Far East Journal of Mathematical Sciences (FJMS)
© 2017 Pushpa Publishing House, Allahabad, India
http://www.pphmj.com
http://dx.doi.org/10.17654/MS102010183
Volume 102, Number 1, 2017, Pages 183-214 **ISSN: 0972-0871**

TORSION GROUPS OF SOME ELLIPTIC CURVES

Jung Won Kwon, Gisoo Oh and Hwasin Park[*]

Department of Mathematics
Chonbuk National University
Jeonju 54896, Korea

Abstract

According to Mordell-Weil theorem, the group $E(\mathbb{Q})$ of an elliptic curve E over $\mathbb{Q}$ is a finitely generated abelian group which is isomorphic to a group of the form $E_{tors}(\mathbb{Q}) \times \mathbb{Z}^r$, where r is a nonnegative integer. We study the torsion groups $E_{tors}(\mathbb{Q})$ for special elliptic curves and the torsion groups of $E : y^2 = x^3 + Ax + B$ for some cases of $A \in \mathbb{Z}$ and $B = \prod_{i=1}^{n} p_i^{e_i}$, where p_i's are all primes such that $p_i \equiv 3 \pmod 8$, $(p_i \equiv 1 \pmod 8$, $p_i = 5 \pmod 8$, $p_i \equiv 7 \pmod 8)$, respectively.

1. Introduction

By Mordell-Weil theorem, we know well that the group $E(\mathbb{Q})$ of an elliptic curve E defined over $\mathbb{Q}$ is finitely generated [4, 11, 13, 14], i.e.,

---

Received: February 22, 2017; Accepted: April 9, 2017
2010 Mathematics Subject Classification: 14H52.
Keywords and phrases: elliptic curves, Mordell-Weil theorem, torsion group.

[*]Corresponding author

$$E(\mathbb{Q}) = E_{tors}(\mathbb{Q}) \times \mathbb{Z}^r.$$

Then in this paper, we study the torsion groups $E_{tors}(\mathbb{Q})$ for some elliptic curves $E : y^2 = x^3 + Ax + B.$ The major steps of this study are as follows:

In Section 2, we discuss some definitions and properties of elliptic curves.

In Section 3, we investigate that if p does not divide the discriminant Δ of an elliptic curve E, then the reduction modulo p map is an isomorphism of $E_{tors}(\mathbb{Q})$ onto a subgroup of $\tilde{E}(\mathbb{F}_p)$.

In Section 4, we investigate the torsion groups $E_{tors}(\mathbb{Q})$ for special elliptic curves.

In Section 5, we study torsion groups of some elliptic curves $E : y^2 = x^3 + Ax + B$ with $A \in \mathbb{Z}$ and $B = \prod_{i=1}^{n} p_i^{e_i}$, where p_i's are all primes such that $p_i \equiv 3 \pmod 8$, $(p_i \equiv 1 \pmod 8), p_i = 5 \pmod 8), p_i \equiv 7 \pmod 8))$, respectively.

If p_i's are all primes such that $p_i \equiv 3 \pmod 8$ and $p_i \neq 3$, then we can obtain the following results:

(1) If all e_i's are even, $e_i = 3m_i$ for all i and

$$A = -\prod_{i=1}^{n} p_i^{2m_i} - \prod_{i=1}^{n} p_i^{e_i - m_i} = -2\prod_{i=1}^{n} p_i^{m_i},$$

then

$$E_{tors}(\mathbb{Q}) = \left\{O, \left(\prod_{i=1}^{n} p_i^{m_i},\ 0\right), \left(0,\ \pm\prod_{i=1}^{n} p_i^{e_i/2}\right)\right\} = \mathbb{Z}/4\mathbb{Z}.$$

(2) For $A \not\equiv 0 \pmod 3$, if

$$A = -\prod_{i=1}^{n} p_i^{2m_i} \pm \prod_{i=1}^{n} p_i^{e_i - m_i},$$

then

$$E_{tors}(\mathbb{Q}) = \left\{O, \left(\mp \prod_{i=1}^{n} p_i^{m_i}, 0\right)\right\} = \mathbb{Z}/2\mathbb{Z},$$

where e_i is odd or $e_i \neq 3m_i$ for some i if $A = -\prod_{i=1}^{n} p_i^{2m_i} - \prod_{i=1}^{n} p_i^{e_i - m_i}$.

(3) For $A \equiv 1 \pmod 3$, if

$$A \neq -\prod_{i=1}^{n} p_i^{2m_i} \pm \prod_{i=1}^{n} p_i^{e_i - m_i},$$

then

$$E_{tors}(\mathbb{Q}) = \{O\}.$$

By using the similar method, we will study torsion groups of an elliptic curve $E: y^2 = x^3 + Ax + \prod_{i=1}^{n} p_i^{e_i}$, where p_i's are all primes such that $p_i \equiv 1 \pmod 8$ ($p_i \equiv 5 \pmod 8$, $p_i \equiv 7 \pmod 8$) in Theorem 5.3 (Theorem 5.4, Theorem 5.5), respectively.

2. Elliptic Curves

If K is a number field, let $\overline{K}$ denote its *algebraic closure*. The *projective n-space* over K, denoted $\mathbb{P}^n$ or $\mathbb{P}^n(\overline{K})$, is the set of all $(n+1)$-tuples

$$(x_0, x_1, ..., x_n) \in \mathbb{A}^{n+1}(\overline{K}),$$

where $\mathbb{A}^{n+1}(\overline{K})$ is an affine (or Euclidean) space, such that at least one x_i is non-zero, modulo the equivalence relation given by

$$(x_0, x_1, ..., x_n) \sim (y_0, y_1, ..., y_n)$$

if there exists $\lambda \in \overline{K}^* = \overline{K} - \{O\}$ with $x_i = \lambda y_i$ for all i. An equivalence class $\{(\lambda x_0, ..., \lambda x_n) | \lambda \in \overline{K}^*\}$ is denoted $[x_0, ..., x_n]$, and $x_0, ..., x_n$ are called *homogeneous coordinates* for the corresponding point in $\mathbb{P}^n$. A *Weierstrass equation* is a homogeneous equation of degree 3 of the form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

where $a_1, a_2, ..., a_6 \in \overline{K}$. The Weierstrass equation is said to be *non-singular* if for all projective points $P = [X, Y, Z] \in \mathbb{P}^n(\overline{K})$ satisfying

$$F(X, Y, Z)$$

$$= Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 = 0,$$

at least one of the three partial derivatives $\frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}, \frac{\partial F}{\partial Z}$ is non-zero at *P*.

An *elliptic curve E* (or an algebraic curve of genus 1) is the set of all solutions in $\mathbb{P}^2(\overline{K})$ of a non-singular Weierstrass equation. There is exactly one point in *E* with *Z*-coordinate equal to 0, namely [0, 1, 0]. We call this point the *point at infinity* and denote it by *O*.

For convenience, we will write the Weierstrass equation for an elliptic curve using non-homogeneous (affine) coordinates $x = \frac{X}{Z}, \quad y = \frac{Y}{Z}$ if $Z \neq 0$,

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where a_i's are in $\overline{K}$. Then an elliptic curve *E* is the set of solutions to the equation in the affine plane $\mathbb{A}^2(\overline{K}) = \overline{K} \times \overline{K}$, together with the extra point at infinity *O*. If $a_1, a_2, ..., a_6 \in K$, then *E* is said to be *defined over K*, and denoted this by E/K. If *E* is defined over *K*, then the set of *K-rational points* of *E*, denoted $E(K)$, is the set of points both of whose coordinates lie in *K*, together with the point *O*.

Then for $char(K) \neq 2$, we can simplify the equation by completing the square. That is, replacing *y* by $\frac{1}{2}(y - a_1x - a_3)$ gives an equation of the form

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

where $b_2 = a_1^2 + 4a_2,\ b_4 = 2a_4 + a_1a_3,\ b_6 = a_3^2 + 4a_6$.

If further $char(K) \neq 2, 3,$ then replacing (x, y) by $((x - 3b_2)/36,\ y/108)$ eliminates the x^2 term, yielding the simpler equation

$$E : y^2 = x^3 - 26c_4x - 54c_6,$$

where $c_4 = b_2^2 - 24b_4,\ c_6 = b_2^3 + 36b_2b_4 - 216b_6$.

Also, we define the *discriminant*

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,$$

where $b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$ and also the *j-invariant* on E, as

$$j(E) = j = \frac{c_4^3}{\Delta} = \frac{12^3c_4^3}{c_4^3 - c_6^2}.$$

Hence, if the characteristic of K is not 2 or 3, then we may assume that our elliptic curves have Weierstrass equations of the form

$$E : y^2 = x^3 + Ax + B.$$

This equation has associated quantities

$$\Delta = -16(4A^3 + 27B^2),$$

$$j = -1728(4A)^3/\Delta.$$

The only change of variables preserving this form of equation is

$$x = u^2x', \quad y = u^3y' \text{ for some } u \in \overline{K}^*;$$

and then

$$u^4 A' = A, \quad u^6 B' = B, \quad u^1 2\Delta' = \Delta.$$

If $\Delta \neq 0,$ then this is an elliptic curve.

Let E be an elliptic curve given by a Weierstrass equation. $E \subset \mathbb{P}^2$ consists of the points $P = (x, y)$ satisfying the equation together with the points $O = [0, 1, 0]$ at infinity. Let $L \subset \mathbb{P}^2$ be a line. Then since the equation has the degree three, L intersects E at exactly 3 points, say P, Q, R.

Composition Law 2.1 [4, 13]**.** *Let $P, Q \in E,$ L be the line connecting P and Q (tangent line to E if $P = Q$), and R be the third point of intersection of L with E. Let L' be the line connecting R and O. Then $P \oplus Q$ is the point such that L' intersects E at R, O and $P \oplus Q$.*

Then the composition law makes E into an abelian group with identity element O. We further have:

Proposition 2.2 [13]**.** *Suppose E is an elliptic curve defined over K. Then*

$$E(K) = \{(x, y) \in K^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\}$$

is a subgroup of E.

Notation. For $m \in \mathbb{Z}$ and $P \in E,$ we let

$$[m]P = P + \cdots + P \text{ (m terms) for } m > 0.$$

$$[0]P = O, \quad \text{and} \quad [m]P = [-m](-P) \text{ for } m < 0.$$

Proposition 2.3 [4, 11, 13]**.** *Let E be an elliptic curve given by a Weierstrass equation*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Here we will use + and – instead of the special symbols $\oplus$ and $\ominus$ *for the group operations on E.*

(1) *Let* $P_0 = (x_0, y_0) \in E$. *Then* $-P_0 = (x_0, -y_0 - a_1x_0 - a_3)$.

Now let

$$P_1 + P_2 = P_3 \text{ with } P_i = (x_i, y_i) \in E.$$

(2) *If* $x_1 = x_2$ *and* $y_1 + y_2 + a_1x_2 + a_3 = 0$, *then* $P_1 + P_2 = O$.

Otherwise, let

$$\begin{cases} \lambda = \dfrac{y_2 - y_1}{x_2 - x_1}, \\ \mu = \dfrac{y_1x_2 - y_2x_1}{x_2 - x_1} \text{ if } x_1 \neq x_2, \end{cases}$$

and

$$\begin{cases} \lambda = \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, \\ \mu = \dfrac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} \text{ if } x_1 = x_2. \end{cases}$$

(*Then* $y = \lambda x + \mu$ *is the line through* P_1 *and* P_2, *or tangent to* E *if* $P_1 = P_2$.)

(3) $P_3 = P_1 + P_2$ *is given by*

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2,$$

$$y_3 = -(\lambda + a_1)x_3 - \mu - a_3.$$

(4) *As special cases of* (3), *for* $P_1 \neq \pm P_2$, *we have*:

$$x(P_1 + P_2) = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 + a_1\left(\frac{y_2 - y_1}{x_2 - x_1}\right) - a_2 - x_1 - x_2.$$

For $P = (x, y) \in E$, *the duplication formula has*

$$x([2]P) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6},$$

where $b_2 = a_1^2 + 4a_2$, $b_4 = 2a_4 + a_1a_3$, $b_6 = a_3^2 + 4a_6$ *and* $b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$.

From now on, we quote some known theorems:

Theorem 2.4 (Mordell-Weil) [4, 11, 13]**.** *Let* K *be a number field and* E/K *be an elliptic curve. Then the group* $E(K)$ *is finitely generated.*

From the Mordell-Weil theorem, we see that Mordell-Weil group $E(K)$ has the form

$$E(K) \cong E_{tors}(K) \times \mathbb{Z}^r,$$

where the *torsion subgroup* $E_{tors}(K)$ is finite and the rank r of $E(K)$ is a non-negative integer.

Theorem 2.5 (Mazur) [4, 11, [13]**.** *Let* $E/\mathbb{Q}$ *be an elliptic curve. Then the torsion subgroup* $E_{tors}(\mathbb{Q})$ *is one of the following fifteen groups*:

$$\mathbb{Z}/N\mathbb{Z}, \quad 1 \leq N \leq 10 \quad or \quad N = 12,$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, \quad 1 \leq N \leq 4.$$

Further, each of these groups occurs as an $E_{tors}(\mathbb{Q})$.

Theorem 2.6 (Lutz-Nagell) [4, 11, 13]**.** *Let* $E/\mathbb{Q}$ *be an elliptic curve with a Weierstrass equation*

$$y^2 = x^3 + Ax + B, \quad A, B \in \mathbb{Z}.$$

Suppose $P \in E(\mathbb{Q})$ *is a non-zero torsion point. Then*

(a) $x(P), y(P) \in \mathbb{Z}$.

(b) *Either* $[2]P = O$, *or else* $y(P)^2$ *divides* $4A^3 + 27B^2$.

3. Reduction Modulo *p*

Let E be an elliptic curve, given as usual by a Weierstrass equation

$$E : y^2 = x^3 + Ax + B$$

with integer coefficients A, B. We showed that this group is finitely generated (Mordell's theorem) and that the points of finite order have integer coordinates (Lutz-Nagell theorem).

In this section, we have been looking at curves with coefficients in a finite field $\mathbb{F}_p$. Suppose that we write $z \mapsto \tilde{z}$ for the map "reduction modulo p",

$$\mathbb{Z} \to \mathbb{Z}/p\,\mathbb{Z} = \mathbb{F}_p, \quad z \mapsto \tilde{z}.$$

Then we can take the equation for E, which has integer coefficients, and we can reduce those coefficients modulo p to get a new curve with coefficients in $\mathbb{F}_p$:

$$E : y^2 = x^3 + \tilde{A}x + \tilde{B}.$$

When will the curve $\tilde{E}$ be non-singular? It will be non-singular provided $p \geq 3$ and provided the discriminant

$$\tilde{\Delta} = -16(4\tilde{A}^3 - 27\tilde{B}^2)$$

is non-zero. But reduction modulo p from $\mathbb{Z}$ to $\mathbb{F}_p$ is a homomorphism, so $\tilde{\Delta}$ is just the reduction modulo p of the discriminant D of the cubic $x^3 + Ax + B$. In other words, the reduced curve $\tilde{E}\ (\text{mod}\ p)$ will be non-singular provided $p \geq 3$ and p does not divide the discriminant Δ.

Having reduced the curve E, it is natural to try taking points on E and reducing them modulo p to get points on $\tilde{E}$. We can do this provided that the coordinates of the point have no p in their denominator. In particular, if a point has integer coordinates, then we can reduce that point modulo p for any prime p. That is, if $P = (x, y)$ is a point in $E(\mathbb{Q})$ with integer coordinates, then x and y satisfy the equation

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

This equation gives a relation among integers, so we can reduce it modulo p to get the equation

$$y^2 = x^3 + \tilde{A}x + \tilde{B}.$$

This last equation says that $\tilde{P} = (\tilde{x}, \tilde{y})$ is a point in $\tilde{E}(\mathbb{F}_p)$. So we get a map from the points in $E(\mathbb{Q})$ with integer coordinates to $\tilde{E}(\mathbb{F}_p)$.

We know that points of finite order in $E(\mathbb{Q})$ always have integer coordinates. This is the hard part of the Lutz-Nagell theorem. We are going to study the collection of points of finite order, so let us give it a name:

$$E_{tors}(\mathbb{Q}) = \{P = (x, y) \in E(\mathbb{Q}) : P \text{ has finite order}\}.$$

Clearly, $E_{tors}(\mathbb{Q})$ is a subgroup of $E(\mathbb{Q})$ because if P_1, P_2 are points of finite order, say $m_1P_1 = O$ and $m_2P_2 = O$, then $(m_1m_2)(P_1 \pm P_2) = O$. So both $P_1 + P_2$ and $P_1 - P_2$ are in $E_{tors}(\mathbb{Q})$.

Since $E_{tors}(\mathbb{Q})$ consists of points with integer coordinates, together with O, we can define a *reduction modulo p map*

$$E_{tors}(\mathbb{Q}) \to \tilde{E}(\mathbb{F}_p), \quad P \mapsto \tilde{P} = \begin{cases} (\tilde{x}, \tilde{y}) & \text{if } P = (x, y), \\ \tilde{O} & \text{if } P = O. \end{cases}$$

Now $E_{tors}(\mathbb{Q})$ is a subgroup of $E(\mathbb{Q})$, so it is a group; and provided p does not divide Δ, we know that $\tilde{E}(\mathbb{F}_p)$ is a group. So we have a map from the group $E_{tors}(\mathbb{Q})$ to the group $\tilde{E}(\mathbb{F}_p)$, and we now want to check that this map is a homomorphism.

First we note that negatives go to negative:

$$\widetilde{-P} = (\widetilde{x, -y}) = (\tilde{x}, \tilde{y}) = -\tilde{P}.$$

So it suffices to show that if $P_1 + P_2 + P_3 = O,$ then $\tilde{P}_1 + \tilde{P}_2 + \tilde{P}_3 = \tilde{O}.$ As usual, there are some special cases to check.

If any of P_1, P_2 or P_3 equals O, then the result we want follows from the fact that negatives go to negatives, So we may assume that P_1, P_2 and P_3 are not equal to O. We write their coordinates as

$$P_1 = (x_1, y_1), \quad P_2 = (x_2, y_2), \quad P_3 = (x_3, y_3).$$

From the definition of the group law on E, the condition $P_1 + P_2 + P_3 = O$ is equivalent to saying that P_1, P_2 and P_3 lie on a line. Let

$$y = \lambda x + \nu$$

be the line through P_1, P_2, P_3. (If two or three of the points coincide, then the line has to satisfy certain tangency conditions.)

Our explicit formula for adding points says that

$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = \lambda x_3 + \nu.$$

Since x_1, x_2, x_3, y_3 and a are all integers, we see that λ and ν are also integers. This fact is what we needed because now we can reduce λ and ν modulo p.

Substituting the equation of the line into the equation of the cubic, we know that the equation

$$x^3 + Ax + B - (\lambda x + \nu)^2 = 0$$

has x_1, x_2, x_3 as its three roots. In other words, we have the factorization

$$x_3 + Ax + B - (\lambda x + \nu)^2 = (x - x_1)(x - x_2)(x - x_3).$$

This is the relation that ensures that $P_1 + P_2 + P_3 = O,$ regardless of whether or not the points are distinct.

Reducing this last equation modulo p, we obtain

$$x^3 + \tilde{A}x + \tilde{B} - (\tilde{\lambda}x + \tilde{\nu})^2 = (x - \tilde{x}_1)(x - \tilde{x}_2)(x - \tilde{x}_3).$$

Of course, we can also reduce the equations $y_i = \lambda x_i + \nu$ to get

$$\tilde{y}_i = \tilde{\lambda}\tilde{x}_i + \tilde{\nu} \text{ for } i = 1, 2, 3.$$

This means that the line $y = \tilde{\lambda}x + \tilde{\nu}$ intersects the curve $\tilde{E}$ at the three points $\tilde{P}_1$, $\tilde{P}_2$ and $\tilde{P}_3$. Further, if two of the points $\tilde{P}_1$, $\tilde{P}_2$ and $\tilde{P}_3$ are the same, say $\tilde{P}_1 = \tilde{P}_2$, then the line is tangent to $\tilde{E}$ at $\tilde{P}_1$; and similarly, if all three coincide, then the line has a triple order contact with $\tilde{E}$. Therefore,

$$\tilde{P}_1 + \tilde{P}_2 + \tilde{P}_3 = \tilde{O},$$

which completes the proof that the reduction modulo p map is a homomorphism from $E_{tors}(\mathbb{Q})$ to $\tilde{E}(\mathbb{F}_p)$.

Now we observe that this homomorphism is one-to-one. A non-zero point $(x, y) \in E_{tors}(\mathbb{Q})$ is sent to the reduced point $(\tilde{x}, \tilde{y}) \in \tilde{E}(\mathbb{F}_p)$, and that reduced point is clearly not $\tilde{O}$. So the kernel of the reduction map consists only of O, and hence the map is one-to-one. This means that $E_{tors}(\mathbb{Q})$ looks like a subgroup of $\tilde{E}(\mathbb{F}_p)$ for every prime p such that p is relatively prime to Δ. Hence we have completed the proof of the following proposition:

Proposition 3.1 (Reduction modulo p theorem)**.** *Let E be a non-singular elliptic curve*

$$E : y^2 = x^3 + Ax + B$$

with integer coefficients A, B and let Δ be the discriminant

$$\Delta = -16(4A^3 + 27B^2).$$

Let $E_{tors}(\mathbb{Q}) \subseteq E(\mathbb{Q})$ *be the subgroup consisting of all points of finite order. For any prime p, let* $P \to \tilde{P}$ *be the reduction modulo p map*

$$E_{tors}(\mathbb{Q}) \to \tilde{E}(\mathbb{F}_p), \quad P \mapsto \tilde{P} = \begin{cases} (\tilde{x}, \tilde{y}) & P = (x, y), \\ \tilde{O} & P = O. \end{cases}$$

If p does not divide Δ, *then the reduction modulo p map is an isomorphism of* $E_{tors}(\mathbb{Q})$ *onto a subgroup of* $\tilde{E}(\mathbb{F}_p)$.

4. Torsion Groups for Special Curves

In this section, we will show that the torsion groups for special elliptic curves using a lemma about $E_p(\mathbb{Z}_p)$ for certain primes *p*. Also, we shall use the form of the duplication formula in Proposition 2.3(4) when specialized to a curve $y^2 = x^3 + Ax + B$:

$$x(2P) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)}. \tag{4.1}$$

Lemma 4.1 (Dirichlet's theorem, [11])**.** *There are infinitely many* (*positive*) *primes* $an + b$ *if* $GCD(a, b) = 1$.

Lemma 4.2. *Let* E_p *be the curve* $y^2 = x^3 + Ax$ *over* $\mathbb{Z}_p$, *and assume that* $p \nmid \Delta$, $p \geq 7$, *and* $p \equiv 3 \pmod 4$. *Then* $E_p(\mathbb{Z}_p)$ *has exactly* $p+1$ *points*.

Proof. We start from the known result that $p \equiv 3 \pmod 4$ implies that –1 is not a square modulo *p*. For $x \neq 0$, consider the pair $\{x, -x\}$. When these elements are substituted into *E*, we obtain $x^3 + Ax$ and $-(x^3 + Ax)$. If the answers are 0, each one has a square root, and we get one solution from each. If they are non-zero, exactly one is a square (since –1 is not a square), and it has two square roots. So in either case, the pair $\{x, -x\}$ gives us two solutions. Thus the non-zero *x*'s give us $p-1$ solutions in all. For $x = 0$, we get one more solution (0, 0), and O gives us one additional solution. Thus $E_p(\mathbb{Z}/p\mathbb{Z})$ has $p+1$ points. □

Proposition 4.3. *Let E be the elliptic curve* $y^2 = x^3 + Ax$ *with A in* $\mathbb{Z}$ *and with A assumed fourth-power free. Then*

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

Proof. The main step is to show that $|E_{tors}(\mathbb{Q})|$ divides 4. By Proposition 3.1, for all sufficiently large primes p, $|E_{tors}(\mathbb{Q})|$ divides $|E_p(\mathbb{Z}/p\mathbb{Z})|$. By Lemma 4.2, $|E_{tors}(\mathbb{Q})|$ divides $p+1$ for all sufficiently large primes p with $p \equiv 3 \pmod 4$.

Let us see that 8 does not divide $|E_{tors}(\mathbb{Q})|$. By Lemma 4.1 (Dirichlet's theorem), we can choose a prime p as in the previous sentence with $p \equiv 3 \pmod 8$. If 8 divides $|E_{tors}(\mathbb{Q})|$, then $8|(p+1)$. But $p \equiv 3 \pmod 8$ means that $p+1 \equiv 4 \pmod 8$; so $8 \nmid (p+1)$, a contradiction.

Now let us see that 3 does not divide $|E_{tors}(\mathbb{Q})|$. By Lemma 4.1, we can choose p large with $p \equiv 7 \pmod{12}$. Then $p \equiv 3 \pmod 4$. Thus $3||E_{tors}(\mathbb{Q})|$ implies $3|(p+1)$. But $p+1 \equiv 8 \pmod{12}$ implies $p+1 \equiv 8 \pmod 3$; so $3 \nmid (p+1)$, a contradiction.

Finally, let us see that no odd prime $q > 3$ divides $|E_{tors}(\mathbb{Q})|$. By Lemma 4.1, we can choose p large with $p \equiv 3 \pmod{4q}$. Then $p \equiv 3 \pmod 4$. Thus $q||E_{tors}(\mathbb{Q})|$ implies $q|(p+1)$. But $p+1 \equiv 4 \pmod{4q}$ implies $p+1 \equiv 4 \pmod q$; so $q \nmid (p+1)$, a contradiction.

This completes the proof that $|E_{tors}(\mathbb{Q})|$ divides 4. The torsion group will then contain $\mathbb{Z}_2 = \{(0, 0), O\}$ as a subgroup, and it will be $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ if and only if $x^3 + Ax$ splits over $\mathbb{Q}$, i.e., if and only if $-A$ is a square. Thus the only question is when (0, 0) is the double of something (so that the torsion group is $\mathbb{Z}_4$ rather than $\mathbb{Z}_2$). So we can check directly for $A = 4$ that (2, 4) doubles to (0, 0).

Consider the equation $2(x, y) = (0, 0)$ for other A. By (4.1), we have

$$0 = x^4 - 2Ax^2 + a^2 = (x^2 - A)^2.$$

Thus $x^2 = A$. Since A is fourth-power free, x is squarefree. But $y^2 = x(x^2 + A) = x(x^2 + x^2) = 2x^3$ then shows that no odd prime can divide x. So $x = \pm 1$ or ± 2. Checking the possibilities, we see that $x = 2$ and $A = 4$. □

Lemma 4.4. *Let* E_p *be the curve* $y^2 = x^3 + B$ *over* $\mathbb{Z}/p\mathbb{Z}$, *and assume that* $p \nmid \Delta$, $p \geq 5$, *and* $p \equiv 2 \pmod 3$. *Then* $E_p(\mathbb{Z}/p\mathbb{Z})$ *has exactly* $p + 1$ *points*.

Proof. Let $p = 3n + 2$. The multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$ has order $p - 1$. Since $3 \nmid (p-1)$, no element has order 3. Therefore, the homomorphism $a \mapsto a^3$ on $(\mathbb{Z}/p\mathbb{Z})^*$ is one-to-one, hence onto. Thus each element of $\mathbb{Z}/p\mathbb{Z}$ has a unique cube root. For each y in $\mathbb{Z}/p\mathbb{Z}$, the element $y^2 - B$ has a unique cube root, which we can take as x. In this way, we obtain p solutions. Adjoining O, we see that $E_p(\mathbb{Z}/p\mathbb{Z})$ has $p + 1$ points. □

Proposition 4.5. *Let E be the elliptic curve* $y^2 = x^3 + B$ *with B in* $\mathbb{Z}$ *and with B assumed sixth-power free*. *Then*

$$E_{tors}(\mathbb{Q}) = \begin{cases} \mathbb{Z}/6\mathbb{Z} & \text{if } B = 1 \\ \mathbb{Z}/3\mathbb{Z} & \text{if } B = -432 = -2^4 3^3, \\ & \text{or if } B \text{ is a square and } B \neq 1 \\ \mathbb{Z}/2\mathbb{Z} & \text{if } B \text{ is a cube and } B \neq 1 \\ \{O\} & \text{otherwise.} \end{cases}$$

Proof. The main step is to show that $|E_{tors}(\mathbb{Q})|$ divides 6. By Proposition 3.1, for all sufficiently large primes *p*, $|E_{tors}(\mathbb{Q})|$ divides $p+1$ for all sufficiently large primes *p* with $p \equiv 2 \pmod 3$.

Let us see that 4 does not divide $|E_{tors}(\mathbb{Q})|$. By Lemma 4.1 (Dirichlet's theorem), we can choose a prime *p* as in the previous sentence with $p \equiv 5 \pmod{12}$. If 4 divides $|E_{tors}(\mathbb{Q})|$, then $4|(p+1)$. But $p \equiv 1 \pmod 4$ means that $p+1 \equiv 2 \pmod 4$; so $4 \nmid (p+1)$, a contradiction.

Now let us see that 9 does not divide $|E_{tors}(\mathbb{Q})|$. By Lemma 4.1, we can choose *p* large with $p \equiv 2 \pmod 9$. Then $p \equiv 2 \pmod 3$. Thus $9 || E_{tors}(\mathbb{Q})|$ implies $9|(p+1)$. But $p+1 \equiv 3 \pmod 9$ implies $9 \nmid (p+1)$, a contradiction.

Finally, let us see that no odd prime $q > 3$ divides $|E_{tors}(\mathbb{Q})|$. By Lemma 4.1, we can choose *p* large with $p \equiv 2 \pmod{3q}$. Then $p \equiv 2 \pmod 3$. Thus $q || E_{tors}(\mathbb{Q})|$ implies $q|(p+1)$. But $p+1 \equiv 3 \pmod{3q}$ implies $p+1 = 3 \pmod q$; so $q \nmid (p+1)$, a contradiction.

This completes the proof that $|E_{tors}(\mathbb{Q})|$ divides 6. The torsion group has an element of order 2 if and only if $x^3 + B$ has a first-degree factor over $\mathbb{Z}$, i.e., if and only if *B* is a cube. Thus the only question is when the torsion group has elements of order 3. Such a point $P = (x, y)$ is characterized by $2P = -P$. Moreover, the *x* coordinate determines everything, since $2P = P$ is impossible for $P \neq O$. By (4.1),

$$\frac{x^4 - 8Bx}{4(x^3 + B)} = x$$

for any rational solutions *x*. Clearing fractions, we have

$$4x^4 + 4Bx = x^4 - 8Bx,$$

$$x^4 = -4Bx.$$

One solution is $x = 0$, which gives $y^2 = B$; so $\mathbb{Z}/3\mathbb{Z}$ occurs if B is a square. The only other possibility is $x^3 = -4B$. Then $y^2 = -3B$. Consequently, $B < 0$. Since B is sixth-power free, the only possible prime divisors of B are 2 and 3. We readily find $B = -2^4 3^3$. So $\mathbb{Z}/3\mathbb{Z}$ occurs if and only if either B is a square or $B = -2^4 3^3$. □

5. Main Results

In this section, we shall study torsion groups of some elliptic curves. Before studying the torsion group of an elliptic curve, we investigate the group of reduction of an elliptic curve modulo 3.

Lemma 5.1. *Let* $E/\mathbb{Q} : y^2 = x^3 + Ax + B$ *be an elliptic curve with* $A, B \in \mathbb{Z}$. *Then the order* $|\tilde{E}(\mathbb{Z}/3\mathbb{Z})|$ *of groups of reduction of E modulo* 3 *is the following*:

$$|\tilde{E}(\mathbb{Z}/3\mathbb{Z})| = \begin{cases} 4 & \text{if } A \equiv 1 \pmod 3,\ B \equiv 0 \pmod 3 \\ 4 & \text{if } A \equiv 2 \pmod 3,\ B \equiv 0 \pmod 3 \\ 4 & \text{if } A \equiv 1 \pmod 3,\ B \equiv 1 \pmod 3 \\ 7 & \text{if } A \equiv 2 \pmod 3,\ B \equiv 1 \pmod 3 \\ 4 & \text{if } A \equiv 1 \pmod 3,\ B \equiv 2 \pmod 3 \\ 1 & \text{if } A \equiv 2 \pmod 3,\ B \equiv 2 \pmod 3. \end{cases}$$

Proof. The proof of this is clear. □

From now on, we determine torsion groups of some elliptic curves.

Theorem 5.2. *Let E be the elliptic curve* $y^2 = x^3 + Ax + \prod_{i=1}^{n} p_i^{e_i}$ *with* $A \in \mathbb{Z}$, *where* p_i*'s are all primes such that* $p_i \equiv 3 \pmod 8$ *and* $p_i \neq 3$. *Then the torsion groups* $E_{tors}(\mathbb{Q})$ *of elliptic curve E are the following*:

(1) *If* $e_i = 3m_i$, m_i*'s are even for all i and*

$$A = -\prod_{i=1}^{n} p_i^{2m_i} - \prod_{i=1}^{n} p_i^{e_i - m_i} = -2\prod_{i=1}^{n} p_i^{m_i},$$

then

$$E_{tors}(\mathbb{Q}) = \left\{O, \left(\prod_{i=1}^{n} p_i^{m_i}, 0\right), \left(0, \pm\prod_{i=1}^{n} p_i^{e_i/2}\right)\right\} = \mathbb{Z}/4\mathbb{Z}.$$

(2) *For* $A \not\equiv 0 \pmod 3$, *if*

$$A = -\prod_{i=1}^{n} p_i^{2m_i} \pm \prod_{i=1}^{n} p_i^{e_i - m_i},$$

then

$$E_{tors}(\mathbb{Q}) = \left\{O, \left(\mp\prod_{i=1}^{n} p_i^{m_i}, 0\right)\right\} = \mathbb{Z}/2\mathbb{Z},$$

where $e_{i'}$ *is odd or* $e_{i'} \neq 3m_{i'}$ *for some* i' *if*

$$A = -\prod_{i=1}^{n} p_i^{2m_i} - \prod_{i=1}^{n} p_i^{e_i - m_i}.$$

(3) *For* $A \equiv 1 \pmod 3$, *if*

$$A \neq -\prod_{i=1}^{n} p_i^{2m_i} \pm \prod_{i=1}^{n} p_i^{e_i - m_i},$$

then

$$E_{tors}(\mathbb{Q}) = \{O\}.$$

Proof. Let $E : y^2 = x^3 + Ax + \prod_{i=1}^{n} p_i^{e_i}$ be the elliptic curve with $A \in \mathbb{Z}$, where p_i's are all primes such that $p_i \equiv 3 \pmod 8$ and $p_i \neq 3$.

Then, by Theorem 2.6(a) (Lutz-Nagell theorem), for $P(x,\ y) \in E_{tors}(\mathbb{Q})$,

$$x(P),\ y(P) \in \mathbb{Z}.$$

Thus, if there exists a point $P \neq O$ such that $2P = O$, then $x(P) \mid \prod_{i=1}^{n} p_i^{e_i}$, i.e.,

$$x(P) = \mp \prod_{i=1}^{n} p_i^{m_i}$$

for $0 \leq m_i \leq e_i$. Then $x(P)$ satisfies the equation

$$\{x(P)\}^3 + A\{x(P)\} + \prod_{i=1}^{n} p_i^{e_i} = 0$$

and so we are also able to express A as

$$A = -\prod_{i=1}^{n} p_i^{2m_i} \pm \prod_{i=1}^{n} p_i^{e_i - m_i}.$$

Hence, if $A = -\prod_{i=1}^{n} p_i^{2m_i} \pm \prod_{i=1}^{n} p_i^{e_i - m_i}$, then we have

$$y^2 = x^3 + Ax + \prod_{i=1}^{n} p_i^{e_i} = \left(x \pm \prod_{i=1}^{n} p_i^{m_i}\right)\left(x^2 \mp \prod_{i=1}^{n} p_i^{m_i} x \pm \prod_{i=1}^{n} p_i^{e_i - m_i}\right).$$

But

$$x^2 \mp \prod_{i=1}^{n} p_i^{m_i} x \pm \prod_{i=1}^{n} p_i^{e_i - m_i} = 0$$

do not have an integer solution. The discriminant of the equation is equal to

$$\prod_{i=1}^{n} p_i^{2m_i} \mp 4 \prod_{i=1}^{n} p_i^{e_i - m_i} \equiv 5 \pmod{8}$$

and so the discriminant is not a square. Hence the point of order 2 in $E_{tors}(\mathbb{Q})$ is only $P\left(\mp\prod_{i=1}^{n} p_i^{m_i}, 0\right)$. Therefore, there is no $l \in \mathbb{N}$ such that

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} < E_{tors}(\mathbb{Q}).$$

Next, we will consider whether $E_{tors}(\mathbb{Q})$ has a subgroup $\mathbb{Z}/2l\mathbb{Z}$ for some $l > 1$. If $E_{tors}(\mathbb{Q})$ has a subgroup $\mathbb{Z}/2l\mathbb{Z}$ for some $l > 1$, then there exists a point $Q(x, y) \in E_{tors}(\mathbb{Q})$ such that

$$2Q = P.$$

Then, by (4.1), we have

$$x(2Q) = \frac{x^4 - 2Ax^2 - 8\prod_{i=1}^{n} p_i^{e_i} x + A^2}{4y^2} = x(P). \tag{5.1}$$

Thus, replacing A by $-\prod_{i=1}^{n} p_i^{2m_i} \pm \prod_{i=1}^{n} p_i^{e_i - m_i}$ in (5.1) gives an equation of the form

$$x^4 \pm 4\prod_{i=1}^{n} p_i^{m_i} x^3 - 2\left(-\prod_{i=1}^{n} p_i^{2m_i} \pm \prod_{i=1}^{n} p_i^{e_i - m_i}\right)x^2$$

$$+\left(\mp 4\prod_{i=1}^{n} p_i^{3m_i} - 4\prod_{i=1}^{n} p_i^{e_i}\right)x + \left(\prod_{i=1}^{n} p_i^{2m_i} \pm \prod_{i=1}^{n} p_i^{e_i - m_i}\right)^2 = 0$$

or

$$\left(x^2 \pm 2\prod_{i=1}^{n} p_i^{m_i} x - \prod_{i=1}^{n} p_i^{2m_i} \mp \prod_{i=1}^{n} p_i^{e_i - m_i}\right)^2 = 0. \tag{5.2}$$

Now, we check the following two cases:

Case I. $A = -\prod_{i=1}^{n} p_i^{2m_i} + \prod_{i=1}^{n} p_i^{e_i - m_i}$.

In equation (5.2), the discriminant of the equation

$$x^2 + 2\prod_{i=1}^{n} p_i^{m_i} x - \prod_{i=1}^{n} p_i^{2m_i} - \prod_{i=1}^{n} p_i^{e_i - m_i} = 0 \tag{5.3}$$

is

$$2\prod_{i=1}^{n} p_i^{2m_i} x + \prod_{i=1}^{n} p_i^{e_i - m_i} \equiv 3 \text{ or } 5 \pmod 8$$

and so it is not a square. Thus equation (5.3) does not have an integer solution.

Case II. $A = -\prod_{i=1}^{n} p_i^{2m_i} - \prod_{i=1}^{n} p_i^{e_i - m_i}$.

In equation (5.2), the discriminant of the equation

$$x^2 - 2\prod_{i=1}^{n} p_i^{m_i} x - \prod_{i=1}^{n} p_i^{2m_i} + \prod_{i=1}^{n} p_i^{e_i - m_i} = 0 \tag{5.4}$$

is

$$2\prod_{i=1}^{n} p_i^{2m_i} - \prod_{i=1}^{n} p_i^{e_i - m_i},$$

say *D*. Then we will investigate the discriminant *D* of (5.4) for the following four cases:

(i) If $e_{i'} - m_{i'}$ is odd and $2m_{i'} > e_{i'} - m_{i'}$ for some i', then we have

$$D = p_{i'}^{e_{i'} - m_{i'}} \left(2 p_{i'}^{3m_{i'} - e_{i'}} \prod_{\substack{i=1 \\ i \neq i'}}^{n} p_i^{2m_i} - \prod_{\substack{i=1 \\ i \neq i'}}^{n} p_i^{e_i - m_i} \right).$$

Since the integer D needs to be a square,

$$p_{i'} \left| \left(2p_{i'}^{3m_{i'}-e_{i'}} \prod_{\substack{i=1\\ i\neq i'}}^{n} p_i^{2m_i} - \prod_{\substack{i=1\\ i\neq i'}}^{n} p_i^{e_i-m_i} \right) \right. .$$

But this is a contradiction.

(ii) If $e_i - m_i$'s are even for all i and $2m_{i'} > e_{i'} - m_{i'}$ for some i', then

$$D = p_{i'}^{e_{i'}-m_{i'}} \left(2p_{i'}^{3m_{i'}-e_{i'}} \prod_{\substack{i=1\\ i\neq i'}}^{n} p_i^{2m_i} - \prod_{\substack{i=1\\ i\neq i'}}^{n} p_i^{e_i-m_i} \right).$$

Since D has to be a square,

$$2p_{i'}^{3m_{i'}-e_{i'}} \prod_{\substack{i=1\\ i\neq i'}}^{n} p_i^{2m_i} - \prod_{\substack{i=1\\ i\neq i'}}^{n} p_i^{e_i-m_i} \tag{5.5}$$

must be a square. But the integer (5.5) is not a square because

$$\left(\frac{D/p_{i'}^{e_{i'}-m_{i'}}}{p_{i'}} \right) = \left(\frac{-1}{p_{i'}} \right) = (-1)^{\frac{p_{i'}-1}{2}} = -1. \tag{5.6}$$

(iii) If $2m_{i'} < e_{i'} - m_{i'}$ for some i', then

$$D = p_{i'}^{2m_{i'}} \left(2\prod_{\substack{i=1\\ i\neq i'}}^{n} p_i^{2m_i} - p_{i'}^{e_{i'}-3m_{i'}} \prod_{\substack{i=1\\ i\neq i'}}^{n} p_i^{e_i-m_i} \right).$$

But

$$\frac{D}{p_{i'}^{2m_{i'}}} = \left(2\prod_{\substack{i=1\\ i\neq i'}}^{n} p_i^{2m_i} - p_{i'}^{e_{i'}-3m_{i'}} \prod_{\substack{i=1\\ i\neq i'}}^{n} p_i^{e_i-m_i} \right)$$

is not a square because

$$\left(\frac{D/p_{i'}^{2m_{i'}}}{p_{i'}}\right) = \left(\frac{2}{p_{i'}}\right) = (-1)^{\frac{p_{i'}^2-1}{8}} = -1. \tag{5.7}$$

(iv) If $2m_i = e_i - m_i$ for all i, then $D = \prod_{i=1}^{n} p_i^{2m_i}$ is a square and so

$$x = 2\prod_{i=1}^{n} p_i^{m_i} \quad \text{and} \quad 0$$

are integer solutions of equation (5.4).

Next, we will consider whether the two integer solutions of (5.4) satisfy the elliptic curve E. If $x = 2\prod_{i=1}^{n} p_i^{m_i}$, then

$$\begin{aligned} y^2 &= x^3 + Ax + \prod_{i=1}^{n} p_i^{e_i} \\ &= x^3 - 2\prod_{i=1}^{n} p_i^{2m_i} x + \prod_{i=1}^{n} p_i^{e_i} \\ &\equiv 5 \text{ or } 7 \pmod 8, \end{aligned}$$

a contradiction. However, if $x = 0$, then $y^2 = x^3 + Ax + \prod_{i=1}^{n} p_i^{e_i} = \prod_{i=1}^{n} p_i^{e_i}$ and so if e_i is even, then

$$Q\left(0, \pm\prod_{i=1}^{n} p_i^{e_i/2}\right)$$

are points of $E_{tors}(\mathbb{Q})$ and satisfy $2Q = P$.

From these results and Lemma 5.1, the theorem is proved. $\square$

Example. (1) Let $E/\mathbb{Q}$ be the elliptic curve

$$\begin{aligned} E : y^2 &= x^3 - 3816059522x + 83344647990241 \\ &= x^3 - 2 \cdot 11^4 \cdot 19^4 x + 11^6 19^6. \end{aligned}$$

Then in Theorem 5.2(1), since $m_1 = 2 = m_2$ and $e_1 = 6 = 3m_1 = 3m_2 = e_2$, the torsion subgroup $E_{tors}(\mathbb{Q})$ of E is

$$E_{tors}(\mathbb{Q}) = \{O, (11^2 19^2, 0), (0, \pm 11^3 19^3)\} = \mathbb{Z}/4\mathbb{Z}.$$

(2) Let $E/\mathbb{Q}$ be the elliptic curve

$$\begin{aligned} E : y^2 &= x^3 + 299564298x + 62618067611 \\ &= x^3 + (-11^2 19^2 + 11^2 19^5) x + 11^3 19^6. \end{aligned}$$

In Theorem 5.2(2), since $e_1 = 3$, $e_2 = 6$ and $m_1 = m_2 = 1$, the torsion subgroup $E_{tors}(\mathbb{Q})$ of E is

$$E_{tors}(\mathbb{Q}) = \{O, (-11 \cdot 19, 0)\} = \mathbb{Z}/2\mathbb{Z}.$$

In the next results, we show that the structures of torsion groups of an elliptic curve $E : y^2 = x^3 + Ax + \prod_{i=1}^n p_i^{e_i}$, where p_i's are all primes such that $p_i \equiv 1 \pmod 8$ ($p_i \equiv 5 \pmod 8$, $p_i \equiv 7 \pmod 8$) in Theorem 5.3 (Theorem 5.4, Theorem 5.5), respectively.

Theorem 5.3. *Let* $E/\mathbb{Q} : y^2 = x^3 + Ax + \prod_{i=1}^n p_i^{e_i}$ *be an elliptic curve with* $A \in \mathbb{Z}$, *where* p_i*'s are all primes such that* $p_i \equiv 1 \pmod 8$. *Then the torsion groups* $E_{tors}(\mathbb{Q})$ *of the elliptic curve E are the following*:

(1) *If* $e_i = 3m_i$, m_i*'s are even for all i and*

$$A = -\prod_{i=1}^n p_i^{2m_i} - \prod_{i=1}^n p_i^{e_i - m_i} = -2\prod_{i=1}^n p_i^{m_i},$$

then the torsion group of elliptic curve E is

$$E_{tors}(\mathbb{Q}) = \left\{O, \left(\prod_{i=1}^{n} p_i^{m_i}, 0\right), \left(0, \pm \prod_{i=1}^{n} p_i^{e_i/2}\right)\right\} = \mathbb{Z}/4\mathbb{Z}.$$

(2) *For* $A \not\equiv 0 \pmod 3$, *if*

$$A = -\prod_{i=1}^{n} p_i^{2m_i} + \prod_{i=1}^{n} p_i^{e_i - m_i},$$

then the torsion group of the elliptic curve E is

$$E_{tors}(\mathbb{Q}) = \left\{O, \left(\mp \prod_{i=1}^{n} p_i^{m_i}, 0\right)\right\} = \mathbb{Z}/2\mathbb{Z}.$$

(3) *Let* A *be equal to* $-\prod_{i=1}^{n} p_i^{2m_i} - \prod_{i=1}^{n} p_i^{e_i - m_i}$ *such that* $A \not\equiv 0 \pmod 3$.

Then

$$\left\{O, \left(\mp \prod_{i=1}^{n} p_i^{m_i}, 0\right)\right\} = \mathbb{Z}/2\mathbb{Z}$$

is the torsion group $E_{tors}(\mathbb{Q})$ *of* $E(\mathbb{Q})$ *each in the following cases*:

(a) $e_i - m_i$ *is odd and* $2m_i > e_i - m_i$ *for some i*.

(b) e_i*'s are equal to* $3m_i$ *for all i and* $m_{i'}$ *is odd for some* i'.

(4) *For* $A \equiv 1 \pmod 3$, *if*

$$A \neq -\prod_{i=1}^{n} p_i^{2m_i} \pm \prod_{i=1}^{n} p_i^{e_i - m_i},$$

then the torsion group is

$$E_{tors}(\mathbb{Q}) = \{O\}.$$

Proof. In the same way as Theorem 5.2, we can know that there is no $l \in \mathbb{N}$ such that

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2l\mathbb{Z} < E_{tors}(\mathbb{Q}).$$

Next, we will consider whether $E_{tors}(\mathbb{Q})$ has a subgroup $\mathbb{Z}/2l\mathbb{Z}$ for some $l > 1$. Also, by using the content of the proof of Theorem 5.2, we can easily check the following results:

Case I. $A = -\prod_{i=1}^{n} p_i^{2m_i} + \prod_{i=1}^{n} p_i^{e_i - m_i}$.

In (5.1), since A is even, x is even and so y^2 is odd. Then $4 \nmid A$ because $x(P) = \mp\prod_{i=1}^{n} p_i^{m_i}$ is odd. But in this case, A satisfies $A \equiv 0 \pmod 8$ and so $4 \mid A$, a contradiction.

Case II. $A = -\prod_{i=1}^{n} p_i^{2m_i} - \prod_{i=1}^{n} p_i^{e_i - m_i}$.

Now we investigate the discriminant $D = 2\prod_{i=1}^{n} p_i^{2m_i} - \prod_{i=1}^{n} p_i^{e_i - m_i}$ of equation (5.4) for the following two cases:

(i) If $e_{i'} - m_{i'}$ is odd for some i' and $2m_{i'} > e_{i'} - m_{i'}$, then we can know that D is not a square in the same method as the proof of Theorem 5.2.

(ii) If $2m_i = e_i - m_i$ for all i, then D is equal to $\prod_{i=1}^{n} p_i^{2m_i}$ and it is a square and so $x = 2\prod_{i=1}^{n} p_i^{m_i}$ and 0 are integer solutions of (5.4). Then as the proof of Theorem 5.2, if $x = 2\prod_{i=1}^{n} p_i^{m_i}$, then it does not satisfy the given elliptic curve E and if x is equal to 0 and e_i is even, then E has torsion points $Q\left(0, \pm\prod_{i=1}^{n} p_i^{e_i/2}\right)$ satisfying $2Q = P$. Thus $E_{tors}(\mathbb{Q})$ has a subgroup $\mathbb{Z}/4\mathbb{Z}$. By using the above statements and Lemma 5.1, the theorem is proved. □

Theorem 5.4. *Let* $E/\mathbb{Q} : y^2 = x^3 + Ax + \prod_{i=1}^{n} p_i^{e_i}$ *be an elliptic curve with* $A \in \mathbb{Z}$, *where* p_i*'s are all primes such that* $p_i \equiv 5 \pmod 8$. *Then the torsion groups* $E_{tors}(\mathbb{Q})$ *of elliptic curve E are the following*:

(1) *If* $e_i = 3m_i$, m_i*'s are even for all i and*

$$A = -\prod_{i=1}^{n} p_i^{2m_i} - \prod_{i=1}^{n} p_i^{e_i - m_i} = -2\prod_{i=1}^{n} p_i^{m_i},$$

then the torsion group of E is

$$E_{tors}(\mathbb{Q}) = \left\{O, \left(\prod_{i=1}^{n} p_i^{m_i}, 0\right), \left(0, \pm\prod_{i=1}^{n} p_i^{e_i/2}\right)\right\} = \mathbb{Z}/4\mathbb{Z}.$$

(2) *For* $A \not\equiv 0 \pmod 3$, *if*

$$A = -\prod_{i=1}^{n} p_i^{2m_i} + \prod_{i=1}^{n} p_i^{e_i - m_i},$$

then the torsion group of E is

$$E_{tors}(\mathbb{Q}) = \left\{O, \left(\mp\prod_{i=1}^{n} p_i^{m_i}, 0\right)\right\} = \mathbb{Z}/2\mathbb{Z}.$$

(3) *Let A be equal to* $-\prod_{i=1}^{n} p_i^{2m_i} - \prod_{i=1}^{n} p_i^{e_i - m_i}$ *such that* $A \not\equiv 0 \pmod 3$. *Then*

$$\left\{O, \left(\mp\prod_{i=1}^{n} p_i^{m_i}, 0\right)\right\} = \mathbb{Z}/2\mathbb{Z}$$

is the torsion group $E_{tors}(\mathbb{Q})$ *of* $E(\mathbb{Q})$ *each in the following cases*:

(a) $e_i - m_i$ *is odd for some i and* $2m_i > e_i - m_i$.

(b) $2m_i < e_i - m_i$ *for some i*.

(c) *e_i's are equal to $3m_i$ for all i and $m_{i'}$ is odd for some i'.*

(4) *For $A \equiv 1 \pmod 3$, if*

$$A \neq -\prod_{i=1}^{n} p_i^{2m_i} \pm \prod_{i=1}^{n} p_i^{e_i - m_i},$$

then the torsion group is

$$E_{tors}(\mathbb{Q}) = \{O\}.$$

Proof. In the same discussion as Theorem 5.2, we can show that there is no $l \in \mathbb{N}$ such that

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2l\mathbb{Z} < E_{tors}(\mathbb{Q}).$$

Next, we will consider whether $E_{tors}(\mathbb{Q})$ has a subgroup $\mathbb{Z}/2l\mathbb{Z}$ for some $l > 1.$ Also, if we use the content in the proof of Theorem 5.2, then we can just see the following results:

Case I. $A = -\prod_{i=1}^{n} p_i^{2m_i} + \prod_{i=1}^{n} p_i^{e_i - m_i}.$

This case A satisfies $A \equiv 0$ or $4 \pmod 8$ and so $4 \mid A,$ a contradiction.

Case II. $A = -\prod_{i=1}^{n} p_i^{2m_i} - \prod_{i=1}^{n} p_i^{e_i - m_i}.$

Now we check the discriminant D of equation (5.4) for the following three cases:

(i) If $e_i - m_i$ is odd for some i and $2m_i > e_i - m_i,$ then we can know that D is not a square in the same method as the proof of Theorem 5.2.

(ii) If $2m_i < e_i - m_i$ for some i, then by using (5.7), we can easily know that D is not a square.

(iii) If $2m_i = e_i - m_i$ for all i, then D is equal to $\prod_{i=1}^{n} p_i^{2m_i}$ and it is a square and so $x = 2\prod_{i=1}^{n} p_i^{2m_i}$ and 0 are integer solutions of (5.4). Then as the proof of Theorem 5.2, if $x = 2\prod_{i=1}^{n} p_i^{m_i}$, then it does not satisfy the given elliptic curve E and if x is equal to 0 and e_i is even, then E has torsion points $Q\left(0, \pm \prod_{i=1}^{n} p_i^{e_i/2}\right)$ satisfying $2Q = P$. Thus $E_{tors}(\mathbb{Q})$ has a subgroup $\mathbb{Z}/4\mathbb{Z}$. The theorem is proved by the above statement and Lemma 5.1. □

Theorem 5.5. *Let* $E/\mathbb{Q} : y^2 = x^3 + Ax + \prod_{i=1}^{n} p_i^{e_i}$ *be an elliptic curve with* $A \in \mathbb{Z}$, *where* p_i*'s are all primes such that* $p_i \equiv 7 \pmod 8$. *Then the torsion groups* $E_{tors}(\mathbb{Q})$ *of elliptic curve E are the following*:

(1) *If* $e_i = 3m_i$, m_i*'s are even for all i and*

$$A = -\prod_{i=1}^{n} p_i^{2m_i} - \prod_{i=1}^{n} p_i^{e_i - m_i} = -2\prod_{i=1}^{n} p_i^{m_i},$$

then

$$E_{tors}(\mathbb{Q}) = \left\{O, \left(\prod_{i=1}^{n} p_i^{m_i}, 0\right), \left(0, \pm \prod_{i=1}^{n} p_i^{e_i/2}\right)\right\} = \mathbb{Z}/4\mathbb{Z}.$$

(2) *Let A be equal to* $A = -\prod_{i=1}^{n} p_i^{2m_i} + \prod_{i=1}^{n} p_i^{e_i - m_i}$ *such that* $A \not\equiv 0 \pmod 3$. *Then*

$$\left\{O, \left(\mp \prod_{i=1}^{n} p_i^{m_i}, 0\right)\right\} = \mathbb{Z}/2\mathbb{Z}$$

is the torsion group $E_{tors}(\mathbb{Q})$ *of* $E(\mathbb{Q})$ *each in the following cases*:

(a) *The number of elements of* $\{i \mid e_i - m_i \text{ is odd}\}$ *is even*.

(b) *The number of elements of* $\{i \mid e_i - m_i \text{ is odd}\}$ *is odd and* $e_i - m_i$ *is odd and* $2m_i > e_i - m_i$ *for some i*.

(3) *Let A be equal to* $-\prod_{i=1}^{n} p_i^{2m_i} - \prod_{i=1}^{n} p_i^{e_i - m_i}$ *with* $A \not\equiv 0 \pmod 3$.

Then

$$\left\{O, \left(\mp \prod_{i=1}^{n} p_i^{m_i}, 0\right)\right\} = \mathbb{Z}/2\mathbb{Z}$$

is the torsion group $E_{tors}(\mathbb{Q})$ *of* $E(\mathbb{Q})$ *each in the following cases*:

(a) $e_i - m_i$ *is odd and* $2m_i > e_i - m_i$ *for some i.*

(b) $e_i - m_i$ *'s are even for all i and* $2m_{i'} > e_{i'} - m_{i'}$ *for some* i'.

(c) e_i *'s are equal to* $3m_i$ *for all i and* $m_{i'}$ *is odd for some* i'.

(4) *For* $A \equiv 1 \pmod 3$, *if*

$$A \neq -\prod_{i=1}^{n} p_i^{2m_i} \pm \prod_{i=1}^{n} p_i^{e_i - m_i},$$

then

$$E_{tors}(\mathbb{Q}) = \{O\}.$$

Proof. Using the same method as Theorem 5.2, we can obtain that there is no $l \in \mathbb{N}$ such that

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2l\mathbb{Z} < E_{tors}(\mathbb{Q}).$$

Next, we will consider whether $E_{tors}(\mathbb{Q})$ has a subgroup $\mathbb{Z}/2l\mathbb{Z}$ for some $l > 1$. Let N be the number of elements of $\{i \mid e_i - m_i \text{ is odd}\}$. Since $4 \nmid A$, if N is odd, then $A = -\prod_{i=1}^{n} p_i^{2m_i} + \prod_{i=1}^{n} p_i^{e_i - m_i}$ and $x(Q)$ need to satisfy (5.3) and if N is even, then $A = -\prod_{i=1}^{n} p_i^{2m_i} - \prod_{i=1}^{n} p_i^{e_i - m_i}$ and $x(Q)$ have to satisfy (5.4).

Case I. N is odd and $A = -\prod_{i=1}^{n} p_i^{2m_i} + \prod_{i=1}^{n} p_i^{e_i - m_i}.$

The discriminant D of (5.3) satisfies $D \equiv 3$ or $5 \pmod 8$ and it is not a square. Thus the equation does not have an integer solution.

Case II. N is even and $A = -\prod_{i=1}^{n} p_i^{2m_i} - \prod_{i=1}^{n} p_i^{e_i - m_i}.$

We check the discriminant D of equation (5.4) for the following three cases:

(i) If $e_{i'} - m_{i'}$ is odd and $2m_{i'} > e_{i'} - m_{i'}$ for some i', then we can know that D is not a square by the same method as the proof of Theorem 5.2.

(ii) If $e_i - m_i$ is even for all i and $2m_{i'} > e_{i'} - m_{i'}$ for some i', then by using (5.6), we can easily know that D is not a square.

(iii) If $2m_i = e_i - m_i$ for all i, then D is equal to $\prod_{i=1}^{n} p_i^{2m_i}$ and it is a square and so $x = 2\prod_{i=1}^{n} p_i^{m_i}$ and 0 are integer solutions of (5.4). Then in the same way as Theorem 5.2, if $x = 2\prod_{i=1}^{n} p_i^{m_i}$, then it does not satisfy the given elliptic curve E and if x is equal to 0 and e_i is even, then E has torsion points $Q\left(0, \pm \prod_{i=1}^{n} p_i^{e_i/2}\right)$ satisfying $2Q = P$. Thus $E_{tors}(\mathbb{Q})$ has a subgroup $\mathbb{Z}/4\mathbb{Z}$. By using the above statements and Lemma 5.1, the theorem is proved. □

References

[1] I. F. Blake, G. Seroussi and N. P. Smart, Elliptic Curves in Cryptography, Cambridge University Press, 1999.

[2] W. Fulton, Algebraic Curves, Benjamin-Cummings Publishing Company, 1969.

[3] G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, Clarendon Press, Oxford, 1979.

[4] Dale Husemöller, Elliptic Curves, Springer-Verlag, 1987.

[5] K. Ireland and M. Rosen, A Classical Introduction to Modern Number Theory, Springer-Verlag, New York, 1990.

[6] S. Lang, Algebraic Number Theory, Springer-Verlag, New York, 1970.

[7] H. McKean and V. Moll, Elliptic Curves, Cambridge University Press, 1997.

[8] Alfred J. Menezes, Elliptic Curve Public Key Cryptosystems, Kluwer Academic Publishers, 1993.

[9] J. S. Milne, Elliptic Curves, 1996 (preprint).

[10] Hans H. Müller, Harald Strocher and Horst G. Zimmer, Torsion groups of elliptic curves with integral j-invariant over quadratic fields, J. Reine Angew. Math. 397 (1989), 100-161.

[11] Anthony W. Knapp, Elliptic Curves, Princeton University Press, 1992.

[12] P. Ribenboim, Algebraic Numbers, Wiley-Interscience, New York, 1972.

[13] Joseph H. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, New York, 1992.

[14] Joseph H. Silverman and J. Tate, Rational Points on Elliptic Curves, Springer-Verlag, New York, 1994.

[15] J. Tate, Arithmetic of elliptic curves, Invent. Math. 23 (1974), 171-206.