FACTA UNIVERSITATIS (NIŠ)
Ser. Math. Inform. Vol. 34, No 4 (2019), 805–813
https://doi.org/10.22190/FUMI1904805K

FAMILY OF ELLIPTIC CURVES $E_{(p,q)} : y^2 = x^3 - p^2x + q^2$ *

Mehrdad Khazali and Hassan Daghigh

Abstract. In this paper we show that for any two primes p and q greater than 5, the elliptic curve $E_{(p,q)} : y^2 = x^3 - p^2x + q^2$ has rank at least 2. We will also provide two independent points on $E_{(p,q)}$. Then we will show that, conjecturally, the family $\{E_{(p,q)}\}$ contains an infinite subfamily of rank three elliptic curves.
Keywords. Elliptic curves; Abelian group; group homomorphism.

1. Introduction

Let E be an elliptic curve over $\mathbb{Q}$ and $E(\mathbb{Q})$ be its Mordell-Weil group over $\mathbb{Q}$ which is a finitely generated Abelian group. The rank of the free part of $E(\mathbb{Q})$ as a $\mathbb{Z}$ -module is called the rank of E over $\mathbb{Q}$. There has been a lot of research to compute the rank of the families of elliptic curves. Despite these attempts, there is no efficient algorithm for finding the rank of elliptic curves. So finding special forms of elliptic curves whose structure is known is very interesting. Many authors [7, 8, 9, 10, 11, 12, 16, 5, 6] have considered different families of elliptic curves and have computed their rank and integral points.
In this paper, we study elliptic curves of the form $E_{(p,q)} : y^2 = x^3 - p^2x + q^2$ over $\mathbb{Q}$, where p and q are primes greater than 5. We show that the torsion group of these curves is trivial, and also find at least two independent points on these curves, which means that $E_{(p,q)}$ has rank at least 2.

2. feature of points in $E(\mathbb{Q})$

In this section, we consider the structure of the group of rational points on the family of the following elliptic curves

$$E = E_{(p,q)} : y^2 = x^3 - p^2x + q^2, \tag{2..1}$$

Received July 03, 2019; accepted September 02, 2019
2010 *Mathematics Subject Classification.* Primary11G05; Secondary 14G05
*The authors were supported in part by the University of Kashan under grant number 808718.

where p and q are primes greater than 5. We will show that E has no torsion points and has rank at least 2. To show that $E(\mathbb{Q})$ has no nontrivial torsion point we need the following lemma.

Lemma 2.1. *Let E be an elliptic curve with integer coefficients. Suppose that E has good reduction modulo the prime r, and E_r is the reduction modulo r. The map*

$$E(\mathbb{Q})_{Tor} \longrightarrow E_r(\mathbb{F}_r)$$

is an injective group homomorphism.

Proof. This is a direct corollary of [14]. □

Theorem 2.2. *Let p and q be prime numbers greater than 5. The torsion part of E is trivial.*

Proof. We have $\Delta_E = -4p^6 + 27q^4$. It is easy to see that $3 \nmid \Delta_E$ and $5 \nmid \Delta_E$, therefore E has good reductions modulo 3 and 5. Let E_3 and E_5 be reductions of E modulo 3 and 5 respectively. By direct computation, we see that $|E_3(\mathbb{F}_3)| = 7$ and we have

$$|E_5(\mathbb{F}_5)| = \begin{cases} 8 & p^2 \equiv 1 \pmod 5. \\ 9 & p^2 \equiv 4 \pmod 5. \end{cases}$$

Now using Lemma 2.1, we see that $|E_{tors}(\mathbb{Q})|$ divides 7, and also 8 or 9, which means that $|E_{tors}(\mathbb{Q})| = 1$. This means that $E_{tors}(\mathbb{Q}) = \{\mathcal{O}\}$. □

By the Mordell-Weil theorem, $E(\mathbb{Q})$ is a finitely generated abelian group. Hence

$$E(\mathbb{Q}) = E(\mathbb{Q})_{Tor} \oplus \mathbb{Z}^r,$$

where r is the rank of $E(\mathbb{Q})$. In fact, (2..1) shows that in our case

$$E(\mathbb{Q}) \cong \mathbb{Z}^r.$$

Using this we have

$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^r.$$

Therefore $E(\mathbb{Q})/2E(\mathbb{Q})$ determines r. We record the above as the following proposition:

Proposition 2.3. *Let E be an elliptic curve on $\mathbb{Q}$ such that $E(\mathbb{Q})$ has no torsion point. Then*

$$E(\mathbb{Q})/2E(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^r,$$

where r is the rank of $E(\mathbb{Q})$.

To study our elliptic curve $E_{(p,q)}$, we start by the following lemmas about the features of the points in $E(\mathbb{Q})$.

Proposition 2.4. *Assume that $P = (x, y) \in E(\mathbb{Z})$. Then*

(i) y is odd.

(ii) $x \not\equiv 2, 4, 6 \pmod 8$.

Proof. The proof of (i) and (ii) are straightforward. □

Lemma 2.5. *Let $P = (x, y)$ be a point in $E(\mathbb{Q})$. Then, $x = \frac{u}{s^2}$ and $y = \frac{u'}{s^3}$, where $s, u, u' \in \mathbb{Z}$ and $gcd(u, s) = gcd(u', s) = 1$.*

Proof. See [17]. □

Lemma 2.6. *For every point $P = (x, y) \in E(\mathbb{Q})$, we have*

$$x(2P) = \frac{x^4 + 2p^2x^2 + p^4 - 8q^2x}{4y^2}. \tag{2..2}$$

Proof. The proof is straightforward. □

In the following proposition, we see some features of elements of $2E(\mathbb{Q})$.

Proposition 2.7. *Let $P = (\frac{u}{s^2}, \frac{u'}{s^3})$ and $Q = (\frac{w}{t^2}, \frac{w'}{t^3}) \in E(\mathbb{Q})$, where $u, u', s, w, w', t \in \mathbb{Z}$ and $gcd(uu', s) = gcd(ww', t) = 1$. If $P = 2Q$ then:*

(i) $t|s$.

(ii) If s is odd, then w and t are odd.

(iii) u is odd and $u \not\equiv s^2 \pmod 4$.

Proof. Suppose that $P = 2Q$, since $x(2Q) = x(P) = \frac{u}{s^2}$, using Lemma 2.6 and the fact that Q is on E we have

$$4ut^2(w^3 - p^2wt^4 + q^2t^6) = s^2[(w^2 + p^2t^4)^2 - 8q^2wt^6]. \tag{2..3}$$

Since $gcd(t, w) = 1$, from the above equality we see that $t|s$. This proves (i). Considering (2..3) modulo 8, proves part (ii). For part (iii), it suffices to consider (2..3) modulo 16. □

3. group structure of $E(\mathbb{Q})$

In this section, using previous results, we will find two independent points in $E(\mathbb{Q})$, which proves that $r \geq 2$. Fix two prime numbers $p > 5$ and $q > 5$ and let E be the elliptic curve $E : y^2 = x^3 - p^2x + q^2$ over $\mathbb{Q}$. Consider the points $P_1 = (0, q)$, $P_2 = (-p, q)$ and $P_3 = (p, q)$ in $E(\mathbb{Q})$. We will show that P_1 and P_2 are independent.

Lemma 3.1. *None of the points P_1, P_2 and P_3 belong to $2E(\mathbb{Q})$.*

Proof. By part (iii) in Proposition 2.7, P_1 and $P_2 \notin 2E(\mathbb{Q})$. We prove the lemma for P_3, other parts is similar. Suppose that there exist $Q = (\frac{w}{t^2}, \frac{w'}{t^3}) \in E(\mathbb{Q})$, such that $P_3 = 2Q$. By Proposition 2.7(i), $t|1$, so $t = \pm 1$ and by Lemma 2.6, we have

$$4p(w^3 - p^2w + q^2) = [(w^2 + p^2)^2 - 8q^2w]. \tag{3..1}$$

Which is equivalent to

$$(w - p)^4 - 4p^2(w - p)^2 - 8q^2(w - p) - 12pq^2 + 4p^4 = 0. \tag{3..2}$$

By Proposition 2.4, we know w is odd, let $w - p = 2s$. We have

$$(2s^2 - p^2)^2 = 4q^2s + 3pq^2. \tag{3..3}$$

Assume that $n = 2s^2 - p^2$ hence $q|n$ so n is odd. Therefore we have

$$s = \frac{n^2 - 3q^2p}{4q^2}.$$

Hence

$$n + p^2 = 2s^2 = \frac{(n^2 - 3pq^2)^2}{8q^4},$$

and therefore

$$n^4 - 6q^2pn^2 - 8q^4n + p^2q^4 = 0. \tag{3..4}$$

On the other hand

$$p = \frac{n^2 - 4q^2s}{3q^2}.$$

So

$$n = 2s^2 - \frac{n^4 + 16q^4s^2 - 8n^2q^2s}{9q^4},$$

and therefore

$$9nq^4 + n^4 - 8n^2q^2s = 2s^2q^4. \tag{3..5}$$

From this we have $n|2s^2q^4$. Since $gcd(n, 2s^2) = 1$, we have $n|q^4$. This is impossible since the product of roots of equation is p^2q^4. In fact, we have no integer roots for the equation (3..4). Therefore, we must reject the assumption that there exist $Q \in E(\mathbb{Q})$, such that $P_3 = 2Q$. Hence $P_3 \neq 2Q$. □

Theorem 3.2. *Let $\overline{P}_i = P_i + 2E(\mathbb{Q})$, $i = 1, 2, 3$, be elements in $E(\mathbb{Q})/2E(\mathbb{Q})$. The set $H = \{\overline{O}, P_1, \overline{P_2}, \overline{P_3}\}$ is a subgroup of $E(\mathbb{Q})/2E(\mathbb{Q})$ of order 4, so $4||E(\mathbb{Q})/2E(\mathbb{Q})|$ and hence $|E(\mathbb{Q})/2E(\mathbb{Q})| \geq 4$.*

Proof. By Lemma 3.1, we know that $\bar{P}_1,\ \bar{P}_2,\ \bar{P}_3 \neq \bar{\mathcal{O}}$. On the other hand, it is easy to see that $-P_3 = P_1 + P_2$ and H is closed. This shows that H is a subgroup of $E(\mathbb{Q})/2E(\mathbb{Q})$. To prove the theorem, we consider the following cases:

1. Suppose that $\bar{P}_1 = \bar{P}_2$ then, $\bar{P}_3 = 2\bar{P}_1 = \bar{\mathcal{O}}$, which is a contradiction according to Lemma 3.1.
2. Suppose that $\bar{P}_1 = \bar{P}_3$ then, $\bar{P}_2 = \bar{\mathcal{O}}$, which is a contradiction according to Lemma 3.1.
3. Suppose that $\bar{P}_2 = \bar{P}_3$ then, $\bar{P}_1 = \bar{\mathcal{O}}$, which is a contradiction according to Lemma 3.1.

Therefore, these four classes are distinct classes of $E(\mathbb{Q})/2E(\mathbb{Q})$, so $|H| = 4$. □

We have shown that $|E(\mathbb{Q})/2E(\mathbb{Q})| \geq 4$, which implies that $rank(E) \geq 2$, by Proposition 2.3. In fact, we have the following theorem.

Theorem 3.3. *The point P_1 and P_2 are independent rational points in $E(\mathbb{Q})$ and so $rank(E(\mathbb{Q})) \geq 2$.*

Proof. Assume on the contrary that two rational points P_1 and P_2 are dependent. Then there exist $m, n \in \mathbb{Z}$,not both zero, such that $mP_1 + nP_2 = \mathcal{O}$. Without loss of generality, let $m \in \mathbb{N}$ be the smallest among all. We have four cases,

1. Assume that m is even and n is odd then, $\bar{\mathcal{O}} = \bar{P}_2$, which contradicts Theorem 3.2.
2. Assume that m is odd and n is even then, $\bar{\mathcal{O}} = \bar{P}_1$, which is a contradiction according to Theorem 3.2.
3. Assume that m is odd and n is odd then, $\bar{\mathcal{O}} = \bar{P}_3$, which contradicts Theorem 3.2.
4. Assume that $m = 2t$ and $n = 2t'$, both are even then $2(tP_1 + t'P_2) = \mathcal{O}$. Now Theorem 2.2 implies that $(tP_1 + t'P_2) = \mathcal{O}$. This contradicts the minimality of m.

This completes the proof. □

Example 3.4. *By Theorem 3.3 the points $P_1 = (0, 7)$ and $P_2 = (-7, 7)$ are independent points on the elliptic curve $E = E_{(7,7)} : y^2 = x^3 - 7^2x + 7^2$. The computer algebra system Sage [15] suggests that the rank of $E = E_{(7,7)}$ is in fact, 2 and the points $P_1 = (0, 7)$ and $P_2 = (-7, 7)$ generate $E = E_{(7,7)}$.*

4. A family of rank 3 elliptic curves

Already, we have identified an infinite family of rank two elliptic curves. In this section, we find a subfamily of rank three elliptic curves in this family. We will show that under a famous conjecture this subfamily has infinitely many members. Suppose that p and q satisfy $p^2+q^2-1=b^2$ for an integer, then the point $P_4=(-1,b)$ is a point on $E_{(p,q)}$. We will show that P_1, P_2 and P_4 are independent. We need the following:

Lemma 4.1. *Let p and q are prime numbers greater than 5. If there exists $b\in\mathbb{Z}$ such that $p^2+q^2-1=b^2$, then the point $P_4=(-1,b)\in E(\mathbb{Q})$, satisfies the followings:*

(i) $P_4\notin 2E(\mathbb{Q})$.

(ii) $P_5=P_4+P_1\notin 2E(\mathbb{Q})$.

(iii) $P_6=P_4+P_2\notin 2E(\mathbb{Q})$.

(iv) $P_7=P_4+P_3\notin 2E(\mathbb{Q})$.

Proof. First, we will show that $P_4\notin 2E(\mathbb{Q})$. Assume on the contrary that there exists $Q=(\frac{w}{t^2},\frac{w'}{t^3})\in E(\mathbb{Q})$, such that $P_4=2Q$. Then, $-1=x(2Q)$. By Proposition 2.7 we can set $t=1$. Now by Lemma 2.6 We have

$$4(w^3-p^2w+q^2)+(w^2+p^2)^2=8q^2w.$$

From this and Proposition 2.4 $1\leq w\in\mathbb{Z}$. We rewrite the above formula as a quadratic equation in p^2. Then we have

$$p^4+2p^2(w^2-2w)+(w^4+4w^3-8wq^2+4q^2)=0. \tag{4..1}$$

The above equation has integer solutions if and only if

$$\Delta_{p^2}=16(-2w^3+w^2+2wq^2-q^2)$$

is the square of an integer. Now from this we have

$$-2w^3+w^2+2wq^2-q^2=m^2$$

for some integer m. Hence w satisfies the equation

$$-2w^3+w^2+2wq^2-q^2-m^2=0.$$

The sum of the roots of this equation is $\frac{1}{2}$. This impossible since $1\leq w\in\mathbb{Z}$. This prove (i).
(ii) Let $P_5=2Q$ we have $(q-b)^2+1\equiv 1 \pmod 4$. This contradicts Proposition 2.7(iii). The proofs of (iii) and (iv) are similar to that of (ii). □

Lemma 4.2. *Let* $\overline{P}_i = P_i + 2E(\mathbb{Q})$, $1 \leq i \leq 7$. *The set*

$$H = \{\overline{O},\ \bar{P}_1,\ \bar{P}_2,\ \bar{P}_3,\ \bar{P}_4,\ \bar{P}_5,\ \bar{P}_6,\ \bar{P}_7\}$$

is a subgroup of $E(\mathbb{Q})/2E(\mathbb{Q})$ *of order 8.*

Proof. The fact that the 8 elements in H are distinct and H is closed under addition is easy to prove using Theorem 3.2 and Lemma 4.1. □

The Lemma 4.2 and Proposition 2.3 show that the rank of $E(\mathbb{Q})$ is at least 3. In fact, we have the following result.

Theorem 4.3. *The points* P_1, P_2 *and* P_4, *are independent rational points on* $E(\mathbb{Q})$ *and therefore the rank of* $E(\mathbb{Q})$ *is at least three.*

Proof. Assume on the contrary that two rational points P_1, P_2 and P_4 are dependent. Then there exist $m, n, s \in \mathbb{Z}$,not both zero, such that $mP_1 + nP_2 + sP_4 = \mathcal{O}$.First we note that since P_1, P_2 are independent by Theorem 3.3 we have $s \neq 0$. Without loss of generality, let $s \in \mathbb{N}$ be the smallest among all. We have eight cases. When s is odd we have the following four cases,

1. Assume that m is even and n is odd. Then, $\bar{\mathcal{O}} = \bar{P}_6$, which contradicts Theorem 4.2.
2. Assume that m is odd and n is even. Then, $\bar{\mathcal{O}} = \bar{P}_5$, which is a contradiction according to Theorem 4.2.
3. Assume that m is odd and n is odd. Then, $\bar{\mathcal{O}} = \bar{P}_7$, which contradicts Theorem 4.2.
4. Assume that m is even and n is even. Then, $\bar{\mathcal{O}} = \bar{P}_4$, which contradicts Theorem 4.2.

If s is even we have four cases,

1. Assume that m is even and n is odd. Then, $\bar{\mathcal{O}} = \bar{P}_2$, which contradicts Theorem 4.2.
2. Assume that m is odd and n is even. Then, $\bar{\mathcal{O}} = \bar{P}_1$, which is a contradiction according to Theorem 4.2.
3. Assume that m is odd and n is odd. Then, $\bar{\mathcal{O}} = \bar{P}_3$, which contradicts Theorem 4.2.
4. Assume that $m = 2t$, $n = 2t'$ and, $s = 2t''$ both are even then

   $$2(tP_1 + t'P_2 + t''P_4) = \mathcal{O}.$$

   Now Theorem 2.2 implies that $(tP_1 + t'P_2 + t''P_4) = \mathcal{O}$. This contradicts the minimality of s.

This completes the proof. □

Example 4.4. *By Theorem* 4.2 *the points* $P_1 = (0, 11)$, $P_2 = (-7, 11)$, $P_4 = (-1, 13)$ *are independent points on the elliptic curves* $E = E_{(7,11)} : y^2 = x^3 - 7^2x + 11^2$. *The computer algebra system Sage [15] suggests that the rank of* $E = E_{(7,11)}$ *is in fact, 3 and the points* $P_1 = (0, 11)$, $P_2 = (-7, 11)$, $P_4 = (-1, 13)$ *generate* $E = E_{(7,11)}$.

Here we investigate the number of primes p and q, for which p^2+q^2-1 is square. For this, we recall the Schinzel and Sierpinski [13] conjecture.

Conjecture 4.5. *Let* $f_1(x), f_2(x), \ldots, f_m(x) \in \mathbb{Z}[x]$ *be irreducible polynomials with positive leading coefficients. Assume that there exists no integer* $n > 1$ *dividing* $f_1(k), f_2(k), \ldots, f_m(k)$ *for all integers* k. *Then there exist infinitely many positive integers* l *such that each of the numbers* $f_1(l), f_2(l), \ldots, f_m(l)$ *is prime.*

Proposition 4.6. *There are infinitely many prime* p *and* q *for which* $p^2 + q^2 - 1$ *is a square.*

Proof. Consider $f_1(x) = 2x + 1$, $f_2(x) = x^2 + x - 1$ and $f_3(x) = x^2 + x + 1$. We have

$$f_1(x)^2 + f_2(x)^2 - 1 = f_3(x)^2.$$

On the other hand if there exist integers k and n such that $n|f_2(k), f_3(k)$, then $n|f_2(k) - f_3(k) = 2$, thus $n \nmid f_1(k)$.
So Conjecture 4.5 implies that there exist infinitely many k, such that $p = f_1(k)$, $q = f_2(k)$ and $b = f_3(k)$ are prime, which completes the proof. □

Corollary 4.7. *Assuming the above conjecture, there is an infinite family elliptic curves of the form* $E = E_{(p,q)}$ *of rank at least 3.*

Proof. This follows from Theorem 4.3. □

Acknowledgment

We would like to thank the referees for their careful reading and valuable comments.

REFERENCES

1. A. Antoniewicz: *On A Famaily Of Elliptic Curves.*, Universitatis Iagellonicae Acta Mathematica,Fasciculus **XLIII** (2005), 21–32.
2. E. Brown and T. Mayer: *Elliptic Curves From Mordell to Diophantus and Back.*, Amer. Math. Monthly, **109**, Aug-sept, 2002, 639–648.

3. J. E. Cremona: *Algorithms for modular elliptic curves* , Cambridge University Press, Springer, 1997.
4. J. E. Cremona:*mwrank*. Avaliable from Ftp://euclid.ex.ac.uk/pub/cremona/prog.
5. H. Daghigh and S. Didari: *On the elliptic curves of the form* $y^2 = x^3 - 3px$. Bulletin of the Iranian Mathematical Society.**40** (2014) 1119-33.
6. H. Daghigh and S. Didari: *On the Elliptic Curves of the Form* $y^2 = x^3 - pqx$. Iranian Journal of Mathematical Sciences and Informatics. **1**0 (2015) 77–86.
7. A. Draziotis and V. Konstantinos: *Practical solution of the Diophantine equation* $y^2 = x(x + 2^a p^b)(x - 2^a p^b)$. Math. Comp.**7**5 (2006) 1585.
8. A. Draziotis and V. Konstantinos: *Integer points on the curve* $Y^2 = X^3 \pm p^k X$.Math. Comp.**7**5 (2006) 1493–1505.
9. K. Feng and M. Xiong: *On elliptic curves* $y^2 = x^3 - n^2x$ *with rank zero*. Journal of Number Theory.**1**09(2004) 1–26.
10. Y. Fujita and N. Terai: *Integer Points and Independent Points on the Elliptic Curve* $y^2 = x^3 - p^k x$. Tokyo Journal of Mathematics.**3**4(2011)367–381.
11. Y. Fujita and N. Terai: *On the Mordell–Weil group of the elliptic curve*. Journal of Number Theory.**1**32(3)(2012) 448–466.
12. F. Lemmermeyer and R. Mollin: *On Tate-Shafarevich groups of* $y^2 = x(x^2 - k^2)$. Acta Math.**7**2(2003) 73–80.
13. A. Schinzel and W. Sierpinski: *Sur certaines hypotheses concernant les nombres premiers. Acta Arith.***4**(1958) 185–208.
14. J. H. Silverman: *The Arithmetic of elliptic curves* , Springer, 2009.
15. W. Stein: *Sage open -source mathematical software system*. Avaliable from **http://www.sagemath.org**.
16. P. Walsh: *Maximal ranks and integer points on a family of elliptic curves*. Glasnik Matematički.**44(64)** (2009) 83–87.
17. Washington, Lawrence C: *Elliptic curves: number theory and cryptography*. Chapman and Hall/CRC, 2003.

Mehrdad. Khazali
Faculty of Mathematical Sciences
Kashan, Iran
merhdad@bam.ac.ir

Hassan. Daghigh
Faculty of Mathematical Sciences
Kashan, Iran
hassan@kashanu.ac.ir