A NEW FAMILY OF ELLIPTIC CURVES WITH POSITIVE RANK ARISING FROM PYTHAGOREAN TRIPLES

F.A.IZADI K.NABARDI F.KHOSHNAM

ABSTRACT. The aim of this paper is to introduce a new family of elliptic curves in the form of $y^2 = x(x-a^2)(x-b^2)$ that have positive ranks. We first generate a list of pythagorean triples (a, b, c) and then construct this family of elliptic curves. It turn out that this new family have positive ranks and search for the upper bound for their ranks.

Keywords: elliptic curves; rank; pythagorean triples

AMS Classification: MSC2000.primary 14H52 ; Secondary 11G05, 14G05.

1. INTRODUCTION

An elliptic curve E over a field F is a curve that is given by an equation of the form

$$Y^2 + a_1XY + a_3 = X^3 + a_2X^2 + a_4X + a_6, \quad a_i \in F. \tag{1.1}$$

We let $E(F)$ denote the set of points $(x, y) \in F^2$ that satisfy this equation, along with a point at infinity denoted O [4].
In order for the curve (1.1) to be an elliptic it must be smooth, in other words, the three equations

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, \tag{1.2}$$

$$a_1Y = 3X^2 + 2a_2X + a_4 \quad and \quad 2Y + a_1X + a_3 = 0$$

cannot be simultaneously satisfied by any $(x, y) \in E(\overline{F})$.

If $Char(F) \neq 2$, then we can reduce (1.1) to the following form

$$Y^2 = X^3 + aX^2 + bX + C \tag{1.3}$$

with the *discriminant* :

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2. \tag{1.4}$$

If furthermore the $Char(F)$ does not divide 6, then we get the simplest form of

$$Y^2 = X^3 + aX + b, \tag{1.5}$$

with the

$$D = -16(4a^3 + 27b^2). \tag{1.6}$$

Remark 1.1. The elliptic curve is smooth if and only if $D \neq 0$ [9].

2. Elliptic curves over Q

Mordell proved that on a rational elliptic curve, the rational points form a finitely generated abelian group, which is denoted by $E(Q)$ [4]. Hence we can apply the structure theorem for the finitely generated abelian groups to $E(Q)$ to obtain a decomposition of $E(Q) \cong Z^r \times Tors_E(Q)$, where r is an integer called the *rank* of E and $Tors_E(Q)$ is the finite abelian group consisting of all the elements of finite order in $E(Q)$.
In 1976, *Barry Mazur*, proved the following fundamental result:

$$\begin{array}{ll} \frac{Z}{mZ} & m = 1, 2, 3, ..., 10, 12 \\ \frac{Z}{2Z} \oplus \frac{Z}{mZ} & m = 2, 4, 6, 8 \end{array} \tag{2.1}$$

which shows that there is no points of order 11, and any $n \geq 13$.
There is an important theorem proved by *Nagell* and *Lutz*, which tells us how to find all of the rational points of finite order.

Theorem 2.1. *(Nagell-Lutz) Let E be given by $y^2 = x^3 + ax^2 + bx + c$ with $a, b, c \in Z$. Let $P = (x, y) \in E(Q)$. Suppose P has finite order, Then $x, y \in Z$ and either $y = 0$ or $y|D$.*

Proof. ([8] . *pp* . 56). □

Theorem 2.2. *Let E be given by $y^2 = x^3 + ax^2 + bx + c$ and, $P = (x, y) \in E(Q)$. P has an order 2 if and only if $y = 0$.*

Proof. ([9]. *pp* .77) . □

On the other hand, it is not known which values of *rank* r are possible. The current record is an example of elliptic curve over Q with *rank* ≥ 28 found by *Elkies* in may 2006 [2].

In this Paper we first introduce a family of elliptic curves over Q and show that they have positive rank, then search for the largest ranks possible.

3. Pythagorean triples

A primitive pythagorean triple is a triple of numbers (a, b, c) so that a , b and c have no common divisors and satisfy

$$a^2 + b^2 = c^2. \tag{3.1}$$

It's not hard to prove that if one of a or b is odd then the other is even, then c is always odd.
In general , we can generate (a, b, c) by the following relations:

$$a = i^2 - j^2 \qquad b = 2ij \qquad c = i^2 + j^2 \tag{3.2}$$

where $(i, j) = 1$ and i, j have oppositive parity.
The other way to generate (a, b, c) is the following forms:

$$a = \frac{i^2 - j^2}{2} \qquad b = ij \qquad c = \frac{i^2 + j^2}{2} \tag{3.3}$$

where $i > j \geq 1$ are chosen to be odd integers with no common factors [7].

The following table gives all possible triples with $i, j < 10$.

i	j	$a = i^2 - j^2$	$b = 2ij$	$c = i^2 + j^2$	(a, b, c)
2	1	3	4	5	$(3, 4, 5)$
3	2	5	12	13	$(5, 12, 13)$
4	1	15	8	17	$(15, 8, 17)$
4	3	7	24	25	$(7, 24, 25)$
5	2	21	20	29	$(21, 20, 29)$
5	4	9	40	41	$(9, 40, 41)$
6	1	35	12	37	$(35, 12, 37)$
6	5	11	60	61	$(11, 60, 61)$
7	2	45	28	53	$(45, 28, 53)$
7	4	33	56	65	$(33, 56, 65)$
7	6	13	84	85	$(13, 84, 85)$
8	1	63	16	65	$(63, 16, 65)$
8	3	55	48	73	$(55, 48, 73)$
8	5	39	80	89	$(39, 80, 89)$
8	7	15	80	113	$(15, 80, 113)$
9	2	77	36	85	$(77, 36, 85)$
9	4	65	72	97	$(65, 72, 97)$
9	8	17	144	145	$(17, 144, 145)$

TABLE 1. Generation pythagorean triples by i, j in range10

4. Structure Of The Curves

First we generate a list of pythagorean triples (a, b, c) with $i, j \leq 1000$. This yields a list of 202461 triples. Each (a, b, c) gives rise to the elliptic curve in the form

$$y^2 = x(x - a^2)(x - b^2). \tag{4.1}$$

Then we compute the $2 -$ *selmer ranks* of these curves as upper bounds on the *Mordell* $-$ *Weil ranks*, finally, by using *Mwrank*, we can obtain the ranks of corresponding curves.

5. Results about the new family of curves

Remark 5.1. The elliptic curve in the form $y^2 = x(x-a^2)(x-b^2)$ for any pythagorean triples (a, b, c) is smooth, in fact $a \neq b$ and both are nonzero.

Remark 5.2. In the equation (4.1), let j be a constant and write (4.1), in the form (1.5). So a and b, are polynomials of i, and their degree are equal to 8 and 12. By [2], we have $r \leq 2\max\{3dega, 2degb\} = 48$

Lemma 5.3. *The elliptic curve in the form* (4.1) *has four 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 $2E(Q) \simeq \frac{Z}{2Z} \oplus \frac{Z}{2Z}$. □

Theorem 5.4. *Let E be an elliptic curve defined over a field F, by the equation $y^2 = (x-\alpha)(x-\beta)(x-\gamma) = x^3 + ax^2 + bx + c$, where $Char(F) \neq 2$. For $(x', y') \in E(F)$, there exists $(x, y) \in E(F)$ with $2(x, y) = (x', y')$, if and only if $x' - \alpha$, $x' - \beta$, and $x' - \gamma$ are squares.*

Proof. ([4]. Th 4.1. pp.37). □

Theorem 5.5. *The elliptic curve in the form* (4.1) *doesn't have any point of order* 4*.*

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

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

If $2P = (0,0)$, then $-a^2$ and $-b^2$, are squares, which is a contradiction. If $2P = (a^2,0)$, then $a^2 - b^2$ is a square. So we have, $a^2 - b^2 = d^2$ for some $d \in Z$ and $a^2 + b^2 = c^2$. Therefore $(\frac{a}{b})^2 - 1 = (\frac{d}{b})^2$ and $(\frac{a}{b})^2 + 1 = (\frac{c}{b})^2$. It turn out that 1 is a congruent number again a contradiction. The case $2P = (b^2,0)$ is similar. □

Corollary 5.6. *There is a no point of order* 8 *on* (4.1) .

Kubert [5], showed that if $y^2 = x(x + r)(x + s)$, with $r, s \neq 0$ and $s \neq r$, then the torsion subgroup is $\frac{Z}{2Z} \times \frac{Z}{2Z}$. So our family have $\frac{Z}{2Z} \times \frac{Z}{2Z}$ as torsion subgroup.

Lemma 5.7. *For each pythagorean triple (a, b, c), the elliptic Curve $y^2 = x(x - a^2)(x - b^2)$ has a positive rank.*

Proof. Choose $x = c^2$, then $P = (c^2, \pm abc)$. We show that for each (a, b, c), abc does not divide the *discriminant* D, where $D = a^4b^4(c^4 - 4a^2b^2)$. If $abc \mid a^4b^4(c^4 - 4a^2b^2)$ then $c \mid a^3b^3(c^4 - 4a^2b^2)$. Let p is a prime number such that $p \mid c$, then $p \mid -4a^2b^2$, but c is odd, then $p \neq 2$ so $p \mid a^2b^2$ and hence $p|a$ or $p|b$, which is a contradiction. So $p = (c^2, \pm abc)$ has integer coordinate in which $y = \pm abc$ does not divide D. Therefore by $Nagell - Lutz$ theorem P does not have finite order. This implies that $r \geq 1$. □

6. Numerical Results

After searching through 202461 curves, we found 12 curves with *selmer* 6. But unfortunately none of them had *rank* 6. Also we found 831 curves with *selmer* 5, leading to 52 curves of rank 5.
The first curve that generated by first pythagorean triple (3, 4, 5) has *rank* 1.

In the following table, we listed the curves that have selmer equals to 6, without being able to compute their exact ranks with MWrank.

i	j	(a, b, c)	curve	bound
598	53	$(354795, 63388, 360413)$	$y^2 = x^3 - 129897530569x^2$ $+50578865085559061160 0x$	$4 \leq r \leq 6$
629	202	$(354837, 254116, 436445)$	$y^2 = x^3 - 190484238025x^2$ $+8130585454709316664464x$	$4 \leq r \leq 6$
760	113	$(564831, 171760, 590369)$	$y^2 = x^3 - 348535556161x^2$ $+9411982512955600953600x$	$4 \leq r \leq 6$
777	232	$(549905, 360528, 657553)$	$y^2 = x^3 - 432375947809x^2$ $+39305500949380532025600x$	$4 \leq r \leq 6$
801	560	$(328001, 897120, 955201)$	$y^2 = x^3 - 912408950401x^2$ $+86586744854271550694400x$	$1 \leq r \leq 6$
821	242	$(615477, 397364, 732605)$	$y^2 = x^3 - 536710086025x^2$ $+59813703564011517306384x$	$2 \leq r \leq 6$
861	788	$(120377, 1356936, 1362265)$	$y^2 = x^3 - 1855765930225x^2$ $+26681224725077190456384x$	$2 \leq r \leq 6$
890	457	$(583251, 813460, 1000949)$	$y^2 = x^3 - 1001898900601x^2$ $+225104091544539413571600x$	$2 \leq r \leq 6$
917	846	$(125173, 1551564, 1556605)$	$y^2 = x^3 - 2423019126025x^2$ $+37719046943947124807184x$	$4 \leq r \leq 6$
957	788	$(294905, 1508232, 1536793)$	$y^2 = x^3 - 2361732724849x^2$ $+197833836741502151361600x$	$2 \leq r \leq 6$
958	691	$(440283, 1323956, 1395245)$	$y^2 = x^3 - 1946708610025x^2$ $+339790269763746950924304x$	$1 \leq r \leq 6$
964	173	$(899367, 333544, 959225)$	$y^2 = x^3 - 920112600625x^2$ $+89987080452485248355904x$	$2 \leq r \leq 6$

TABLE 2. The curves with selmer-rank 6.

In the following table, we listed some curves which have rank 5.

n	i	j	(a, b, c)	curve	*rank*
1	65	58	$(861, 7540, 7589)$	$y^2 = x^3 - 57592921x^2$ $+42145284963600x$	5
2	206	73	$(37107, 30076, 47765)$	$y^2 = x^3 - 2281495225x^2$ $+1245523255531937424x$	5
3	219	122	$(33077, 53436, 62845)$	$y^2 = x^3 - 3949494025x^2$ $+3124065342026615184x$	5
4	221	74	$(43365, 32708, 54317)$	$y^2 = x^3 - 2950336489x^2$ $+2011808689365056400x$	5
5	226	197	$(12267, 89044, 89885)$	$y^2 = x^3 - 8079313225x^2$ $+1193125293288351504x$	5
6	277	148	$(54825, 81992, 98633)$	$y^2 = x^3 - 9728468689x^2$ $+20206925530689960000x$	5
7	291	130	$(67781, 75660, 101581)$	$y^2 = x^3 - 10318699561x^2$ $+26299568174145411600x$	5
8	298	241	$(30723, 143636, 146885)$	$y^2 = x^3 - 21575203225x^2$ $+19473940840993453584x$	5
9	305	146	$(71709, 89060, 114341))$	$y^2 = x^3 - 13073864281x^2$ $+40786150175724531600x$	5
10	325	132	$(88201, 85800, 123049)$	$y^2 = x^3 - 15141056401x^2$ $+57269262954257640000x$	5

TABLE 3. Some curves with ranks 5.

n	Independent points
1	$(\frac{57564577194761}{1008016}, \frac{29006793653594700125}{1012048064}),(\frac{165532287616200}{2745649}, \frac{5053942580951215566600}{4549540393})$ $(\frac{6192906993}{64}, \frac{311795186829399}{512}),(\frac{24834332880}{121}, \frac{3321719539155360}{1331})$ $(341015696, 5742307020800)$
2	$(\frac{166618634504}{121}, \frac{311255416873240}{1331}),(\frac{12790926337}{9}, \frac{-153963331881884}{27})$ $(1862526649, 29434944424380),(\frac{14584697373888197298}{2226990481}, \frac{4595306032342994919592951945 8}{105093907788871})$ $(11173929032, 1060281679441544)$
3	$(\frac{1420783000225}{2704}, \frac{-3709951931018864055}{140608}),(\frac{3426388189979546}{3150625}, \frac{-198627986662927141534 06}{5592359375})$ $(\frac{3209176809789192}{1100401}, \frac{20777492819646247103496}{1154320649}),(\frac{5079795156916250}{1371241}, \frac{14550483032160729130895 0}{1605723211})$ $(11153906082, 964957876872066)$
4	$(1883980800, 2302931030400),(2049417864, 18414019508040)$ $(\frac{2442134720068225}{602176}, \frac{-7583340118114294623862 5}{467288576}),(8778656250, -683241762498750)$ $(\frac{389025929026}{9}, \frac{-234351164774907530}{27})$
5	$(\frac{40247709912197}{724201}, \frac{-39714502749350889700 94}{616295051}),(\frac{14644921094163784}{1292769}, \frac{96438697974718247422540 0}{1469878353})$ $(\frac{87950467020096}{6889}, \frac{504745975500657035040}{571787}),(18277955208, 1851757920077688)$ $(42787752953, 7974645953968408)$
6	$(\frac{52434265914}{249001}, \frac{-2562930282129146180 10}{124251499}),(120296250, -47872494168750)$ $(6723284800, 3861958531200),(\frac{112595270161250}{16129}, \frac{173400086111756488750}{2048383})$ $(\frac{14340640706653}{361}, \frac{47589097042950453054}{6859})$
7	$(\frac{2676650962237850}{1394761}, \frac{-23023471487528264011025 0}{1647212741}),(\frac{22163879894522425}{5216656}, \frac{-55462876566657254328592 5}{11914842304})$ $(\frac{34346962133043282}{5997601}, \frac{57316484301139284256098}{14688124849}),(6253062480, 74048765888160)$ $(\frac{109261411840568520}{717409}, \frac{3489231461884291715945652 0}{607645423})$
8	$(\frac{730404089870769}{891136}, \frac{-37789359740568919672425}{841232384}),(\frac{5478549187165109}{6056521}, \frac{-39487422947402698353371 0}{14905098181})$ $(20665851602, 118667705326126),(\frac{73166967363875922}{2745649}, \frac{923629275601913020162908 6}{4549540393})$ $(51598853768, 8996724544134712)$
9	$(1837492490, -192369433165070),(2274211682, -192094032181618)$ $(\frac{3557867077800}{361}, \frac{2050506769597435800}{6859})$ $(\frac{699532475085000}{32761}, \frac{127805414145000718410 00}{5929741}), (\frac{831997800678440}{29929}, \frac{18315695665342299799960}{5177717})$
10	$(7819306560, 11947900423680),(\frac{947937694496}{121}, \frac{18954422023540640}{1331})$ $(7908659200, 23645902425600),(\frac{49352010853464722}{4977361}, \frac{25823866566764625139051 18}{11104492391})$ $(\frac{6348468129250}{49}, \frac{-15061017382562550750}{343})$

TABLE 4. Independent points of curves of table 3.

i	j	(a,b,c)	curve	*rank*
26	17	$(387, 884, 965)$	$y^2 = x^3 - 931225x^2$ $+117037883664x$	4
43	24	$(1273, 2064, 2425)$	$y^2 = x^3 - 5880625x^2$ $+6903609110784x$	4
55	34	$(1869, 3740, 4181)$	$y^2 = x^3 - 17480761x^2$ $+48860938803600x$	4
63	40	$(2369, 5040, 5569)$	$y^2 = x^3 - 31013761x^2$ $+142557868857600x$	4
66	47	$(2147, 6204, 6565)$	$y^2 = x^3 - 43099225x^2$ $+177422080320144x$	4
71	58	$(1677, 8236, 8405)$	$y^2 = x^3 - 70644025x^2$ $+190765045779984x$	4
74	5	$(5451, 740, 5501)$	$y^2 = x^3 - 30261001x^2$ $+16271058387600x$	4
74	23	$(4947, 3404, 6005)$	$y^2 = x^3 - 36060025x^2$ $+283571724009744$	4
74	53	$(2667, 7844, 8285)$	$y^2 = x^3 - 68641225x^2$ $+437644224322704x$	4
78	35	$(4859, 5460, 7309)$	$y^2 = x^3 - 53421481x^2$ $+703848328419600x$	4

TABLE 5. Some curves with ranks 4.

i	j	(a,b,c)	curve	*rank*
13	6	$(133,156,205)$	$y^2 = x^3 - 42025x^2 + 430479504x$	3
13	10	$(69,260,269)$	$y^2 = x^3 - 72361x^2 + 321843600x$	3
19	6	$(325,228,397)$	$y^2 = x^3 - 157609x^2 + 5490810000x$	3
20	3	$(391,120,409)$	$y^2 = x^3 - 167281x^2 + 2201486400x$	3
21	8	$(377,336,505)$	$y^2 = x^3 - 255025x^2 + 16045795584x$	3
21	10	$(341,420,541)$	$y^2 = x^3 - 292681x^2 + 20511968400x$	3
4	3	$(7,24,25)$	$y^2 = x^3 - 625x^2 + 28224x$	2
5	2	$(21,20,29)$	$y^2 = x^3 - 841x^2 + 176400x$	2
7	4	$(33,56,65)$	$y^2 = x^3 - 4225x^2 + 3415104x$	2
8	1	$(63,16,65)$	$y^2 = x^3 - 4225x^2 + 1016064x$	2
9	2	$(77,36,85)$	$y^2 = x^3 - 7225x^2 + 7683984x$	2
2	1	$(3,4,5)$	$y^2 - 25x^2 + 144x$	1
3	2	$(5,12,13)$	$y^2 = x^3 - 169x^2 + 3600x$	1
4	1	$(15,8,17)$	$y^2 = x^2 - 289x^2 + 14400x$	1
5	4	$(9,40,41)$	$y^2 = x^3 - 1681x^2 + 129600x$	1
6	1	$(35,12,37)$	$y^2 = x^3 - 1369x^2 + 176400x$	1

TABLE 6. Some curves with rank 3,2, and 1.

REFERENCES

[1] J. Cremona, mwrank program, http://maths.nottingham.ac.uk/personal/jec/ftp/progs/.

[2] A. Dujella, History of Elliptic Curves Ranks Records, http://web.math.hr/˜ duje /tors/rankhist.html (2010) .

[3] E. Fouvry And J. Pomykala, Rang Des Courbes Et Sommes D'exponentielles. Monatsh.Math.116(1993), no.2 111-125.

[4] D. Husemoller, Elliptic Curves. Springer-Verlag, 1987.

[5] D. S. Kubert, Universal Bounds On The Torsion Of Elliptic Curves, Proc. London Math.Soc. (3), 33, 1976,pp.193-237.

[6] Sage software, version 4.3.5, http://sagemath.org.

[7] J. H. Silverman, A Friendly Introduction To Number Theory, Prentice-Hall, 2001.

[8] J. H. Silverman And J. Tate, Rational Points On Elliptic Curves, Springer-Verlag, 1992.
[9] L. C. Washington, Elliptic Curves Number Theory And Cryptography, Chapman-Hall, 2008.

Mathematics Department Azerbaijan university of Tarbiat Moallem , Tabriz, Iran f.izadi@utoronto.ca farzali.izadi@gmail.com

Mathematics Department Azerbaijan university of Tarbiat Moallem , Tabriz, Iran nabardi@azaruniv.edu

Mathematics Department Azerbaijan university of Tarbiat Moallem , Tabriz, Iran khoshnam@azaruniv.edu