Generators and number fields for torsion points of a special elliptic curve

Hasan Sankari and Mustafa Bojakli
Department of Mathematics, Faculty of Science, Tishreen University, Lattakia, Syria

Received 3 August 2019
Revised 19 September 2019
Accepted 21 October 2019

Abstract
Let E be an elliptic curve with Weierstrass form $y^2 = x^3 - px$, where p is a prime number and let $E[m]$ be its m-torsion subgroup. Let $p_1 = (x_1, y_1)$ and $p_2 = (x_2, y_2)$ be a basis for $E[m]$, then we prove that $\mathbb{Q}(E[m]) = \mathbb{Q}(x_1, x_2, \xi_m, y_1)$ in general. We also find all the generators and degrees of the extensions $\mathbb{Q}(E[m])/\mathbb{Q}$ for $m = 3$ and $m = 4$.

Keywords Elliptic curves, Torsion points, Algebraic extensions
Paper type Original Article

1. Introduction
Let E be an elliptic curve with Weierstrass form $y^2 = x^3 - px$, where p is a prime number. Let m be a positive number, we denote by $E[m]$ the m -torsion subgroup of E, by $\mathbb{Q}(E[m])$ the number field generated by the coordinates of the m -torsion points of E, and by $\mathbb{Q}(E_x[m])$ the number field generated by the abscissas of m -torsion points of E. Mazur proves the m -torsion subgroup is isomorphic to one of 15 finite groups [5]. Let $p_1 = (x_1, y_1)$ and $p_2 = (x_2, y_2)$ be two points in E forming a basis of $E[m]$, then $\mathbb{Q}(E[m]) = \mathbb{Q}(x_1, x_2, y_1, y_2)$. By Artin's primitive element theorem the extension $\mathbb{Q}(x_1, x_2, y_1, y_2)/\mathbb{Q}$ is monogeneous and we can find unique generator for $\mathbb{Q}(x_1, x_2, y_1, y_2)/\mathbb{Q}$ by combining the above coordinates. As usual, we denote by μ_m the group of mth roots of unity and by ξ_m one of its generators. By Weil pairing, we have $\xi_m \in \mathbb{Q}(E[m])$, so $\mathbb{Q}(\xi_m) \subseteq \mathbb{Q}(E[m])$ for all m [5]. In [3] Paladino gives a family of elliptic curves such that $\mathbb{Q}(E[3]) = \mathbb{Q}(\xi_3)$ and in [4] finds the number fields generated by the 4th torsion points, degrees and Galois groups of an elliptic curve $y^2 = (x-\alpha)(x-\beta)(x-\gamma)$ where $\alpha, \beta, \gamma \in \mathbb{Q}$, and $\alpha \neq \beta \neq \gamma$. In [1] Bandini and Paladino determine the number fields generated by the 3-torsion points, degrees and Galois groups of an elliptic curve $y^2 = x^3 + c$ where $c \in \mathbb{Q}^*$. In [2] the result of Brau and Jones says that the rational points on the modular

JEL Classification — 11G04, 12F05

Declaration of Competing Interest: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

The publisher wishes to inform readers that the article "Generators and number fields for torsion points of a special elliptic curve" was originally published by the previous publisher of the *Arab Journal of Mathematical Sciences* and the pagination of this article has been subsequently changed. There has been no change to the content of the article. This change was necessary for the journal to transition from the previous publisher to the new one. The publisher sincerely apologises for any inconvenience caused. To access and cite this article, please use Sankari, H., Bojakli, M. (2019), "Generators and number fields for torsion points of a special elliptic curve", *Arab Journal of Mathematical Sciences*, Vol. 26 No. 1/2, pp. 227-231. The original publication date for this paper was 29/10/2019

Arab Journal of Mathematical Sciences
Vol. 26 No. 1/2, 2020
pp. 227-231
Emerald Publishing Limited
e-ISSN: 2588-9214
p-ISSN: 1319-5166
DOI 10.1016/j.ajmsc.2019.10.002

curve of level 6 yield elliptic curve E satisfying the given containment. In the first part of this paper we prove $\xi_m \in \mathbb{Q}(E_x[m])$ and $\mathbb{Q}(E[m]) = \mathbb{Q}(x_1, x_2, \xi_m, y_1)$ for all m. In the second part of this paper we find the number fields of torsion points $E[m]$ for cases $m = 3, 4$, extensions and degrees. These theorems have applications in local–global divisibility problem [4] and modular curves [2].

2. Generators for $\mathbb{Q}(E[m])$

Let $p_1 = (x_1, y_1)$ and $p_2 = (x_2, y_2)$ form a basis of $E[m]$. We have $\mathbb{Q}(E[m]) = \mathbb{Q}(x_1, x_2, y_1, y_2)$. We will denote by L the field $\mathbb{Q}(x_1, x_2)$ and by K the field $\mathbb{Q}(E[m])$. Suppose (x_3, y_3) be the coordinates of the point $p_3 = p_1 + p_2$ and (x_4, y_4) be the coordinates of the point $p_4 = p_1 - p_2$. In next theorem we will prove $\xi_m \in \mathbb{Q}(E_x[m])$ for all m.

Lemma 2.1. *Let $\{P, Q\}$ be a basis for $E[m]$. Then $e_m(P, Q)$ is a primitive mth root of unity.*

Proof. We know that there are $S, T \in E[m]$ such that $e_m(S, T) = \xi_m$, a primitive mth root of unity. Write $S = aP + bQ$ and $T = cP + dQ$. Then the antisymmetry properties of the Weil pairing imply that

$$\xi_m = e_m(S, T) = e_m(P, Q)^{ad-bc}.$$

Since $e_m(P, Q)$ is an mth root of unity and a power of it is a primitive mth root of unity, it follows that $e_m(P, Q)$ is a primitive mth root of unity. □

Theorem 2.2. *Let $\{p_1, p_2\}$ be a basis for $E[m]$, let $p_3 = p_1 + p_2$ and $p_4 = p_1 - p_2$, and write $p_i = (x_i, y_i)$. Then*

$$\mathbb{Q}(\xi_m) \subseteq \mathbb{Q}(x_1, x_2, x_3, x_4) \subseteq \mathbb{Q}(E_x[m]).$$

Proof. The second inclusion is by the definition of $\mathbb{Q}(E_x[m])$. For the first inclusion. Let σ be an automorphism of $\mathbb{Q}(E[m])$ that fixes $\mathbb{Q}(x_1, x_2, x_3, x_4)$. Then $\sigma(y_i) = \pm y_i$ since $\sigma(y_i^2) = y_i^2$. The equation

$$y_1 y_2 = \frac{(x_4 - x_3)(x_1 - x_2)^2}{4}$$

shows that $\sigma(y_1 y_2) = y_1 y_2$. This means that either $\sigma(y_i) = y_i$ for $i = 1, 2$, or $\sigma(y_i) = -y_i$ for $i = 1, 2$. These mean that either $\sigma(p_i) = p_i$ for $i = 1, 2$, or $\sigma(p_i) = -p_i$ for $i = 1, 2$. In the first case,

$$e_m(p_1, p_2)^\sigma = e_m(\sigma(p_1), \sigma(p_2)) = e_m(p_1, p_2).$$

In the second case,

$$e_m(p_1, p_2)^\sigma = e_m(\sigma(p_1), \sigma(p_2)) = e_m(-p_1, -p_2) = e_m(p_1, p_2).$$

Since $e_m(p_1, p_2)$ is a primitive mth root of unity, we find that $\mathbb{Q}(\xi_m) \subseteq \mathbb{Q}(x_1, x_2, x_3, x_4)$. □

We know that $\mathbb{Q}(x_1, x_2, y_1, y_2) = \mathbb{Q}(x_1, x_2, y_1, y_1 y_2)$. In next theorem we will prove that $\mathbb{Q}(E[m])$ is equal to the field $\mathbb{Q}(x_1, x_2)$ by adding ξ_m and y_1.

Theorem 2.3. $\mathbb{Q}(E[m]) = \mathbb{Q}(x_1, x_2, \xi_m, y_1)$.

Proof. We have $\mathbb{Q}(x_1, x_2, \xi_m, y_1, y_2) = \mathbb{Q}(E[m])$. If we do not have the equality in the theorem, then $y_2 \notin \mathbb{Q}(x_1, x_2, \xi_m, y_1)$. Since y_2^2 is in this field, there is an automorphism σ such that $\sigma(y_2) = -y_2$ and σ is the identity on $\mathbb{Q}(x_1, x_2, \xi_m, y_1)$. Then

$$e_m(p_1,p_2) = e_m(p_1,p_2)^\sigma = e_m(\sigma(p_1),\sigma(p_2)) = e_m(p_1,-p_2) = e_m(p_1,p_2)^{-1}.$$

This implies that $e_m(p_1,p_2)^2 = 1$. Since $e_m(p_1,p_2)$ is a primitive mth root of unity, we must have $m = 2$. But then $y_1 = y_2 = 0$, in which case the theorem is true. □

3. Number fields $\mathbb{Q}(E[m])$ for cases $m = 3, 4$

It is well known that the abscissas of the 3-torsion points of an elliptic curve $y^2 = x^3 - px$ are the roots of the polynomial

$$\varphi_3 = 3x^4 - 6px^2 - p^2,$$

then the roots $\widehat{x_1}, \widehat{x_2}, \widehat{x_3}, \widehat{x_4}$ of φ_3 are:

$$\widehat{x_1} = \sqrt{p - \frac{2p}{\sqrt{3}}}, \widehat{x_2} = -\sqrt{p - \frac{2p}{\sqrt{3}}}, \widehat{x_3} = \sqrt{p + \frac{2p}{\sqrt{3}}}, \widehat{x_4} = -\sqrt{p + \frac{2p}{\sqrt{3}}}.$$

In next theorems we will determine the field generated by 3 and 4 torsion points.

Theorem 3.1. *Let E be an elliptic curve with Weierstrass form $E : y^2 = x^3 - px$, where p is a prime number. Then*

$$\mathbb{Q}(E_x[3]) = \mathbb{Q}\left(\sqrt{p - \frac{2p}{\sqrt{3}}}, \xi_3\right) \qquad \textit{with } [\mathbb{Q}(E_x[3]) : \mathbb{Q}] = 8,$$

$$\mathbb{Q}(E[3]) = \mathbb{Q}\left(\sqrt{\frac{2p\sqrt{2p\sqrt{3} - 3p}}{3}}, \xi_3\right) \quad \textit{with } [\mathbb{Q}(E[3]) : \mathbb{Q}] = 16.$$

Proof. We have $\mathbb{Q}(\widehat{x_1}, \widehat{x_2}, \widehat{x_3}, \widehat{x_4}) = \mathbb{Q}(\widehat{x_1}, \widehat{x_3})$. On the other hand we have

$$\widehat{x_1}\widehat{x_3} = \sqrt{\left(p - \frac{2p}{\sqrt{3}}\right)\left(p + \frac{2p}{\sqrt{3}}\right)} = \sqrt{\frac{-p^2}{3}} = \frac{\sqrt{-3}p}{3},$$

so $\mathbb{Q}(\widehat{x_1}, \widehat{x_3}) = \mathbb{Q}(\widehat{x_1}, \widehat{x_1}\widehat{x_3}) = \mathbb{Q}(\widehat{x_1}, \xi_3) = \mathbb{Q}\left(\sqrt{p - \frac{2p}{\sqrt{3}}}, \xi_3\right)$.

We have

$$\left[\mathbb{Q}\left(\sqrt{p - \frac{2p}{\sqrt{3}}}, \xi_3\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt{p - \frac{2p}{\sqrt{3}}}, \xi_3\right) : \mathbb{Q}(\xi_3)\right][\mathbb{Q}(\xi_3) : \mathbb{Q}].$$

Put $\alpha = \sqrt{p - \frac{2p}{\sqrt{3}}}$, then

$$f(x) = min(\alpha, \mathbb{Q}(\xi_3)) = 3\alpha^4 + 6p\alpha^2 - p^2 = 0$$

is irreducible over $\mathbb{Q}(\xi_3)$, because the roots of $f(x)$ are $\widehat{x_1}, \widehat{x_2}, \widehat{x_3}, \widehat{x_4}$. They are irrational, so either $f(x)$ is irreducible or it has a quadratic factor that has $\widehat{x_1}$ and some other $\widehat{x_i}$ as roots. Since $\widehat{x_1}\widehat{x_2} \notin \mathbb{Q}(\xi_3)$, the other root is not $\widehat{x_2}$. Suppose the other root is $\widehat{x_3}$ or $\widehat{x_4}$. Then (using $\widehat{x_3}$)

$$\frac{2p}{3}\left(3 \pm \sqrt{-3}\right) = (\widehat{x_1} + \widehat{x_3})^2$$

is a square in $\mathbb{Q}(\xi_3)$. But its norm to $\mathbb{Q}$ is $\frac{16p^2}{3}$, which is not a square, so it cannot be a square. Therefore, there is no quadratic factor and $f(x)$ is irreducible. So $\left[\mathbb{Q}\left(\sqrt{p-\frac{2p}{\sqrt{3}}},\xi_3\right):\mathbb{Q}(\xi_3)\right]=4$.
It is easy to verify that $[\mathbb{Q}(\xi_3):\mathbb{Q}]=2$. Hence

$$[\mathbb{Q}(E_x[3]:\mathbb{Q})]=\left[\mathbb{Q}\left(\sqrt{p-\frac{2p}{\sqrt{3}}},\xi_3\right):\mathbb{Q}\right]=4\bullet 2=8.$$

By Theorem 2.2 we proved that $\mathbb{Q}(E[3])=\mathbb{Q}(\widehat{x_1},\widehat{x_2},\xi_3,\widehat{y_1})=\mathbb{Q}(\widehat{x_1},\xi_3,\widehat{y_1})$, where $\widehat{x_1}=-\widehat{x_2}$. As $\widehat{y_1}^2=\widehat{x_1}^3-p\widehat{x_1}$, then

$$y_1=\sqrt{\widehat{x}_1^3-p\widehat{x_1}}=\sqrt{\left(\sqrt{p-\frac{2p}{\sqrt{3}}}\right)^3-p\left(\sqrt{p-\frac{2p}{\sqrt{3}}}\right)}=\sqrt{\frac{2p\sqrt{2p\sqrt{3}-3p}}{3}}$$

and $[\mathbb{Q}(\widehat{x_1},\xi_3,\widehat{y_1}):\mathbb{Q}(\widehat{x_1},\xi_3)]=2$. We found in previous case that $[\mathbb{Q}(\widehat{x_1},\xi_3):\mathbb{Q}]=8$. Hence

$$[\mathbb{Q}(E[3]):\mathbb{Q}]=[\mathbb{Q}(\widehat{x_1},\xi_3,\widehat{y_1}):\mathbb{Q}]=[\mathbb{Q}(\widehat{x_1},\xi_3,\widehat{y_1}):\mathbb{Q}(\widehat{x_1},\xi_3)][\mathbb{Q}(\widehat{x_1},\xi_3):\mathbb{Q}]=2\bullet 8=16.\quad\square$$

It is well known that the abscissas of the 4-torsion points of an elliptic curve $y^2=x^3-px$ are the roots of the polynomial

$$\varphi_4=x^6-5px^4-5p^2x^2+p^3,$$

then the roots $\widehat{x_1},\widehat{x_2},\widehat{x_3},\widehat{x_4},\widehat{x_5},\widehat{x_6}$ of φ_4 are

$$\begin{array}{lll}\widehat{x_1}=i\sqrt{p}, & \widehat{x_2}=+\sqrt{p}+\sqrt{2p}, & \widehat{x_3}=-i\sqrt{p},\\ \widehat{x_4}=\sqrt{p}-\sqrt{2p}, & \widehat{x_5}=-\sqrt{p}+\sqrt{2p}, & \widehat{x_6}=-\sqrt{p}-\sqrt{2p}.\end{array}$$

Theorem 3.2. *Let E be an elliptic curve with Weierstrass form $y^2=x^3-px$, where p is a prime number. Then*

$$\mathbb{Q}(E_x[4])=\begin{cases}\mathbb{Q}(i,\sqrt{2},\sqrt{p}) & with[\mathbb{Q}(E_x[4]):\mathbb{Q}]=8\ \ if\ \ p\neq 2,\\ \mathbb{Q}(i,\sqrt{2}) & with[\mathbb{Q}(E_x[4]):\mathbb{Q}]=4\ \ if\ \ p=2.\end{cases}$$

$$\mathbb{Q}(E[4])=\begin{cases}\mathbb{Q}(i,\sqrt{2},\sqrt[4]{p}) & with[\mathbb{Q}(E[4]):\mathbb{Q}]=16\ \ if\ \ p\neq 2,\\ \mathbb{Q}(i,\sqrt[4]{8}) & with[\mathbb{Q}(E[4]):\mathbb{Q}]=8\ \ if\ \ p=2.\end{cases}$$

Proof. The points of exact order 4 of $y^2=x^3-px$ are $\pm p_1,\pm p_2,\pm p_3,\pm p_4,\pm p_5,\pm p_6$, where

$$p_1=\left(i\sqrt{p},-\sqrt[4]{p^3}+i\sqrt[4]{p^3}\right),\qquad p_2=\left(\sqrt{p}+\sqrt{2p},2\sqrt[4]{p^3}+\sqrt{2}\sqrt[4]{p^3}\right),$$

$$p_3=\left(-i\sqrt{p},-\sqrt[4]{p^3}-i\sqrt[4]{p^3}\right),\qquad p_4=\left(\sqrt{p}-\sqrt{2p},-2\sqrt[4]{p^3}+\sqrt{2}\sqrt[4]{p^3}\right),$$

$$p_5=\left(-\sqrt{p}+\sqrt{2p},\frac{2p}{\sqrt[4]{p^3}}+\frac{2p}{i\sqrt{2}\sqrt[4]{p^3}}\right),\quad p_6=\left(-\sqrt{p}-\sqrt{2p},\frac{2p}{\sqrt[4]{p^3}}-\frac{2p}{i\sqrt{2}\sqrt[4]{p^3}}\right).$$

We have:

$$\begin{aligned}\mathbb{Q}(E_x[4]) &= \mathbb{Q}(\widehat{x_1}, \widehat{x_2}, \widehat{x_3}, \widehat{x_4}, \widehat{x_5}, \widehat{x_6}) \\ &= \mathbb{Q}\left(i\sqrt{p}, \sqrt{p} + \sqrt{2p}, -i\sqrt{p}, \sqrt{p} - \sqrt{2p}, -\sqrt{p} + \sqrt{2p}, -\sqrt{2} - \sqrt{2p}\right) \\ &= \mathbb{Q}\left(i, \sqrt{2}, \sqrt{p}\right)\end{aligned}$$

with $[\mathbb{Q}(E_x[4]) : \mathbb{Q}] = 8$ if $p \neq 2$ and $[\mathbb{Q}(E_x[4]) : \mathbb{Q}] = 4$ if $p = 2$. □

Let $\{p_1, p_2\}$ be a basis for $E[4]$, then

$$\begin{aligned}\mathbb{Q}(E[4]) &= \mathbb{Q}(\widehat{x_1}, \widehat{x_2}, \widehat{y_1}, \widehat{y_2}) \\ &= \mathbb{Q}\left(i\sqrt{p}, \sqrt{p} + \sqrt{2p}, -\sqrt[4]{p^3} + i\sqrt[4]{p^3}, 2\sqrt[4]{p^3} + \sqrt{2}\sqrt[4]{p^3}\right) \\ &= \mathbb{Q}\left(i, \sqrt{2}, \sqrt[4]{p^3}\right)\end{aligned}$$

with $[\mathbb{Q}(E[4]) : \mathbb{Q}] = 16$ if $p \neq 2$ and $[\mathbb{Q}(E[4]) : \mathbb{Q}] = [\mathbb{Q}(i, \sqrt[4]{8})] = 8$ if $p = 2$. □

References

[1] A. Bandini, L. Paladino, Number fields generated by the torsion points of an elliptic curve, J. Number Theory 169 (2016) 103–133.

[2] J. Brau, J. Jones, Elliptic curves with 2-torsion contained in the 3-torsion field, AMS 144 (2016) 925–936.

[3] L. Paladino, Elliptic curves with $\mathbb{Q}(E[3]) = \mathbb{Q}(\xi_3)$and counterexamples to local global divisibility by 9, J. Théor. Nombres Bordeaux 22 (2010) 138–160.

[4] L. Paladino, Local global divisibility by 4 in elliptic curves defined over $\mathbb{Q}$, Ann. Mat. Pura Appl. 189 (2010) 17–23.

[5] H. Silverman, The Arithematic of Elliptic Curves, Springer-Verlag, Heidelberg, 2009.

Corresponding author
Mustafa Bojakli can be contacted at: mustafa.bojakli@gmail.com