TORSION ON CERTAIN ELLIPTIC CURVES OVER $\mathbb{Q}(\sqrt{d})$

Jonathan Hanke

1. Introduction

In this paper, we set out to generalize theorems that classify the $\mathbb{Q}$ rational torsion points on two special families of elliptic curves with complex multiplication. We shall generalize the theorems to a classification of the torsion points on these kinds of curves over an arbitrary quadratic number field. We denote the quadratic number field by $k = \mathbb{Q}(\sqrt{d})$ and its ring of integers by O_k. To achieve this goal, our strategy will be to consider these elliptic curves over the finite fields $O_k/\mathfrak{p}$, where $\mathfrak{p}$ is some prime ideal in O_k, and determine the number of points there. For most prime ideals $\mathfrak{p}$ we can define a homomorphism $r_\mathfrak{p} : E(k) \to E_\mathfrak{p}(O_k/\mathfrak{p})$, which is one-to-one when restricted to the torsion subgroup $E(k)_{\text{Tors}}$. This will be useful because it relates $E(k)_{\text{Tors}}$ to these smaller groups, which we will be able to understand fairly well. From this relationship we can obtain a strong divisibility condition, and thus a bound, on the size of $E(k)_{\text{Tors}}$.

We then change our strategy slightly and try to construct all possible torsion group structures within the previous bound. This gives us a classification of all possible torsion groups. Then we look at some examples and use this classification to calculate the torsion for some elliptic curves.

2. Background

Here we outline some of the basic definitions and ideas necessary for our discussion. For a more in depth discussion, see [Kn].

First, we define an **elliptic curve over a field** K to be any nonsingular projective cubic curve E with coefficients in K which has at least one K rational point. It turns out that any elliptic curve can be put into the following form by an appropriate change of variables:

$$E : y^2w + a_1xyw + a_3yw^2 = x^3 + a_2x^2w + a_4xw^2 + a_6w^3 \qquad \text{where } a_i \in K,$$

the K rational point mapping to the K rational point O on E at infinity (i.e. $w = 0$). We say that a cubic of this form is in **Weierstrass form**.

The point O on a cubic in Weierstrass form is also special in that it is a **flex** for this cubic. This will become important later when we consider the group law on E. Since we will be dealing only with elliptic curves in Weierstrass form, it is convenient for us to take this as our definition of an elliptic curve from now on.

I would like to thank Prof. Anthony Knapp for his valuable support and advice without which this thesis would not have been a reality. .

It is also natural to examine changes of variables which send Weierstrass curves into other Weierstrass curves. We call such a change of variables an **admissible change of variables**, and is given by

$$x = u^2x' + r$$
$$y = u^3y' + su^2x' + t$$

for some $u, r, s, t \in K$. If two curves are related by an admissible change of variables, we say that the two curves are **isomorphic**.

In the special case where $r = s = t = 0$, our change of variables reduces to

$$x = u^2x'$$
$$y = u^3y'.$$

After changing variables and normalizing the x^3 and yw^2 coefficients to 1, we see that the a_i coefficients are each multiplied by a factor of u^{-i}. To describe this transformation property, we say that a_i has **weight** i.

These transformations are useful for us in two ways. First, if we are given as elliptic curve with coefficients in K, we can clear the denominators of all the coefficients by setting $u =$ product of all denominators of a_i. In this way, we obtain an isomorphic elliptic curve with coefficients in O_K. Unless otherwise stated, we will only consider curves with K integral coefficients. Also, the two families of elliptic curves we are considering,

$$E^1 : y^2 = x^3 + Ax$$
$$E^2 : y^2 = x^3 + B,$$

the coefficients A and B have weight 4 and 6 respectively. So by choosing an appropriate value for u, we can transform our ellpitic curve into an isomorphic elliptic curve where A is 4^{th} power free and B is 6^{th} power free. We will make use of this fact when we classify the torsion. Our classification will be up to isomorphism, so we will assume that the coefficients A and B have this form.

The condition that E be **nonsingular** means that the tangent line to E is nonzero at every point of E. To determine easily whether an algebraic curve is nonsingular, we associate to each curve a number Δ_E in K called the **discriminant of** E. The discriminant of E has the property that $\Delta_E = 0$ if and only if E is singular. We will always use Δ_E to test the singularity of E.

Now on this elliptic curve we can define a group law given by a K rational map in such a way that O is the group identity. Thus, with this addition defined, the K rational points $E(K)$ on E form a group. The addition law may be defined by the following geometrical construction. Let P and Q be two points in the set $E(K)$. We define $P + Q$ by connecting P and Q by a line, then connecting the third intersection point of the line through P and Q (with E) to O by a second line. We then define $P + Q$ as the third intersection point of the second line with E. Since the point O is an inflection point of E (i.e., its intersection multiplicity is

3) and its tangent line is the line at infinity, we see by this construction that O is the identity element for our group operation.

Suppose we are given an elliptic curve E over number field k and we wish to consider this curve over the finite field $O_k/\mathfrak{p}$ where $\mathfrak{p}$ is some prime ideal in O_k. Since the reduction map $k \to O_k/\mathfrak{p}$ is only defined on the $\mathfrak{p}$-integral elements of k, we wish to define a **reduced elliptic curve** $E_\mathfrak{p}$ for a given prime ideal $\mathfrak{p}$ in O_k such that $ord_\mathfrak{p} a_i \geq 0$ for all i, and $ord_\mathfrak{p} a_i = 0$ for at least one i. To do this consistently, we consider the following construction due to Silverman. Consider E over the $\mathfrak{p}$-adic integers $R_\mathfrak{p}$ of k. In $R_\mathfrak{p}$, the prime ideal $\mathfrak{p}$ embeds into the unique maximal ideal of $R_\mathfrak{p}$. It turns out that this maximal ideal is principal, generated by some $\pi \in R_\mathfrak{p}$. We then use an admissible change of variables in $R_\mathfrak{p}$ to transform E into a $\mathfrak{p}$-reduced curve $E_\mathfrak{p}$ with coefficients in $R_\mathfrak{p}$. Since

$$R_\mathfrak{p}/(\pi) \cong O_k/\mathfrak{p},$$

we can consider the $\mathfrak{p}$-reduced curve $E_\mathfrak{p}$ over $O_k/\mathfrak{p}$. (For more details about this reduction, see [Sil 1].) Then we see that $E_\mathfrak{p}(O_k/\mathfrak{p})$ is nonsingular if and only if $\mathfrak{p} \nmid \Delta_E$.

With this, we can define a natural group homomorphism $r_\mathfrak{p} : E(k) \to E_\mathfrak{p}(O_k/\mathfrak{p})$. This turns out to be an injective map when restricted to the torsion subgroup $E(k)_{\text{Tors}}$ for most prime ideals $\mathfrak{p}$ when $\mathfrak{p} \nmid \Delta_E$. We state the actual results in Theorems 3.7 and 3.8 in the next section.

If $K = k = \mathbb{Q}(\sqrt{d})$, by clearing denominators, we can arrange that the coefficients a_i are numbers in O_k. When we are working with an elliptic curve over k in Weierstrass form, we will always assume that the a_i's are elements of O_k.

3. Useful Results

Now we shall take a moment to discuss some useful results that form the foundation for much of our work.

Theorem 3.1. *Let k be a number field and let $E : y^2 = \alpha x^3$ be the singular elliptic curve with singular point $R = (0, 0)$ and $\alpha \in k$. Then there is a one-to-one correspondence between the k-rational points $P \neq R$ in $E(k)$ and the points in k, given by*

$$P = (x, y) = \left(\frac{m^2}{\alpha}, \frac{m^3}{\alpha}\right)$$

where $m \in k$.

Proof. Consider the line $L : y = mx$ with slope m through the singular point R. If $m \in k$, the line L will intersect E at exactly two distinct points, R and at some other point P. To find P, substitute L into the equation for E. This gives

$$\alpha x^2 - m^2 x^2 = \alpha x^2 \left(x - \frac{m^2}{\alpha}\right) = 0.$$

Since we are interested in the point $P \neq R$, we have

$$P = (x, y) = \left(\frac{m^2}{\alpha}, \frac{m^3}{\alpha}\right),$$

which, since $\alpha \in k$, is clearly a k rational point on E. Conversely, if $P \neq R$ is a rational point on E, then the line $L : y = mx$ through P and R has slope

$$m = \left(\frac{p_2 - r_2}{p_1 - r_1}\right) = \frac{p_2}{p_1} \in K. \quad \square$$

Remark. *For more details about the chord-secant method see [Sil-Ta].*

Theorem 3.2. *(Mordell-Weil) The group $E(k)$ is finitely generated.*

Proof. See [Sil 1], p189.

Remark. *This allows us to write $E(k)$ in the form*

$$E(k) \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_n^{\alpha_n}} \times \mathbb{Z}^r$$

where r is called the **rank** *of $E(k)$.*

Theorem 3.3. *(Quadratic Reciprocity) If $p, q > 0$ are odd primes, then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Proof. See [H-W].

Theorem 3.4. *(Dirichlet's Theorem) If m and b are relatively prime integers with $m > 0$, then there exist infinitely many primes of the form $kn + b$ with k a positive integer.*

Proof. See [Kn].

Theorem 3.5. *(Chinese Remainder Theorem) Suppose that $m = m_1 m_2 \cdots m_n$ and that $gcd(m_i, m_j) = 1$ for $i \neq j$. Let $b_1, b_2, \cdots, b_t$ be integers and consider the system of congruences:*

$$x \equiv b_1 \bmod m_1, x \equiv b_2 \bmod m_2, \cdots, x \equiv b_t \bmod m_t.$$

This system always has solutions and any two solutions differ by a multiple of m.

Proof. See [I-R], pp34-6.

Theorem 3.6. *Let E be an elliptic curve over k and let m be an integer relatively prime to $\mathrm{char}(O_k/\mathfrak{p}) = p$. Then there is a well defined reduction homomorphism*

$$r_{\mathfrak{p}} : E(k)[m] \hookrightarrow E_{\mathfrak{p}}(O_k/\mathfrak{p})$$

which is one-to-one when $\mathfrak{p} \nmid \Delta_E$. Here $E(k)[m]$ denotes the group of points with order m in $E(k)$.

Proof. See [Sil 1], pp173-6.

Theorem 3.7. *(Cassels) Let k be a number field, $\mathfrak{p}$ be a prime ideal in O_k, K be the $\mathfrak{p}$-adic completion of k. Suppose* char(K)=0 *and* char$(O_k/\mathfrak{p}) = p$ *where p is prime . Let E be a Weierstrass curve with a_i in the integers R_K of K and let $P = (x, y) \in E(k)_{\text{Tors}}$ be a point with exact order $m \geq 2$.*
(a) If m is not a power of p, then $x(P)$ and $y(P) \in R_K$.
(b) If $m = p^n$, then

$$\pi^{2r}x(P), \pi^{2r}y(P) \in R_K \text{ with } r = \left[\frac{v(p)}{p^n - p^{n-1}}\right].$$

where $v(p)$ is the $\mathfrak{p}$-adic valuation on K.

Proof. See [Sil 1], pp177-8.

Theorem 3.8. *Let E be a Weierstrass curve over a number field k with $a_i \in O_k$ and let $P = (x, y) \in E(k)_{\text{Tors}}$ be a point with exact order $m \geq 2$.*
(a) If m is not a power of p, then $x, y \in O_k$.
(b) If $m = p^n$, then for each non-archimedian absolute value v on k, let

$$r = \left[\frac{ord_v(p)}{p^n - p^{n-1}}\right].$$

Then

$$ord_v(x) \geq -2r_v \text{ and } ord_v(y) \geq -3r_v.$$

Proof. See [Sil 1], pp220-1.

Corollary 3.9. *Let k is a quadratic number field and let $E : y^2 = x^3 + Ax + B$ be elliptic curve with $A, B \in k$. If $P = (x, y) \in E(k)_{\text{Tors}}$ is a point with exact order $m \geq 2$, then $x, y \in O_k$ unless $m = 3$ and 3 ramifies or $m = 4$ and 2 ramifies. In these cases, we have*

$$\left.\begin{array}{c} m = 3 \text{ and } (3) = \mathfrak{p}^2 \\ \text{or} \\ m = 4 \text{ and } (2) = \mathfrak{p}^2 \end{array}\right\} \Longrightarrow \left\{\begin{array}{l} ord_{\mathfrak{p}}x \geq -2 \\ ord_{\mathfrak{p}}y \geq -3 \end{array}\right.$$

Proof. To know how big these denominators can be, we use Theorem 3.8 and look for those values of p and n for which $r_{\mathfrak{p}} > 0$. Since k is a quadratic number field, $\text{ord}_{\mathfrak{p}}p = 1$ or 2. For all primes $p > 5$, $p^n - p^{n-1} > 2$ when $n > 0$. So for these, $r_{\mathfrak{p}} = 0$ and x and y are in O_k. For the primes 2 and 3, we summarize our results in the following table:

p	n	splits or ramifies	r_v	$m = p^n =$ order of P
2	1	splits	1	2
2	1	ramifies	2	2
3	1	ramifies	1	3
2	2	ramifies	1	4

If P were a point of order 2 ($m = 2$), then we know that $x \in O_k$. We know this because P is an order 2 point, the group law implies $y = 0$. Therefore x is the root of a monic polynomial, and is in O_k. Thus only points of orders 3 and 4 may have denominators > 1. From Theorem 3.8 we know $\text{ord}_{\mathfrak{p}} x, \text{ord}_{\mathfrak{p}} y \geq 0$ unless $\mathfrak{p} \mid 2$ or $\mathfrak{p} \mid 3$, depending on m. If this happens, Theorem 3.8 gives the desired lower bound for $\text{ord}_{\mathfrak{p}} x, \text{ord}_{\mathfrak{p}} y$. $\square$

4. Theorems over $\mathbb{Q}$

Theorems over $\mathbb{Q}$. *If $E^1 : y^2 = x^3 + Ax$ and $E^2 : y^2 = x^3 + B$ are elliptic curves with $A, B \in \mathbb{Z}$ such that A is 4^{th} power free and B is 6^{th} power free, then*

$$E^1(\mathbb{Q})_{\text{Tors}} \cong \begin{cases} \mathbb{Z}_4 & \text{if } A = 4 \\ \mathbb{Z}_2 \times \mathbb{Z}_2 & \text{if } A = -\square \\ \mathbb{Z}_2 & \text{otherwise} \end{cases} \tag{1}$$

$$E^2(\mathbb{Q})_{\text{Tors}} \cong \begin{cases} \mathbb{Z}_6 & \text{if } B = 1 \\ \mathbb{Z}_3 & \text{if } B = -432, \text{ or if } B = \square \text{ and } B \neq 1 \\ \mathbb{Z}_2 & \text{if } B = \text{a cube and } B \neq 1 \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

5. Complex Mutiplication

Given an elliptic curve over any number field, we can look at the ring of endomorphisms of E, denoted by $End\ E$. For most curves, the members of this ring consist only of the multiplication-by-n endomorphisms sending a point P to nP for all $n \in \mathbb{Z}$. In such a case $End\ E \cong \mathbb{Z}$. However, some elliptic curves have a bigger endomorphism ring. It can be shown that these other endomorphism rings are always isomorphic to the ring of integers of some imaginary quadratic number field. Curves with this larger endomorphism ring are said to have **complex multiplication**. The curves E^1 and E^2 considered here both have complex multiplication.

$E^1 : y^2 = x^3 + Ax$ has complex multiplication by $i = \sqrt{-1}$. The multiplication-by-i endomorphism looks like

$$i : (x, y) \longrightarrow (-x, iy)$$

$E^2 : y^2 = x^3 + B$ has complex multiplication by $\omega = \frac{1+\sqrt{-3}}{2}$. Again we have a representation for the multiplication-by-ω endomorphism as

$$\omega : (x, y) \longrightarrow (\omega x, y)$$

6. Establishing a Bound for $E(k)_{\text{Tors}}$

Let us now specialize to study the elliptic curves over $k = \mathbb{Q}(\sqrt{d})$ given by

$$E^1 : y^2 = x^3 + Ax$$
$$E^2 : y^2 = x^3 + B,$$

where A and B are nonzero members of O_k. We use the complex multiplication symmetries of these curves to determine exactly the size of $E_{\mathfrak{p}}(O_k/\mathfrak{p})$ for some class of prime ideals $\mathfrak{p} \in O_k$.

Theorem 6.1. *If $\mathfrak{p}$ is a prime ideal in O_k such that $\mathfrak{p} \nmid \Delta_{E^1}$ and if $N(\mathfrak{p}) = p$ for some rational prime $p \equiv 3$ mod 4, then $|E_1^{\mathfrak{p}}(O_k/\mathfrak{p})| = p + 1$.*

Proof. The relation $N(\mathfrak{p}) = p$ means that $O_k/\mathfrak{p}$ is a field of order p. Hence the multiplicative group $(O_k/\mathfrak{p})^\times$ has order $p - 1$. Since $p \equiv 3 \bmod 4$, -1 is not a square in $O_k/\mathfrak{p}$.

Now consider pairs $\{x, -x\}$ for $x \in (O_k/\mathfrak{p})^\times$. Suppose x gives a solution (x, y) to $E_{\mathfrak{p}}$ with $y \not\equiv 0 \bmod p$ (i.e. $x^3 + Ax \equiv \square \bmod \mathfrak{p}$). Then $-x$ does not give a solution to $E_{\mathfrak{p}}$ since $x^3 + Ax \equiv (-1)\square \bmod \mathfrak{p}$ and -1 is not a square in $O_k/\mathfrak{p}$. Similarly if x does not generate a solution to E, then $x^3 + Ax \not\equiv \square \bmod \mathfrak{p}$. But then $-x$ generates a solution to $E_{\mathfrak{p}}$ since $(-x)^3 + A(-x) = -1(x^3 + Ax) \equiv \square$. We know this is congruent to a square because the product of any two non-squares is again a square and as before, $-1 \not\equiv \square \bmod \mathfrak{p}$. Therefore, every pair $\{x, -x\}$ with $x \in (O_k/\mathfrak{p})^\times$ generates exactly two solutions when the corresponding y is $\not\equiv 0 \bmod \mathfrak{p}$. When the corresponding y is $\equiv 0$, the pair $\{x, -x\}$ still generates exactly two solutions, namely $(x, 0)$ and $(-x, 0)$. So from all $x \in (O_k/\mathfrak{p})^\times$ we have $p - 1$ solutions. Then we have the two additional solutions $(0, 0)$ and ∞, which gives us a total of $p + 1$ solutions. $\square$

Theorem 6.2. *If $\mathfrak{p}$ is a prime ideal in O_k such that $\mathfrak{p} \nmid \Delta_{E^2}$ and if $N(\mathfrak{p}) = p$ for some rational prime $p \equiv 2$ mod 3, then $|E_2^{\mathfrak{p}}(O_k/\mathfrak{p})| = p + 1$.*

Proof. The relation $N(\mathfrak{p}) = p$ means that $O_k/\mathfrak{p}$ is a field of order p. Hence the multiplicative group $(O_k/\mathfrak{p})^\times$ has order $p-1$. Since $3 \nmid p-1$, there are no elements of order 3. This means that the kernel of the map $x \to x^3$ is $\{1\}$. Therefore the map $x \to x^3$ is one-to-one and also onto.

Now consider the expression $y^2 - B$. For each choice of $y \in O_k/\mathfrak{p}$ there is a unique $x \in O_k/\mathfrak{p}$ such that $y^2 - B = x^3$. These solutions (x, y) together with the solution at ∞ give us $p + 1$ solutions. $\square$

The above theorems give us the size of $E_{\mathfrak{p}}(O_k/\mathfrak{p})$ whenever $N(\mathfrak{p})$ equals a rational prime p and p satisfies some additional congruence condition. So now it is natural to ask: How much does this tell us and how often does this happen? For our purposes, we are most concerned with finding those rational primes p for which there is some $E_{\mathfrak{p}}(O_k/\mathfrak{p})$ with $p + 1$ elements.

From algebraic number theory, we know that the principal ideal (p) generated by a rational prime p can factor in three ways over O_k when $k = \mathbb{Q}(\sqrt{d})$; we say that (p) can **ramify**, **split**, or remain **inert**. If there is a prime ideal $\mathfrak{p}$ in O_k such that the ideal (p) generated by p can be written as $(p) = \mathfrak{p}^2$, then we say that p ramifies in O_k. If p is such that the ideal (p) can be written as $(p) = \mathfrak{p}\bar{\mathfrak{p}}$, we say that p splits in O_k. The third possibility is that the ideal (p) has no nontrivial factorization, in which case we say that p is inert. Quadratic residues give an easy way to determine whether a rational prime p ramifies, splits, or remains inert in O_k, as follows.

Theorem 6.3. *Let p be an odd rational prime and O_k be the ring of integers of a quadratic number field with discriminant Δ. Then the factorization of the ideal*

(p) generated by p is given in terms of Legendre symbols by

$$\left(\frac{\Delta}{p}\right) = 0 \Longleftrightarrow p \text{ ramifies in } O_k$$
$$\left(\frac{\Delta}{p}\right) = 1 \Longleftrightarrow p \text{ splits in } O_k$$
$$\left(\frac{\Delta}{p}\right) = -1 \Longleftrightarrow p \text{ remains inert in } O_k$$

Proof. See [He], p97.

For our purposes we will be interested only in those primes p that split in O_k, since there are only a finite number of primes that ramify, namely those rational primes dividing Δ. The following two theorems will tell us which primes we can use with Theorems 6.1 and 6.2.

Theorem 6.4. *For all values of d except $d = -1$, the rational primes $p \equiv 3 \bmod 4$ that split in O_k are given by a nonempty union of congruence conditions $p \equiv a_i \bmod 4d$, $1 \leq i \leq r$. When $d = -1$, there are no rational primes $p \equiv 3 \bmod 4$ that split in O_k.*

Proof. From Theorem 6.3, we know that

$$p \text{ splits in } O_k \Longleftrightarrow \left(\frac{\Delta}{p}\right) = 1, \tag{3}$$

where Δ is the discriminant of O_k. Since $\mathbb{Q}(\sqrt{d})$ is a quadratic number field, we can calculate its discriminant as

$$\Delta = \begin{cases} d & \text{if } d \equiv 1 \bmod 4 \\ 4d & \text{if } d \equiv 2 \text{ or } 3 \bmod 4. \end{cases} \tag{4}$$

To solve the equation on the right side of (3), we write the prime factorization of d as

$$d = (-1)^{\varepsilon} 2^{\varepsilon'} p_1 \cdots p_n q_1 \cdots q_m, \tag{5}$$

where $p_i \equiv 1 \bmod 4$, $q_j \equiv 3 \bmod 4$, and d is assumed to be square-free. We can then factor the Legendre symbol $(\frac{\Delta}{p})$ as

$$\left(\frac{\Delta}{p}\right) = \left(\frac{d}{p}\right) = \left(\frac{-1}{p}\right)^{\varepsilon} \left(\frac{2}{p}\right)^{\varepsilon'} \left(\frac{p_1}{p}\right) \cdots \left(\frac{p_n}{p}\right) \left(\frac{q_1}{p}\right) \cdots \left(\frac{q_m}{p}\right) = 1. \tag{6}$$

Since we are considering only primes $p \equiv 3 \bmod 4$, we know $(\frac{-1}{p}) = -1$. Thus our equation becomes

$$(-1)^{\varepsilon} \left(\frac{2}{p}\right)^{\varepsilon'} \left(\frac{p_1}{p}\right) \cdots \left(\frac{p_n}{p}\right) \left(\frac{q_1}{p}\right) \cdots \left(\frac{q_m}{p}\right) = 1 \tag{7}$$

Now we use Quadratic Reciprocity to simplify (7) further. From this formula, for each factor we have one of the following:

$$\left(\frac{p_i}{p}\right) = \left(\frac{p}{p_i}\right) \quad \text{since} \quad p_i \equiv 1 \bmod 4 \tag{8}$$

$$\left(\frac{q_j}{p}\right) = -\left(\frac{p}{q_j}\right) \quad \text{since} \quad q_j \equiv 3 \bmod 4. \tag{9}$$

Putting these into (7), we get

$$\left(\frac{2}{p}\right)^{\varepsilon'} \left(\frac{p}{p_1}\right) \cdots \left(\frac{p}{p_n}\right) \left(\frac{p}{q_1}\right) \cdots \left(\frac{p}{q_m}\right) = (-1)^{\varepsilon+m}. \tag{10}$$

We also know that for the prime 2, we have

$$\left(\frac{2}{p}\right) = \begin{cases} +1 & p \equiv \pm 1 \bmod 8 \\ -1 & p \equiv \pm 3 \bmod 8, \end{cases} \tag{11}$$

and the constraint $p \equiv 3 \bmod 4$ gives

$$\left(\frac{2}{p}\right) = \begin{cases} +1 & p \equiv 7 \bmod 8 \\ -1 & p \equiv 3 \bmod 8. \end{cases} \tag{12}$$

Thus the value of $(\frac{2}{p})$ is not determined by the condition $p \equiv 3 \bmod 4$ and may be either ± 1 depending on the residue of p mod 8.

To solve (10), we need to consider all possible products (of ± 1's) on the left side of (10) that multiply to $(-1)^{\varepsilon+m}$. We represent each possible product by an $(\varepsilon'+n+m)$-tuple t of $+1$'s and -1's such that the k^{th} entry t_k represents the value of the k^{th} Legendre symbol L_k and

$$\prod_{k=1}^{\varepsilon'+n+m} t_k = (-1)^{\varepsilon+m}. \tag{13}$$

Let T denote the set of all such $(\varepsilon' + n + m)$-tuples t. Under this association, it is more convenient to write (10) as

$$\prod_{k=1}^{\varepsilon'+n+m} L_k(p) = (-1)^{\varepsilon+m}.$$

where $L_k(p)$ represents the value of the k^{th} Legendre symbol evaluated at p and an empty product is taken to be 1. Thus the complete solution set S to (10) of primes $p \equiv 3 \bmod 4$ that split in O_k is given by

$$S = \left\{ \text{primes } p \equiv 3 \bmod 4 \;\middle|\; p \in \bigcup_{t \in T} \left(\bigcap_{k=1}^{\varepsilon'+n+m} \{p \mid L_k(p) = t_k\} \right) \right\}. \tag{14}$$

For each $t \in T$, we solve the equation

$$L_k(p) = t_k \tag{15}$$

for all odd primes p. The solutions to (15) can be written as a set of congruence conditions mod 8, p_i, or q_j depending on the choice of k. By applying the Chinese Remainder Theorem, we can combine the congruence conditions in (14) and write

$$\begin{aligned} S &= \left\{ \text{primes } p \;\middle|\; p \equiv a_1, \cdots, a_r \bmod 2^{\varepsilon'+2} p_1 \dots p_n q_1 \dots q_m \right\} \\ &= \left\{ \text{primes } p \;\middle|\; p \equiv a_1, \cdots, a_r \bmod 4d \right\} \end{aligned}$$

for some a_i, $1 \le i \le r$.

Now let us see for which d we have $S = \emptyset$. Clearly if $\varepsilon' + n + m > 0$, then $S \neq \emptyset$. Looking back at (10) and letting $\varepsilon' = n = m = 0$, we obtain $(-1)^{\varepsilon} = 1$. This is true for every p unless $\varepsilon = 1$. Thus $S = \emptyset$ only when $d = -1$. $\square$

Theorem 6.5. *When $d \neq -3$, the rational primes $p \equiv 2 \bmod 3$ that split in O_k are given by a nonempty union of congruence conditions $p \equiv a_i \bmod \kappa d$, $1 \le i \le r$. Here κd is defined as*

$$\kappa d = 2^{\alpha} 3 \prod_{p \le 5} p^{\operatorname{ord}_p d} \tag{16}$$

where

$$\alpha = \begin{cases} 1 & \text{if } 2 \nmid d \text{ and } \varepsilon'' \equiv \varepsilon + m \bmod 2 \\ 2 & \text{if } 2 \nmid d \text{ and } \varepsilon'' \not\equiv \varepsilon + m \bmod 2 \\ 3 & \text{if } 2 \mid d. \end{cases}$$

and when the prime factorization of d is written as

$$d = (-1)^{\varepsilon} 2^{\varepsilon'} 3^{\varepsilon''} p_1 \cdots p_n q_1 \cdots q_m, \tag{17}$$

where $p_i \equiv 1 \bmod 4$, $q_j \equiv 3 \bmod 4$, $q_j \neq 3$, and d is assumed to be square-free. When $d = -3$, there are no rational primes $p \equiv 2 \bmod 3$ that split in O_k.

Proof. Let p be an odd prime. From Theorem 6.3, we know that

$$p \text{ splits in } O_k \iff \left(\frac{\Delta}{p}\right) = 1 \tag{18}$$

where Δ is the discriminant of O_k. Since $\mathbb{Q}(\sqrt{d})$ is a quadratic number field, we can calculate its discriminant Δ as

$$\Delta = \begin{cases} d & \text{if } d \equiv 1 \bmod 4 \\ 4d & \text{if } d \equiv 2 \text{ or } 3 \bmod 4 \end{cases} \tag{19}$$

To solve the equation on the right side of (18), we use (17) to factor the Legendre symbol $(\frac{\Delta}{p})$ as

$$\left(\frac{\Delta}{p}\right) = \left(\frac{d}{p}\right) = \left(\frac{-1}{p}\right)^{\varepsilon} \left(\frac{2}{p}\right)^{\varepsilon'} \left(\frac{3}{p}\right)^{\varepsilon''} \left(\frac{p_1}{p}\right) \cdots \left(\frac{p_n}{p}\right) \left(\frac{q_1}{p}\right) \cdots \left(\frac{q_m}{p}\right) = 1. \tag{20}$$

Since we are considering only primes $p \equiv 2 \bmod 3$, we know $(\frac{p}{3}) = -1$. For convenience, we shall consider the primes $p \equiv 1 \bmod 4$ and $p \equiv 3 \bmod 4$ separately. If $p \equiv 1 \bmod 4$, we have $(\frac{-1}{p}) = 1$ and for the other terms

$$\left(\frac{p_i}{p}\right) = \left(\frac{p}{p_i}\right) \quad \text{since} \quad p_i \equiv 1 \bmod 4 \tag{21}$$

$$\left(\frac{q_j}{p}\right) = \left(\frac{p}{q_j}\right) \quad \text{since} \quad q_j \equiv 3 \bmod 4. \tag{22}$$

Putting these into (20), we get

$$\left(\frac{2}{p}\right)^{\varepsilon'} \left(\frac{p}{p_1}\right) \cdots \left(\frac{p}{p_n}\right) \left(\frac{p}{q_1}\right) \cdots \left(\frac{p}{q_m}\right) = \left(\frac{p}{3}\right)^{\varepsilon''} = (-1)^{\varepsilon''}. \tag{23}$$

If $p \equiv 3 \bmod 4$, we have $(\frac{-1}{p}) = -1$ and for the other terms

$$\left(\frac{p_i}{p}\right) = \left(\frac{p}{p_i}\right) \quad \text{since} \quad p_i \equiv 1 \bmod 4 \tag{24}$$

$$\left(\frac{q_j}{p}\right) = -\left(\frac{p}{q_j}\right) \quad \text{since} \quad q_j \equiv 3 \bmod 4. \tag{25}$$

Putting these into (20), we get

$$\left(\frac{2}{p}\right)^{\varepsilon'} \left(\frac{p}{p_1}\right) \cdots \left(\frac{p}{p_n}\right) \left(\frac{p}{q_1}\right) \cdots \left(\frac{p}{q_m}\right) = (-1)^{\varepsilon+\varepsilon''+m+\varepsilon''} = (-1)^{\varepsilon+m}. \tag{26}$$

For simplicity, we will rewrite (23) and (26) together as

$$\left(\frac{2}{p}\right)^{\varepsilon'} \left(\frac{p}{p_1}\right) \cdots \left(\frac{p}{p_n}\right) \left(\frac{p}{q_1}\right) \cdots \left(\frac{p}{q_m}\right) = \begin{cases} (-1)^{\varepsilon''} & \text{if } p \equiv 1 \bmod 4 \\ (-1)^{\varepsilon+m} & \text{if } p \equiv 3 \bmod 4. \end{cases} \tag{27}$$

From (12) in the previous proof, we know that the value of $(\frac{2}{p})$ is not determined by the condition $p \equiv 1$ or $3 \bmod 4$, and may be either ± 1 depending on the residue of $p \bmod 8$.

To solve (27), we need to consider all possible products (of ± 1's) on the left side of (10) that multiply to either $(-1)^{\varepsilon''}$ if $p \equiv 1 \bmod 4$ or $(-1)^{\varepsilon+m}$ if $p \equiv 3 \bmod 4$. We represent each possible product by an $(\varepsilon' + n + m)$-tuple t of $+1$'s and -1's such that the k^{th} entry t_k represents the value of the k^{th} Legendre symbol L_k and

$$\prod_{k=1}^{\varepsilon'+n+m} t_k = \begin{cases} (-1)^{\varepsilon''} & \text{if } p \equiv 1 \bmod 4 \\ (-1)^{\varepsilon+m} & \text{if } p \equiv 3 \bmod 4. \end{cases} \tag{28}$$

Let T_1 denote the set of all such $(\varepsilon' + n + m)$-tuples t when $p \equiv 1 \bmod 4$ and let T_2 denote the set of all such $(\varepsilon' + n + m)$-tuples t when $p \equiv 3 \bmod 4$. Under this association, it is more convenient to write (27) as

$$\prod_{k=1}^{\varepsilon'+n+m} L_k(p) = \begin{cases} (-1)^{\varepsilon''} & \text{if } p \equiv 1 \bmod 4 \\ (-1)^{\varepsilon+m} & \text{if } p \equiv 3 \bmod 4. \end{cases}.$$

where $L_k(p)$ represents the value of the k^{th} Legendre symbol evaluated at p and an empty product is taken to be 1. Thus the complete solution set S to (27) of odd primes $p \equiv 2 \bmod 3$ that split in O_k is given by

$$S = \left\{ \text{odd primes } p \equiv 2 \bmod 3 \;\middle|\; p \in \bigcup_{l'=1}^{2} \bigcup_{t \in T_{l'}} \left(\bigcap_{k=0}^{\varepsilon'+n+m} \{p \mid L_k(p) = t_k\} \right) \right\} \tag{29}$$

where $L_0 = (\frac{-1}{p})$ and $t_0 = (-1)^{l'-1}$ to reflect the congruence $p \equiv 1$ or $3 \bmod 4$.

For each $t \in T_{l'}$, we solve the equation

$$L_k(p) = t_k \tag{30}$$

for all odd primes p. The solutions to (30) can be written as a set of congruence conditions mod 4, 8, p_i, or q_j depending on the choice of k. By applying the Chinese Remainder Theorem, we can combine the congruence conditions in (29) and write S as

$$S = \left\{ \text{primes } p \;\middle|\; p \equiv a_1, \cdots, a_r \bmod 2^\alpha \; 3 \prod_{p \le 5} p^{\operatorname{ord}_p d} \right\}$$

where

$$\alpha = \begin{cases} 1 & \text{if } 2 \nmid d \text{ and } \varepsilon'' \equiv \varepsilon + m \bmod 2 \\ 2 & \text{if } 2 \nmid d \text{ and } \varepsilon'' \not\equiv \varepsilon + m \bmod 2 \\ 3 & \text{if } 2 \mid d. \end{cases}$$

Thus by defining κ as in the statement of the theorem, we can write S more compactly as

$$S = \{\text{primes } p \mid p \equiv a_1, \cdots, a_r \bmod \kappa d\}$$

for some a_i, $1 \le i \le r$.

Now let us see for which d we have $S = \emptyset$. Clearly if $\varepsilon' + n + m > 0$, then $S \neq \emptyset$. Now consider when $\varepsilon' = n = m = 0$. In this case

$$d = (-1)^{\varepsilon} 3^{\varepsilon''}.$$

Looking back at (27) when $\varepsilon' = n = m = 0$, we obtain

$$1 = \begin{cases} (-1)^{\varepsilon''} & \text{if } p \equiv 1 \bmod 4 \\ (-1)^{\varepsilon} & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

If $p \equiv 1 \bmod 4$, then (27) admits no solutions if and only if $d = \pm 3$. If $p \equiv 3 \bmod 4$, then (27) admits no solutions if and only if $d = -1$ or -3. Combining these two cases, we see that the only value of d that gives no solutions to (27) for any odd prime p is $d = -3$. $\square$

Now that we have a union of congruence classes (mod $4d$ or κd) of rational primes p for which we know $|E_{\mathfrak{p}}(O_k/\mathfrak{p})| = p + 1$, we can use the one-to-one group homomorphism

$$E(k)_{\text{Tors}} \hookrightarrow E_{\mathfrak{p}}(O_k/\mathfrak{p}) \quad \text{when} \quad \mathfrak{p} \nmid \Delta_E \tag{31}$$

to obtain a bound for $|E(k)_{\text{Tors}}|$.

Theorem 6.6. *When $d \neq -1$, $|E^1(k)_{\text{Tors}}|$ divides $4d$.*

Proof. Let $q = |E^1(k)_{\text{Tors}}|$ and let q' be some odd prime divisor of $|E^1(k)_{\text{Tors}}|$. Suppose that $q' \nmid 4d$. Then, using the Chinese Remainder Theorem and Dirichlet's Theorem, we can choose a prime $p > \Delta_{E^1}, q$ such that

$$p \equiv 1 \bmod q'$$
$$p \equiv a_i \bmod 4d,$$

for some a_i as in Theorem 6.4. Since $\gcd(|E^1(k)_{\text{Tors}}|,p)=1$ and $\mathfrak{p} \nmid \Delta_E$, by Theorem 3.6, the group homomorphism

$$r_p : E^1(k)_{\text{Tors}} \hookrightarrow E^1_{\mathfrak{p}}(O_k/\mathfrak{p})$$

is one-to-one. Hence the image of $E^1(k)_{\text{Tors}}$ is a subgroup of both $E^1_{\mathfrak{p}}(O_k/\mathfrak{p})$ whose order is known from Theorem 6.1 as $p+1$. Since the order of a subgroup divides the order of the group, we have

$$q' \mid (p+1).$$

But we know the congruence class of $p \bmod q'$; so this reduces to

$$q' \mid 2$$

which is nonsense since q' was assumes to be odd. Therefore $q' \mid 4d$. Because this is true for every odd prime divisor q' of $|E^1(k)_{\text{Tors}}|$ and 2 divides $4d$, we know that $\gcd(a_i, 4dq')=\gcd(a_i, 4d) = 1$.

Since $\gcd(a_i, 4dq')=1$ for each odd prime divisor of q, we know that $\gcd(a_i, 4dq)=1$. Therefore we can use Dirichlet's Theorem to choose two primes $p_1, p_2 > \Delta_{E^1}, q$ such that

$$p_1 \equiv a_i \bmod 4dq$$
$$p_2 \equiv a_i + 4d \bmod 4dq.$$

for some a_i as in Theorem 6.4, $1 \leq i \leq r$. Since p_1 and p_2 are both $> \Delta_{E^1}, q$, the group homomorphisms

$$r_{p_1} : E^1(k)_{\text{Tors}} \hookrightarrow E^1_{\mathfrak{p}_1}(O_k/\mathfrak{p}_1)$$
$$r_{p_2} : E^1(k)_{\text{Tors}} \hookrightarrow E^1_{\mathfrak{p}_2}(O_k/\mathfrak{p}_2),$$

are one-to-one. Hence the image of $E^1(k)_{\text{Tors}}$ is a subgroup of both $E^1_{\mathfrak{p}_1}(O_k/\mathfrak{p}_1)$ and $E^1_{\mathfrak{p}_2}(O_k/\mathfrak{p}_2)$ whose orders are p_1+1 and p_2+1 respectively (from Theorem 6.1). Since they are subgroups and since the order of a subgroup divides the order of the group, we have

$$q \mid (p_1+1)$$
$$q \mid (p_2+1).$$

But we know the congruence classes of p_1 and $p_2 \bmod q$; so these reduce to

$$q \mid (a_i+1)$$
$$q \mid (a_i+4d+1).$$

Therefore, $q \mid 4d$. $\square$

Theorem 6.7. *When $d \neq -3$, $|E^2(k)_{\mathrm{Tors}}|$ divides κd, where κ is as in Theorem 6.5.*

Proof. The proof is exactly as for Theorem 6.6 if we replace E^1 with E^2 and $4d$ with κd. □

Theorem 6.8. *When $d \neq -1$,*

$$|E^1(k)_{\mathrm{Tors}}| \text{ divides } \begin{cases} 12 & \text{if } d = 3 \\ 8 & \text{if } d = 2 \\ 4 & \text{otherwise.} \end{cases} \tag{32}$$

Proof. Let $q = |E^1(k)_{\mathrm{Tors}}|$. From Theorem 6.6, we know $q \mid 4d$. By Dirichlet's Theorem choose a set of primes $p_i > q, \Delta_{E^1}$ such that $p_i \equiv a_i \bmod 4d$ for each $1 \leq i \leq r$. Since $\gcd(p_i, q)=1$, we use our one-to-one group homomorphism from Theorem 0.5 to see that $q \mid (p_i + 1)$. Hence $q \mid (a_i + 1)$ since $q \mid 4d$. Therefore,

$$a_i \equiv -1 \bmod q, \tag{33}$$

for all $1 \leq i \leq r$. Certainly $4 \mid q$ since our primes p_i are chosen a priori $\equiv 3 \bmod 4$.

Suppose $q > 4$. Then either $8 \mid q$ or $p' \mid q$ where p' is some odd prime dividing $4d$. Thus either $a_i \equiv -1 \bmod 8$ or $a_i \equiv -1 \bmod p'$. In either case, we obtain a single congruence condition that all odd primes $p \equiv 3 \bmod 4$ which split in O_k must satisfy. Therefore, in (10), the corresponding Legendre symbol ($(\frac{2}{p})$ or $(\frac{p}{p'})$ respectively) must assume only one value for all such primes p. This occurs only when there is exactly one Legendre symbol on the left side of (10). Moreover, since (33) is a single congruence, there must be exactly one residue (or non-residue) that corresponds to each value of the Legendre symbol.

If $8 \mid q$, then 2 must be the only prime dividing $4d$. Therefore $\varepsilon' = 1, m = 0$, and (10) reduces to

$$\left(\frac{2}{p}\right) = (-1)^{\varepsilon+m} = (-1)^{\varepsilon}.$$

From (12), $p \equiv -1$ implies that $(\frac{2}{p}) = 1$. Thus $\varepsilon = 0$ and, using (5), we see $d = 2$.

If $p' \mid q$, then p' must be the only prime dividing d. Therefore $\varepsilon' = 0$ and (10) reduces to

$$\left(\frac{p}{p'}\right) = (-1)^{\varepsilon+m} \tag{34}$$

Since (33) requires that the solution to (34) is a single congruence condition mod p', there must be exactly one residue (and one non-residue) mod p'. The number of residues mod $p' = \frac{p'-1}{2} = 1$, so $p' = 3$. With this, (34) becomes

$$\left(\frac{p}{3}\right) = (-1)^{\varepsilon+1} = -1$$

which implies $\varepsilon = 0$. Thus from (5), we see $d = 3$. □

Theorem 6.9. *When $d \neq -3$,*

$$|E^2(k)_{\text{Tors}}| \text{ divides } \begin{cases} 12 & \text{if } d = 3 \\ 6 & \text{otherwise.} \end{cases} \tag{35}$$

Proof. Let $q = |E^2(k)_{\text{Tors}}|$. From Theorem 6.7, we know $q \mid \kappa d$. By Dirichlet's Theorem choose a set of primes $p_i > q, \Delta_{E^2}$ such that $p_i \equiv a_i \bmod 4d$ for each $1 \leq i \leq r$. Using our one-to-one group homomorphism as in the last proof, we see that $q \mid (p_i + 1)$ and so $q \mid (a_i + 1)$ since $q \mid \kappa d$. Therefore,

$$a_i \equiv -1 \bmod q, \tag{36}$$

for all $1 \leq i \leq r$. Certainly $6 \mid q$ since our primes p_i are chosen a priori $\equiv 5 \bmod 6$.

Suppose $q > 6$. Then either $8 \mid q$ or $p' \mid q$ where p' is some odd prime dividing $4d$. Thus either $a_i \equiv -1 \bmod 8$ or $a_i \equiv -1 \bmod p'$. In either case, (36) requires that all odd primes $p \equiv 2 \bmod 3$ which split in O_k must satisfy a single congruence condition. Therefore, in (27), the corresponding Legendre symbol ($(\frac{2}{p})$ or $(\frac{p}{p'})$ respectively) must assume only one value for all such primes p. This occurs only when there is exactly one Legendre symbol on the left side of (27). Moreover, since (36) is a single congruence, there must be exactly one residue (or non-residue) that corresponds to each value of the Legendre symbol.

If $8 \mid q$, then 2 must be the only prime dividing κd. Therefore $\varepsilon' = 1, \varepsilon = m = 0$, and (27) reduces to

$$\left(\frac{2}{p}\right) = (-1)^{\varepsilon + m} = \begin{cases} (-1)^{\varepsilon''} = 1 & \text{if } p \equiv 1 \bmod 4 \\ (-1)^{\varepsilon + m} = (-1)^{\varepsilon} & \text{if } p \equiv 3 \bmod 4. \end{cases}$$

However, from (11), the $p \equiv 3 \bmod 4$ condition above will always have a solution, giving either $p \equiv 1$ or $5 \bmod 8$. Since this contradicts (36), we know $8 \nmid q$.

If $p' \mid q$, then p' must be the only prime dividing κd. Therefore $\varepsilon' = 0$ and (27) reduces to

$$\left(\frac{p}{p'}\right) = \begin{cases} (-1)^{\varepsilon''} & \text{if } p \equiv 1 \bmod 4 \\ (-1)^{\varepsilon + m} & \text{if } p \equiv 3 \bmod 4. \end{cases} \tag{37}$$

Since (36) requires that the solution to (37) is a single congruence condition mod p', there must be exactly one residue (and one non-residue) mod p'. The number of residues mod$p' = \frac{p'-1}{2} = 1$, so $p' = 3$. With this, we know that $\varepsilon''1, m = 0$, and (36) requires $p \equiv -1 \bmod 3$. Therefore (37) becomes

$$\left(\frac{p}{3}\right) = \left\{ \begin{matrix} (-1)^{\varepsilon''} = 1 & \text{if } p \equiv 1 \bmod 4 \\ (-1)^{\varepsilon + m} = (-1)^{\varepsilon} & \text{if } p \equiv 3 \bmod 4 \end{matrix} \right\} = -1.$$

which admits a solution only when $p \equiv 3 \bmod 4$ and $\varepsilon = 0$. Thus, from (17), we see that $d = 3$ and from above we see that $p \equiv -1 \bmod 12$. So when $d = 3$, we have $q = 12$. $\square$

7. The Group Structure of $E^1(k)_{\text{Tors}}$

Now that we have a reasonable bound for the size of the torsion subgroup, we will examine the conditions for points of certain orders to exist. By combining these conditions, we determine the group structure of the torsion subgroup.

Lemma 7.1. *(Doubling Formula) Suppose $P = (x, y)$ is a point in $E^1(k)$, then the x coordinate of $2P$ is given by*

$$x(2P) = \frac{(x^2 - A)^2}{4(x^3 + Ax)}.$$

Proof. See [Kn], p76.

Theorem 7.2.

(1) $\mathbb{Z}_2 \subseteq E^1(k)$
(2) $\mathbb{Z}_2 \times \mathbb{Z}_2 \subseteq E^1(k) \iff A = -\square$
(3) $\mathbb{Z}_3 \subseteq E^1(k) \iff A = \left(3 \pm 2\sqrt{3}\right) l^4$ *for some* $l \in O_k$.

Proof. (1). We have

$$\begin{aligned} P \text{ is a point of order } 2 &\iff P = -P, P \neq \infty \\ &\iff (x, y) = (x, -y) \\ &\iff y = 0. \end{aligned}$$

Therefore $(0, 0)$ is a point on $y^2 = x^3 + Ax$ of order 2. So $\mathbb{Z}_2 \subseteq E^1(k)$.

(2). We have

$$\begin{aligned} \mathbb{Z}_2 \times \mathbb{Z}_2 \subseteq E^1(k) &\iff \text{There are 4 points of order 2} \\ &\iff x^3 + Ax \text{ has 3 roots in } O_k. \end{aligned}$$

By the factorization

$$x^3 + Ax = x\left(x - \sqrt{-A}\right)\left(x + \sqrt{-A}\right) = 0$$

we see that these 3 roots are in O_k if and only if $A = -\square$ in O_k.

(3). Suppose there is a point P of order 3. Then $3P = 0$ or alternatively $2P = -P$. From this we can again use the doubling formula to obtain the relation

$$x(2P) = \frac{(x^2 - A)^2}{4(x^3 + Ax)} = x.$$

After some algebra, we have

$$-A^2 + 6Ax^2 + 3x^4 = 0.$$

Since this is a homogeneous polynomial in A and x^2, it is convenient to rewrite this as

$$-\left(\frac{A}{x^2}\right)^2 + 6\left(\frac{A}{x^2}\right) + 3 = 0.$$

Using the quadratic formula, we obtain

$$\frac{A}{x^2} = \left(3 \pm 2\sqrt{3}\right)$$

and thus

$$A = \left(3 \pm 2\sqrt{3}\right) x^2. \tag{38}$$

Putting this result back into the equation for the elliptic curve E^1, we get

$$y^2 = x^3 + Ax = x^3 + \left(3 \pm 2\sqrt{3}\right) x^3$$

and therefore

$$y^2 = 2\left(2 \pm \sqrt{3}\right) x^3. \tag{39}$$

What we have done is taken our point $P = (x, y)$ of order 3 on E^1 and shown that it must also be a (rational) point on the singular cubic curve $E : y^2 = 2(2 \pm \sqrt{3})x^3$. Theorem 3.1 gives us the general form of a rational point on E as

$$\begin{aligned}(x, y) &= \left(\frac{(2 \mp \sqrt{3})m^2}{\left(2 \mp \sqrt{3}\right)\left(1 \pm \sqrt{3}\right)^2}, \frac{(2 \mp \sqrt{3})m^3}{\left(2 \mp \sqrt{3}\right)\left(1 \pm \sqrt{3}\right)^2}\right) \\ &= \left(\frac{m^2}{(1 \pm \sqrt{3})^2}, \frac{m^3}{(1 \pm \sqrt{3})^2}\right)\end{aligned} \tag{40}$$

where we substituted the factorization $2 = \left(2 \mp \sqrt{3}\right)\left(1 \pm \sqrt{3}\right)^2$. Among these, we look for points whose (coordinate) denominators are consistent with the bounds given by Corollary 3.9. Since we are dealing with points of order 3 and $(3) = (\sqrt{3})^2 = \mathfrak{p}^2$ in $\mathbb{Z}[\sqrt{3}]$, Corollary 3.9 states that

$$\begin{aligned}\operatorname{ord}_{\sqrt{3}} x &\geq -2 \\ \operatorname{ord}_{\sqrt{3}} y &\geq -3.\end{aligned}$$

This allows only $\operatorname{ord}_{\sqrt{3}} m \geq -1$. Since $N(1 + \sqrt{3}) = -2$ and $N(2 - \sqrt{3}) = 1$, we can write m in the form $m = \frac{(1 \pm \sqrt{3})l}{\sqrt{3}}$ for some l in O_k. Putting this back into (40), we get

$$(x, y) = \left(\frac{l^2}{\left(\sqrt{3}\right)^2}, \frac{(1 \pm \sqrt{3})l^3}{\left(\sqrt{3}\right)^3}\right). \tag{41}$$

Using (38), we solve for A as

$$\begin{aligned}A &= (3 \pm 2\sqrt{3})x^2 \\ &= (3 \pm 2\sqrt{3})\left(\frac{l^2}{\left(\sqrt{3}\right)^2}\right)^2.\end{aligned} \tag{42}$$

But we also require that $A \in O_k$, so $l = \sqrt{3}l'$. Therefore

$$A = (3 \pm 2\sqrt{3}).$$

□

Theorem 7.3. *Suppose $E^1(k)$ contains a point Q of order 4, then Q must double to a point P of order 2. We classify the points of order 4 according to the order 2 points to which they double.*

(1) *$Q \in \mathbb{Z}_4 \subseteq E^1(k)$ is an order 4 point which doubles to $P = (0,0)$ iff*

$$A = \begin{cases} 4l^4 & \text{if 2 splits or is inert in } O_k \text{ for some } l \in O_k \\ \frac{l^4}{4} & \text{if } (2) = \mathfrak{p}^2 \text{ for some } l \in \mathfrak{p} \end{cases}$$

(2) *$Q \in \mathbb{Z}_4 \subseteq E^1(k)$ is an order 4 point which doubles to $P \neq (0,0)$ iff $k = \mathbb{Q}(\sqrt{2})$ and $A = -l^4$, for some $l \in O_k$.*

Proof. (1). Suppose there is a point Q of order 4 and only one point of order 2 (namely $P = (0,0)$). For $E^1(k)$ to contain a $\mathbb{Z}_4$ structure, Q must double to P. By the Doubling Formula, we have

$$x(2Q) = \frac{(x^2 - A)^2}{4(x^3 + Ax)} = 0.$$

Therefore,

$$A = x^2 \tag{43}$$

$$y^2 = x^3 + Ax = 2x^3. \tag{44}$$

What we have done is taken our point $Q = (x, y)$ of order 4 on E^1 and shown that it must also be a (rational) point on the singular cubic curve $E : y^2 = 2x^3$. Theorem 3.1 gives us the general form of a rational point on E as

$$(x, y) = \left(\frac{m^2}{2}, \frac{m^3}{2}\right) \tag{45}$$

Among these, we look for points whose (coordinate) denominators are consistent with the bounds given by Corollary 3.9. Since we are dealing with points of order 4 over an arbitrary quadratic number field k, there are two cases to consider depending on the factorization of 2 in O_k.

(1a) 2 does not ramify. Corollary 3.9 tells us that $x, y \in O_k$. Therefore $2 \mid m$ and so (45) can be written as

$$(x, y) = \left(2l^2, 4l^3\right) \tag{46}$$

where $m = 2l$, $l \in O_k$. Using (43) to calculate A, we get $A = x^2 = (2l^2)^2 = 4l^4$.

(1b) 2 ramifies. We write $(2) = \mathfrak{p}^2$. Corollary 3.9 tells us that $\mathrm{ord}_{\mathfrak{p}} x \geq -2$ and $\mathrm{ord}_{\mathfrak{p}} y \geq -3$. This allows only $\mathrm{ord}_{\mathfrak{p}} m \geq 0$, so $m \in O_k$. Using (43) to calculate A, we see that $A = \frac{m^4}{4}$. However this value of A is only in O_k if $m \in \mathfrak{p}$.

(2). Suppose Q doubles to a point $P = (x_1, y_1) \neq (0,0)$ of order 2. Then by the Doubling Formula, we have

$$x(2P) = \frac{(x^2 - A)^2}{4x^3 + 4Ax} = x_1. \tag{47}$$

Clearing denominators and collecting terms, we obtain

$$x^4 - 4x_1x^3 - 2Ax^2 - 4Ax_1x + A^2 = 0. \tag{48}$$

Since P is a point of order 2 different from $O = (0,0)$, we know from the proof of part 2 of Theorem 7.2 that $A = -x_1^2$. This allows us to simplify (48) into the homogeneous polynomial

$$x_1^4 + 4x_1^3x + 2x_1^2x^2 - 4x_1x^3 + x^4 = 0. \tag{49}$$

By changing variables, letting $x' = \frac{x_1}{x}$, we can write (49) as

$$x'^4 + 4x'^3 + 2x'^2 - 4x' + 1 = (x'^2 + 2x' - 1)^2 = 0 \tag{50}$$

with roots

$$x' = \frac{x_1}{x} = -1 \pm \sqrt{2}. \tag{51}$$

With this, we find A to be

$$A = -x_1^2 = (-3 \pm 2\sqrt{2})x^2. \tag{52}$$

Putting this value of A back into equation for E^1, we get

$$y^2 = 2(-1 \pm \sqrt{2})x^3. \tag{53}$$

What we have done is taken our point $P = (x, y)$ of order 4 on E^1 and shown that it must also be a (rational) point on the singular cubic curve $E : y^2 = 2(-1 \pm \sqrt{2})x^3$. Theorem 3.1 gives us the general form of a rational point on E as

$$(x, y) = \left(\frac{(1 \pm \sqrt{2})m^2}{\left(\sqrt{2}\right)^2}, \frac{(1 \pm \sqrt{2})m^3}{\left(\sqrt{2}\right)^2} \right) \tag{54}$$

where we substituted the factorization $2 = \left(\sqrt{2}\right)^2$ and $(1 \pm \sqrt{2}) = (-1 \pm \sqrt{2})^{-1}$. Among these, we look for points whose (coordinate) denominators are consistent with the bounds given by Corollary 3.9. Since we are dealing with points of order 4 and $(2) = (\sqrt{2})^2 = \mathfrak{p}^2$ in $O_k = \mathbb{Z}[\sqrt{2}]$, Corollary 3.9 states that

$$\begin{aligned} \operatorname{ord}_{\sqrt{2}} x &\geq -2 \\ \operatorname{ord}_{\sqrt{2}} y &\geq -3. \end{aligned}$$

This allows only m such that $\operatorname{ord}_{\sqrt{3}} m \geq 0$, thus $m \in O_k$. Using (52), we can solve for A as

$$\begin{aligned} A &= (-1)(-1 \pm 2\sqrt{2})^2 x^2 \\ &= (-1)(-1 \pm \sqrt{2})^2 \left(\frac{(1 \pm \sqrt{2})m^2}{\left(\sqrt{2}\right)^2} \right)^2 \\ &= \frac{-m^4}{\sqrt{2}^4}. \end{aligned} \tag{55}$$

If we then require that $A \in O_k$, then we have $A = -l^4$ for some $l \in O_k$. $\square$

Corollary 7.4. *Suppose that $k = \mathbb{Q}(\sqrt{d})$ is a UFD and that $E^1(k)$ contains a point Q of order 4 that doubles to $P = (0, 0)$. If $2 = \pi^2 u$ where π is a prime and u is a unit, then*

$$A = u^2 l^4$$

for some $l \in O_k$.

Proof. The factorization $2 = \pi^2 u$ tells us that 2 splits and that the prime ideal $\mathfrak{p}$ which divides 2 is just the principal ideal (π). From Theorem 7.3, we know $A = \frac{l^4}{4}$ for some $l \in \mathfrak{p}$. Thus we can write $l = \pi m$ for some $m \in O_k$. This gives us

$$A = \frac{\pi^4}{4} m^4 = \frac{\pi^4}{u^2 \pi^4} m^4 = \frac{m^4}{u^2}$$

Since u is a unit, we can make the change of variables $m' = um$. This gives

$$A = u^2 m'^4.$$

□

Theorem 7.5. *When $d \neq -1,\ 2,\ 3$, and A is 4^{th} power free, then*

$$E^1(k)_{\text{Tors}} \cong \begin{cases} \mathbb{Z}_4 & \text{when 2 either splits or is inert in } O_k \text{ and } A = 4 \\ \mathbb{Z}_4 & \text{when } (2) = \mathfrak{p}^2 \text{ and } A = \frac{l^4}{4} \text{ for some } l \in \mathfrak{p} \\ \mathbb{Z}_2 \times \mathbb{Z}_2 & \text{when } A = -\square \\ \mathbb{Z}_2 & \text{otherwise.} \end{cases}$$

Proof. From Theorem 6.8, we have a divisibility condition on the size of $E^1(k)_{\text{Tors}}$. So when $d \neq -1$, we have

$$|E^1(k)_{\text{Tors}}| \text{ divides } \begin{cases} 12 & \text{if } d = 3 \\ 8 & \text{if } d = 2 \\ 4 & \text{otherwise.} \end{cases}$$

So if $d \neq -1, 2$, or 3, we know that $|E^1(k)_{\text{Tors}}|$ divides 4. The result follows directly from Theorems 7.2 and 7.3 by requiring that A be 4^{th} power free. □

Theorem 7.6. *When $d = 3$ and A is 4^{th} power free, we have*

$$E^1(\mathbb{Q}(\sqrt{3}))_{\text{Tors}} \cong \begin{cases} \mathbb{Z}_3 & \text{when } A = (3 \pm 2\sqrt{3}) \\ \mathbb{Z}_4 & \text{when } A = (2 + \sqrt{3})^2 = (13 + 4\sqrt{3}) \\ \mathbb{Z}_2 \times \mathbb{Z}_2 & \text{when } A = -\square \\ \mathbb{Z}_2 & \text{otherwise.} \end{cases}$$

Remark. *$(2 + \sqrt{3})$ is the fundamental unit in $\mathbb{Z}[\sqrt{3}]$.*

Proof. $\mathbb{Z}[\sqrt{3}]$ is a UFD. The $\mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2$, and $\mathbb{Z}_3$ classifications follow directly from Theorem 7.2, where A is 4^{th} power free. Given the factorization of 2 in $\mathbb{Z}[\sqrt{3}]$ as

$$2 = (2 + \sqrt{3})(1 - \sqrt{3})^2,$$

the result follows directly from Corollary 7.4, by requiring that A is 4^{th} power free. □

Theorem 7.7. *When $d = 2$ and A is 4^{th} power free, we have*

$$E^1(\mathbb{Q}(\sqrt{2}))_{\text{Tors}} \cong \begin{cases} \mathbb{Z}_2 \times \mathbb{Z}_4 & \text{when } A = -1 \\ \mathbb{Z}_4 & \text{when } A = 1 \\ \mathbb{Z}_2 \times \mathbb{Z}_2 & \text{when } A = -\square \neq -1 \\ \mathbb{Z}_2 & \text{otherwise.} \end{cases}$$

Proof. From Theorem 1.8, we know $|E^1(k)_{\text{Tors}}|$ divides 8. All possibilities for the group structure except $\mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_8$ follow directly from Theorems 7.2 and 7.3, by requiring that A be 4^{th} power free.

To see the $\mathbb{Z}_2 \times \mathbb{Z}_4$ structure, we look at part 2 of the proof of Theorem 7.3. There we have

$$A = \frac{-m^4}{\left(\sqrt{2}\right)^4}$$
$$(x, y) = \left(\frac{(1 \pm \sqrt{2})m^2}{\left(\sqrt{2}\right)^2}, \frac{(1 \pm \sqrt{2})m^3}{\left(\sqrt{2}\right)^2} \right)$$

which, since $\mathbb{Z}[\sqrt{2}]^\times \cong \mathbb{Z}_2 \times \mathbb{Z}$, admits two possibilities for m for any given A, namely m and $-m$. Therefore we have four points $Q = (x, y)$ of order 4, three order 2 points, and the point at ∞. So $E^1(\mathbb{Z}[\sqrt{2}])_{\text{Tors}} \cong \mathbb{Z}_2 \times \mathbb{Z}_4$. By taking A to be 4^{th} power free, we get $A = -1$.

For a $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ structure, there would have to be 7 points of order 2 in $E^1(k)$. However, points $P = (x, y)$ of order 2 must lie on the x axis ($y = 0$), so x must be a root of $x^3 + Ax = 0$. However, there can be at most 3 distinct roots to $x^3 + Ax = 0$.

For a $\mathbb{Z}_8$ structure to exist, we need both points of order 4 (in the $\mathbb{Z}_4$ subgroup) to be doubles. We know that in $\mathbb{Z}[\sqrt{2}]$, $2 = (\sqrt{2})^2$. Therefore, by Corollary 7.4, the only possibility for A (which is 4^{th} power free) is $A = 1$. From the proof of Theorem 7.3, we can construct the points of order 4 for $A = 1$. They are $(1, \pm\sqrt{2})$. Now let $P = (x, y)$ be a point of order 8. Using the Doubling Formula, we see that

$$x(2P) = \frac{(x^2 - A)^2}{4(x^3 + Ax)} = \frac{(x^2 - 1)^2}{4(x^3 + x)} = 1.$$

After a little algebra, we find this is equivalent to

$$x^4 - 4x^3 - 2x^2 - 4x + 1 = 0.$$

Luckily, this factors as

$$(x^2 - (2 + \sqrt{2})x + 1)(x^2 - (2 - \sqrt{2})x + 1) = 0$$

which, by calculating discriminants, we can see has no roots in $\mathbb{Z}[\sqrt{2}]$. $\square$

8. The Group Structure of $E^2(k)_{\text{Tors}}$

Using the bound obtained on Theorem 6.9, we now proceed to classify the possible group structures for $E^2(k)_{\text{Tors}}$ when $d \neq -3$.

Lemma 8.1. *(Doubling Formula) Suppose $P = (x, y)$ is a point in $E^2(k)$, then the x coordinate of $2P$ is given by*

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

Proof. See [Kn], p76.

Theorem 8.2.

(1) $\mathbb{Z}_2 \subseteq E^2(k) \Longleftrightarrow d \neq -3$ *and* $B = l^3$ *for some* $l \in O_k$
(2) $\mathbb{Z}_2 \times \mathbb{Z}_2 \subseteq E^2(k) \Longleftrightarrow d = -3$ *and* $B = l^3$ *for some* $l \in O_k$
(3) $\mathbb{Z}_3 \subseteq E^2(k) \Longleftrightarrow$

$$B = \begin{cases} l^2 & \text{for some } l \in O_k \\ -2^4 3^2 l^6 & \text{if 3 splits or is inert in } O_k \text{ for some } l \in O_k \\ \frac{-16l^6}{27} & \text{if } (3) = \mathfrak{p}^2 \text{ for some } l \in \mathfrak{p} \end{cases}$$

(4) $\mathbb{Z}_4 \subseteq E^2(k) \Longleftrightarrow B = -(3 \pm 2\sqrt{3})^3 l^6$ *for some* $l \in O_k$.

Proof. (1) and (2). We have

$$\begin{aligned} P \text{ is a point of order 2} &\Longleftrightarrow P = -P, P \neq \infty \\ &\Longleftrightarrow (x, y) = (x, -y) \\ &\Longleftrightarrow y = 0. \end{aligned}$$

Putting $y = 0$ into the equation for E^2, we obtain

$$x^3 + B = (x + \sqrt[3]{B})(x + \omega\sqrt[3]{B})(x + \omega^2\sqrt[3]{B}) = 0$$

This has no roots if $B \neq l^3$, one root if $B = l^3$ and $\omega \notin O_k$, and three roots if $B = l^3$ and $\omega \in O_k$. Thus $E^2(k)$ contains at most one point of order 2, and exactly one point of order 2 only when $B \neq l^3$.

(3). Suppose there is a point P of order 3. Then $3P = 0$ and so $2P = -P$. By applying the Doubling Formula, we have

$$x(2P) = \frac{x^4 - 8Bx}{4x^3 + 4B} = x \tag{56}$$

which is equivalent to

$$x^4 + 4Bx = 0. \tag{57}$$

Since $d \neq -3$, the two roots of (57) are $x = 0$ and $x = \sqrt[3]{-4B}$. If $x = 0$, then E^2 becomes $y^2 = B$. If $x \neq 0$, then

$$B = \frac{-x^3}{4}. \tag{58}$$

Substituting this expression for B into the equation for E^2, we see

$$y^2 = \frac{3}{4}x^3$$

What we have done is taken our point $P = (x, y)$ of order 3 on E^2 and shown that it must also be a (rational) point on the singular cubic curve $E : y^2 = \frac{3}{4}x^3$. Theorem 3.1 gives us the general form of a rational point on E as

$$(x, y) = \left(\frac{4m^2}{3}, \frac{4m^3}{3}\right) \tag{59}$$

Among these, we look for points whose (coordinate) denominators are consistent with the bounds given by Corollary 3.9. Since we are dealing with points of order 3 over an arbitrary quadratic number field k, there are two cases to consider depending on the factorization of 3 in O_k.

(3a) 3 does not ramify. Corollary 3.9 tells us that $x, y \in O_k$. Therefore $2 \mid m$ and so (59) can be written as

$$(x, y) = \left(12l^2, 36l^3\right) \tag{60}$$

where $m = 2l$, $l \in O_k$. Using (58) to calculate B, we get $B = \frac{-x^3}{4} = \frac{-(12l^2)^3}{4} = -2^4 3^2 l^6$.

(3b) 3 ramifies. We write $(3) = \mathfrak{p}^2$. Corollary 3.9 tells us that $\mathrm{ord}_{\mathfrak{p}} x \geq -2$ and $\mathrm{ord}_{\mathfrak{p}} y \geq -3$. This allows only $\mathrm{ord}_{\mathfrak{p}} m \geq 0$, so $m \in O_k$. Using (58) to calculate B, we see that $B = \frac{-x^3}{4} = \frac{-(\frac{4m^2}{3})^3}{4} = -\frac{16m^6}{27}$. However this value of B is only in O_k if $m \in \mathfrak{p}$.

(4). Let $P_1 = (x_1, y_1)$ be the unique point of order 2 on E^2. Since P_1 is a point of order 2, from part (1) of this proof we know

$$-B = x_1^3. \tag{61}$$

Then if $P = (x, y)$ is a point of order 4, then P must double to P_1. Thus by the Doubling Formula, we have

$$x(2P) = \frac{x^4 - 8Bx}{4x^3 + 4B} = x_1. \tag{62}$$

By multiplying out (62) and substituting x_1^3 for $-B$, we obtain the homogeneous polynomial

$$x^4 - 4x_1x^3 + 8x_1^3x + 4x_1^4 = 0. \tag{63}$$

To solve (63), we change variables by letting $x' = \frac{x_1}{x}$. Since E^2 is non-singular, $x_1 \neq 0$ and so we can rewrite (63) as

$$4x'^4 + 8x'^3 - 4x' + 1 = 0 \tag{64}$$

which factors as

$$\frac{1}{4}(2x' - (-1+\sqrt{3}))^2(2x' - (-1-\sqrt{3}))^2 = 0. \tag{65}$$

Clearly the roots of (65) are $x' = \frac{-1\pm\sqrt{3}}{2}$ and so $x_1 = \frac{-1\pm\sqrt{3}}{2}x$. Substituting this back into the equation for E^2, we see

$$y^2 = x^3 + B = x^3 - x_1^3 = x^3 - \left(\frac{(-1\pm\sqrt{3})x}{2}\right)^3 = \frac{3(3\mp\sqrt{3})}{4}x^3. \tag{66}$$

What we have done is taken our point $P = (x, y)$ of order 4 on E^2 and shown that it must also be a (rational) point on the singular cubic curve $E : y^2 = \frac{3(3\mp\sqrt{3})}{4}x^3$. Theorem 3.1 gives us the general form of a rational point on E as

$$(x, y) = \left(\frac{4m^2}{(\sqrt{3})^3(\mp 1+\sqrt{3})}, \frac{4m^3}{(\sqrt{3})^3(\mp 1+\sqrt{3})}\right). \tag{67}$$

Among these, we look for points whose (coordinate) denominators are consistent with the bounds given by Corollary 3.9. Since we are dealing with points of order 4 and $(2) = (2\pm\sqrt{3})(1\mp\sqrt{3})^2 = \mathfrak{p}^2$ in $\mathbb{Z}[\sqrt{3}]$, Corollary 3.9 states that

$$\begin{aligned} \operatorname{ord}_{1\mp\sqrt{3}} x &\geq -2 \\ \operatorname{ord}_{1\mp\sqrt{3}} y &\geq -3. \end{aligned}$$

Since $\operatorname{ord}_{1\mp\sqrt{3}} x = 3 + 2\operatorname{ord}_{1\mp\sqrt{3}} m$ and $\operatorname{ord}_{1\mp\sqrt{3}} y = 3 + 3\operatorname{ord}_{1\mp\sqrt{3}} m$, the above conditions allow only those $m \in O_k$ such that $\operatorname{ord}_{1\mp\sqrt{3}} m \geq -2$. Since $N(\mp 1+\sqrt{3}) = -2$ and $N(-4) = 16$, we rewrite (67) so the factorization and divisibility of the coefficients are clear. Doing this we see

(68)

$$\begin{aligned} (x, y) &= \left(\frac{4m^2}{(\sqrt{3})^3(\mp 1+\sqrt{3})}, \frac{4m^3}{(\sqrt{3})^3(\mp 1+\sqrt{3})}\right) \\ &= \left(\frac{\mp 4m^2}{(\sqrt{3})^3(1\mp\sqrt{3})}, \frac{\mp 4m^3}{(\sqrt{3})^3(1\mp\sqrt{3})}\right) \\ &= \left(\frac{\mp\left((2\pm\sqrt{3})(1\mp\sqrt{3})^2\right)^2 m^2}{(\sqrt{3})^3(1\mp\sqrt{3})}, \frac{\mp\left((2\pm\sqrt{3})(1\mp\sqrt{3})^2\right)^2 m^3}{(\sqrt{3})^3(1\mp\sqrt{3})}\right) \\ &= \left(\frac{\mp(2\pm\sqrt{3})^2(1\mp\sqrt{3})^3 m^2}{(\sqrt{3})^3}, \frac{\mp(2\pm\sqrt{3})^2(1\mp\sqrt{3})^3 m^3}{(\sqrt{3})^3}\right) \end{aligned}$$

Thus we may write m in the form $m = \frac{3l}{2} = \frac{3(2\mp\sqrt{3})l}{(1\mp\sqrt{3})^2}$ for some l in O_k. Putting this back into (68), we get

$$(x,y) = \left(\frac{\mp(\sqrt{3})l^2}{(1\mp\sqrt{3})}, \frac{\mp(3\sqrt{3})(2\mp\sqrt{3})l^3}{(1\mp\sqrt{3})^3}\right). \tag{69}$$

Using (66) and (69), we solve for B as

$$\begin{aligned} B &= -\left(\frac{(-1\pm\sqrt{3})x}{2}\right)^3 \\ &= -\left(\frac{(-1\pm\sqrt{3})(\frac{\mp(\sqrt{3})l^2}{(1\mp\sqrt{3})})}{2}\right)^3 \\ &= \left(\frac{\mp(\sqrt{3})l^2}{2}\right)^3 \end{aligned} \tag{70}$$

However, we also require that B be an element of O_k. Therefore we again change variables as $l = (1\mp\sqrt{3})(2\pm\sqrt{3})l'$ to eliminate the denominator. This gives

$$\begin{aligned} B &= \left(\frac{\mp(\sqrt{3})\left((1\mp\sqrt{3})(2\pm\sqrt{3})l'\right)^2}{2}\right)^3 \\ &= \left(\mp(\sqrt{3})(2\pm\sqrt{3})\right)^3 l'^6 \\ &= -\left(3\pm 2\sqrt{3}\right)^3 l'^6. \end{aligned}$$

□

Theorem 8.3. *Suppose that $k = \mathbb{Q}(\sqrt{d})$ is a UFD and that $E^2(k)$ contains a point P of order 3. If $3 = \pi^2 u$ where π is a prime and u is a unit, then*

$$B = -16u^3 l^6$$

for some $l \in O_k$.

Proof. The factorization $3 = \pi^2 u$ tells us that 3 splits and that the prime ideal $\mathfrak{p}$ which divides 3 is just the principal ideal (π). From part 3 of Theorem 8.2, we know $B = \frac{-16l^6}{27}$ for some $l \in \mathfrak{p}$. Thus we can write $l = \pi m$ for some $m \in O_k$. This gives us

$$B = \frac{-16l^6}{27} = \frac{-16\pi^6 m^6}{u^3\pi^6} = \frac{-16m^6}{u^3}$$

Since u is a unit, we can make the change of variables $m' = um$. This gives

$$B = -16u^3 m'^6.$$

□

Theorem 8.4. *If $d \neq \pm 3$ and B is 6^{th} power free, we have*

$$E^2(k)_{\text{Tors}} \cong \begin{cases} \mathbb{Z}_6 & \text{when } B = l^2 = l'^3 \text{ for some } l, l' \in O_k \\ \mathbb{Z}_3 & \text{when } B = \begin{cases} l^2 \neq \text{cube} & \text{for some } l \in O_k \\ -2^4 3^2 l^6 & \text{if 3 splits or is inert in } O_k \\ & \text{and for some } l \in O_k \\ \frac{-16 l^6}{27} & \text{if } (3) = \mathfrak{p}^2 \text{ for some } l \in \mathfrak{p} \end{cases} \\ \mathbb{Z}_2 & \text{when } B = l^3 \neq \square \text{ for some } l \in O_k \\ \{0\} & \text{otherwise.} \end{cases}$$

Also, when $d = 3$ we have

$$E^2(k)_{\text{Tors}} \cong \begin{cases} \mathbb{Z}_6 & \text{when } B = 1 \\ \mathbb{Z}_4 & \text{when } B = -(3 \pm 2\sqrt{3})^3 \\ \mathbb{Z}_3 & \text{when } B = \begin{cases} -16 \\ l^2 \neq \text{cube} & \text{for some } l \in O_k \end{cases} \\ \mathbb{Z}_2 & \text{when } B = l^3 \neq \square \text{ for some } l \in O_k \\ \{0\} & \text{otherwise.} \end{cases}$$

Proof. From Theorem 6.9, we know that when $d \neq -3$,

$$|E^2(k)_{\text{Tors}}| \text{ divides } \begin{cases} 12 & \text{if } d = 3 \\ 6 & \text{otherwise.} \end{cases} \tag{71}$$

Almost all of the conditions above follow directly from Theorem 8.2 to all possible group structures satisfying (71). Those possibilities which do not folllow directly from Theorem 8.2 are proved below.

We now examine under what conditions $\mathbb{Z}_3$ and $\mathbb{Z}_2$ (or $\mathbb{Z}_4$) are compatible.

Suppose $B = l_1^2 = l_2^3$, then we find a $\mathbb{Z}_6$ structure. For example, $B = 1$ always gives a $\mathbb{Z}_6$.

Suppose $B = -2^4 3^2 l^6$ for some $l \in O_k$. Then if $B = l_1^3$ for some $l_1 \in O_k$, $N(B) = 2^8 3^4 l^{12}$ =cube. Since $N(B)$ is not a cube, this is not possible.

Suppose $B = \frac{-16}{27} l^6$ for some $l \in O_k$. Then if $B = l_1^3$ for some $l_1 \in O_k$, $N(B) = \frac{2^8}{3^4} l^{12}$ =cube. Since $N(B)$ is not a cube, this is not possible.

When $d = 3$, we can refine condition (3) of Theorem 8.2 slightly. We can write the factorization of 2 as

$$2 = (1 + \sqrt{3})^2 (2 + \sqrt{3}) \qquad \text{where } 2 + \sqrt{3} \text{ is the fundamental unit.}$$

Thus the condition $4B = (1 + \sqrt{3})^4 (2 + \sqrt{3})^2 B = l^3$ is equivalent to saying

$$\begin{cases} ord_{1+\sqrt{3}} B = 2 \text{ or } 5 \\ ord_{2+\sqrt{3}} B = 1 \text{ or } 4 \end{cases}$$

under the condition that B is 6^{th} power free. Therefore, without loss of generality, we write

$$B = (1 + \sqrt{3})^2 (2 + \sqrt{3}) l'^3 = 2 l'^3$$

for some $l' \in O_k$. $\square$

9. Torsion over $\mathbb{Z}[i]$ and $\mathbb{Z}[\omega]$

Up to now, we have been fortunate enough to have, for each choice of d, at least one congruence class of primes p which split in O_k. This allowed us to look at the group $E_{\mathfrak{p}}(O_k/\mathfrak{p})$ where $\mathfrak{p}$ divides p for such primes. Since $O_k/\mathfrak{p}$ is a field with p elements, we were able to use the complex multiplication symmetries of these elliptic curves to determine the size of $E_{\mathfrak{p}}(O_k/\mathfrak{p})$ to be exactly $p+1$ elements. However, his approach does not work for the two special number fields $\mathbb{Z}[i]$ with E^1 and $\mathbb{Z}[\omega]$ with E^2. To continue in this way, we must either know the size of $E_{\mathfrak{p}}(O_k/\mathfrak{p})$ for some other congruence class of primes or know the size of $E_{\mathfrak{p}}(O_k/\mathfrak{p})$ when p is inert. As it happens, there is a powerful theorem from the theory of L-functions which will tell us the size of $E_p(\mathbb{F}_{p^2})$ where $\mathbb{F}_{p^n}$ is the finite field with p^n elements.

Theorem 9.1. *Let E be an elliptic curve. Then there exist complex numbers $\alpha, \beta \in \mathbb{C}$ such that*

$$|E_p(\mathbb{F}_{p^n})| = p^n + 1 - \alpha^n - \beta^n \tag{72}$$

for all $n \geq 1$. Also α and β satisfy

$$|\alpha| = |\beta| = \sqrt{p} \quad \text{and} \quad \alpha\beta = p.$$

Proof. See [Sil 1], p136 top.

Corollary 9.2. *If either $E = E^1$, $d = -1$, and $p \equiv 3 \bmod 4$ or $E = E^2$, $d = -3$, and $p \equiv 2 \bmod 3$, then*

$$|E_p(O_k/p)| = |E_p(\mathbb{F}_{p^2})| = (p+1)^2$$

Proof. Since p is inert over k and k is a quadratic number field, $O_k/p \cong \mathbb{F}_{p^2}$. From Theorems 6.1 and 6.2, we know $|E_p(\mathbb{F}_p)| = p+1$, so $\alpha + \beta = 0$. Since $\alpha\beta = p$, we must have $\alpha, \beta = \pm i\sqrt{p}$. Now letting $n = 2$ and using (72), we obtain

$$|E_p(\mathbb{F}_{p^2})| = p^2 + 1 + p + p = (p+1)^2.$$

□

Lemma 9.3. *If $k = \mathbb{Q}(\sqrt{-3})$, then $E^2(k)$ has no points of order 5.*

Proof. Suppose there is a point $P = (x, y)$ on $E^2(k)$ with order 5. Then $4P = 2\,2P = -P$. Using the Doubling Formula, we see that

$$x(4P) = \frac{\dfrac{(x^4 - 8Bx)^4}{(4x^3 + 4B)^4} - 8\dfrac{B(x^4 - 8Bx)}{4x^3 + 4B}}{4\dfrac{(x^4 - 8Bx)^3}{(4x^3 + 4B)^3} + 4B} = -x. \tag{73}$$

After considerable manipulation, we can rewrite (73) as

$$\frac{1}{16}\frac{(17x^{15} + 112x^{12}B + 9728x^9B^2 + 9728x^6B^3 + 11776x^3B^4)}{(x^3 + B)(x^{12} + 40x^9B + 384x^6B^2 - 320x^3B^3 + 64B^4)} = 0. \tag{74}$$

Since the numerator of (74) is irreducible over $k = \mathbb{Q}(\sqrt{-3})$, there are no points of order 5 in $E^2(k)$. □

Theorem 9.4. *When $d = -1$, $|E^1(k)_{\text{Tors}}|$ divides 16.*

Proof. Let $q = |E^1(k)_{\text{Tors}}|$. From Theorem 7.2, $3 \nmid q$ so we may choose a prime $p > \Delta_{E^1}, q$ such that $p \equiv 3 \bmod 4q$. Since $p \nmid \Delta_{E^1}$, the reduction homomorphism r_p is one-to-one when restriced to $|E^1(k)_{\text{Tors}}|$. So $q \mid (p+1)^2$ and because $p \equiv 3 \bmod 4q$, $q \mid (3+1)^2 = 16$. $\square$

Theorem 9.5. *When $d = -3$, $|E^2(k)_{\text{Tors}}|$ divides 36.*

Proof. Let $q = |E^2(k)_{\text{Tors}}|$. From Lemma 9.3 we know that $5 \nmid q$ and we can choose a prime $p > \Delta_{E^2}, q$ such that $p \equiv 5 \bmod 3q$. Since $p \nmid \Delta_{E^2}$, the reduction homomorphism r_p is one-to-one when restriced to $|E^2(k)_{\text{Tors}}|$. So $q \mid (p+1)^2$ and because $p \equiv 5 \bmod 3q$, $q \mid (5+1)^2 = 36$. $\square$

Now that we have a good bound for $E(k)_{\text{Tors}}$, we will attempt to construct all possible group structure within that bound.

Theorem 9.6. *When $d = -1$ and A is 4^{th} power free,*

$$E^1(k)_{\text{Tors}} \cong \begin{cases} \mathbb{Z}_4 \times \mathbb{Z}_2 & \text{if } A = -1 \\ \mathbb{Z}_2 \times \mathbb{Z}_2 & \text{if } A = \square \neq -1 \\ \mathbb{Z}_2 & \text{otherwise.} \end{cases}$$

Proof. (1). Since $O = (0,0)$ is always a point of order 2 on E^1, we have $\mathbb{Z}_2 \subset E^1(k)$.

(2). If $E^1(k)_{\text{Tors}}$ has a $\mathbb{Z}_2 \times \mathbb{Z}_2$ subgroup, then there must be three points of order 2. So $x^3 + Ax = 0$ must have exactly three roots in O_k, namely $x = 0, \pm i\sqrt{A}$. Thus $A = \square$.

(3). Suppose there were a point P of order 4. We know that in $\mathbb{Z}[i]$, the factorization of 2 can be written as $2 = -i(1+i)^2$. Then from Lemma 2 and Corollary 3, we know that $A = -l^4$ for some $l \in O_k$. However since we require that A be 4^{th} power free, we have $A = -1$.

(4). Suppose there is a point $P' = (x', y')$ of order 8. Then P' must double to a point $P = (x, y)$ of order 4. From the preceding paragraph, we know that $x = il^2$ for some $l \in O_k$. Thus the Doubling Formula gives

$$x(2P') = \frac{({x'}^2 - A)^2}{4{x'}^3 + 4Ax'} = \frac{({x'}^2 - A)^2}{4{y'}^2} = x = il^2. \tag{75}$$

Clearing denominators, we have

$$({x'}^2 - A)^2 = 4il^2{y'}^2 = i(2ly')^2 \tag{76}$$

which is nonsense since i is not a square in $\mathbb{Z}[i]$. Therefore there are no points of order 8. $\square$

Theorem 9.7. *When $d = -3$, and B is 6^{th} power free,*

$$E^2(k)_{\text{Tors}} \cong \begin{cases} \mathbb{Z}_2 \times \mathbb{Z}_6 & \text{when } B = 1 \\ \mathbb{Z}_3 & \text{when } B = \begin{cases} 16 \\ l^2 \neq \text{cube} \quad \text{for some } l \in O_k \end{cases} \\ \mathbb{Z}_2 \times \mathbb{Z}_2 & \text{when } B = l^3 \neq \square \text{ and for some } l \in O_k \\ \{0\} & \text{otherwise.} \end{cases}$$

Proof. (1). The above classification follows directly from Theorems 8.2 and 8.3. From the group law, every point of order 3 must also be a flex. Since there are at most 3 flexes on a cubic, there can be at most 3 points of order 3.

(2). Suppose there is a point P of order 9. From the group law formulas in [Kn], pp75-6, we can calculate the tripling formula for a point P as

$$x(3P) = \left(\frac{x^9 - 96x^6B + 48x^3B^2 + 64B^3}{9x^2(x^3 + 4B)^2} \right).$$

Thus a point of order 9 must satisfy $x(6P) = -x(3P)$, which after much algebra, is equivalent to

$$\begin{aligned}(\,X^3 - 96\,X^2 + 48\,X + 64\,)(+5\,X^9 - 4356\,X^8 + 68976\,X^7 - 5260800\,X^6 + 2753280\,X^5 \\ - 5575680\,X^4 - 26148864\,X^3 - 15630336\,X^2 + 2949120\,X + 1310720) = 0\end{aligned}$$

where $X = \frac{x^3}{B}$. Since this has no roots on $\mathbb{Z}[\omega]$, there are no points of order 9. □

10. Glossary of Symbols

d	square-free integer
$\mathbb{Z}$	integers
$\mathbb{Q}$	rational numbers
$k = \mathbb{Q}(\sqrt{d})$	quadratic number field
O_k	ring of integers in k
$\mathfrak{p}$	prime ideal in O_k
E	elliptic curve
E^1	elliptic curve with affine form $y^2 = x^3 + Ax$
E^2	elliptic curve with affine form $y^2 = x^3 + B$
$E_\mathfrak{p}$	$\mathfrak{p}$-reduced elliptic curve
$E(k), E(O_k/\mathfrak{p})$	the group of points (x, y) on E with both coordinates $x, y \in k$ or $O_k/\mathfrak{p}$, respectively, together with the point at ∞.
$E(k)_{\text{Tors}}, E(O_k/\mathfrak{p})_{\text{Tors}}$	the subgroup of points on E in $E(k)$, $E(O_k/\mathfrak{p})$, respectively, with finite order.
Δ_E	the discriminant of E.

11. Summary and Examples of Special Curves

In this section, we summarize our results about $E(k)_{\text{Tors}}$ where $k = \mathbb{Q}(\sqrt{d})$ and give examples of those new group structures which appear when we consider $k = \mathbb{Q}(\sqrt{d})$ in place of $k = \mathbb{Q}$. Then, when $d > 0$, we plot the points of $E(k)_{\text{Tors}}$ on the graph of $E(\mathbb{R})$.

Theorem. *Consider the elliptic curves $E^1 : y^2 = x^3 + Ax$ over the quadratic number field $k = \mathbb{Q}(\sqrt{d})$, where A is in the ring of integers O_k of k and A is 4^{th} power free. Then if $d \neq -1, 2, 3$, we have*

$$E^1(k)_{\text{Tors}} \cong \begin{cases} \mathbb{Z}_4 & \text{when 2 either splits or is inert in } O_k \text{ and } A = 4 \\ \mathbb{Z}_4 & \text{when } (2) = \mathfrak{p}^2 \text{ and } A = \frac{l^4}{4} \text{ for some } l \in \mathfrak{p} \\ \mathbb{Z}_2 \times \mathbb{Z}_2 & \text{when } A = -\square \\ \mathbb{Z}_2 & \text{otherwise.} \end{cases}$$

For the special cases $d = -1, 2, 3$, we have

$$E^1(\mathbb{Q}(\sqrt{3}))_{\text{Tors}} \cong \begin{cases} \mathbb{Z}_3 & \text{when } A = (3 \pm 2\sqrt{3}) \\ \mathbb{Z}_4 & \text{when } A = (2 + \sqrt{3})^2 = (13 + 4\sqrt{3}) \\ \mathbb{Z}_2 \times \mathbb{Z}_2 & \text{when } A = -\square \\ \mathbb{Z}_2 & \text{otherwise.} \end{cases}$$

$$E^1(\mathbb{Q}(\sqrt{2}))_{\text{Tors}} \cong \begin{cases} \mathbb{Z}_2 \times \mathbb{Z}_4 & \text{when } A = -1 \\ \mathbb{Z}_4 & \text{when } A = 1 \\ \mathbb{Z}_2 \times \mathbb{Z}_2 & \text{when } A = -\square \neq -1 \\ \mathbb{Z}_2 & \text{otherwise.} \end{cases}$$

$$E^1(\mathbb{Q}(i))_{\text{Tors}} \cong \begin{cases} \mathbb{Z}_4 \times \mathbb{Z}_2 & \text{if } A = -1 \\ \mathbb{Z}_2 \times \mathbb{Z}_2 & \text{if } A = \square \neq -1 \\ \mathbb{Z}_2 & \text{otherwise.} \end{cases}$$

Theorem. *Consider the elliptic curves $E^2 : y^2 = x^3 + B$ over the quadratic number field $k = \mathbb{Q}(\sqrt{d})$, where B is in the ring of integers O_k of k and B is 6^{th} power free. Then if $d \neq \pm 3$, we have*

$$E^2(k)_{\text{Tors}} \cong \begin{cases} \mathbb{Z}_6 & \text{when } B = l^2 = l'^3 \text{ for some } l, l' \in O_k \\ \mathbb{Z}_3 & \text{when } B = \begin{cases} l^2 \neq \text{cube} & \text{for some } l \in O_k \\ -2^4 3^2 l^6 & \text{if 3 splits or is inert in } O_k \text{ and for some } l \in O_k \\ \frac{-16l^6}{27} & \text{if } (3) = \mathfrak{p}^2 \text{ for some } l \in \mathfrak{p} \end{cases} \\ \mathbb{Z}_2 & \text{when } B = l^3 \neq \square \text{ for some } l \in O_k \\ \{0\} & \text{otherwise.} \end{cases}$$

For the special cases $d = \pm 3$, we have

$$E^2(\mathbb{Q}(\sqrt{3}))_{\text{Tors}} \cong \begin{cases} \mathbb{Z}_6 & \text{when } B = 1 \\ \mathbb{Z}_4 & \text{when } B = -(3 \pm 2\sqrt{3})^3 \\ \mathbb{Z}_3 & \text{when } B = \begin{cases} -16 \\ l^2 \neq \text{cube} \quad \text{for some } l \in O_k \end{cases} \\ \mathbb{Z}_2 & \text{when } B = l^3 \neq \square \text{ for some } l \in O_k \\ \{0\} & \text{otherwise} \end{cases}$$

$$E^2(\mathbb{Q}(\sqrt{-3}))_{\text{Tors}} \cong \begin{cases} \mathbb{Z}_2 \times \mathbb{Z}_6 & \text{when } B = 1 \\ \mathbb{Z}_3 & \text{when } B = \begin{cases} 16 \\ l^2 \neq \text{cube} \quad \text{for some } l \in O_k \end{cases} \\ \mathbb{Z}_2 \times \mathbb{Z}_2 & \text{when } B = l^3 \neq \square \text{ and for some } l \in O_k \\ \{0\} & \text{otherwise.} \end{cases}$$

Some Special E^1 Elliptic Curves.

$$E^1 : y^2 = x^3 + (3 - 2\sqrt{3})x \qquad E^1(\mathbb{Q}(\sqrt{3})) \cong \mathbb{Z}_3$$

$$0 \leftrightarrow O$$
$$1 \leftrightarrow P_1 = (1, 1 - \sqrt{3})$$
$$2 \leftrightarrow P_2 = (1, -1 + \sqrt{3})$$

$$E^1 : y^2 = x^3 - x \qquad E^1(\mathbb{Q}(\sqrt{3})) \cong \mathbb{Z}_2 \times \mathbb{Z}_4$$

$$(0,0) \leftrightarrow O \qquad (0,1) \leftrightarrow P_1 = (-1, 0)$$
$$(1,0) \leftrightarrow Q_1 = (1 - \sqrt{2}, 2 - \sqrt{2}) \qquad (1,1) \leftrightarrow Q_4 = (1 + \sqrt{2}, -2 - \sqrt{2})$$
$$(2,0) \leftrightarrow P_3 = (1, 0) \qquad (2,1) \leftrightarrow P_2 = (0, 0)$$
$$(3,0) \leftrightarrow Q_2 = (1 - \sqrt{2}, -2 + \sqrt{2}) \qquad (3,1) \leftrightarrow Q_3 = (1 + \sqrt{2}, 2 + \sqrt{2})$$

$$E^1 : y^2 = x^3 - x \qquad E^1(\mathbb{Q}(i)) \cong \mathbb{Z}_2 \times \mathbb{Z}_4$$

$$(0,0) \leftrightarrow O \qquad (0,1) \leftrightarrow P_1 = (-1, 0)$$
$$(1,0) \leftrightarrow Q_1 = (i, 1 - i) \qquad (1,1) \leftrightarrow Q = (,)$$
$$(2,0) \leftrightarrow P_2 = (1, 0) \qquad (2,1) \leftrightarrow P_3 = (1, 0)$$
$$(3,0) \leftrightarrow Q_3 = (i, -1 + i) \qquad (3,1) \leftrightarrow Q = (,)$$

Remark. *Here, the complex multiplication symmetry of E^1 can be clearly seen since the multiplication-by-i map is closed in $O_k = \mathbb{Z}[i]$. Moreover, since the multiplication-by-i map is a unit (invertible) in End $E \cong \mathbb{Z}[i]$, this map induces an automorphism on $E^1(\mathbb{Q}(i))_{\text{Tors}}$.*

Some Special E^2 Elliptic Curves.

$$E^2 : y^2 = x^3 - (3 - 2\sqrt{3})^3 \qquad\qquad E^2(\mathbb{Q}(\sqrt{3})) \cong \mathbb{Z}_4$$

$$\begin{aligned} 0 &\leftrightarrow O \\ 1 &\leftrightarrow Q_1 = (9 - 5\sqrt{3}, 36 - 21\sqrt{3}) \\ 2 &\leftrightarrow P = (3 - 2\sqrt{3}, 0) \\ 3 &\leftrightarrow Q_2 = (9 - 5\sqrt{3}, -36 + 21\sqrt{3}) \end{aligned}$$

$$E^2 : y^2 = x^3 + 8 \qquad\qquad E^2(\mathbb{Q}(\sqrt{-3})) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$$

$$\begin{aligned} (0,0) &\leftrightarrow O & (0,1) &\leftrightarrow (-2\omega, 0) \\ (1,0) &\leftrightarrow (-2, 0) & (1,1) &\leftrightarrow (-2\omega^2, 0) \end{aligned}$$

$$E^2 : y^2 = x^3 + 1 \qquad\qquad E^2(\mathbb{Q}(\sqrt{-3})) \cong \mathbb{Z}_2 \times \mathbb{Z}_6$$

$$\begin{aligned} (0,0) &\leftrightarrow O & (0,1) &\leftrightarrow P_2 = (-\omega, 0) \\ (1,0) &\leftrightarrow = (,) & (1,1) &\leftrightarrow = (,) \\ (2,0) &\leftrightarrow Q_1 = (1,0) & (2,1) &\leftrightarrow = (,) \\ (3,0) &\leftrightarrow P_1 = (-1,0) & (3,1) &\leftrightarrow P_3 = (-\omega^2, 0) \\ (4,0) &\leftrightarrow Q_2 = (1,0) & (4,1) &\leftrightarrow = (,) \\ (5,0) &\leftrightarrow = (,) & (5,1) &\leftrightarrow = (,) \end{aligned}$$

Remark. *Here, the complex multiplication symmetry of E^2 can be clearly seen since the multiplication-by-i map is closed in $O_k = \mathbb{Z}[\omega]$. Moreover, since the multiplication-by-ω map is a unit (invertible) in End $E \cong \mathbb{Z}[\omega]$, this map induces an automorphism on $E^2(\mathbb{Q}(\sqrt{-3}))_{\text{Tors}}$.*

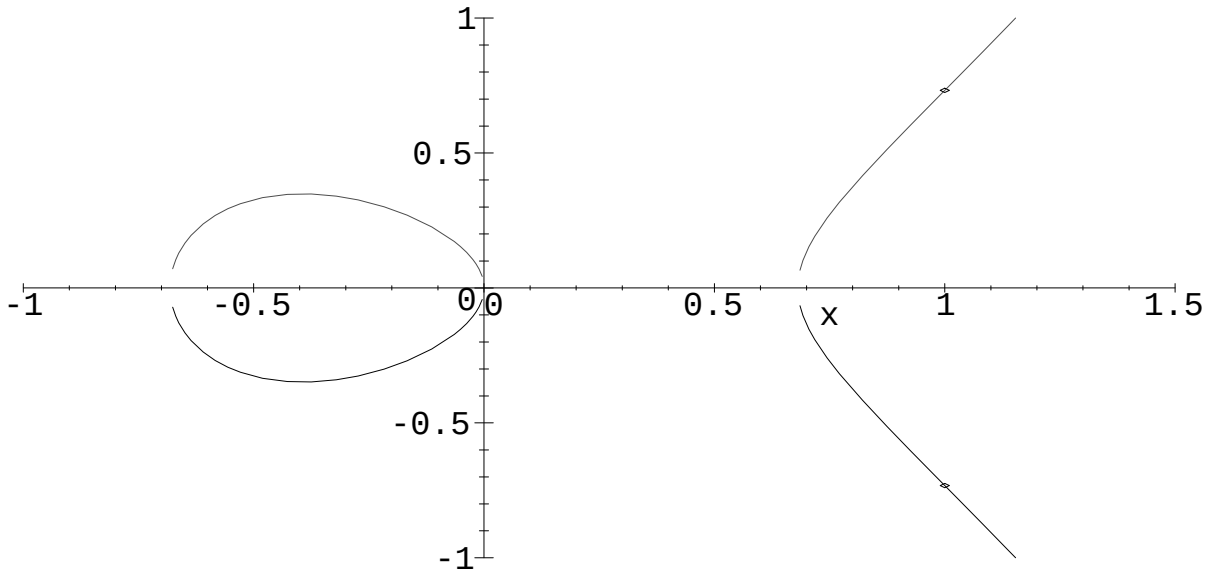

FIGURE 1. $E^1 : y^2 = x^3 + (3 - 2\sqrt{3})x$ over $\mathbb{Q}(\sqrt{3})$.

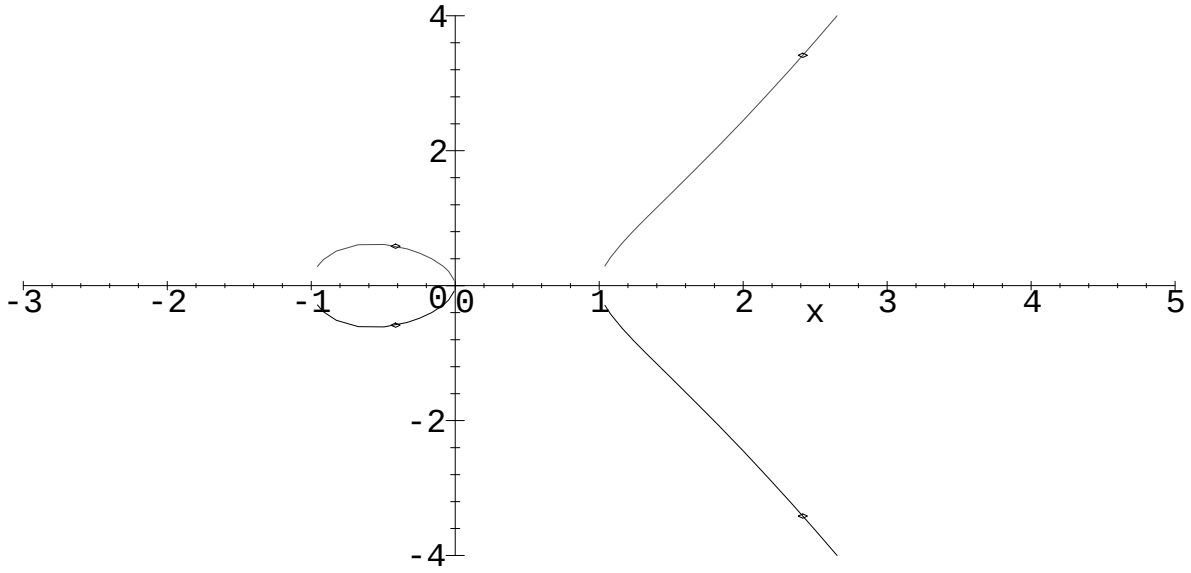

FIGURE 2. $E^1 : y^2 = x^3 - x$ over $\mathbb{Q}(\sqrt{2})$.

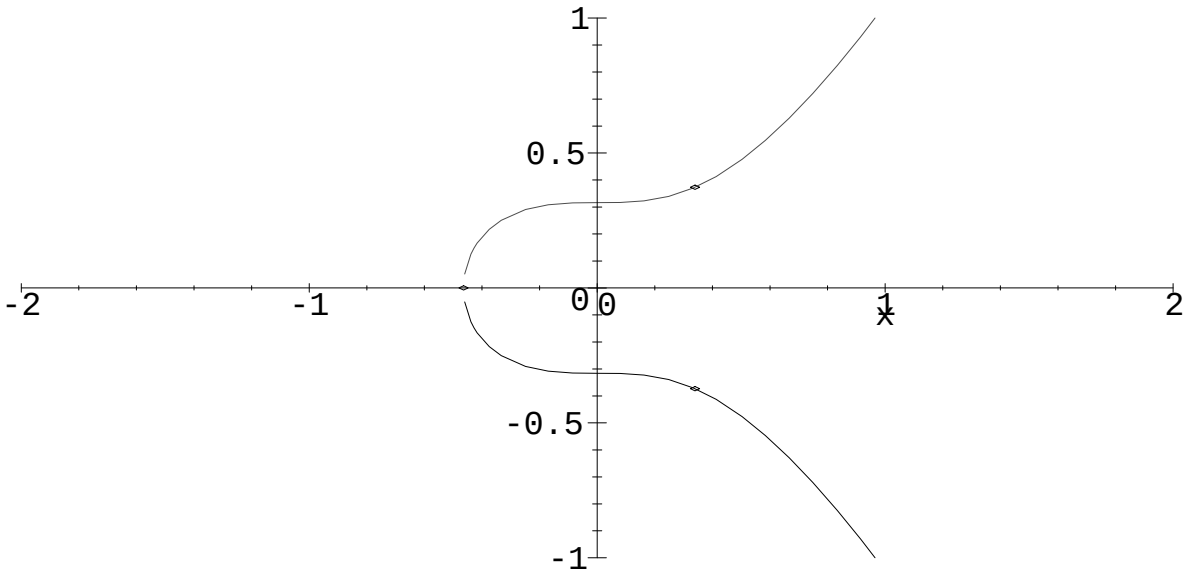

FIGURE 3. $E^2 : y^2 = x^3 - (3 - 2\sqrt{2})^3$ over $\mathbb{Q}(\sqrt{3})$.

12. REFERENCES

[H-W] G. Hardy and E. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, Oxford, 1960.

[I-R] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory, 2nd ed.*, Springer-Verlag, New York, 1990.

[Kn] A. W. Knapp, *Elliptic Curves*, Princeton University Press, Princeton, 1992.

[Sil 1] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.

[Sil 2] J. H. Silverman, *Advanced Topics in the Arithmetic Elliptic Curves*, Springer-Verlag, New York, 1994.