***Advances in Pure Mathematics*, 2013, 3, 304-308**
http://dx.doi.org/10.4236/apm.2013.32043 Published Online March 2013 (http://www.scirp.org/journal/apm)

On the Torsion Subgroups of Certain Elliptic Curves over $\mathbb{Q}^*$

Yoon Kyung Park
School of Mathematics, Korea Institute for Advanced Study, Seoul, Republic of Korea
Email: ykpark@math.kaist.ac.kr

Received October 2, 2012; revised December 3, 2012; accepted December 15, 2012

ABSTRACT

Let E be an elliptic curve over a given number field K. By Mordell's Theorem, the torsion subgroup of E defined over $\mathbb{Q}$ is a finite group. Using Lutz-Nagell Theorem, we explicitly calculate the torsion subgroup $E(\mathbb{Q})_{tors}$ for certain elliptic curves depending on their coefficients.

Keywords: Elliptic Curve; Rational Point

1. Introduction

A cubic curve over the field K in Weierstrass form is given by projectively

$$y^2w + a_1xyw + a_3yw^2 = x^3 + a_2x^2w + a_4xw^2 + a_6w^3,$$

with coefficients in K. Then there is a unique $\bar{K}$ rational point $(x,y,w) = (0,1,0)$ on the line at infinite $w = 0$. If the above is an elliptic curve, then $(0,1,0)$ is a nonsingular point and we deal with the curve by working with the affine form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{1}$$

Hereafter assume that K is a number field. Since the field characteristic of K is 0, we can study

$$y^2 = x^3 + Ax + B \tag{2}$$

instead of (1.1). When the discriminant $\Delta_E = 4A^3 - 27B^2$ is nonzero, E is a nonsingular curve. By Mordell's theorem, $E(K)$ is a finitely generated abelian group and its torsion subgroup $E(K)_{tors}$ is a finite abelian group. Mazur proved that $E(\mathbb{Q})$ of an elliptic curve E over the rational numbers must be isomorphic to one of the following 15 types [1]:

$$\mathbb{Z}/N\mathbb{Z}, N = 1-10,12$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N'\mathbb{Z}, N' = 1-4.$$

This paper is focused on knowing how the coefficients A and B of (1.2) determine $E(\mathbb{Q})_{tors}$. For the earlier work, we see the cases A or B is zero in [2]:

Theorem 1. *Let E be the elliptic curve $y^2 = x^3 + Ax + B$ with A and B in $\mathbb{Z}$.*

1) If A is fourth-power free and $B = 0$, then

$$E(\mathbb{Q})_{tors} = \begin{cases} \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}, & \text{if } -A \text{ is a square in } \mathbb{Z}, \\ \mathbb{Z}/4\mathbb{Z}, & \text{if } A = 4, \\ \mathbb{Z}/2\mathbb{Z}, & \text{otherwise.} \end{cases}$$

2) If B is sixth-power free and $A = 0$, then

$$E(\mathbb{Q})_{tors} = \begin{cases} \mathbb{Z}/6\mathbb{Z}, \text{if } B = 1, \\ \mathbb{Z}/3\mathbb{Z}, \text{if } B = -432 = -2^4 3^3, \text{or if } B \text{ is square not } 1, \\ \mathbb{Z}/2\mathbb{Z}, \text{if } B \text{ is cubic not } 1, \\ 0, \quad \text{otherwise.} \end{cases}$$

It is too hard to determine the group $E(\mathbb{Q})_{tors}$ without any relation between the coefficients. Hence we consider the elliptic curve as follows:

$$y^2 = x^3 + f(k)x + g(k) \tag{3}$$

with $f(k), g(k) \in \mathbb{Z}[k]$. Then Theorem 1 yields the case when one of $f(k)$ and $g(k)$ is zero and $\max\{\deg_k f(k), \deg_k g(k)\} = 1$. In this paper, we deal with the case $\max\{\deg_k f(k), \deg_k g(k)\} = 2$.

Theorem 2. *Let*

$$E: y^2 = x^3 - (6k+3)x - (3k^2 + 6k + 2) \tag{4}$$

be the elliptic curve with k in $\mathbb{Z}$. Suppose that k is an integer such that $35 \nmid k(9k+4)$ and there is no integer h satisfying $k = 4h(3h^2 + 3h + 1)$ or $-4(h+1)(3h^2 + 3h + 1)$. Then

[*] This work was supported by NRF 2012-0006901.

$$E(\mathbb{Q})_{tors} = \begin{cases} \mathbb{Z}/4\mathbb{Z}, & k \equiv 20 \text{ or } 34 \pmod{35}, \exists l \in \mathbb{Z} \text{ such that } k = -3l^2(1+l) \text{ and} \\ & \exists m \in \mathbb{Z} \text{ satisfying } m^2 = l(3l-2) \text{ and } 6(6l^2 - 5lm - 2) \text{ is square,} \\ \mathbb{Z}/2\mathbb{Z}, & k \equiv 20 \text{ or } 34 \pmod{35}, \exists l \in \mathbb{Z} \text{ such that } k = -3l^2(1+l) \text{ and} \\ & \nexists m \in \mathbb{Z} \text{ satisfying } m^2 = l(3l-2) \text{ and } 6(6l^2 - 5lm - 2) \text{ is square,} \\ \mathbb{Z}/2\mathbb{Z}, & k \text{ is congruent to one of the elements of the set } K_2 \text{ modulo } 35 \\ & \text{and } \exists l \in \mathbb{Z} \text{ such that } k = -3l^2(1+l), \\ 0, & \text{otherwise.} \end{cases}$$

where $K_2 = \{x \in \mathbb{Z}/35\mathbb{Z} : x \equiv 4, 7, 12, 15, 22, 25, 27, 29, 32\}$.

2. The Proof of Theorem 2

We use the Lutz-Nagell Theorem and we have to calculate $E_p(\mathbb{F}_p)$ if E has a good reduction at the prime p.

Theorem 3. (Lutz-Nagell) *Let E be an elliptic curve* (1.1) *with coefficients in $\mathbb{Z}$ and E_p be a obtained curve by reducing coefficients of E modulo p. And let Δ_E be the discriminant of E.*

1) If $a_1 = 0$ and if $P = (x(P), y(P), 1)$ is in $E(\mathbb{Q})_{tors}$, then $x(P)$ and $y(P)$ are integers;

2) For any a_1, if $P = (x(P), y(P), 1)$ is in $E(\mathbb{Q})_{tors}$, then $4x(P)$ and $8y(P)$ are integers;

3) If p is an odd prime such that $p \nmid \Delta_E$, then the restriction to $E(\mathbb{Q})_{tors}$ of the reduction homomorphism $r_p : E(\mathbb{Q}) \to E_p(\mathbb{Q}_p)$ is one-to-one. The same conclusion is valid for $p = 2$ if $2 \nmid \Delta_E$ and $a_1 = 0$;

4) If $a_1 = a_3 = a_2 = 0$, so that E is given by

$$y^2 = x^3 + Ax + B,$$

and if $P(x(P), y(P), 1)$ is in $E(\mathbb{Q})_{tors}$, then either $y(P) = 0$ (and P has order 2) or else $y(P) \neq 0$ and $y(P)^2$ divides $d = -4A^3 - 27B^2$.

Proof. See [2]. □

Lemma 4. *Let $E : y^2 = x^3 + Ax + B$ be the elliptic curve over $\mathbb{F}_p$ and $P = (x, y)$ be a point in $E(\mathbb{F}_p)$ which is not a point at infinity. Then the followings are equivalent.*

1) $P = (x, y)$ is a point of order 3 in $E(\mathbb{F}_p)$;

2) $3x^4 + 6Ax^2 + 12Bx - A^2$ is congruent to 0 modulo p.

Proof. 1) $\Rightarrow$ 2) Let (x_2, y_2) be the point $2P = P + P$. Then by the group law algorithm ([2]),

$$x_2 = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4y^2}$$

$$y_2 = \frac{-(3x^2 + A)\left(\frac{(3x^2 + A)^2}{4y^2} - 2x\right)}{2y} - \frac{-x^3 + Ax + 2B}{2y}$$

and

$$-P = (x, -y).$$

Then $3P = O$ means that

$$x^4 - 2Ax^2 - 8Bx + A^2 = 4xy^2 \tag{5}$$

$$-(3x^2 + A)\left(\frac{(3x^2 + A)^2}{4y^2} - 2x\right) - (-x^3 + Ax + 2B) = -2y^2. \tag{6}$$

Since $y^2 = x^3 + Ax + B$, x should satisfy that $3x^4 + 6Ax^2 + 12Bx - A^2 = 0$ in $\mathbb{F}_p$.

2) $\Rightarrow$ 1) Assume that $3x^4 + 6Ax^2 + 12Bx - A^2 = 0$, y is not zero and $y^2 = x^3 + Ax + B$ in $\mathbb{F}_p$. By simple calculation, such x, y satisfy (5) and (6) and if P is the point (x, y) then $2P = -P$. We are done. □

Here we choose two rational primes $5, 7$ and calculate the groups $E(\mathbb{F}_5)$ and $E(\mathbb{F}_7)$. For the integer k unmentioned in our main theorem, we can take another prime and apply it as same manner.

Lemma 5. *Let p be the rational prime and E be the elliptic curve defined as*

$$y^2 = x^3 - (6k + 3)x - (3k^2 + 6k + 2)$$

where k is a nonzero integer. And using the natural surjection from $\mathbb{Z}$ to $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$, we can get E_p by reducing the coefficients of E modulo p. If p does not divide the discriminant $-2^4 \times 3^3 \times k^3(9k + 4)$ then the group E_p consisting of the points defined over the finite field $\mathbb{F}_p$ with p elements is

1) $E_5(\mathbb{F}_5) = \begin{cases} \mathbb{Z}/9\mathbb{Z}, k \equiv 1 \pmod 5, \\ \mathbb{Z}/6\mathbb{Z}, k \equiv 2 \pmod 5, \\ \mathbb{Z}/3\mathbb{Z}, k \equiv 3 \pmod 5. \end{cases}$

2) $E_7(\mathbb{F}_7) = \begin{cases} \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}, k \equiv 3 \pmod 7, \\ \mathbb{Z}/6\mathbb{Z}, & k \equiv 1, 4 \pmod 7, \\ \mathbb{Z}/9\mathbb{Z}, & k \equiv 2 \pmod 7, \\ \mathbb{Z}/12\mathbb{Z}, & k \equiv 6 \pmod 7. \end{cases}$

Table 1. Point in $E_5(\mathbb{Z}_5)$.

$k \pmod 5$	$E_5(\mathbb{Z}_5)-\{O\}$	$\lvert E_5(\mathbb{Z}_5)\rvert$	generators in $E_5(\mathbb{Z}_5)$
1	$0,(0,\pm2),(1,\pm1),(2,\pm2),(3,\pm2)$	9	$0,(0,\pm2),(1,\pm1),(2,\pm2)$
2	$0,(0,\pm2),(1,0),(3,\pm1)$	6	$(3,\pm1)$
3	$(2,\pm2)$	3	$(2,\pm2)$

Proof. By [3], every $E_p(\mathbb{F}_p)$ has a subgroup of $\mathbb{Z}/3\mathbb{Z}$. **Table 1** is the proof of (1).

Both cases can be calculated as using simple calculation. For 2), since $p=7$ and $p \nmid k(9k+4)$, k can not be congruent to 0 and $5 \pmod 7$. When $k \equiv 1 \pmod 7$, E_7 becomes $y^2 = x^3 - 2x + 3$. By substituting all elements of $\mathbb{F}_7$ to x in E_7, we can find that $E_7(\mathbb{F}_7) = \{(1,\pm3),(2,0),(6,\pm2),\infty\}$. Since it is an abelian group with 6 elements, $E_7(\mathbb{F}_7) \cong \mathbb{Z}/6\mathbb{Z}$. Like this, if $k \equiv 4 \pmod 7$,
$E_7(\mathbb{F}_7) = \{(4,\pm1),(5,0),(6,\pm1),\infty\}$ has 6 elements. Hence it is isomorphic to $\mathbb{Z}/6\mathbb{Z}$.

In the case $k \equiv 2 \pmod 7$ $E_7 : y^2 = x^3 - x + 2$ has a torsion subgroup $\{(1,\pm3),(2,\pm1),(6,\pm3),(0,\pm3),\infty\}$ over $\mathbb{F}_7$. To find the point of order 3 in the elliptic curve as the form ((2) in Section 1), we have to get the root of the equation $3x^4 + 6Ax^2 + 12Bx - A^2 = 0$ in given field and it is the x-coordinate of the order 3 point by Lemma 4. In this case, the equation is $3(x+1)(x^3+6x^2+6x+2)$ in $\mathbb{F}_7$. Hence there is no point of order 3 except $(6,\pm3)$ and $E_7(\mathbb{F}_7) \cong \mathbb{Z}/9\mathbb{Z}$.

For $k \equiv 3 \pmod 7$, $E_7(\mathbb{F}_7)$ has 9 elements. But the equation giving criterion of order 3 is $3x(x+1)(x+2)(x+4)$ in $\mathbb{F}_7$ and $(0,\pm3),(3,\pm1),(5,\pm1),(6,\pm1) \in E_7(\mathbb{F}_7)$. Therefore, $E_7(\mathbb{Z}_7) \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$.

Last, if $k \equiv 6 \pmod 7$,

$$E_7(\mathbb{F}_7) = \{(0,\pm1),(2,\pm1),(3,\pm3),(4,0),(5,\pm1),(6,\pm2),\infty\}$$

has only one point $(4,0)$ of order 2. It means that $E_7(\mathbb{F}_7) \cong \mathbb{Z}/12\mathbb{Z}$.

To get 1), we use the same process as 2), I omit it. □

Propositions 6 and 7 give the necessary and sufficient condition to have order 2 and 3 points.

Proposition 6. *Let $E : y^2 = x^3 - (6k+3)x - (3k^2+6k+2)$ be the elliptic curve with k in $\mathbb{Z}$. There is a point of order 2 if and only if k is an integer of the form $-3l^2(1-l)$. Moreover, the point of order 2 is unique.*

Proof. Assume that k is an integer of the form $-3l^2(1-l)$. Through easy calculation, k satisfies $k^2 + 6l^2k + 9l^4 - 9l^6 = 0$. Then $x = 3l^2 - 1$ is a root of $x^3 - (6k+3)x - (3k^2+6k+2) = 0$ and $(3l^2-1,0)$ is the point of order 2 in $E(\mathbb{Q})$.

Conversely, suppose that the equation of $x^3 - (6k+3)x - (3k^2+6k+2) = 0$ has a solution in $\mathbb{Z}$. To have solution of the equation with respect to k, x should be congruent to 2 modulo 3. By substituting $3m-1$ to x, the equation becomes $-3\{k^2 + 6km - 9m^2(m-1)\}$. Since it has an integral solution, $m = l^2$ and $k = -3l^2(1-l)$ for an integer l.

Now we show that there is no point of order 2 except $(3l^2-1,0)$ in $E(\mathbb{Q})$. Assume that $(3l^2-1,0) \in E(\mathbb{Q})$. Then $k = -3l^2(1-l)$.

$$x^3 - (6k+3)x - (3k^2+6k+2)$$
$$= (x - 3l^2 + 1)\left(x^2 - (1-3l^2)x + (9l^4 - 18l^3 + 12l^2 - 2)\right).$$

Let $Q(x)$ be $x^2 - (1-3l^2)x + (9l^4 - 18l^3 + 12l^2 - 2)$ with discriminant $-9(3l-1)(l+1)^3$. If the solution of $Q(x)$ exists, then $-(3l+1)(l-1) \geq 0$. It gives us the value $l=0$ or 1. Hence $k=0$ and E is singular. □

Proposition 7. *Let $E : y^2 = x^3 - (6k+3)x - (3k^2+6k+2)$ be the elliptic curve with k in $\mathbb{Z}$. Assume that there is no integer h such that $k = 4h(3h^2+3h+1)$ or $-4(h+1)(3h^2+3h+1)$. Then $E(\mathbb{Q})$ has no point of order 3.*

Proof. As we mentioned in the proof of the previous lemma, the point $P = (x,y)$ is of order 3 if and only if x is the root of

$$T_E(X)$$
$$= 3(X+1)\left(X^3 - X^2 - (12k+5)X - (12k^2+12k+3)\right).$$

Let $S_E(X)$ be the polynomial

$$T_E(X)/3(X+1)$$
$$= X^3 - X^2 - (12k+5)X - (12k^2+12k+3).$$

Since $\left(-1, \pm\sqrt{-3k^2}\right)$ is not in $E(\mathbb{Q})$, it suffices to check whether x is a root of $S_E(X) = 0$ or not.

Suppose that $S_E(X) = 0$ has a root x' in $\mathbb{Q}$. Then it is an integer. In other words, for an integer k not the form $4h(3h^2+3h+1)$ or $-4(h+1)(3h^2+3h+1)$ by sorting again as k, we can fine an integer x' such that

$$x'^3 - x'^2 - (12k+5)x' - (12k^2+12k+3)$$
$$= -12k^2 - 12(x'+1)k + x'^3 - x'^2 - 5x' - 3 = 0.$$

From, this $x'^3 - x'^2 - 5x' - 3$ must be a multiple of 12 and x is one of $12m+3,5,9$ or 11 for a suitable integer m.

When $x = 12m+3$, S_E becomes $-12\left(k^2 + 12km + 4k - 144m^3 - 96m^2 - 16m\right)$. Because it has integral solutions as a quadratic equation with respect to k, its discriminant $16(4m+1)(1+3m)^2$ is a square. That means that $4m+1 = (2h+1)^2$ for an integer h. Through this we get $k = 4h\left(3h^2 + 3h + 1\right)$ or $-4(h+1)\left(3h^2 + 3h + 1\right)$.

If $x = 12m+5, 12m+9$ or $x = 12m+11$ then discriminant of the quadratic equations with respect to k is $3(12m+5)\{2(2m+1)\}^2, (4m+3)\{2(6m+5)\}^2$ or $3(12m+11)\{4(m+1)\}^2$ respectively. Neither case has a perfect square discriminant and admit any integral root. □

Proof of Theorem 2. Use the Lemma 5 and Theorem 3 3), we can determine which finite abelian group has a subgroup of $E(\mathbb{Q})$ for the case $k \equiv 1 \pmod{35}$, *i.e.*, $k \equiv 1 \pmod 5$ and $k \equiv 1 \pmod 7$. In fact, $E(\mathbb{Q})_{tors}$ is a subgroup of both $\mathbb{Z}/9\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z}$. It yields that it is $\mathbb{Z}/3\mathbb{Z}$ or trivial. Since our group has no point of order 3, it is trivial.

Note that $E(\mathbb{Q})_{tors}$ is a subgroup of order N, if it is a subgroup of order $3^r \cdot N$ with $(3,N)=1$, then. So it is resolved as trivial group in many cases.

To observe easily, we can refer **Table 2**: In this table, k takes the value modulo 5 at the horizontal line and modulo 7 at the vertical line respectively. The groups $C_n = \mathbb{Z}/n\mathbb{Z}$ in the brackets at top line and at the very left line are result from Lemma 5 .

Each entry implies that the type of group: "A", "B" or "C" implies one of subgroups of $\mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z}$ or trivial, respectively. The same alphabet does not mean the same group. And "D" means that both curves $E_5(\mathbb{F}_5)$ and $E_7(\mathbb{F}_7)$ are singular. In this table since "C" is trivial, it remains that a few cases $k \equiv 4,7,12,15,20,22,25,27,29,32$ or $34 \pmod{35}$.

For the cases that the subgroup is nontrivial Proposition 6 makes us know which curve has the point of order 2 or not. Hence, it is sufficient to check the value k having order 4 points.

Table 2. Type of group $E(\mathbb{Q})_{tors}$.

$k \pmod 7$	$k \pmod 5$	0	1 (C_9)	2 (C_6)	3 (C_3)	4
0		D	C	B	C	D
1	(C_6)	B	C	B	C	B
2	(C_9)	C	C	C	C	C
3	$(C_3 \oplus C_3)$	C	C	C	C	C
4	(C_6)	B	C	B	C	B
5		D	C	B	C	D
6	(C_{12})	A	C	B	C	A

Assume that $k \equiv 20, 34 \pmod{35}$ and there exists an integer l such that $k = -3l(1-l)$. In fact $k \equiv 20 \pmod{35}$ (respectively, $34 \pmod{35}$) if and only if $l \equiv 5$ or $26 \pmod{35}$ (respectively, 19 or $33 \pmod{35}$). $\left(3l^2 - 1, 0\right)$ is the unique point of order 2. Using duplication formula for the elliptic curve, let $P = (x', y')$ be the point satisfying $2P = \left(3l^2 - 1, 0\right)$. By Substituting $x', y', -(6k+3)$ and $-\left(3k^2 + 6k + 2\right)$ for x, y, A and B in (in the formulas for x_2 and y_2 in the proof of Lemma 4), we get two equations affirming the existence of point of order 4:

$$\left(x'^2 + 2\left(1-3l^2\right)x' - 18l^4 + 18l^3 - 6l^2 + 1\right)^2 = 0$$

$$\left(x'^2 + 2\left(1-3l^2\right)x' - 18l^4 + 18l^3 - 6l^2 + 1\right) \times F(x') = 0$$

where

$$\begin{aligned} F(x) = {} & x^4 - 2\left(1-3l^2\right)x^3 + 6\left(9l^4 - 18l^3 + 12l^2 - 2\right)x^2 \\ & - 2\left(54l^6 - 162l^5 + 108l^4 + 54l^3 - 63l^2 + 7\right)x \\ & + 324l^8 - 972l^7 + 864l^6 - 270l^4 + 60l^2 - 5. \end{aligned}$$

To have an integral solution of $x^2 + 2\left(1-3l^2\right)x - 18l^4 + 18l^3 - 6l^2 + 1 = 0$, its discriminant $36l^3(3l-2)$ have to be a square. Suppose that we can find an integer m such that $m^2 = l(3l-2)$ and $x' = 3l^2 - 1 + 6lm$ (or $3l^2 - 1 - 6lm$). It is easy to check that the integer m satisfying the above condition exists in each case determined by l. Furthermore, by substituting x', $k = -3l(1-l)$ and $m^2 = l(3l-2)$ to the right hand side of (1.4) we get a numerical formula

$$\begin{aligned} & 54l^3(3l-2)\left(6l^2 - 5lm - 2\right) \\ & = 9l^2 \cdot 6l(3l-2) \cdot 6\left(6l^2 - 5lm - 2\right) \\ & = 9l^2m^2 \cdot 6\left(6l^2 - 5lm - 2\right) \end{aligned}$$

Since $l \neq 0$ makes the curve (1.4) singular, $6\left(6l^2 - 5lm - 2\right)$ is a square of a suitable integer if and only if there exists a point of order 4.

So we are done. □

3. Conclusions

By the help of Theorem 2, we explicitly calculate the torsion part of Modell-Weil group.

Example 8. *Let* $E: y^2 = x^3 - 75x - 506$ *be the elliptic curve. Then*

$$E(\mathbb{Q})_{tors} = \mathbb{Z}/2\mathbb{Z}.$$

Given elliptic curve is the form $k = 12$ in Theorem 2 and $12 = -3 \times 2^2 \times (1-2)$. Therefore $E(\mathbb{Q})_{tors} = \mathbb{Z}/2\mathbb{Z}$. And $(11,0)$ is the nontrivial torsion point on $E(\mathbb{Q})$.

The method to find $E(\mathbb{Q})_{tors}$ is able to be applied to all elliptic curve without a condition for k by choosing another prime $p > 7$.

For example, in Theorem 2, there is a condition $35 \nmid k(9k+4)$ for k. This is one for nonsingular curve. For the case that $35 | k(9k+4)$, choose the another prime $p > 7$ such that $p \nmid k(9k+4)$. Calculate $E_p(\mathbb{F}_p)$ and eliminate the order 3 point and check the condition for having order 2 point. Since $|E(\mathbb{F}_p)| \le 2p+1$, the smaller p gives simpler necessary condition. For example, if $k = -16$ then the elliptic curve is

$$E : y^2 = x^3 + 93x - 674$$

with discriminant $2^6 \times 5 \times 7$. Find $E_p(\mathbb{Z}_p)$ with $p = 11$ and 17, $|E_{11}(\mathbb{Z}_{11})| = 15$ and $|E_{17}(\mathbb{Z}_{17})| = 18$. Using Lemma 4, we observe that $E(\mathbb{Q})$ has no point of order 3. So it is a trivial group.

Remark 9. *Generalize our elliptic curve*

$$E : y^2 = x^3 + f(k)x + g(k)$$

for $k \in \mathbb{Z}$ and $\max\{\deg f(k), \deg g(k)\} \le 2$. We can use the criterion for the quadratic equation to find a point of order 2 or 3. Of course, it is indispensable to consider some exceptional cases in the similar way to Proposition 7.

REFERENCES

[1] B. Mazur, "Modular Curves and the Eisenstein Ideal," *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, No. 47, 1977, pp. 33-168.

[2] A. Knapp, "Elliptic Curves," Princeton University Press, Princeton, 1992.

[3] D. Kim, J. K. Koo and Y. K. Park, "On the Elliptic Curves Modulo *p*," *Journal of Number Theory*, Vol. 128, No. 4, 2008, pp. 945-953. doi:10.1016/j.jnt.2007.04.015

