeroes. Mordell proved that on an elliptic curve over $\mathbb{Q}$, the rational points form a finitely generated abelian group which is denoted by $E(\mathbb{Q})$ [2]. Here we can apply the structure theorem for the finitely generated abelian groups to $E(\mathbb{Q})$ to obtain a decomposition of $E(\mathbb{Q}) \simeq \mathbb{Z}^r \times E(\mathbb{Q})_{\text{tors}}$, where r is an integer called the rank of E and $E(\mathbb{Q})_{\text{tors}}$ is the finite abelian group consisting of all elements of finite order in $E(\mathbb{Q})$.

In 1976, Barry Mazur proved the following seminal result [4]. The torsion group $E(\mathbb{Q})_{\text{tors}}$ of any elliptic curve E over $\mathbb{Q}$ is one of the following 15 types. Moreover, each of these cases occurs for infinitely many curves E over $\mathbb{Q}$.

$$\begin{cases} \mathbb{Z}/m\mathbb{Z} & m = 1,2,3,\ldots,10,12, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} & m = 2,4,6,8. \end{cases} \tag{2}$$

This shows that $E(\mathbb{Q})$ cannot contain a point of order 11, nor of any order $n \geq 13$.

*Corresponding author.

Email addresses: farzali.izadi@azaruniv.edu (F. Izadi), nabardi@azaruniv.edu (K. Nabardi)

On the other hand, it is not known which values of r are possible. The current record is an example of elliptic curve over $\mathbb{Q}$ with $r \geq 28$ found by Elkies in May 2006.

In this paper, we first introduce a family of elliptic curves over $\mathbb{Q}$ of the form

$$y^2 = x(x-a^2)(x-b^2),$$

where, (a,b,c) is a pythagorean triple and show that they have positive ranks. In section 2, we briefly describe the construction of this family and show that its the torsion group is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Then we prove that it has positive rank. Finally by using by MRANK program [1], we can find some curves with rank 5. In section 3, we describe a method to find a subfamily with rank ≥ 2. The resulting subfamily corresponds to the points of a specific elliptic curve having positive rank too. Finally in section 4, by letting $a = t^2 - 1$, $b = 2t$, and $c = t^2 + 1$ as functions of the rational parameter t, we study the family as a parameter family and show that it has a subfamily of rank ≥ 2. By this method we can find 4 curves of rank equal to 6.

Remark 1. *If s is any nonzero rational number, then replacing (a,b,c) by (sa,sb,sc), one has $(sa)^2 + (sb)^2 = (sc)^2$ (but possibly these numbers are rational rather than integral), and the corresponding elliptic curve*

$$y^2 = x(x-(sa)^2)(x-(sb)^2),$$

is over $\mathbb{Q}$ isomorphic to the original one. The isomorphism is given by $(x,y) \to (s^2x, s^3y)$. In particular this implies that it is not necessary to demand that the pythagorean triple is primitive. Whenever it is convenient in some proof, we can assume the triple to be primitive, without loss of generality.

Our main motivation for the study of this family is its similarity with the well-known Frey curves of the form

$$y^2 = x(x-a^2)(x+b^2) \tag{3}$$

with $a^2 + b^2 = c^2$.

2. Results About The New Family of Curves

A primitive pythagorean triple is a triple of nonzero integers (a,b,c) so that a, b, and c have no common divisors and satisfy the relation $a^2 + b^2 = c^2$. In general, we can generate (a,b,c) by the following relations:

$$a = i^2 - j^2, \quad b = 2ij, \quad c = i^2 + j^2, \tag{4}$$

where gcd $(i,j) = 1$, and i, j have opposite parity.

Throughout, we focus on the elliptic curves of the form

$$y^2 = x(x-a^2)(x-b^2), \tag{5}$$

where (a,b,c) is a primitive pythagorean triple.

Lemma 1. *Let E be given by $y^2 = x^3 + ax^2 + bx + c$ and $P = (x, y) \in E(\mathbb{Q})$. Then P has order 2 if and only if $y = 0$.*

Proof. Please see [10, page 77]. □

Lemma 2. *The elliptic curve defined by* (5) *has three points of order 2.*

Proof. It is clear that the points $P_1 = (0,0), P_2 = (a^2, 0), P_3 = (b^2, 0)$ are of order 2. Then $E(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ □.

We wish to show the torsion group of (5) is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. So we have to prove that there are no points of order 4, 6, and 8. In order to show that the above family has no point of order 4, we need the following theorem.

Theorem 1. *Let E be an elliptic curve defined over a field $\mathbf{F}$ by the equation*

$$y^2 = (x-\alpha)(x-\beta)(x-\gamma) = x^3 + ax^2 + bx + c,$$

where $Char(\mathbf{F}) \neq 2$. For $(x', y') \in E(\mathbf{F})$, there exists $(x, y) \in E(\mathbf{F})$ with $2(x, y) = (x', y')$, if and only if $x' - \alpha$, $x' - \beta$, and $x' - \gamma$ are squares.

Proof. See [2, Theorem 4.1, page 37]. □

Applying this theorem to our family, we get the following result.

Proposition 1. *The elliptic curve in the form* (5) *does not have any points of order* 4.

Proof. Let $P = (x, y) \in E(\mathbb{Q})$ be such that $4P = \mathcal{O}$. Then one of following cases must be true:

$$2P = (0,0), \qquad 2P = (a^2, 0), \qquad 2P = (b^2, 0).$$

If $2P = (0,0)$, then $-a^2$ and $-b^2$ are squares which are contradiction.

Let $2P = (a^2, 0)$, then $a^2 - b^2$ is a square. So we have, $a^2 - b^2 = d^2$ for some $d \in \mathbb{Z}$ and $a^2 + b^2 = c^2$. Therefore $(\frac{a}{b})^2 - 1 = (\frac{d}{b})^2$ and $(\frac{a}{b})^2 + 1 = (\frac{c}{b})^2$. This means that 1 is a congruent number again a contradiction. The case $2P = (b^2, 0)$ is similar. □

Corollary 1. *There is no points of order* 8 *on* (5).

The following proposition is also necessary.

Proposition 2. *The elliptic curve in the form* (5) *does not have any points of order* 6.

Proof. By interchanging a and b if necessary, one may assume $a^2 < b^2$. Then after one replaces x by $x + b^2$, the elliptic curve E is given by

$$y^2 = x(x + b^2)(x + b^2 - a^2).$$

Applying a result of Ono [5, Main Theorem 1] to this equation, it follows that $E(\mathbb{Q})$ contains a point of order 6 iff $A, B \in \mathbb{Z}$ exist satisfying

$$\begin{cases} A^4 + 2A^3B = b^2; \\ B^4 + 2B^3A = b^2 - a^2. \end{cases}$$

Recall that without loss of generality we can assume (a, b, c) to be a primitive pythagorean triple. Then only two possibilities may occur:

if b is even, then a is odd, and modulo 4 the above system looks like

$$\begin{cases} A^4 + 2A^3B \equiv 0 \pmod 4; \\ B^4 + 2B^3A \equiv -1 \pmod 4. \end{cases}$$

this is impossible since it implies that A is even and hence -1 would be a square modulo 4.

Similarly, if b is odd, then a is even since otherwise $a^2 + b^2$ cannot be a square. Hence one obtains the system

$$\begin{cases} A^4 + 2A^3B \equiv 1 \pmod 4; \\ B^4 + 2B^3A \equiv 1 \pmod 4 \end{cases}$$

implying that both A and B are odd. So it would follow that $1 + 2 \equiv 1 \pmod 4$ which is again a contradiction. □

Now the following corollary is immediate.

Corollary 2. *$E(\mathbb{Q})_{tors}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

Theorem 2. *For each pythagorean triple (a, b, c), the elliptic curve $y^2 = x(x - a^2)(x - b^2)$ has a positive rank.*

Proof. It suffices to consider the point $Q = (c^2, abc)$ on (5). Clearly $Q \notin \{P_1, P_2, P_3, \mathcal{O}\}$ and so it is a point of infinite order. □

After searching through 202,461 curves with $i, j \leq 1000$, we found 53 curves of rank 5. The first curve with rank 5 is generated with $(i, j) = (65, 58)$ and its generators are the following:

P1 =[57564577194761/1008016,29006793653594700125/1012048064],

P2 =[165532287616200/2745649,505394258095121556600/4549540393],

P3 =[6192906993/64,311795186829399/512],

P4 =[24834332880/121,3321719539155360/1331],

P5 =[341015696,5742307020800].

3. Subfamily of Rank ≥ 2

In this section, we consider a subfamily of (5) having rank ≥ 2. To do this, let the point $R=(2a^2, y_0)$ be on (5). We are going to show that the points Q and R are independent.

If $R=(2a^2, y_0)$ be on (5), then we have $y_0^2 = 2a^4(2a^2-b^2)$. This implies that $2a^2-b^2=2k^2$ ($k\in\mathbb{Z}$) or equivalently

$$u^4-4u^2+1=v^2, \tag{6}$$

where $u=i/j$ (or $u=j/i$) and $v=k/j^2$ (or $v=k/j^2$). From (6) one can easily get an elliptic curve of the form

$$y^2=x^3-4x^2-4x+16=(x+2)(x-2)(x-4). \tag{7}$$

This elliptic curve has a group of rational points isomorphic to

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

The group of rational points is generated by the torsion points $(\pm 2, 0)$ together with the point of infinite order $T=(0,4)$. For each $n\in\mathbb{N}$ we have point $(x_n, y_n)=nT$ on (7), which corresponds to a point (u_n, v_n) on (6) (see [10, section 2.17, p. 37]) by

$$u_n=\frac{\pm 2(x_n-4)}{y_n}\,, \qquad v_n=\frac{\mp(2-u_n^2x_n)}{2}. \tag{8}$$

This turn in gives rise to some particular values of (i,j,k) two points of the forms (c^2, abc) and $(2a^2, 2a^2k)$ on (5) where k is dependent on i, j.

In the next step, showing that these two points $((i^2+j^2)^2, 2ij(i^4-j^4))$ and $(2(i^2-j^2)^2, 2(i^2-j^2)^2k)$ are independent.

Now we are going to find a value of n and the corresponding (i,j,k) such that these two points be independent. For $n=2$ and consequently $(i,j,k)=(15,4,191)$, we obtain the elliptic curve

$$y^2=x^3-58081x^2+629006400x,$$

and the points

$$P=(58081, 6044280),$$
$$Q=(87362, 16686142).$$

By using the SAGE software [6], we see that the associated height matrix has non-zero determinant 50.3755 showing that the points are independent. So the specialization result of Silverman implies that for all but finitely many rational numbers, the specialized curve also has rank at least 2. In the following we have listed some curves of this type with rank ≥ 2.

Table 1: Some curves with rank≥ 2.

nT	(i,j)	curve	rank
$3T$	$(442,161)$	$y^2 = x^3 - 48967051225x^2$ $+581572076457241803024x$	$2 \leq rank \leq 4$
$4T$	$(50369,22920)$	$y^2 = x^3 - 9378064455014478721x^2$ $+215747872399923602935500974868111936 00x$	$2 \leq rank \leq 3$
$5T$	$(21771082,2706401)$	$y^2 = x^3 - 231654135138249459108043425625x^2$ $+302410530362469817550063467517780 4$ $150875856530043176017358 4x$	$2 \leq rank \leq 4$

4. General Case

We began the paper with the equation $a^2 + b^2 = c^2$, which can be regarded as the defining equation of a rational curve B in $\mathbb{P}^2$, defined over $\mathbb{Q}$. The curve **B** parameterizes a family of cubic curves, given as $y^2 = x(x-a^2)(x-b^2)$. These curves are elliptic, except over 8 points of **B**, namely over $(1 : \pm 1 : \pm\sqrt{2})$ and $(0 : 1 : \pm 1)$ and $(1 : 0 : \pm 1)$. The curve **B** is isomorphic to $\mathbb{P}^1$; the isomorphism is presented in (4):

$$\mathbb{P}^1 \simeq \mathrm{B}: \quad (i : j) \longmapsto (i^2 - j^2 : 2ij : i^2 + j^2).$$

With $t := i/j$ as a coordinate function on $\mathbb{P}^1$, this allows to write the family of cubics as

$$y^2 = x(x-(t^2-1)^2)(x-4t^2). \tag{9}$$

This equation corresponds to an elliptic surface $\pi : \mathscr{E} \to \mathbb{P}^1$ defined over $\mathbb{Q}$, or equivalently, an elliptic curve E over the rational function field $\mathbb{Q}(t)$. The surface $\mathscr{E}$ is a so-called **K3**-surface. From Tate's algorithm one calculates that of the 8 singular fibers of π, 4 are of type I_4 and the other 4 are of type I_2. Moreover one finds two points in $E(\mathbb{Q}[\sqrt{-2}](t))$ namely $S_1 := ((t^2+1)^2, 2t(t^4-1))$ and $S_2 := (-4t^2, 4t(t+1)\sqrt{-2})$. Note that S_1 specializes to the point Q used in the proof of the Theorem 2. A standard intersection calculation [9] shows that S_1 and S_2 are linearly independent. Using the Shioda-Tate formula for $\pi : \mathscr{E} \to \mathbb{P}^1$ and the fact that $\mathscr{E}$ is **K3**, it follows that

$$20 \geq 2 + 4 \cdot 3 + 4 \cdot 1 + \mathrm{rank}(E(\mathbb{Q}[\sqrt{-2}](t))) \geq 20,$$

hence

$$\mathrm{rank}(E(\mathbb{Q}[\sqrt{-2}](t))) = 2.$$

The nontrivial element $\sigma \in \mathrm{Gal}(\mathbb{Q}[\sqrt{-2}]/\mathbb{Q})$ satisfies $\sigma(S_1) = S_1$ and $\sigma(S_2) = -S_2$. As a consequence, the $+1$-eigenspace of σ, i.e., the subgroup $E(\mathbb{Q}(t))$, has rank 1. Silverman's specialization result implies that for all but infinitely many specialization of t to a rational number, the specialized elliptic curve over $\mathbb{Q}$ obtained in this way has positive rank as well.

Theorem 2 shows that in fact a stronger assertion is true: whenever this specialization defines an elliptic curve (so, for all rational $t_0 \neq \{0, \pm 1\}$), the rank is positive. It is interesting to remark that $\mathscr{E}$ provides an example of a so-called singular **K3**-surface defined over $\mathbb{Q}$: one such that the Picard number attains the maximal value 20. However, this value 20 is only attained over an extension of $\mathbb{Q}$; a small calculation shows it is the extension $\mathbb{Q}[\sqrt{2}, \sqrt{-2}]$. More on such singular **K3**'s over $\mathbb{Q}$ can be read in [7].

To obtain larger ranks over $\mathbb{Q}$ one now applies base changes. This idea is well known; for example, it was used in [3]. A simple explanation is that one replace the field $\mathbb{Q}(t)$ by a finite extension $\mathbb{Q}(C)$, the function field of some curve C defined over $\mathbb{Q}$. If $E(\mathbb{Q}(C))$ has rank r, then the same specialization result of Silverman implies that for all but only finitely many rational points on C, the specialized curve also has rank at least r. In particular, this can only be used for constructing infinitely many specializations with high rank, of the curve C contains infinitely many rational points.

If one wants a point in $E(\mathbb{Q}(C))$ with x-coordinate equal to $2(t^2-1)^2$, one needs that

$$2(2(t^2-1)^2 - 4t^2) = 4t^4 - 16t^2 + 4,$$

is a square, say $= s^2$. The equation $s^2 = 4t^4 - 16t^2 + 4$ defines a curve C_1 of genus 1 with infinitely many rational points, namely this is the example discussed in Section 3. The two points S_1 (defined earlier) and

$$S_3 := (2(t^2-1)^2, (t^2-1)^2 s)$$

are independent in $E(\mathbb{Q}(C_1))$, since their images after a given specialization are independent.

Instead of a point with x-coordinate equal to $2(t^2-1)^2$, other slightly simpler points work as well. For example, take $x = 8t^2$. Then one wants $2(8t^2 - (t^2-1)^2)$ to be a square. The curve C_2 defined by $u^2 = -2t^4 + 20t^2 - 2$ has infinitely many rational many points as well. It corresponds to the elliptic curve given by

$$y^2 = x(x + \frac{3}{2})(x + \frac{1}{2}),$$

which has

$$\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}),$$

as its group of rational points. In $E(\mathbb{Q}(C_2))$ one has by construction the point $S_4 := (8t^2, 4t^2 s)$ which turns out to be independent of S_1. So again, specialization yields infinitely many example of rank at least 2 over $\mathbb{Q}$.

By taking $x = t^2 - 1$, one needs that $3t^4 - 5t^2 - 2$ is a square, say $= s^2$. The curve C_3 defined by $s^2 = 3t^4 - 5t^2 - 2$ has infinitely many rational points as well. It corresponds to the elliptic curve given by

$$y^2 = (x-3)(x^2 + 4x + 28),$$

which has

$$\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z}),$$

as its group or rational points. So in $E(\mathbb{Q}(C_3))$ one has by construction the point $S_5 := (t^2-1,(t^2-1)^2 s)$ which turns out to be independent of S_1.

Now We would like to follow the method described on [8, Page 89], to find a subfamily of rank at least 2.

Consider $A=-(t^2+1)^2$ and $B=4t^2(t^2-1)^2$. Let $B=b_1b_2$, if one can find integers M,N,e such that $\gcd(M,e)=\gcd(N,e)=\gcd(b_1,e)=1$ and $b_1M^4+AM^2e^2+b_2e^4=N^2$, then $(b_1M^2/e^2, b_1MN/e^3)$ is a point on (9) as well. We let $b_1=(t^2-1)$, $M=2$ and $e=1$. After a little computation one gets

$$4t^2-20=N^2. \tag{10}$$

A particular solution for (10) is $(t,N)=(3,4)$. Using this solution we can parameterize the corresponding hyperbola as following:

$$t=\frac{3m^2-8m+12}{m^2-4}, \qquad N=\frac{4(m^2-6m+4)}{4-m^2},\ m\in\mathbb{Q}. \tag{11}$$

It is clear that $|t|\geq\sqrt{5}$ or equivalency $|m|>2$. By taking any rational values $m>2$, we get a rational value of t as (11), we see that the point $(4(t^2-1),2(t^2-1)N)$ is on (9). In order to show that the points $S_1=((t^2+1)^2,2t(t^4-1))$ and $S_6:=(4(t^2-1),2(t^2-1)N)$ are independent we use specialization $(m,t,N)=(4,7/3,4/3)$. This gives rise to following elliptic curve

$$E_{7/3}: y^2=x^3-\frac{3364}{81}x^2+\frac{313600}{729}x,$$

and the points

$$P=(\frac{3364}{81},\frac{32480}{243}), \quad Q=(\frac{160}{9},\frac{320}{27}).$$

Now the associated height matrix of the above points has non-zero determinant 1.011058 showing that they are independent. By letting m as $m=\alpha/\beta$ with $\alpha\ ,\beta\leq 350$, we found 4 curves of rank 6. In particular $m=128/33$, $m=152/27$, $m=252/29$, and $m=348/71$ we get the following curves with rank exactly 6.

$$\begin{aligned}
y^2=&x^3-3546380914044004/81758650118401x^2\\
&+34741313501027127696000 0/739265720544437643649x,\\
y^2=&x^3-23507162841329764/648833431339681x^2\\
&+53598351057957534044736 00/16527220769271504425329x,\\
y^2=&x^3-3546380914044004/81758650118401x^2\\
&+34741313501027127696000 0/739265720544437643649x,\\
y^2=&x^3-23507162841329764/648833431339681x^2\\
&+53598351057957534044736 00/16527220769271504425329x.
\end{aligned}$$

References

[1] J. Cremona. MWRANK program, available from http://www.maths.nottingham.ac.uk/personal/jec/ftp/progs/

[2] D. Husemoller. Elliptic Curves, Springer-Verlag, New York, 1987.

[3] M. Kuwata and J. Top. A singular **K3** surface related to sums of consecutive cubes, Indagationes Mathematicae, 11(3), 419-435, 2000.

[4] B. Mazur. Rational Isogenies of Prime Degree (with an Appendix by D.Goldfeld), Inventions Mathematicae, 44(2), 129-162, 1978.

[5] K. Ono. Euler's Concordant Forms, Acta Arithmetica 78, pp. 101-123. 1996.

[6] Sage Team. SAGE software, available from http://sagemath.org.

[7] M. Schütt. **K3**-surfaces of Picard rank 20 over $\mathbb{Q}$, Algebra & Number Theory, 4(3), 335-356, 2010.

[8] J.H. Silverman and J. Tate. Rational Points on Elliptic Curves, Undergraduate Texts in Mathemathics, Springer-Verlag, New York, 1992.

[9] T. Shioda. On the Mordell-Weil Lattices, Commentarii Mathematici Universitatis Sancti Pauli, 39(2), 211-240, 1990

[10] L.C. Washington. Elliptic Curves: Number Theory and Cryptography, Chapman-Hall, 2008.