TORSION FOR CM ELLIPTIC CURVES DEFINED OVER NUMBER FIELDS OF DEGREE $2P$

BY

HOLLY PAIGE CHAOS

A Thesis Submitted to the Graduate Faculty of

WAKE FOREST UNIVERSITY GRADUATE SCHOOL OF ARTS AND SCIENCES

in Partial Fulfillment of the Requirements

for the Degree of

MASTER OF ARTS

Mathematics & Statistics

May 2020

Winston-Salem, North Carolina

Approved By:

Abbey Bourdon, Ph.D., Advisor

Jeremy Rouse, Ph.D., Chair

Frank Moore, Ph.D.

Acknowledgments

I am incredibly grateful to my advisor, Dr. Abbey Bourdon, for all of her time, guidance, and unwavering support. She has been an exceptional source of inspiration and encouragement throughout my time at Wake Forest.

I would also like to thank two extraordinary professors who taught, inspired, and believed in me: Dr. Carrie E. Finch-Smith and Dr. Mitch Keller.

Finally, I would like to extend a special thanks to my parents, Cynthia and Stephen, and my sisters, Rachel Grace and Megan Claire, without whom this would not have been possible.

Table of Contents

List of Figures

Abstract

Holly Paige Chaos

Let E be an elliptic curve with complex multiplication defined over a number field F of degree $2p$ for prime $p > 3$.In this thesis, we completely classify the torsion subgroups that can arise for number fields of degree $2p$ for any prime $p > 3$.

Chapter 1: Introduction and Statement of Results

Elliptic curves have been of interest to mathematicians since the third century when they appeared in the writing of Greek mathematician Diophantus; his research included finding rational and integer solutions to polynomial equations. This thesis begins with our interest in rational solutions to equations of the form $y^2 = x^3 + Ax + B$ where $A, B \in \mathbb{Q}$. The corresponding curve is smooth, that is it has no cusps or self-intersections, if the discriminant $-16(4A^3 + 27B^2) \neq 0$. With this condition, this polynomial equation represents an elliptic curve E defined over $\mathbb{Q}$.

In 1922, Louis Mordell, an American born British mathematician, proved that the collection of points on E with coordinates in $\mathbb{Q}$ along with the point at infinity, denoted $E(\mathbb{Q})$, is a finitely generated abelian group [17]. This, consequently, implies that $E(\mathbb{Q}) \cong E(\mathbb{Q})[\text{tors}] \times \mathbb{Z}^r$ where $E(\mathbb{Q})[\text{tors}]$ denotes the finite collection of torsion points and r denotes the rank of $E(\mathbb{Q})$. For a fixed E, r is some finite number. For example if $E : y^2 = x^3 - 5x + 4$, then we can show that $E(\mathbb{Q})[\text{tors}] = \langle (1,0) \rangle \cong \mathbb{Z}/2\mathbb{Z}$, $r = 1$, and $\langle (0,2) \rangle \cong \mathbb{Z}$.

Since the points on an elliptic curve can be given the structure of a finitely generated abelian group, it is natural to inquire as to precisely what finite groups arise as $E(\mathbb{Q})[\text{tors}]$. In 1977 Barry Mazur published the complete classification of torsion subgroups for elliptic curves defined over the rationals.

Theorem 1 (Mazur, [9])**.** *Let E be an elliptic curve defined over the rationals. Then $E(\mathbb{Q})[\text{tors}]$ is isomorphic to*

$$\begin{array}{ll} \mathbb{Z}/m\mathbb{Z} & 1 \leq m \leq 10 \text{ or } m = 12 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} & 1 \leq m \leq 4. \end{array}$$

Furthermore, each of these groups occurs as a torsion subgroup of an elliptic curve $E/\mathbb{Q}$.

Knowing this, why restrict to elliptic curves defined over the rationals? What if we let E be an elliptic curve defined over a number field F of degree d? French mathematician André Weil proved that the abelian group $E(F)$ has a finite number of generators and $E(F) \cong E(F)[\text{tors}] \times \mathbb{Z}^r$ where r, again, is the rank of E/F. See [10]. In 1996, Loïc Merel [11] proved that if we consider all elliptic curves E defined over F and we allow F to vary over all number fields of fixed degree d then only finitely many groups arise as torsion subgroups.

The essential question of this thesis concerns what $E(F)[\text{tors}]$ arise if we consider all number fields F of degree d and all elliptic curves E/F. For $d = 2$ we have the complete classification.

Theorem 2 (Kamienny-Kenku-Momose, [12], [13], [14])**.** *Let F be a quadratic field. For an elliptic curve E/F, the group $E(F)[\text{tors}]$ is isomorphic to one of the following groups*

$$\begin{array}{ll} \mathbb{Z}/m\mathbb{Z} & 1 \leq m \leq 18,\ m \neq 17 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} & 1 \leq m \leq 6 \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3m\mathbb{Z} & 1 \leq m \leq 2 \\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} & \end{array}$$

It was announced that there is a result for $d = 3$ but the complete classification of the torsion subgroups that arise has yet to be published [16]. So almost a century after Mordell's proof we only have seen the complete classification for the torsion subgroups arising over the rationals or a quadratic field. One way to extend the classification is to restrict the elliptic curves under consideration. Some of the most common options for doing this include looking at elliptic curves $E/\mathbb{Q}$ under base extension, looking at what groups occur infinitely often, or looking at elliptic curves with complex multiplication, CM.

This third option is our focus. That is, this thesis focuses on extending the classification of what torsion subgroups arise for elliptic curves with complex multiplication. If E/F is a CM elliptic curve, then we know the complete classification for what groups $E(F)[\text{tors}]$ is isomorphic to for $[F : \mathbb{Q}] = d$ when $d \leq 13$ (see [6], [15]) and $d \equiv 1 \pmod 2$ (see [8], [2]).

However, for $d \geq 14$ and even, the classification was previously unknown.

In this thesis, we completely classify the torsion subgroups that can arise for number fields of degree $2p$ for any prime $p > 3$. A consequence of [5, p.86] is that if E/F is an elliptic curve, then $E(F)[\text{tors}] \cong \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ for $M \mid N$. If $M = 1$, we simply write $\mathbb{Z}/N\mathbb{Z}$. In addition, by Theorem 2.1 in [2] we know that if a torsion subgroup arises in degree d', then it arises in any degree d for which $d' \mid d$. We say a torsion subgroup is **new** if it occurs in degree d and not in any degree $d' < d$ such that $d' \mid d$.

Theorem 3. *Let F be a number field of degree $2p$ for $p > 3$ prime and E/F be a CM elliptic curve. If $E(F)[\text{tors}]$ is new and*

- $j(E) \neq 0$ *or* 1728*, then*

$$E(F)[\text{tors}] \cong \begin{cases} \mathbb{Z}/m\mathbb{Z} & m = 5, 8, 12, \text{ or } 2p+1, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z} & m = 2p+1, \end{cases}$$

- $j(E) = 1728$*, then*

$$E(F)[\text{tors}] \cong \begin{cases} \mathbb{Z}/m\mathbb{Z} & m = 4p+1, \\ \mathbb{Z}/2m\mathbb{Z} & m = 4p+1, \end{cases}$$

- $j(E) = 0$ *and* $p \neq 7$*, then*

$$E(F)[\text{tors}] \cong \begin{cases} \mathbb{Z}/m\mathbb{Z} & m = 6p+1, \end{cases}$$

- $j(E) = 0$ *and* $p = 7$*, then*

$$E(F)[\text{tors}] \cong \begin{cases} \mathbb{Z}/m\mathbb{Z} & m = 6p+1, \\ \mathbb{Z}/m^2\mathbb{Z} & m = 7, \end{cases}$$

where $2p+1$, $4p+1$, and $6p+1$ are primes greater than 3.

Theorem 3 tells us that if $j(E) \neq 0$ or 1728 the only torsion subgroups that can arise that did not occur over a number field of degree 2 or degree p must have the form $\mathbb{Z}/N\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2(2p+1)\mathbb{Z}$ with $N = 5, 8, 12$ or $2p+1$ where p is a Sophie Germain prime. Furthermore, if $j \neq 0$ or 1728 and $p > 3$ is not a Sophie Germain prime then the torsion that occurs in degree $2p$ is the same as that in degree 2. It is conjectured that there are infinitely many Sophie Germain primes, though this remains unproven. These primes were a vital piece of French mathematician Sophie Germain's investigations concerning Fermat's Last Theorem.

From this result, we can deduce the torsion subgroups that arise for the first previously unknown degree, $d = 14$. Notice 7 is not a Sophie Germain prime, so we need only consider $j = 0$ and $j = 1728$.

Theorem 4. *Let F be a number field of degree 14. Let E/F be a CM elliptic curve. The group $E(F)[\text{tors}]$ is isomorphic to one of the following:*

$$\begin{array}{ll} \mathbb{Z}/m\mathbb{Z} & 1 \leq m \leq 7 \text{ or } m = 10, 29, 43, 49, 58 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} & 1 \leq m \leq 3 \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} & \end{array}$$

In degree 2, $\mathbb{Z}/29\mathbb{Z}$, $\mathbb{Z}/43\mathbb{Z}$, $\mathbb{Z}/49\mathbb{Z}$, and $\mathbb{Z}/58\mathbb{Z}$ did not occur.

In this thesis we also classify the first known example of an even degree for which no new torsion subgroups arise. In degree $d = 22$ we see that the only torsion subgroups that occur are those that occur for $d = 2$. This finding is significant since in [8] we see many examples where F is a number field of odd degree and the torsion subgroups that appear are the same as those that appear over $\mathbb{Q}$ or another number field of lesser odd degree d' where d' is a proper divisor of d.

Theorem 5. *Let F be a number field of degree 22 and let E/F be a CM elliptic curve. Then $E(F)[\text{tors}]$ is isomorphic to one of the groups that arise for CM elliptic curves over quadratic fields.*

Chapter 2: Background

2.1 Elliptic Curves

Definition 1. Let K be a number field and $\overline{K}$ its algebraic closure. $\mathbb{A}^3$ denotes **affine 3-space** over K, which is the set of 3-tuples

$$\mathbb{A}^3 = \mathbb{A}^3(\overline{K}) = \{(x_1, x_2, x_3) : x_i \in \overline{K}\}.$$

Projective 2-space or simply **projective space**, denoted $\mathbb{P}^2$, is the set of all lines through $(0,0,0)$ in $\mathbb{A}^3$.

Definition 2. An **elliptic curve** E defined over a number field F is a curve in projective space that corresponds to solutions of a Weierstrass equation of the form

$$Y^2Z = X^3 + aXZ^2 + bZ^3, \tag{2.1}$$

where $a, b \in F$ and $-16(4a^3 + 27b^2) \neq 0$.

Requiring that $-16(4a^3 + 27b^2)$ be nonzero ensures that the corresponding curve is smooth so it does not have any cusps or self-intersections, as seen in Figure 2.1 and Figure 2.2 respectively.

Notice that if $Z = 0$ in equation 2.1 above, the only possible solution is $(0 : 1 : 0)$. This is the **point at infinity**, sometimes denoted O. Furthermore, if $Z \neq 0$, then we can simply scale the representatives of our point so that it is of the form $(x : y : 1)$. Thus, we instead may simply consider E to be the point at infinity and the solutions to $y^2 = x^3 + ax + b$ in affine space.

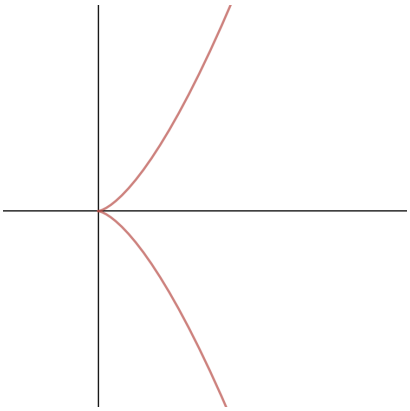


Figure 2.1: Graph of $y^2 = x^3$

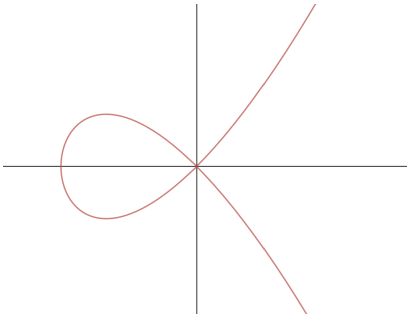


Figure 2.2: Graph of $y^2 = x^3 + x^2$

Definition 3. The **j-invariant** of an elliptic curve of the form $y^2 = x^3 + ax + b$ is

$$j := -1728\frac{(4a)^3}{-16(4a^3+27b^2)}.$$

We write $j(E)$ to denote the j-invariant of an elliptic curve E.

Proposition 1 ([5], p.45)**.** *Two elliptic curves have the same j-invariant if and only if they are isomorphic over $\overline{K}$, where $\overline{K}$ is the algebraic closure of a number field K.*

An impressive feature of elliptic curves is the fact that we may define a binary operation on the points of E so that they form an abelian group with identity O. The **group law** is as follows: Let P and Q be points on E. To compute $P+Q$ we must first draw a line l_1 through the two points. If $P = Q$, then we take l_1 to be the tangent line to the curve at P. We know, by a classical result of Bézout, that l_1 intersects E in exactly three points (counting multiplicity) and we let R denote that third point on E. Now we draw a second line l_2 through the point at infinity and R. Where l_2 intersects E is $P+Q$. This is illustrated in Figure 2.3.

Definition 4. A point P on an elliptic curve E is a **torsion point** of order n if adding P to itself n times yields the point at infinity and n is the least positive integer with this property. If no such n exists, then it has infinite order. $E[n]$ denotes the collection of all torsion points with order dividing n, that is

$$E[n] := \{P \in E : [n]P = O\}.$$

An element of $E[n]$ is often referred to as an n-torsion point.

Theorem 6 ([5], p.86)**.** *Let E be an elliptic curve over a number field K and let $n \in \mathbb{Z}^+$. Then*

$$E[n] = \frac{\mathbb{Z}}{n\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}.$$

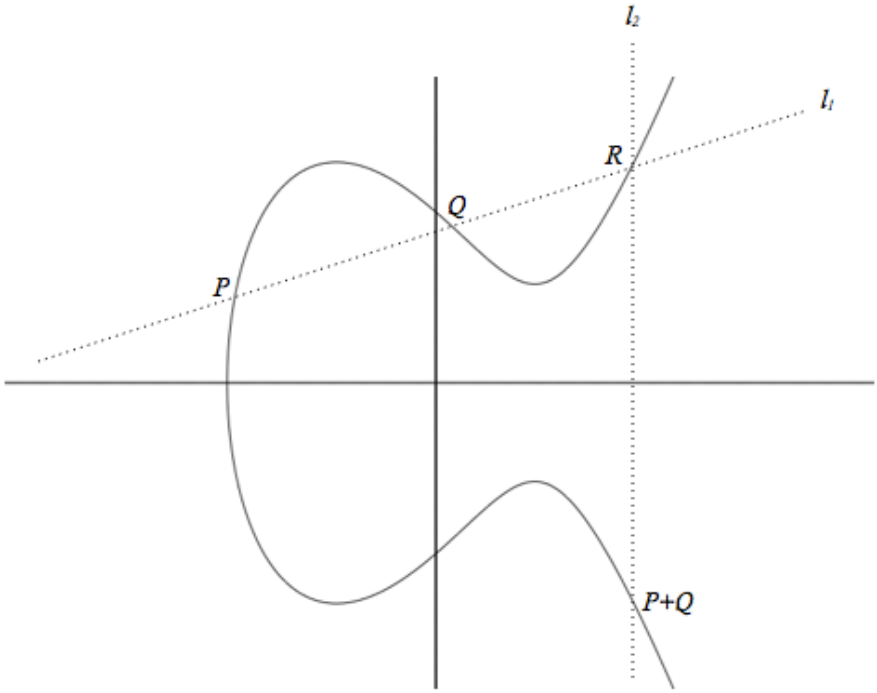


Figure 2.3: Elliptic Curve Group Law

Corollary 1. *Let E be an elliptic curve over a number field K. $E(K)[\text{tors}] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, where $m \mid n$.*

There is a connection between torsion and roots of unity that can be particularly helpful in classification problems. Recall an m^{th} root of unity is a root of the polynomial $x^m - 1$. We denote the group of the m^{th} roots of unity with μ_m.

Theorem 7 ([5], p.96)**.** *Let K be a number field and let E/K be an elliptic curve. If $E[m] \subset E(K)$, then $\mu_m \subset K^*$*

It will also be important to consider endomorphisms of elliptic curves.

Definition 5. An **endomorphism** of an elliptic curve, E, is a group homomorphism from E to itself that is locally defined by polynomials. The collection of endomorphisms for an elliptic curve E/F for some number field F form a ring, denoted $\text{End}_{\bar{F}}(E)$. Notice that

we are allowing the coefficients of these polynomials to be in $\bar{F}$. We use ω to denote the number of units in the endomorphism ring of E.

For most elliptic curves E defined over a number field F, $\mathrm{End}_{\bar{F}}(E) \cong \mathbb{Z}$. The usual endomorphisms for a point on E are multiplication by $n \in \mathbb{Z}$ maps. For example, if P is a point on our elliptic curve then $P \mapsto [n]P$ for $n \in \mathbb{Z}$. Thus, $\mathbb{Z}$ is always a subring of $\mathrm{End}_{\bar{F}}(E)$.

2.2 Algebraic Number Theory

The endomorphism ring of an elliptic curve with complex multiplication can be viewed as a subring of an imaginary quadratic field and so we recall some results about these fields from algebraic number theory. Recall a **quadratic field** is a number field K of degree 2 over $\mathbb{Q}$. We also know that $K = \mathbb{Q}(\sqrt{D})$ for D a squarefree element of $\mathbb{Z}$ (p. 522, [7]).

Definition 6. An element in K is an **algebraic integer** if it is a root of a monic polynomial with integer coefficients. The set of all algebraic integers in K is the **ring of integers**, denoted $\mathscr{O}_K$.

In fact, given a quadratic field, K, we can precisely describe the ring of integers for K.

Proposition 2 ([1], p.64)**.** *Let $K = \mathbb{Q}(\sqrt{D})$ for D squarefree. If $D \equiv 1 \pmod 4$ then $\mathscr{O}_K = \mathbb{Z}[\frac{1+\sqrt{D}}{2}]$ and if $D \equiv 2$ or $3 \pmod 4$ then $\mathscr{O}_K = \mathbb{Z}[\sqrt{D}]$.*

The discriminant of K, denoted Δ_K, can loosely be thought of as measuring the size of $\mathscr{O}_K$; see section 3.1 in [1] for details. In the case where K is quadratic, we can easily compute the discriminant via the following proposition.

Proposition 3 ([1], p.65)**.** *Let $K = \mathbb{Q}(\sqrt{D})$ where D is squarefree and Δ_K is discriminant of K.*

- *If $D \equiv 1 \pmod 4$ then $\Delta_K = D$.*

- *If* $D \equiv 2$, *or* $3 \pmod 4$ *then* $\Delta_K = 4D$.

If $D > 0$, then the group of units in the ring of integers of $\mathbb{Q}(\sqrt{D})$ is infinite. However, for so-called imaginary quadratic fields, the unit group has at most 6 elements.

Proposition 4. *The group of units* U *of the integers in* $\mathbb{Q}(\sqrt{d})$ *where* d *is negative and square free are as follows:*

- *For* $d = -1$, $U = \{\pm 1, \pm i\}$.
- *For* $d = -3$, $U = \{\pm 1, \pm w, \pm w^2\}$ *where* $w = e^{2\pi/3}$.
- *For all other* $d < 0$, $U = \{\pm 1\}$.

Proof. See Proposition 4.3 on page 79 in [1]. □

For a number field K, the class number, denoted h_K, is the order of the ideal class group. This group essentially measures the extent that $\mathscr{O}_K$ fails to be a principal ideal domain. In other words, h_K measures how non-unique factorization is in $\mathscr{O}_K$. For more information on class number see Chapter 9 of [1].

Definition 7. Suppose $K/\mathbb{Q}$ is a quadratic field, and let p be a rational prime. Note that $p\mathscr{O}_K$ is not necessarily a prime ideal. We say:

- that p is **ramified** in $\mathscr{O}_K$ if $p\mathscr{O}_K = \mathfrak{p}^2$ for a prime ideal $\mathfrak{p}$ of $\mathscr{O}_K$.
- that p is **inert** in $\mathscr{O}_K$ if $p\mathscr{O}_K = \mathfrak{p}$ for a prime ideal $\mathfrak{p}$ of $\mathscr{O}_K$.
- that p is **split** in $\mathscr{O}_K$ if $p\mathscr{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ for distinct prime ideals $\mathfrak{p}_1, \mathfrak{p}_2$ of $\mathscr{O}_K$.

For any prime p, the Kronecker symbol, $\left(\frac{\Delta_K}{p}\right)$, evaluates to 0 if p is ramified, -1 if p is inert, and 1 if p is split.

2.3 Elliptic Curves with Complex Multiplication

Elliptic curves with complex multiplication, often referred to as CM Elliptic curves, have extra structure because they have "more endomorphisms than expected." Recall that for most elliptic curves E/F, $\mathrm{End}_{\bar{F}}(E) \cong \mathbb{Z}$, since the usual endomorphisms are multiplication by n maps where $n \in \mathbb{Z}$.

Definition 8. An elliptic curve E defined over a number field F has **complex multiplication** if its endomorphism ring is larger than $\mathbb{Z}$.

Moreover, for a CM elliptic curve E/F, there is an imaginary quadratic field K such that $\mathrm{End}_{\bar{F}}(E) \cong \mathscr{O} = \mathbb{Z} + f\mathscr{O}_K$, the order in K of conductor f. Any order in an imaginary quadratic field can be uniquely identified using its discriminant, $\Delta = f^2 \cdot \Delta_K$. Clearly $\mathbb{Z} + f\mathscr{O}_K$ is a subring of $\mathscr{O}_K$ and therefore the largest it could possibly be is $\mathscr{O}_K$; this occurs when $f = 1$ and so we call $\mathscr{O}_K$ the maximal order. Recall that ω denotes the number of units in the endomorphism ring of E. Therefore, by Proposition 4 we have $\omega \in \{2,4,6\}$.

We say that an elliptic curve has CM by $\mathscr{O}$ when the endomorphism ring of E is isomorphic to $\mathscr{O}$. For example, the elliptic curve $y^2 = x^3 + 1$ has CM by the maximal order in $\mathbb{Q}(\sqrt{-3})$ and thus there is an extra endomorphism:

$$(x,y) \mapsto \left(\frac{-1+\sqrt{-3}}{2}x, y\right).$$

2.4 Divisibility Conditions for Torsion on CM Elliptic Curves

The study of torsion for CM elliptic curves has developed significantly in recent years and the following are theoretical results that are critical to the proofs of this thesis.

Theorem 8. *(Theorem 4.1, [4]). Let K be an imaginary quadratic field, and let $\mathscr{O}$ be the order in K of conductor f. Let $M = \ell_1^{a_1} \cdots \ell_r^{a_r} \mid N = \ell_1^{b_1} \cdots \ell_r^{b_r}$ where $\ell_1 < \cdots < \ell_r$ are prime numbers and a_i, b_i are nonnegative integers.*

1. *There is $T(\mathscr{O},M,N) \in \mathbb{Z}^+$ such that: for all $d \in \mathbb{Z}^+$, there is a number field $F \supset K(j(E))$ such that $[F : K(j(E))] = d$ and an $\mathscr{O}$-CM elliptic curve $E_{/F}$ such that $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow E(F)$ iff $T(\mathscr{O},M,N) \mid d$.*

2. *If $N = 2$ or 3, then $T(\mathscr{O},M,N)$ is as follows:*

$$T(\mathscr{O},1,2) = \begin{cases} 3 & \left(\frac{\Delta}{2}\right) = -1 \text{ and } \Delta \neq -3 \\ 1 & \text{otherwise} \end{cases},$$

$$T(\mathscr{O},1,3) = \begin{cases} 8/\omega & \left(\frac{\Delta}{3}\right) = -1 \\ 1 & \text{otherwise} \end{cases},$$

$$T(\mathscr{O},2,2) = \frac{2(2-\left(\frac{\Delta}{2}\right))}{\omega},$$

$$T(\mathscr{O},3,3) = \frac{2(3-\left(\frac{\Delta}{3}\right))}{\omega}.$$

3. *If $N = 2$, then $\widetilde{T}(\mathscr{O},M,N)$ is as follows:*

$$\widetilde{T}(\mathscr{O},1,2) = \begin{cases} 1 & \left(\frac{\Delta}{2}\right) \neq -1 \\ 3 & \left(\frac{\Delta}{2}\right) = -1 \end{cases},$$

$$\widetilde{T}(\mathscr{O},2,2) = 2 - \left(\frac{\Delta}{2}\right).$$

4. *Suppose $N \geq 3$ and $r = 1$, and write $M = \ell^a$, $N = \ell^b$ for $0 \leq a \leq b$. Put $c := \mathrm{ord}_\ell(f)$. Then:*

   i) If $\left(\frac{\Delta}{\ell}\right) = -1$, then

$$\widetilde{T}(\mathscr{O},\ell^a,\ell^b) = \ell^{2b-2}(\ell^2-1).$$

   ii) If $\left(\frac{\Delta}{\ell}\right) = 1$, then

$$\widetilde{T}(\mathscr{O},\ell^a,\ell^b) = \begin{cases} \ell^{b-1}(\ell-1) & a = 0 \\ \ell^{a+b-2}(\ell-1)^2 & a \geq 1 \end{cases}.$$

iii) If $\ell \mid \mathfrak{f}$ *and* $\left(\frac{\Delta_K}{\ell}\right) = 1$*, then*

$$\widetilde{T}(\mathscr{O}, \ell^a, \ell^b) = \ell^{a+b-1}(\ell - 1).$$

iv) If $\left(\frac{\Delta_K}{\ell}\right) = 0$*, then*

$$\widetilde{T}(\mathscr{O}, \ell^a, \ell^b) = \begin{cases} \ell^{a+b-1}(\ell-1) & b \leq 2c+1 \\ \ell^{\max(a+b-1, 2b-2c-2)}(\ell-1) & b > 2c+1 \end{cases}.$$

v) If $\ell \mid f$ *and* $\left(\frac{\Delta_K}{\ell}\right) = -1$*, then*

$$\widetilde{T}(\mathscr{O}, \ell^a, \ell^b) = \begin{cases} \ell^{a+b-1}(\ell-1) & b \leq 2c \\ \ell^{\max(a+b-1, 2b-2c-1)}(\ell-1) & b > 2c \end{cases}.$$

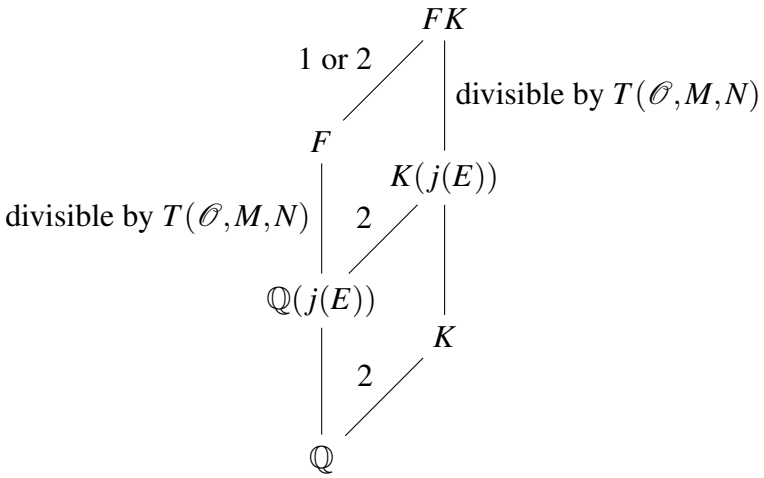
5. Suppose $N \geq 4$*. Then we have*

$$T(\mathscr{O}, M, N) = \frac{\prod_{i=1}^{r} \widetilde{T}(\mathscr{O}, \ell_i^{a_i}, \ell_i^{b_i})}{\omega}.$$

Corollary 2. *Let* $\mathscr{O}$ *be an order in an imaginary quadratic field* K*, and let* E *be an* $\mathscr{O}$*-CM elliptic curve defined over a number field* $F \supset K$*. If* $E(F)$ *has a point of order* $N \in \mathbb{Z}^+$*, then*

$$\varphi(N) \mid \omega \cdot [F : \mathbb{Q}].$$

Furthermore, note that the divisibility conditions in Theorem 8 are over $K(j(E))$ and thus are weakest when $j(E) \in \mathbb{Q}$. There are exactly 13 such j-invariants; see [5]. We also recall that $[K(j(E)) : K] = [\mathbb{Q}(j(E)) : \mathbb{Q}]$ since $\mathbb{Q}(j(E))$ has a real embedding, so we can actually consider these divisibility conditions in Theorem 8 over $\mathbb{Q}(j(E))$. This is illustrated by the field diagram below. In fact, if we have CM by the maximal order in K then $[K : K(j(E))] = h_K$ by Theorem 11.1 in [18].



In [4] they also give explicit formulas for computing $T^o(\mathscr{O},M,N)$, the least degree over $\mathbb{Q}(j)$ in which we can have a point of order N. Note that if we have $j(E) \in \mathbb{Q}$, the least degree over $\mathbb{Q}$ is also $T^o(\mathscr{O},M,N)$.

Chapter 3: Results

From Corollary 1 we know that if F is a number field of degree $2p$ for $p > 3$ prime and E/F a CM elliptic curve then $E(F)[\text{tors}] \cong \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ where $M \mid N$. Consequently, in order to completely classify what $E(F)[\text{tors}]$ occur we must determine the possibilities for N and M. We begin with a preliminary lemma and then work to rule out what N cannot be before constructing the possibilities for N and corresponding M.

3.1 Preliminaries

Lemma 1. *Let $\mathscr{O}$ be the order of discriminant Δ and let $\ell_1^{a_1} \cdots \ell_n^{a_n}$ denote the prime power decomposition of $N \geq 4$. If $\frac{\varphi(N)}{\omega} = d$, then, in order to have a point of order N occur in degree d, we must have $\left(\frac{\Delta}{\ell}\right) = 0$ for every odd prime $\ell \mid N$. Furthermore, if the largest power of two dividing N is 2, then two may be split but otherwise 2 must also be ramified.*

Proof. Suppose $\frac{\varphi(N)}{\omega} = d$ and $T^o(\mathscr{O},1,N) = d$ for some $N \geq 4$. By Theorem 8 we know $T(\mathscr{O},1,N)$ divides d but we also know that $\frac{\varphi(N)}{\omega}$ must divide $T(\mathscr{O},1,N)$. Thus, $\frac{\varphi(N)}{\omega} = T(\mathscr{O},1,N)$. Consider some prime power $\ell_i^{a_i} \geq 3$ with $\ell_i^{a_i} \mid N$.

If $\left(\frac{\Delta}{\ell}\right) = 1$, then by Theorem 1.3 and Theorem 6.2 in [4] we must have $T^o(\mathscr{O},1,N) = 2 \cdot T(\mathscr{O},1,N)$. This implies that $T^o(\mathscr{O},1,N) = 2d$ and therefore we have reached a contradiction.

Suppose $\left(\frac{\Delta}{\ell}\right) = -1$. Recall from Theorem 8 that

$$T(\mathscr{O},1,N) = \frac{\prod_{i=1}^{r} \widetilde{T}(\mathscr{O},1,\ell_i^{a_i})}{\omega}.$$

Since $\frac{\varphi(N)}{\omega} = d$, and therefore $T(\mathscr{O},1,N) = d$, we must have that $\varphi(N) = \prod_{i=1}^{r} \widetilde{T}(\mathscr{O},1,\ell_i^{a_i})$.

Moreover, we must have $\varphi(\ell^a) = \widetilde{T}(\mathscr{O},1,\ell^a)$. By Theorem 8 we have

$$\tilde{T}(\mathscr{O},1,\ell^a) = \ell^{2a-2}(\ell^2-1) = (\ell^{a-1})(\ell^{a-1})(\ell-1)(\ell+1).$$

Furthermore, since ℓ is prime, we have $\varphi(\ell^a) = \ell^{a-1}(\ell-1)$. Thus, $\varphi(\ell^a) < \widetilde{T}(\mathscr{O},1,\ell^a)$. Consequently, if any $\ell \mid N$ is inert then $T(\mathscr{O},1,N) > d$ and therefore we have reached a contradiction.

Behold, the only possible way to have $\frac{\varphi(N)}{\omega} = d$ and $T^o(\mathscr{O},1,N) = d$ is if every prime divisor of N is ramified. □

3.2 Eliminating Possibilities for N

Theorem 9. *If N is divisible by two or more distinct primes greater than three, then a point of order N does not occur in degree $2p$ for p prime.*

Proof. Suppose $\ell_1\ell_2 \mid N$ for distinct primes $\ell_1,\ell_2 > 3$. Since ℓ_1 and ℓ_2 are prime we know that $(\ell_1-1)(\ell_2-1) \mid \varphi(N)$ and given that $\ell_1,\ell_2 > 3$ we can write $\ell_1 = 2k_1+1$ and $\ell_2 = 2k_2+1$ for distinct integers $k_1,k_2 > 1$. Recall that by Corollary 2 to have a point of order N occur in degree $2p$ we must have that $\varphi(N) \mid \omega \cdot 2p$. Thus, we need $2k_1k_2$ to divide $\omega \cdot p$.

If $\omega = 2$, then to have a point of order N, we must have $k_1k_2 \mid p$. However, we have a contradiction because a composite k_1k_2 will not divide a prime p.

If $\omega = 4$, then to have a point of order N we must have $k_1k_2 \mid 2p$. Since a composite k_1k_2 will not divide a prime p we must have that $k_1k_2 = 2p$. This implies that $5(2p+1) \mid N$ for $2p+1$ prime. Notice that $\frac{\varphi(5(2p+1))}{\omega} = 2p$ and therefore, by Lemma 1, we must have 5 and $2p+1$ are both ramified. Since $\omega = 4$ we know that the only ramified prime is the prime 2 and therefore we have reached a contradiction.

If $\omega = 6$, then to have a point of order N, we need $k_1k_2 \mid 3p$. Again, since a composite k_1k_2 will not divide a prime p we must have that $k_1k_2 = 3p$. This implies that $7(2p+1) \mid N$ for $2p+1$ prime. Notice that $\frac{\varphi(7(2p+1))}{\omega} = 2p$ and therefore, by Lemma 1, we must have 7 and $2p+1$ are both ramified. Since $\omega = 6$ we know that the only ramified prime is the prime 3 and therefore we have reached a contradiction.

Hence, if N is divisible by two distinct primes greater than three, then a point of order N does not occur in degree $2p$. □

Remark. *By the previous theorem, if a point of order N occurs in degree $2p$, we must have $N = 2^a \cdot 3^b \cdot \ell^c$ where $a,b,c \geq 0$ are integers and prime $\ell > 3$.*

Theorem 10. *If $\ell^2 \mid N$ for a prime $\ell > 3$, then a point of order N does not occur in degree $2p$ for $p \neq 7$. If $p = 7$, then a point of order $N = 49$ occurs in degree 14.*

Proof. Suppose $\ell^2 \mid N$ for a prime $\ell > 3$. Given that $\ell > 3$ is prime we know that $\ell(\ell-1) \mid \varphi(N)$ and since ℓ is odd we can write $\ell = 2k+1$ for some integer $k > 1$. Recall that to have a point of order N in degree $2p$ we must have that $\varphi(N) \mid \omega \cdot 2p$. Therefore, we need $(2k+1)k \mid \omega \cdot p$.

If $\omega = 2$, then to have a point of order N we need $k(2k+1) \mid 2p$. This implies we must have $k(2k+1) = 2p$ and consequently $25 \mid N$ in $d = 10$. However, using Theorem 8 we see that if $\left(\frac{\Delta}{5}\right) = -1$, then $T(\mathscr{O},1,25) = 600 \nmid 10$ and thus, 5 cannot be inert. If $\left(\frac{\Delta}{5}\right) = 1$ then $T(\mathscr{O},1,25) = 10$. But by Theorem 1.3 and 6.2 in [4] we see that $T^o(\mathscr{O},1,25) = 20 > 10$. So the only possibility remaining is for $\left(\frac{\Delta}{5}\right) = 0$. Again, by Theorem 8 we find that $T(\mathscr{O},1,25) = 10$. However, this forces $h_K = 1$ and 5 is never ramified in an imaginary quadratic field of class number one. Thus, $\omega \neq 2$. Notice, that in [6] $N \neq 25$ in degree 10.

If $\omega = 4$, then to have a point of order N we need $k(2k+1) \mid 4p$. Therefore, we must have $k(2k+1) = 2p$ or $4p$. Suppose $k(2k+1) = 4p$. This implies that $k = 4$ and $\ell = 9$ but this is a contradiction because ℓ is, by assumption, prime. Therefore, we must have

$k(2k+1) = 2p$. This implies that $k = 2$, and $\ell = p = 5$. But using Theorem 8 we see that $T(\mathscr{O}, 1, 25) = 10$ because $\left(\frac{-4}{5}\right) = 1$. However, using Theorem 1.3 and Theorem 6.2 in [4] we see that $T^o(\mathscr{O}, 1, 25) = 20 > 10$. Thus, $\omega \neq 4$.

If $\omega = 6$, then to have a point of order N we need $k(2k+1) \mid 6p$. Therefore, we must have $k(2k+1) = 2p, 3p$ or $6p$. If $k(2k+1) = 2p$, then $k = 2$, and $\ell = p = 5$. Since $\omega = 6$ we know that $\Delta = -3$ and have $\left(\frac{-3}{5}\right) = -1$, therefore Theorem 8 gives us that $T(\mathscr{O}, 1, 25) = 600 \nmid 10$ and we have a contradiction. If $k\ell^{x-1} = 6p$, then $k = 6$ and $\ell = p = 13$. Since $\left(\frac{-3}{13}\right) = 1$, by Theorem 8 we see that $T(\mathscr{O}, 1, 169) = 156 \nmid 26$ and again we have a contradiction. Consider the last remaining possible case where $k\ell^{x-1} = 3p$. This implies that $k = 3$, $\ell = p = 7$. But $p \neq 7$ by assumption and so $k\ell^{x-1} \neq 3p$. However, if $p = 7$ then since $\left(\frac{-3}{7}\right) = 1$, we have $T(\mathscr{O}, 1, 49) = 7$ by Theorem 8 and by Theorem 1.3 and Theorem 6.2 in [4], $T^o(\mathscr{O}, 1, 49) = 14$. Again, since we are in the case where $\omega = 6$, we know what $\mathscr{O}$ is and know it corresponds to elliptic curve with $j(E) \in \mathbb{Q}$. Notice, that this is the only possibility and we saw that this appeared in Theorem 4 where we computed degree 14.

Hence, if $\ell^2 \mid N$ for prime $\ell > 3$, then a point of order N does not occur in degree $2p$ for $p \neq 7$. □

Remark. *First suppose $p \neq 7$. By the theorems above, if a point of order N occurs in degree $2p$ for prime $p > 3$, then we must have $N = 2^a \cdot 3^b \cdot \ell$ or $N = 2^a 3^b$ where $a, b \geq 0$ are integers and $\ell > 3$ is prime. If $p = 7$, then it is also possible for $N = 2^a \cdot 3^b \cdot 7^2$ but only in the case where $\Delta = -3$.*

Theorem 11. *If $2 \cdot \ell^2 \mid N$ for prime $\ell > 3$, then a point of order N does not occur in degree $2p$ for p prime.*

Proof. By Theorem 10 we know that if $\ell > 3$ is prime and $\ell^2 \mid N$ then $\ell = 7$, $p = 7$, and $\omega = 6$. Thus, it suffices to show that if $2 \cdot 7^2 \mid N$, then a point of order N does not occur in degree 14. Suppose $\ell = 7$ and $2 \cdot 7^2 \mid N$. Since $\omega = 6$ we know that $\Delta = -3$ and note that

$\left(\frac{-3}{7}\right) = 1$ and $\left(\frac{-3}{2}\right) = -1$. So, using Theorem 8, we have $T(\mathscr{O}, 1, 98) = 21 \nmid 14$. Hence, we have our contradiction. □

Remark. *First suppose $p \neq 7$. By the theorems above, if a point of order N occurs in degree $2p$ for prime $p > 3$, then we must have $N = 2^a \cdot 3^b \cdot \ell$ or $N = 2^a 3^b$ where $a, b \geq 0$ are integers and $\ell > 3$ is prime. If $p = 7$, then it is also possible for $N = 3^b \cdot 7^2$ but only in the case where $\Delta = -3$.*

Theorem 12. *If $3 \cdot \ell^2 \mid N$ for prime $\ell > 3$, then a point of order N does not occur in degree $2p$ for p prime.*

Proof. By Theorem 10 we know that if $\ell > 3$ is prime and $\ell^2 \mid N$ then $\ell = 7$, $p = 7$, and $\omega = 6$. Thus, it suffices to show that if $3 \cdot 7^2 \mid N$, then a point of order N does not occur in degree 14. Suppose $\ell = p = 7$ and $3 \cdot 7^2 \mid N$. Since $\omega = 6$ we know that $\Delta = -3$ and note that $\left(\frac{-3}{7}\right) = 1$ and $\left(\frac{-3}{3}\right) = 0$. So, using Theorem 8, we have $T(\mathscr{O}, 1, 147) = 14 \mid 14$. But since $\left(\frac{-3}{7}\right) = 1$ we know, by Theorem 1.3 and Theorem 6.2 in [4], that $T^o(\mathscr{O}, 1, 147) = 28 > 14$. Hence, we have our contradiction. □

Remark. *First suppose $p \neq 7$. By the theorems above, if a point of order N occurs in degree $2p$ for prime $p > 3$, then we must have $N = 2^a \cdot 3^b \cdot \ell$ or $N = 2^a 3^b$ where $a, b \geq 0$ are integers and $\ell > 3$ is prime. If $p = 7$, then it is also possible for $N = 7^2$ but only in the case where $\Delta = -3$.*

Theorem 13. *If $4\ell \mid N$ for a prime $\ell > 3$, then a point of order N does not occur in degree $2p$ for p prime.*

Proof. Suppose $4\ell \mid N$ for a prime $\ell > 3$. Given that $\ell > 3$ is prime we know that $2(\ell - 1) \mid \varphi(N)$ and since ℓ is odd we can write $\ell = 2k + 1$ for some integer $k > 1$. Recall that to have a point of order N in degree $2p$ we must have that $\varphi(N) \mid \omega \cdot 2p$. Therefore, we need $2k \mid \omega \cdot p$. Furthermore note that if we have a point P of order N defined over a number field

F where $4\ell \mid N$, then $\frac{N}{4\ell}P$ is a point of order 4ℓ defined over F. So $T(\mathscr{O},1,4\ell) \mid [F:\mathbb{Q}]$. We will use Theorem 8 to construct the possibilities for $T(\mathscr{O},1,4\ell) \mid 2p$.

If $\omega = 2$, then to have a point of order N we need $k \mid p$. This implies we must have $k = p$ and therefore $4(2p+1) \mid N$. By Theorem 8 if $\left(\frac{\Delta}{2}\right) = 0$ then $\widetilde{T}(\mathscr{O},1,4) = 4$, if $\left(\frac{\Delta}{2}\right) = 1$ then $\widetilde{T}(\mathscr{O},1,4) = 2$, and if $\left(\frac{\Delta}{2}\right) = -1$ then $\widetilde{T}(\mathscr{O},1,4) = 12$. Similarly, if $\left(\frac{\Delta}{2p+1}\right) = 1$ or $\left(\frac{\Delta}{2p+1}\right) = 0$ then $\widetilde{T}(\mathscr{O},1,2p+1) = 2p$ but if $\left(\frac{\Delta}{2p+1}\right) = -1$ then $\widetilde{T}(\mathscr{O},1,2p+1) = 4p(p+1)$. Recall, in order to have a point of order N in degree $2p$ we must have $T(\mathscr{O},M,N) \mid 2p$. Thus, we must have $\widetilde{T}(\mathscr{O},1,2p+1) = 2p$ and $\widetilde{T}(\mathscr{O},1,4) = 2$ so that $T(\mathscr{O},1,4(2p+1)) = 2p \mid 2p$. However, in order to have $T(\mathscr{O},1,4(2p+1)) = 2p$ we must have $\left(\frac{\Delta}{2}\right) = 1$ and therefore by Theorem 1.3 and Theorem 6.2 in [4] we have that $T^o(\mathscr{O},1,4(2p+1)) = 4p > 2p$. Hence, we have our contradiction.

If $\omega = 4$, then to have a point of order N we need $k \mid 2p$. This implies we must have $\ell = 5, 2p+1$, or $4p+1$. Notice that $4\ell \mid N$ implies $T(\mathscr{O},1,4\ell) \mid T(\mathscr{O},M,N)$. We use Theorem 8 to construct the possibilities for $\widetilde{T}(\mathscr{O},1,\ell)$ and $\widetilde{T}(\mathscr{O},1,4)$. Since $\omega = 4$ we know that $\Delta = -4$ and have $\left(\frac{\Delta}{2}\right) = 0$ so $\widetilde{T}(\mathscr{O},1,4) = 4$. If $\ell = 5$, then $\widetilde{T}(\mathscr{O},1,5) = 4$, because $\left(\frac{-4}{5}\right) = 1$, and therefore $T(\mathscr{O},M,20) = 4 \nmid 2p$. If $\ell = 2p+1$ then $\left(\frac{\Delta}{\ell}\right) = \pm 1$ since 2 is the only ramified prime when $\Delta = -4$. If $\left(\frac{\Delta}{\ell}\right) = 1$ then $\widetilde{T}(\mathscr{O},1,2p+1) = 2p$, and therefore $T(\mathscr{O},2,4(2p+1)) = 2p$. However, since $\left(\frac{\Delta}{\ell}\right) = 1$ by Theorem 1.3 and Theorem 6.2 in [4] we have that $T^o(\mathscr{O},2,4(2p+1)) = 4p > 2p$, a contradiction. If $\left(\frac{\Delta}{\ell}\right) = -1$ then $\widetilde{T}(\mathscr{O},1,2p+1) = 4p(p+1)$. Therefore $T(\mathscr{O},2,4(2p+1)) = 4p(p+1) \nmid 2p$, and we have a contradiction. Similarly, if $\ell = 4p+1$ then $\left(\frac{\Delta}{\ell}\right) = \pm 1$, and $T(\mathscr{O},2,4(4p+1)) = 4p \nmid 2p$ or $T(\mathscr{O},2,4(4p+1)) = 8p(p+1) \nmid 2p$. Hence, $\omega \neq 4$.

If $\omega = 6$, then to have a point of order N we need $k \mid 3p$. This implies we must have $\ell = 7, 2p+1$, or $6p+1$. Recall that $4\ell \mid N$ implies $T(\mathscr{O},1,4\ell) \mid T(\mathscr{O},M,N)$. We use Theorem 8 to construct the possibilities for $\widetilde{T}(\mathscr{O},1,\ell)$ and $\widetilde{T}(\mathscr{O},1,4)$. Since $\omega = 6$ we know that

$\Delta = -3$ and have $\left(\frac{\Delta}{2}\right) = -1$ so $\widetilde{T}(\mathscr{O},1,4) = 12$. If $\ell = 7$, then $\widetilde{T}(\mathscr{O},1,7) = 6$, because $\left(\frac{-3}{7}\right) = 1$, and therefore $T(\mathscr{O},1,21) = 12 \nmid 2p$. If $\ell = 2p+1$ then $\left(\frac{\Delta}{\ell}\right) = \pm 1$ since 3 is the only ramified prime when $\Delta = -3$. If $\left(\frac{\Delta}{\ell}\right) = 1$ then $\widetilde{T}(\mathscr{O},1,2p+1) = 2p$, and therefore $T(\mathscr{O},1,4(2p+1)) = 4p \nmid 2p$, a contradiction. If $\left(\frac{\Delta}{\ell}\right) = -1$ then $\widetilde{T}(\mathscr{O},1,2p+1) = 4p(p+1)$. Therefore $T(\mathscr{O},1,4(2p+1)) = 8p(p+1) \nmid 2p$, and we have another contradiction. Similarly, if $\ell = 6p+1$ then $\left(\frac{\Delta}{\ell}\right) = \pm 1$, and $T(\mathscr{O},2,4(6p+1)) = 12p \nmid 2p$ or $T(\mathscr{O},2,4(6p+1)) = 24p(3p+1) \nmid 2p$. Hence, $\omega \neq 6$. □

Remark. *Thus far we have proved that, when $p \neq 7$, if a point of order N occurs in degree $2p$ for prime $p > 3$, we must have $N = 2^a \cdot 3^b$, $N = 3^b \cdot \ell$, or $N = 2 \cdot 3^b \cdot \ell$ where $a, b \geq 0$ are integers and $\ell > 3$ is prime. If $p = 7$, then it is also possible for $N = 7^2$ but only in the case where $\Delta = -3$.*

Theorem 14. *If $3\ell \mid N$ for a prime $\ell > 3$, then a point of order N does not occur in degree $2p$ for prime $p > 3$.*

Proof. Suppose $3\ell \mid N$ for a prime $\ell > 3$. Given that $\ell > 3$ is prime we know that $2(\ell-1) \mid \varphi(N)$ and since ℓ is odd we can write $\ell = 2k+1$ for some integer $k > 1$. Recall that to have a point of order N in degree $2p$ we must have that $\varphi(N) \mid \omega \cdot 2p$. Therefore, we need $2k \mid \omega \cdot p$. Furthermore note that if we have a point P of order N defined over a number field F where $3\ell \mid N$, then $\frac{N}{3\ell}P$ is a point of order 3ℓ defined over F. So $T(\mathscr{O},1,3\ell) \mid [F : \mathbb{Q}]$. We will use Theorem 8 to construct the possibilities for $T(\mathscr{O},1,3\ell) \mid 2p$.

If $\omega = 2$, then to have a point of order N we need $k \mid p$. This implies we must have $k = p$ and therefore $3(2p+1) \mid N$. We use Theorem 8 to construct the possibilities for $\widetilde{T}(\mathscr{O},1,2p+1)$ and $\widetilde{T}(\mathscr{O},1,3)$. If $\left(\frac{\Delta}{3}\right) = 1$ or $\left(\frac{\Delta}{3}\right) = 0$ then $\widetilde{T}(\mathscr{O},1,3) = 2$ and if $\left(\frac{\Delta}{3}\right) = -1$ then $\widetilde{T}(\mathscr{O},1,3) = 8$. Similarly, if $\left(\frac{\Delta}{2p+1}\right) = 1$ or $\left(\frac{\Delta}{2p+1}\right) = 0$ then $\widetilde{T}(\mathscr{O},1,2p+1) = 2p$ but if $\left(\frac{\Delta}{2p+1}\right) = -1$ then $\widetilde{T}(\mathscr{O},1,2p+1) = 4p(p+1)$. Recall, in order to have a point of order

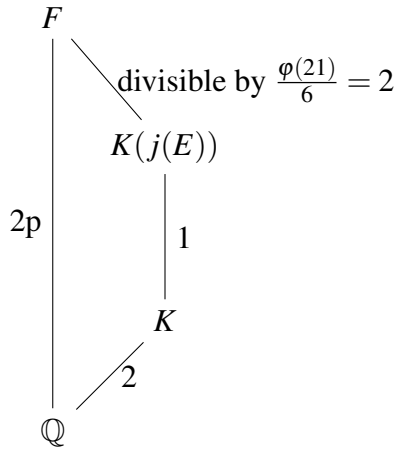
N in degree $2p$ we must have $T(\mathscr{O},1,N) \mid 2p$. Thus, we must have $\widetilde{T}(\mathscr{O},1,2p+1) = 2p$ and $\widetilde{T}(\mathscr{O},1,3) = 2$ so that $T(\mathscr{O},1,3(2p+1)) = 2p \mid 2p$. However, if $\left(\frac{\Delta}{2p+1}\right) = 1$ or $\left(\frac{\Delta}{3}\right) = 1$, then by Theorem 1.3 and Theorem 6.2 in [4] we have that $T^o(\mathscr{O},1,3(2p+1)) = 4p > 2p$ and have a contradiction. Therefore, to have $T^o(\mathscr{O},1,3(2p+1)) = 2p$ we must have that $2p+1$ and 3 are ramified. However, since $T(\mathscr{O},1,3(2p+1)) = 2p$ this forces $h_K = 1$ and there is not an imaginary quadratic field of class number one where $2p+1$ and 3 are both ramified. Thus, $\omega \neq 2$.

If $\omega = 4$, then to have a point of order N we need $k \mid 2p$. This implies we must have $\ell = 5, 2p+1$, or $4p+1$. Notice that $3\ell \mid N$ implies $T(\mathscr{O},1,3\ell) \mid T(\mathscr{O},M,N)$. We use Theorem 8 to construct the possibilities for $\widetilde{T}(\mathscr{O},1,\ell)$ and $\widetilde{T}(\mathscr{O},1,3)$. Since $\omega = 4$ we know that $\Delta = -4$ and have $\left(\frac{\Delta}{3}\right) = -1$ so $\widetilde{T}(\mathscr{O},1,3) = 8$. If $\ell = 5$, then $\widetilde{T}(\mathscr{O},1,5) = 4$, because $\left(\frac{-4}{5}\right) = 1$, and therefore $T(\mathscr{O},1,15) = 8 \nmid 2p$. If $\ell = 2p+1$ then $\left(\frac{\Delta}{\ell}\right) = \pm 1$ since 2 is the only ramified prime when $\Delta = -4$. If $\left(\frac{\Delta}{\ell}\right) = 1$ then $\widetilde{T}(\mathscr{O},1,2p+1) = 2p$, and therefore $T(\mathscr{O},1,3(2p+1)) = 4p \nmid 2p$ and we have a contradiction. If $\left(\frac{\Delta}{\ell}\right) = -1$ then $\widetilde{T}(\mathscr{O},1,2p+1) = 4p(p+1)$. Therefore $T(\mathscr{O},1,3(2p+1)) = 8p(p+1) \nmid 2p$, and we have another contradiction. Similarly, if $\ell = 4p+1$ then $\left(\frac{\Delta}{\ell}\right) = \pm 1$, and if $\left(\frac{\Delta}{\ell}\right) = 1$ then $T(\mathscr{O},3,3(4p+1)) = 8p \nmid 2p$ and if $\left(\frac{\Delta}{\ell}\right) = -1$ then $T(\mathscr{O},3,3(4p+1)) = 16p(2p+1) \nmid 2p$. Hence, $\omega \neq 4$.

If $\omega = 6$, then to have a point of order N we need $k \mid 3p$. This implies we must have $\ell = 7, 2p+1$, or $6p+1$. Recall that $3\ell \mid N$ implies $T(\mathscr{O},1,3\ell) \mid T(\mathscr{O},M,N)$. We use Theorem 8 to construct the possibilities for $\widetilde{T}(\mathscr{O},1,\ell)$ and $\widetilde{T}(\mathscr{O},1,3)$. Since $\omega = 6$ we know that $\Delta = -3$ and have $\left(\frac{\Delta}{3}\right) = 0$ so $\widetilde{T}(\mathscr{O},1,3) = 2$.

If $\ell = 7$, then $\widetilde{T}(\mathscr{O},1,7) = 6$, because $\left(\frac{-3}{7}\right) = 1$, and therefore $T(\mathscr{O},1,21) = 2 \mid 2p$. We consider two cases. Suppose $F \not\supset K$ then by Proposition 6.3(a) in [4] $\frac{\varphi(7)^2}{\omega} \mid 2p$ that is 6 should divide $2p$ and since $p > 3$ we have a contradiction. So in order to have a point of order $N = 21$ we must have $F \supset K$. Note that since $\omega = 6$ we have $h_K = 1$ and therefore

$[F:K] = [F:K(j(E))]$. We know that $[K:\mathbb{Q}] = 2$ and that $\frac{\varphi(21)}{6} \mid [F:K]$ and thus since $\frac{\varphi(21)}{6} = 2$ we must have that $4 \mid [F:\mathbb{Q}] = 2p$. Thus, we have a contradiction so $N \neq 21$ and $\ell \neq 7$. This is illustrated by the field diagram below.



If $\ell = 2p+1$ then $\left(\frac{\Delta}{\ell}\right) = \pm 1$ since 3 is the only ramified prime when $\Delta = -3$. If $\left(\frac{\Delta}{\ell}\right) = -1$ then $\widetilde{T}(\mathscr{O}, 1, 2p+1) = 4p(p+1)$. Therefore $T(\mathscr{O}, 1, 3(2p+1)) = p(p+1) \nmid 2p$, and we have a contradiction. If $\left(\frac{\Delta}{\ell}\right) = 1$ then $\widetilde{T}(\mathscr{O}, 1, 2p+1) = 2p$, and therefore $T(\mathscr{O}, 1, 3(2p+1)) = \frac{2p}{3}$. However, $T(\mathscr{O}, M, N)$ is an integer and since $p > 3$ this shows that $\left(\frac{\Delta}{\ell}\right) \neq 1$. Thus, $\ell \neq 2p+1$.

If $\ell = 6p+1$ then $\left(\frac{\Delta}{\ell}\right) = \pm 1$, again since 3 is the only ramified prime when $\Delta = -3$. If $\left(\frac{\Delta}{\ell}\right) = 1$ then $\widetilde{T}(\mathscr{O}, 1, 6p+1) = 6p$, and therefore $T(\mathscr{O}, 1, 3(6p+1)) = 2p \mid 2p$. However, since $\left(\frac{\Delta}{\ell}\right) = 1$ by Theorem 1.3 and Theorem 6.2 in [4] we have that $T^o(\mathscr{O}, 3, 3(6p+1)) = 4p > 2p$ and we have a contradiction. Similarly, if $\left(\frac{\Delta}{\ell}\right) = -1$ then $\widetilde{T}(\mathscr{O}, 1, 6p+1) = 12p(3p+1)$ and therefore $T(\mathscr{O}, 1, 3(6p+1)) = 4p(3p+1) \nmid 2p$ and, again, we have a contradiction. Hence, $\omega \neq 6$. □

Remark. *By now we have shown that, provided $p \neq 7$, if a point of order N occurs in degree $2p$ for prime $p > 3$, we must have $N = 2^a \cdot 3^b$, $N = \ell$, or $N = 2 \cdot \ell$ where $a, b \geq 0$ are integers and $\ell > 3$ is prime. If $p = 7$, then it is also possible for $N = 7^2$ but only in the case*

where $\Delta = -3$.

3.3 Possible N

Definition 9. Let N denote the order of a point P on E. We say that N is **new** in degree $2p$ if a point of order N occurs in degree $2p$ but did not occur in degree 2 or degree p.

Theorem 15. *If* $N = 2^a 3^b$ *for integers* $a, b \geq 0$ *and a point of order* N *is new in degree* $2p$ *for prime* $p > 3$, *then* $N = 12$ *or* $N = 8$.

Proof. Suppose $2^a \cdot 3^b = N$ for integers $a, b \geq 0$. Recall that to have a point of order N in degree $2p$ we must have that $\varphi(N) \mid \omega \cdot 2p$. Therefore, we need $2^{a-1} \cdot 3^{b-1} \mid \omega \cdot p$. Recall in order to have a point of order N in degree $2p$ we must have $T(\mathscr{O}, 1, N) \mid 2p$.

Suppose $a = 0$. Then to have a point of order N we need $3^{b-1} \mid \omega p$.

If $\omega = 6$, we must have $b \leq 2$. Using Theorem 8 we see that $T^o(\mathscr{O}, 1, 3) = 1$. This verifies the result that $N = 3$ occurs over $\mathbb{Q}$ [6], but this N are not new and we are interested in new N. Since $\Delta = -3$ we have $\left(\frac{\Delta}{3}\right) = 0$ therefore, by Theorem 8 we have $T(\mathscr{O}, 1, 9) = 3 \nmid 2p$.

If $\omega = 4$, or $\omega = 2$ then we must have $b \leq 1$. Above we verify that a point of order 3 does occur over $\mathbb{Q}$ and thus this case is complete.

Hence, if $N = 3^b$ then no new points of order N occur.

Suppose $b = 0$. Then to have a new point of order N we need $2^{a-2} \mid \omega p$. Note we may assume $a \geq 2$ since $N = 2$ is not new.

If $\omega = 6$ then we must have $a \leq 3$. Using Theorem 8 we see that $T^o(\mathscr{O}, 1, 2) = 1$. This verifies the result that $N = 2$ occurs over $\mathbb{Q}$ [6], but this N is not new and we are interested in new N. By Theorem 8 we see that $T(\mathscr{O}, 1, 4) = 4 \nmid 2p$ and $T(\mathscr{O}, 1, 8) = 8 \nmid 2p$ and thus this case is complete.

If $\omega = 4$, we must have $a \leq 3$. Using Theorem 8 we see that $T^o(\mathscr{O},1,4) = 1$. This verifies the result that $N = 4$ occurs over $\mathbb{Q}$ [6], but this N is not new and we are interested in new N. Using Theorem 8 we compute $T(\mathscr{O},1,8) = 4 \nmid 2p$ and thus this case is eliminated.

If $\omega = 2$ then we must also have $a \leq 3$ but we just verified that a point of order 2 and 4 occur over $\mathbb{Q}$ so we check the remaining case. If 2 is inert then $T(\mathscr{O},1,8) = 24/nmid2p$. If 2 is split then $T(\mathscr{O},1,8) = 2$ but since $2^2 \mid N$ we gain an extra factor of 2 by Theorem 6.2(a) in [4]. So the least degree over $\mathbb{Q}(j(E))$ is 4. This means the least degree overall would be $4p$, which is a contradiction. Therefore the only way to have a point of order 8 is if 2 is ramified in an imaginary quadratic field of class number p.

Hence, if $N = 2^a$ is new in degree $2p$ then $N = 8$.

Suppose $a \neq 0$ and $b \neq 0$.

If $\omega = 6$, then to have a new point of order N we need $2^{a-1} \cdot 3^{b-1} \mid 6p$. Since $p > 3$, then we must have $a = 1$, or 2 and $b = 1$, or 2. Using Theorem 8 we compute that it is possible to have $T^o(\mathscr{O},1,6) = 1$, which verifies the result that $N = 6$ occurs over $\mathbb{Q}$ [6], but this N is not new and we are interested in new N. Since $\Delta = -3$ we have $\left(\frac{\Delta}{3}\right) = 0$ and $\left(\frac{\Delta}{2}\right) = -1$. Therefore, by Theorem 8 we have $T(\mathscr{O},1,18) = 6 \nmid 2p$, $T(\mathscr{O},1,12) = 4 \nmid 2p$, and $T(\mathscr{O},1,36) = 36 \nmid 2p$.

If $\omega = 4$, then to have a new point of order N we need $2^{a-1} \cdot 3^{b-1} \mid 4p$. Since $p > 3$, then we must have $a = 1,2$, or 3 and $b = 1$. Above we verify that a point of order six can occur over $\mathbb{Q}$. So it remains to check the two remaining cases. Since $\Delta = -4$ we have $\left(\frac{\Delta}{3}\right) = -1$ and $\left(\frac{\Delta}{2}\right) = 0$. Therefore, by Theorem 8 we have $T(\mathscr{O},1,12) = 8 \nmid 2p$ and $T(\mathscr{O},1,24) = 32 \nmid 2p$.

If $\omega = 2$, then to have a new point of order N we need $2^{a-1} \cdot 3^{b-1} \mid 2p$. Since $p > 3$, then we must have $a = 1$, or 2 and $b = 1$. Above we verify that a point of order six can occur over $\mathbb{Q}$. So it remains to check the remaining case. Using Theorem 8 we compute that if $\left(\frac{\Delta}{3}\right) = 0$ or 1 and $\left(\frac{\Delta}{2}\right) = 0$ or 1 then $T(\mathscr{O},1,12) = 2$. However, if either 2 or 3 is split, then

we gain an extra factor of 2 by Theorem 6.2(a) in [4], and so the least degree over $\mathbb{Q}(j(E))$ is 4. This means the least degree overall would be $4p$, which is a contradiction. Therefore the only way to have a point of order 12 is if 2 and 3 are ramified in an imaginary quadratic field of class number p.

Thus if $N = 2^a 3^b$ is new in degree $2p$ and $a, b \neq 0$, then $N = 12$.

Hence, if $N = 2^a \cdot 3^b$ is new in degree $2p$ and $a, b \geq 0$ are integers, then $N = 8$ or $N = 12$. □

Remark. *Thus we have shown that, provided $p \neq 7$, if a point of new order N occurs in degree $2p$ for prime $p > 3$, we must have $N = 8, 12, \ell$, or $N = 2 \cdot \ell$ where $a, b \geq 0$ are integers and $\ell > 3$ is prime. If $p = 7$, then it is also possible for $N = 7^2$ but only in the case where $\Delta = -3$.*

Theorem 16. *Let $N = 2\ell$ and a point of order N be new in degree $2p$ for $p > 3$ prime on a CM elliptic curve E. If $j(E) \neq 0$ or 1728, then $\ell = 2p + 1$. If $j(E) = 1728$, then $\ell = 4p + 1$.*

Proof. Suppose $2\ell = N$ for a prime $\ell > 3$. Given that $\ell > 3$ is prime we know that $\ell - 1 = \varphi(N)$ and since ℓ is odd we can write $\ell = 2k + 1$ for some integer $k > 1$. Recall that to have a point of order N in degree $2p$ we must have that $\varphi(N) \mid \omega \cdot 2p$. Therefore, we need $k \mid \omega \cdot p$. We use Theorem 8 to construct the possibilities for $\widetilde{T}(\mathscr{O}, 1, \ell)$ and $\widetilde{T}(\mathscr{O}, 1, 2)$.

If $\omega = 2$, then to have a point of order N we need $k \mid 2p$. This implies we must have $\ell = 5, 4p + 1$ or $2p + 1$. We will show the first two cases cannot occur.

Suppose $\ell = 5$. Using Theorem 8 if $\left(\frac{\Delta}{5}\right) = -1$ then $T(\mathscr{O}, 1, 10) \nmid 2p$ and therefore we must have $\left(\frac{\Delta}{5}\right) = 1$ or $\left(\frac{\Delta}{5}\right) = 0$. If 5 is not inert and $\left(\frac{\Delta}{2}\right) = 1$ or $\left(\frac{\Delta}{2}\right) = 0$ then $T(\mathscr{O}, 1, 10) = 2 \mid 2p$. This verifies the result that $N = 10$ occurs in degree 2 [6], but this N is not new and we are interested in new N.

Suppose $\ell = 4p + 1$. If $\left(\frac{\Delta}{4p+1}\right) = 1$ or 0 then $\widetilde{T}(\mathscr{O}, 1, 4p + 1) = 4p$, and if $\left(\frac{\Delta}{2p+1}\right) = -1$ then $\widetilde{T}(\mathscr{O}, 1, 2p + 1) = 8p(2p + 1)$. If $\left(\frac{\Delta}{2}\right) = 1$ or 0 then $\widetilde{T}(\mathscr{O}, 1, 2) = 1$, and if $\left(\frac{\Delta}{2}\right) = -1$

then $\widetilde{T}(\mathscr{O},1,2)=3$. Recall, in order to have a point of order N in degree $2p$ we must have $T(\mathscr{O},1,N) \mid 2p$. Thus, this forces $\widetilde{T}(\mathscr{O},1,4p+1)=4p$ and $\widetilde{T}(\mathscr{O},1,2)=1$ so that $T(\mathscr{O},1,2(4p+1))=2p$. However, if $\left(\frac{\Delta}{4p+1}\right)=1$ or $\left(\frac{\Delta}{2}\right)=1$, then by Theorem 1.3 and Theorem 6.2 in [4] we have that $T^o(\mathscr{O},1,2(4p+1))=4p>2p$ and have a contradiction. Therefore, in order to have $T^o(\mathscr{O},1,2(4p+1))=2p$ we must have that $4p+1$ and 2 are ramified. However, since $T(\mathscr{O},1,2(4p+1))=2p$ this forces $j(E)\in\mathbb{Q}$ and there is not an imaginary quadratic field of class number one where $4p+1$ and 2 are both ramified. Therefore $\ell \neq 4p+1$.

If $\omega=4$, then to have a point of order N we need $k \mid 4p$. It remains to rule out $\ell = 5, 2p+1$ or $8p+1$.

Suppose $\ell=5$. Since $\omega=4$ we know that $\Delta=-4$, so $\left(\frac{\Delta}{2}\right)=0$ and $\left(\frac{\Delta}{5}\right)=1$. Therefore $\widetilde{T}(\mathscr{O},1,2)=1$, $\widetilde{T}(\mathscr{O},1,5)=4$, and $T(\mathscr{O},1,10)=1$. However, $\left(\frac{\Delta}{5}\right)=1$ and therefore by Theorem 1.3 and Theorem 6.2 in [4] we have that $T^o(\mathscr{O},1,10)=2$. This verifies the result that $N=10$ occurs in degree 2 [6], but $N=10$ is not new and we are interested in new N.

Suppose $\ell=2p+1$. Since $\omega=4$ we know that $\Delta=-4$, so $\left(\frac{\Delta}{2}\right)=0$ and $\widetilde{T}(\mathscr{O},1,2)=1$. If $\left(\frac{\Delta}{2p+1}\right)=1$ then $\widetilde{T}(\mathscr{O},1,2p+1)=2p$, and if $\left(\frac{\Delta}{2p+1}\right)=-1$ then $\widetilde{T}(\mathscr{O},1,2p+1)=4p(p+1)$. therefore we must have $\left(\frac{\Delta}{2p+1}\right)=1$. Thus, by Theorem 8 we have that $T(\mathscr{O},1,2(2p+1))=\frac{p}{2}$. However, since $p>3$ this is a contradiction because $T(\mathscr{O},1,N)$ will not be an integer. Thus, this case can never occur.

Suppose $\ell=8p+1$. Since $\omega=4$ we know that $\Delta=-4$, so $\left(\frac{\Delta}{2}\right)=0$ and $\widetilde{T}(\mathscr{O},1,2)=1$. If $\left(\frac{\Delta}{8p+1}\right)=1$ then $\widetilde{T}(\mathscr{O},1,8p+1)=8p$, and if $\left(\frac{\Delta}{8p+1}\right)=-1$ then $\widetilde{T}(\mathscr{O},1,8p+1)=16p(4p+1)$. Recall, in order to have a point of order N in degree $2p$ we must have $T(\mathscr{O},1,N) \mid 2p$. Thus, this forces $\widetilde{T}(\mathscr{O},1,8p+1)=8p$ so that $T(\mathscr{O},1,2(8p+1))=2p$. However, in order to have $\widetilde{T}(\mathscr{O},1,8p+1)=8p$ and we must have $\left(\frac{\Delta}{8p+1}\right)=1$ and there-

fore by Theorem 1.3 and Theorem 6.2 in [4] we have that $T^o(\mathscr{O},1,2(8p+1)) = 4p > 2p$. A contradiction.

If $\omega = 6$, then in order to have a point of order N we must have $k \mid 6p$. This implies we must rule out $\ell = 5,7,13,4p+1,6p+1,12p+1$. Since $\omega = 6$ we know that $\Delta = -3$, so $\left(\frac{\Delta}{2}\right) = -1$. Suppose $\ell = 5$. We have $\widetilde{T}(\mathscr{O},1,2) = 3$, and since $\left(\frac{-3}{5}\right) = -1$ we have $\widetilde{T}(\mathscr{O},1,5) = 24$, and therefore $T(\mathscr{O},1,10) = 12 \nmid 2p$. A contradiction. Suppose $\ell = 7$. We have $\widetilde{T}(\mathscr{O},1,2) = 3$, and since $\left(\frac{-3}{7}\right) = 1$ we have$\widetilde{T}(\mathscr{O},1,7) = 6$, and therefore $T(\mathscr{O},1,14) = 3 \nmid 2p$. A contradiction. Suppose $\ell = 13$. We have $\widetilde{T}(\mathscr{O},1,2) = 3$, and since $\left(\frac{-3}{13}\right) = 1$ we have$\widetilde{T}(\mathscr{O},1,13) = 12$, and therefore $T(\mathscr{O},1,26) = 6 \nmid 2p$. A contradiction.

Suppose $\ell = 2p+1$. We have $\widetilde{T}(\mathscr{O},1,2) = 3$. If $\left(\frac{\Delta}{2p+1}\right) = 1$ then $\widetilde{T}(\mathscr{O},1,2p+1) = 3p \nmid 2p$, and if $\left(\frac{\Delta}{2p+1}\right) = -1$ then $\widetilde{T}(\mathscr{O},1,2p+1) = 6p(p+1) \nmid 2p$. Thus, in order to have $\ell = 2p+1$ we must have $\left(\frac{-3}{2p+1}\right) = 0$ but this never occurs. Hence, this case is eliminated.

Suppose $\ell = 4p+1$. We have $\widetilde{T}(\mathscr{O},1,2) = 3$. If $\left(\frac{\Delta}{4p+1}\right) = 1$ then $\widetilde{T}(\mathscr{O},1,4p+1) = 4p$, and if $\left(\frac{\Delta}{4p+1}\right) = -1$ then $\widetilde{T}(\mathscr{O},1,4p+1) = 8p(2p+1)$. Recall, in order to have a point of order N in degree $2p$ we must have $T(\mathscr{O},1,N) \mid 2p$. Thus, this forces $\widetilde{T}(\mathscr{O},1,4p+1) = 4p$ so that $T(\mathscr{O},1,2(4p+1)) = 2p$. However, in order to have $\widetilde{T}(\mathscr{O},1,4p+1) = 4p$ and we must have $\left(\frac{\Delta}{4p+1}\right) = 1$ and therefore by Theorem 1.3 and Theorem 6.2 in [4] we have that $T^o(\mathscr{O},1,2(4p+1)) = 4p > 2p$. A contradiction.

Suppose $\ell = 6p+1$. We have $\widetilde{T}(\mathscr{O},1,2) = 3$. If $\left(\frac{\Delta}{6p+1}\right) = 1$ then $\widetilde{T}(\mathscr{O},1,6p+1) = 6p$, and if $\left(\frac{\Delta}{6p+1}\right) = -1$ then $\widetilde{T}(\mathscr{O},1,6p+1) = 12p(3p+1)$. Either way $T(\mathscr{O},1,2(6p+1)) \geq 2p$ and therefore can not divide $2p$. A contradiction.

Suppose $\ell = 12p+1$. We have $\widetilde{T}(\mathscr{O},1,2) = 3$. If $\left(\frac{\Delta}{12p+1}\right) = 1$ then $\widetilde{T}(\mathscr{O},1,12p+1) = 12p$, and if $\left(\frac{\Delta}{12p+1}\right) = -1$ then $\widetilde{T}(\mathscr{O},1,12p+1) = 24p(6p+1)$. Either way $T(\mathscr{O},1,2(12p+$

$1)) \geq 2p$ and therefore can not divide $2p$. A contradiction.

Therefore only two cases remain, $\ell = 4p+1$ when $j(E) = 1728$, and $\ell = 2p+1$ when $j(E) \neq 0$, or 1728. We will now verify that these are indeed the only possibilities for ℓ.

Suppose $\ell = 2p+1$ and $\omega = 2$. If $\left(\frac{\Delta}{2p+1}\right) = 1$ then $\widetilde{T}(\mathscr{O}, 1, 2p+1) = 2p$, and if $\left(\frac{\Delta}{2p+1}\right) = -1$ we have $\widetilde{T}(\mathscr{O}, 1, 2p+1) = 4p(p+1)$. If $\left(\frac{\Delta}{2}\right) = 1$ or 0 then $\widetilde{T}(\mathscr{O}, 1, 2) = 1$, and if $\left(\frac{\Delta}{2}\right) = -1$ then $\widetilde{T}(\mathscr{O}, 1, 2) = 3$. Recall, in order to have a point of order N in degree $2p$ we must have $T(\mathscr{O}, M, N) \mid 2p$. Thus, this forces $\widetilde{T}(\mathscr{O}, 1, 2p+1) = 2p$ and $\widetilde{T}(\mathscr{O}, 1, 2) = 1$ so that $T(\mathscr{O}, 1, 2(2p+1)) = p \mid 2p$. However, in order to have $\widetilde{T}(\mathscr{O}, 1, 2p+1) = 2p$ and we must have $\left(\frac{\Delta}{2p+1}\right) = 1$ and therefore by Theorem 1.3 and Theorem 6.2 in [4] we have that $T^o(\mathscr{O}, 1, 2(2p+1)) = 2p$.

Suppose $\ell = 4p+1$ and $\omega = 4$. Then we know that $\Delta = -4$, so $\left(\frac{\Delta}{2}\right) = 0$ and $\widetilde{T}(\mathscr{O}, 1, 2) = 1$. If $\left(\frac{\Delta}{4p+1}\right) = 1$ then $\widetilde{T}(\mathscr{O}, 1, 4p+1) = 4p$, and if $\left(\frac{\Delta}{2p+1}\right) = -1$ then $\widetilde{T}(\mathscr{O}, 1, 4p+1) = 8p(2p+1)$. Recall, in order to have a point of order N in degree $2p$ we must have $T(\mathscr{O}, M, N) \mid 2p$. Thus, this forces $\widetilde{T}(\mathscr{O}, 1, 4p+1) = 4p$ so that $T(\mathscr{O}, 1, 2(4p+1)) = p$. However, in order to have $\widetilde{T}(\mathscr{O}, 1, 4p+1) = 4p$ and we must have $\left(\frac{\Delta}{4p+1}\right) = 1$ and therefore by Theorem 1.3 and Theorem 6.2 in [4] we have that $T^o(\mathscr{O}, 1, 2(4p+1)) = 2p$.

□

Theorem 17. *Let F be a number field of degree $2p$ for prime $p > 3$ and E/F a CM elliptic curve. If $E(F)$ has a point of new order $N > 5$ and N is prime, then $N = \omega p + 1$ and $\left(\frac{\Delta}{N}\right) \neq -1$. If $j(E) \neq 1728$, $j(E) \neq 0$, and 5 is ramified in an imaginary quadratic field of class number p, then $E(F)$ may also have a point of new order $N = 5$.*

Proposition 5. *Let F be a number field of degree $2p$ for prime $p > 3$ and E/F be a CM elliptic curve with $j(E) \neq 0$, or 1728. If $E(F)$ has a point of new order $N > 5$ and N is prime, then $N = 2p+1$ and $\left(\frac{\Delta}{N}\right) \neq -1$. If 5 is ramified in an imaginary quadratic field of*

class number p, then $E(F)$ may also have a point of new order $N = 5$.

Proof. Assume E/F has a point of order N and $N > 3$ is prime. We can write $N = 2k+1$ for some $k \in \mathbb{Z}^+$ because it is odd. We know that if we have a point of order N then we must have $\varphi(N) \mid \omega \cdot 2p$ by Corollary 2. Furthermore, since $j \neq 0, 1728$ we know $\omega = 2$ and must have $k \mid 2p$. This implies that $N = 5, 2p+1$, or $4p+1$.

Case 1: $N = 4p+1$

Since $\frac{\varphi(4p+1)}{2} = 2p$ we know by Lemma 1 that we must have $\left(\frac{\Delta}{4p+1}\right) = 0$ if we want $T^o(\mathscr{O}, 1, 4p+1) = 2p$. Using Theorem 8 we see that $T(\mathscr{O}, 1, 4p+1) = 2p$ when $4p+1$ is ramified in K and therefore since $[F : \mathbb{Q}] = 2p$ and $T(\mathscr{O}, M, N) \mid [F : \mathbb{Q}(j(E))]$ we only need to consider imaginary quadratic fields with $[\mathbb{Q}(j(E)) : \mathbb{Q}] = 1$. However, there are only a finite number of imaginary quadratic fields of class number one with $\omega = 2$. Thus, there are only finitely many ramified primes and one can easily check that none of these are of the form $4p+1$. Thus, this case will never occur.

Case 2: $N = 5$

Using Theorem 8 we see that if $\left(\frac{\Delta}{5}\right) = -1$ then $T(\mathscr{O}, 1, 5) = 12 \nmid 2p$ and if $\left(\frac{\Delta}{5}\right) = 0$ or $\left(\frac{\Delta}{5}\right) = 1$ then $T(\mathscr{O}, 1, 5) = 2$. However, if 5 is split, then we gain an extra factor of 2 by Theorem 6.2(a) in [4], and so the least degree over $\mathbb{Q}(j(E))$ is 4. This means the least degree overall would be $4p$, which is a contradiction. Therefore the only way to have a point of order 5 is if 5 is ramified in an imaginary quadratic field of class number p.

Case 3: $N = 2p+1$

Applying Theorem 8 we see that $T(\mathscr{O}, 1, 2p+1) = p$ if $\left(\frac{\Delta}{2p+1}\right) = 1$ or 0 and or $T(\mathscr{O}, 1, 2p+1) = 2p^2 + 2p$ if $\left(\frac{\Delta}{2p+1}\right) = -1$. Furthermore, since $2p^2 + 2p \nmid 2p$ we must have that $2p+1$ is not inert. If $2p+1$ is split then by Theorems 6.1, 6.2, and 6.6 in [4] $T^o(\mathscr{O}, 1, 2p+1) = 2p$. Thus, this case can occur. □

Proposition 6. *Let F be a number field of degree $2p$ for prime $p > 3$ and E/F a CM*

elliptic curve with $j(E) = 1728$. *If* $E(F)$ *has a point of new order* $N > 3$ *and* N *is prime, then* $N = 4p+1$ *and* $\left(\frac{\Delta}{N}\right) = 1$.

Proof. Assume E/F has a point of order $N = \ell$, and assume N is a prime greater than 3. We can write $\ell = 2k+1$ for some $k \in \mathbb{Z}^+$ since ℓ is odd. By Corollary 2 we know $\varphi(N) \mid \omega \cdot 2p$. Furthermore, since we are considering $j = 1728$ we know $\omega = 4$ and we must have $k \mid 4p$. Thus, $\ell = 5, 2p+1, 4p+1, 8p+1$.

Case 1: $\ell = 5$

Applying Theorem 6.2 in [4] we see that $T^o(\mathscr{O}, 1, 5) = 2$ since $\left(\frac{\Delta}{5}\right) = 1$. Since $j(E) = 1728$, E corresponds to an equation of the form $y^2 = x^3 + Ax$. Points of order 2 correspond to roots of $x^3 + Ax$, and this polynomial always has a root over any number field. Thus we can't have a rational point of order 5 without a point of order 2. Using computational results in [6] we see that $\mathbb{Z}/10\mathbb{Z}$ occurs when K is a number field of degree 2 and the j-invariant is 1728. Thus, this case is not new.

Case 2: $\ell = 8p+1$

Applying Theorem 8 and Theorem 6.2 in [4] we see that the only way to get $T^o(\mathscr{O}, 1, 8p+1) \leq 2p$ requires $\left(\frac{\Delta}{8p+1}\right) = 0$. However, since $\omega = 4$, the only ramified prime is 2. Thus, this case will never occur.

Case 3: $\ell = 2p+1$

Applying Theorem 8 and Theorem 6.2 in [4] we see that the only way to get $T^o(\mathscr{O}, 1, 2p+1) \leq 2p$ requires $\left(\frac{\Delta}{2p+1}\right) = 0$. However, since $\omega = 4$, the only ramified prime is 2. Thus, this case will never occur.

Case 4: $\ell = 4p+1$

Applying Theorem 8 we see that we see that if $\left(\frac{\Delta}{4p+1}\right) = 1$ or if $\left(\frac{\Delta}{4p+1}\right) = 0$ then $T(\mathscr{O}, 1, 4p+1) = p$ and if $\left(\frac{\Delta}{4p+1}\right) = -1$ then $T(\mathscr{O}, 1, 4p+1) = 4p^2 + 2p$. Note that $\Delta_K = -4$ and thus the only ramified prime is 2. Furthermore, since $4p^2 + 2p \nmid 2p$ we must have that $4p+1$ is

split. If $4p+1$ is split then by Theorem 6.2 in [4] $T^o(\mathscr{O},1,4p+1)=2p$. Thus, this is the only case that can occur. □

Proposition 7. *Let F be a number field of degree $2p$ for prime $p>3$ and let E/F be a CM elliptic curve with $j(E)=0$. If $E(F)$ has a point of new order $N>3$ and N is prime, then $N=6p+1$ and $\left(\frac{\Delta}{N}\right)=1$.*

Proof. Assume E/F has a point of order $N=\ell$, and assume N is a prime greater than 3. We can write $\ell=2k+1$ for some $k\in\mathbb{Z}^+$ since ℓ is odd. We know by Corollary 2 that $\varphi(N)\mid\omega\cdot 2p$. Furthermore, since $j(E)=0$ we know $\omega=6$ we must have $k\mid 6p$. Thus, $\ell=5,7,13,2p+1,4p+1,6p+1,8p+1,12p+1$.

Case 1: $\ell=5$

Since $\left(\frac{\Delta}{5}\right)=-1$, applying Theorem 8 we have $T(\mathscr{O},1,5)=4\nmid 2p$. Thus, this case does not occur.

Case 2: $\ell=7$

Applying Theorem 6.2 in [4] we see that $T^o(\mathscr{O},1,7)=2$ since $\left(\frac{\Delta}{7}\right)=1$. Moreover, we see in [6] that $\mathbb{Z}/7\mathbb{Z}$ occurs when K is a number field of degree 2 and the j-invariant is 0. Thus, $N=7$ is not new and we have a contradiction.

Case 3: $\ell=13$

Since $\omega=6$ we know that $\Delta=-3$ and have $\left(\frac{\Delta}{13}\right)=1$. Therefore, by Theorem 6.2 in [4] we have that $T^o(\mathscr{O},1,13)=4$. By Table 2 in [2] we see that a point of order $N=13$ does not occur in some prime degree greater than four. Hence, this case will never occur.

Case 4: $\ell=2p+1$

Applying Theorem 8 we see that we see that $T(\mathscr{O},1,2p+1)=\frac{p}{3}$ if $\left(\frac{\Delta}{2p+1}\right)=1$, or 0. However, $T(\mathscr{O},M,N)$ is an integer and since $p>3$ this shows that $\ell=2p+1$ must be inert in this field but $\ell=2p+1$ inert implies that $T(\mathscr{O},1,2p+1)=4p(p+1)\nmid 2p$. Thus, this case will never occur.

Case 5: $\ell = 4p+1$

Applying Theorem 8 we see that we see that $T(\mathscr{O},1,4p+1) = \frac{2p}{3}$ if $\left(\frac{\Delta}{4p+1}\right) = 1$, or 0. However, $T(\mathscr{O},M,N)$ is an integer and since $p > 3$ this shows that $\ell = 4p+1$ must be inert in this field but $\ell = 4p+1$ inert implies that $T(\mathscr{O},1,4p+1) = 16p^2+8p \nmid 2p$. Thus, this case will never occur.

Case 6: $\ell = 8p+1$

Applying Theorem 8 we see that we see that $T(\mathscr{O},1,8p+1) = \frac{4p}{3}$ if $\left(\frac{\Delta}{8p+1}\right) = 1$, or 0. However, $T(\mathscr{O},M,N)$ is an integer and since $p > 3$ this shows that $\ell = 8p+1$ must be inert in this field but $\ell = 8p+1$ inert implies that $T(\mathscr{O},1,8p+1) = 64p^2+16p \nmid 2p$. Thus, this case will never occur.

Case 7: $\ell = 12p+1$

Applying Lemma 1 we see that the only way to get $T^o(\mathscr{O},1,12p+1) \leq 2p$ requires $\left(\frac{\Delta}{12p+1}\right) = 0$. However, since $\omega = 6$, the only ramified prime is 3. Thus, this case will never occur.

Case 8: $\ell = 6p+1$

Applying Theorem 8 we see that the possibilities for $T(\mathscr{O},1,6p+1) = p$ or $6p^2+2p$ for $\left(\frac{\Delta}{6p+1}\right) = 1$ or $\left(\frac{\Delta}{6p+1}\right) = -1$ respectively. Note that $\Delta_K = -3$ and thus the only ramified prime is 3. Furthermore, since $6p^2+2p \nmid 2p$ we must have that $6p+1$ is split. If $6p+1$ is split then by Theorem 6.2 in [4] $T^o(\mathscr{O},1,6p+1) = 2p$. Thus, this is the only case that can occur. □

3.4 Possible M

In this section we let F be a number field of degree $d = 2p$ for $p > 3$ a prime and E/F a CM elliptic curve. By Corollary 1 we know $E(F)[\text{tors}] \cong \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ for $M \mid N$, and therefore in order to completely classify the torsion subgroups that arise for number fields

of degree $2p$ for any prime $p > 3$ we must also determine the possibilities for M. We are only concerned with possibilities for M where $M \neq 1$.

Theorem 18. *Suppose F is a number field of degree $2p$ for prime $p > 3$ and E/F is a CM elliptic curve. If $E(F)[\text{tors}]$ is new and $M \neq 1$, then $M = 2$.*

Proposition 8. *If $\ell \mid M$ for a prime $\ell > 3$, then full M torsion does not occur in degree $2p$ for $p > 3$ prime.*

Proof. Let $\ell > 3$ be prime and suppose $\ell \mid M$ for a prime $\ell > 3$. Note if we have full M torsion in degree $2p$ for $p > 3$ prime then we must have $T(\mathscr{O}, \ell, \ell) \mid 2p$ since $\ell \mid M$, $M \mid N$ and $T(\mathscr{O}, M, N) \mid 2p$.

Given $\ell \mid M$, our field extension must contain the ℓth roots of unity by Corollary 7 and thus we know that $\varphi(\ell)$ must divide $2p$. We can write $\ell = 2k+1$ for $k \in \mathbb{N}$ because $\ell > 3$ is prime and therefore we must have $k \mid p$. Thus, $\ell = 2p+1$ for a Sophie Germain prime p.

Using Theorem 8 we have $\tilde{T}(\mathscr{O}, \ell, \ell) = 4p(p+1), 4p^2$ or $2p(2p+1)$. Recall $T(\mathscr{O}, \ell, \ell) = \frac{\tilde{T}(\mathscr{O}, \ell, \ell)}{\omega}$ must be an integer and $\omega \in \{2, 4, 6\}$. So clearly in every case $T(\mathscr{O}, \ell, \ell) > p$. By Remark 8.1 in [4], K is contained in the field over which E has full M-torsion when $M \geq 3$. Therefore, we can only have cases where $T(\mathscr{O}, M, M)$ is 1 or p. Thus, $\ell \nmid M$. □

Remark. *If full M torsion with a point of order N occurs in degree $2p$ for $p > 3$, we must have $M = 2^a 3^b$ where $a, b \geq 0$ are integers.*

Proposition 9. *Let F be a number field of degree $2p$ for prime $p > 3$ and E/F a CM elliptic curve. If over a quadratic field L there exists a CM elliptic curve E'/L with $E'(L)[\text{tors}] \cong \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$, then in degree $2p$ there is no $M' > M$ with $M' \mid N$ and $E(F)[\text{tors}] \cong \mathbb{Z}/M'\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$.*

Proof. Recall that as result of Theorem 2.1 in [2] we know that if a torsion subgroup arises in degree d', then it arises in any degree d for which $d' \mid d$. By definition a new torsion

subgroup is a subgroup that occurs in degree d and not in any degree $d' < d$ such that $d' \mid d$. Thus, since $[F : \mathbb{Q}] = 2p$ we know that any possibilities for M and N that occur in degree 2 or degree p will also occur in degree $2p$. However, in [4] we see that for prime $p > 5$ the torsion subgroups that arise over a number field of degree p are simply those that occur over $\mathbb{Q}$. Moreover, by [6] we know that in degree 5 the only N that did not occur over $\mathbb{Q}$ is $N = 11$ and since the only possibilities are $M = 2$ or $M = 3$ and $N = 11$ is prime. So there are no possibilities for new torsion in this case. Thus, the only remaining possible full torsion would be $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ for an N occurring in degree 2 and $M \mid N$ but $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ does not occur in degree 2. By [6] we see that for F a number field of degree $d = 2$ and an elliptic curve E/F, the group $E(F)[\text{tors}]$ is isomorphic to one of the following groups

$$\begin{array}{ll} \mathbb{Z}/N\mathbb{Z} & \text{for } N = 1,2,3,4,6,7,10, \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z} & \text{for } N = 2,4,6, \\ \text{and} & \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}. \end{array}$$

Using Theorem 8 we compute $T(\mathscr{O}, M, N)$ and see, with the exception of $T(\mathscr{O}, 2, 10)$, that $T(\mathscr{O}, M, N) \nmid 2p$ for every $M \mid N$ where N occurs in degree 2 but $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ does not. Since $T(\mathscr{O}, 2, 10) = 2$ and we are in the case where $j(E) = 1728$, we know that $\Delta = -4$. and have $\left(\frac{\Delta}{5}\right) = 1$ and $\left(\frac{\Delta}{2}\right) = 0$. If $F \not\supset K$, then by Proposition 6.3(a) in [4] sine $\left(\frac{\Delta}{5}\right) = 1$, we need $\frac{\varphi(5)^2}{\omega} \mid 2p$ but $4 \nmid 2p$. Thus, since $p > 3$ we have a contradiction and must have $F \supset K$. Recall that $[K : \mathbb{Q}] = 2$ and $T(\mathscr{O}, 2, 5) = 2 \mid [F : K]$. Thus, this implies that $4 \mid [F : \mathbb{Q}] = 2p$ and we have a contradiction. □

Corollary 3. *If $M' \mid M$ for $M' \in \{4, 6, 9\}$, then full M torsion with a point of order N does not occur in degree $2p$ for $p > 3$ prime.*

Proof. If $M' \mid M$ for $M' \in \{4, 6, 9\}$, then because $M \mid N$ we must have that $M' \mid N$ and therefore that N is not prime. However, from above we see that if N is new and composite then N is 49, $2(2p+1)$, or $2(4p+1)$ with $2p+1$ and $4p+1$ prime. Thus, since none of the

composite possibilities for N are divisible by $4, 6$, or 9 we have a contradiction. The case where N is not new follows from the previous proposition. □

Corollary 4. *If full M torsion with a point of order N occurs in degree $2p$ for $p > 3$, we must have M is 2 or 3.*

Remark. *In [6] we see that $M = 2$ and $M = 3$ occur in degree 2.*

Proposition 10. *Let F be a number field of degree $2p$ for prime $p > 3$ and E/F a CM elliptic curve. If $E(F)[\text{tors}]$ is new and $M \neq 1$, then $M = 2$ and $N = 2(2p+1)$ with $2p+1$ prime.*

Proof. Suppose $E(F)[\text{tors}]$ is new. By Corollary 1 we know that $E(F)[\text{tors}] \cong \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ and $M \mid N$. By Corollary 4 we know that if $M \neq 1$ then for full M torsion to occur in degree $2p$ we must have $M \in \{2,3\}$. Using Theorem 10 and Theorem 17 we see that the only possibilities for new N composite are $49, 2(2p+1)$, and $2(4p+1)$. The case of N not new follows from Prop 9. Clearly, this implies $M \neq 3$ and since $2 \nmid 49$ we also have $N \neq 49$. Recall that $N = 2(4p+1)$ is only a possibility if $j(E) = 1728$. Using Theorem 8 we see that $T(\mathcal{O}, 2, 2(4p+1)) = 8p^2 \nmid 2p$ and therefore this case does not occur. Recall that $N = 2(2p+1)$ is only a possibility if $j(E) \neq 0$, or 1728. Applying Theorem 8 we see that if $\left(\frac{\Delta}{2p+1}\right) \neq -1$ and $\left(\frac{\Delta}{2}\right) = 1$ then we have $T^o(\mathcal{O}, 2, 2(2p+1)) = 2p$. Thus, if $E(F)[\text{tors}]$ is new and $M \neq 1$, then $M = 2$ and $N = 2(2p+1)$ for prime $2p+1$. □

3.5 Torsion in Degrees 2, 14, 22, 26, 34 &38

Now we illustrate how our main results can be used to give classification for specific primes $p = 7, 11, 13, 17, 19$. But we first include $E(F)[\text{tors}]$ for $d = 2$ so that one may easily see when we get groups that did not occur for $d = 2$.

Theorem 19. *Let F be a number field of degree 2. Let E/F be a CM elliptic curve. For E/F the group $E(F)$*[tors] *is isomorphic to one of the following:*

$$\begin{array}{ll} \mathbb{Z}/m\mathbb{Z} & 1 \leq m \leq 7 \text{ or } m = 10 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z} & m = 2,4,6 \text{ and} \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} & \end{array}$$

The only subgroups which did not occur over $\mathbb{Q}$ are:

$$\mathbb{Z}/7\mathbb{Z}, \mathbb{Z}/10\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$$

Proof. See section 4.2 in [6]. □

Theorem 20. *Let F be a number field of degree 14. Let E/F be a CM elliptic curve. The group $E(F)$*[tors] *is isomorphic to one of the following:*

$$\begin{array}{ll} \mathbb{Z}/m\mathbb{Z} & 1 \leq m \leq 7 \text{ or } m = 10,29,43,49,58 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} & 1 \leq m \leq 3 \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} & \end{array}$$

In degree 2, $\mathbb{Z}/29\mathbb{Z}$, $\mathbb{Z}/43\mathbb{Z}$, $\mathbb{Z}/49\mathbb{Z}$, and $\mathbb{Z}/58\mathbb{Z}$ did not occur.

Theorem 21. *Let F be a number field of degree 22. Let E/F be a CM elliptic curve. For E/F the group $E(F)$*[tors] *is isomorphic to one of the following:*

$$\begin{array}{ll} \mathbb{Z}/m\mathbb{Z} & 1 \leq m \leq 7 \text{ or } m = 10 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} & 1 \leq m \leq 3 \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} & \end{array}$$

All of these groups arose in degree 2.

Theorem 22. *Let F be a number field of degree 26. Let E/F be a CM elliptic curve. For E/F the group $E(F)$*[tors] *is isomorphic to one of the following:*

$$\begin{array}{ll} \mathbb{Z}/m\mathbb{Z} & 1 \leq m \leq 7 \text{ or } m = 10,53,79,106 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} & 1 \leq m \leq 3 \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} & \end{array}$$

In degree 2, $\mathbb{Z}/53\mathbb{Z}$, $\mathbb{Z}/79\mathbb{Z}$, and $\mathbb{Z}/106\mathbb{Z}$ did not occur.

Theorem 23. *Let F be a number field of degree 34. Let E/F be a CM elliptic curve. For E/F the group $E(F)[\text{tors}]$ is isomorphic to one of the following:*

$$\begin{array}{ll} \mathbb{Z}/m\mathbb{Z} & 1 \leq m \leq 7 \text{ or } m = 10, 103 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} & 1 \leq m \leq 3 \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} & \end{array}$$

In degree 2, $\mathbb{Z}/103\mathbb{Z}$ did not occur.

Theorem 24. *Let F be a number field of degree 38. Let E/F be a CM elliptic curve. For E/F the group $E(F)[\text{tors}]$ is isomorphic to one of the following:*

$$\begin{array}{ll} \mathbb{Z}/m\mathbb{Z} & 1 \leq m \leq 7 \text{ or } m = 10 \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} & 1 \leq m \leq 3 \\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} & \end{array}$$

All of these groups arose in degree 2.

Bibliography

[1] Ian Stewart and David Tall, *Algebraic number theory and Fermat's last theorem*, 4th ed., CRC Press, Boca Raton, FL, 2016. MR3443702

[2] Abbey Bourdon, Pete L. Clark, and James Stankewicz, *Torsion points on CM elliptic curves over real number fields*, Trans. Amer. Math. Soc. **369** (2017), no. 12, 8457–8496, DOI 10.1090/tran/6905. MR3710632

[3] Abbey Bourdon and Pete L. Clark, *Torsion points and Galois representations on CM elliptic curves*. To appear in Pacific J. Math. Available at arXiv:1612.03229.

[4] ———, *Torsion points and isogenis on CM elliptic curves*. To appear in J. London Math. Available at arXiv:1906.07121.

[5] Joseph H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094

[6] Pete L. Clark, Patrick Corn, Alex Rice, and James Stankewicz, *Computation on elliptic curves with complex multiplication*, LMS J. Comput. Math. **17** (2014), no. 1, 509–535, DOI 10.1112/S1461157014000072. MR3356044

[7] David S. Dummit and Richard M. Foote, *Abstract algebra*, 3rd ed., John Wiley & Sons, Inc., Hoboken, NJ, 2004. MR2286236

[8] Abbey Bourdon and Paul Pollack, *Torsion subgroups of CM elliptic curves over odd degree number fields*, Int. Math. Res. Not. IMRN **16** (2017), 4923–4961, DOI 10.1093/imrn/rnw163. MR3687120

[9] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186 (1978). With an appendix by Mazur and M. Rapoport. MR488287

[10] André Weil, *L'arithmétique sur les courbes algébriques*, Acta Math. **52** (1929), no. 1, 281–315, DOI 10.1007/BF02547409 (French). MR1555278

[11] Loïc Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), no. 1-3, 437–449, DOI 10.1007/s002220050059 (French). MR1369424

[12] S. Kamienny, *Torsion points on elliptic curves over all quadratic fields*, Duke Math. J. **53** (1986), no. 1, 157–162, DOI 10.1215/S0012-7094-86-05310-X. MR835802

[13] ———, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. **109** (1992), no. 2, 221–229, DOI 10.1007/BF01232025. MR1172689

[14] M. A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149, DOI 10.1017/S0027763000002816. MR931956

[15] Loren D. Olson, *Points of finite order on elliptic curves with complex multiplication*, Manuscripta Math. **14** (1974), 195–205, DOI 10.1007/BF01171442. MR352104

[16] Maarten Derickx, Anastassia Etropolski, Mark van Hoeij, Jackson S. Morrow, and David Zureick-Brown, *Sporadic cubic torsion*. In preparation.

[17] L. J. Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees*, Proc. Camb. Philos. Soc. **21** (1922), 179–192.

[18] David A. Cox, *Primes of the form $x^2 + ny^2$*, A Wiley-Interscience Publication, John Wiley & Sons, Inc., New York, 1989. Fermat, class field theory and complex multiplication. MR1028322

Holly Paige Chaos

Contact Information

Mathematics Department
Wake Forest University

Phone: (540) 797-1693
E-mail: chaohp18@wfu.edu

Research Interests

I am interested in Number Theory, Algebraic Geometry, and Arithmetic Geometry. Specifically I have experience with elliptic curves and coverings of the integers.

Education

Wake Forest University, Winston-Salem, North Carolina

M.A., Mathematics, May 2020

- Thesis Topic: "Torsion for CM Elliptic Curves in Degree $2p$"
- Advisor: Dr. Abbey Bourdon

Washington and Lee University, Lexington, Virginia

B.A., Mathematics, May 2017

Employment

Wake Forest University, Winston-Salem, North Carolina **August 2018-May 2020**
Graduate Teaching Assistant

Central Elementary School, Lexington, VA **September 2017 - June 2018**
Kindergarten Teacher

Washington and Lee University, Lexington, Virginia **June 2016-June 2018**
Robert E. Lee Summer Research Scholar

Washington and Lee University, Lexington, Virginia **September 2014-May 2017**
Biology Teaching Assistant

Scholarly Work

1. "Iterated Sierpinski and Riesel Numbers" (joint work with Carrie E. Finch-Smith) *Combinatorial and Additive Number Theory* (M. Nathanson, editor). Springer Proceedings in Mathematics and Statistics (2020), 39-54.
2. "Torsion for CM Elliptic Curves in Degree $2p$" (In Preparation)

Teaching Experience

Wake Forest University, Winston-Salem, North Carolina **August 2018 - May 2020**

Teaching Assistant

- Math 111: Calculus with Analytic Geometry I (Fall 2018, Spring 2019, Spring 2020)
- Math 121: Linear Algebra I (Fall 2019)

Math and Stats Center Tutor

- Math 117: Discrete Mathematics

- Math 321/322: Modern Algebra I and II
- Math 345: Elementary Number Theory

Conference & Seminar Presentations

Torsion for CM Elliptic Curves in Degree $2p$, PANTS 33 , Clemson University, December 2019.

Torsion for CM Elliptic Curves Defined over Number Fields of Degree $2p$, Number Theory Seminar, Wake Forest University, November 2019.

Spiraloteral Graphs, Parents' Weekend Seminar, Washington and Lee University, October 2016.

Exploring Spirolateral Graphs, SUMS, James Madison University, September 2016.

Other Conferences & Workshops Attended

PANTS 32, UNCC, Charlotte, NC, September 2019

Sage Days 103, St. Louis, MO, August 2019.

49th John H. Barrett Memorial Lectures: Recent Developments in Number Theory, University of Tennessee, Knoxville, TN, May 2019.

SERMON 2019, UNCG, Greensboro, NC, April 2019.

Triangle Lectures in Combinatorics, Wake Forest University, Winston-Salem, NC, March 2019.

AWM Piedmont-Triad Conference, Wake Forest University, Winston-Salem, NC, March 2019.

Leadership & Service

Vice President, Wake Forest Association of Women in Mathematics

AWM Undergraduate Mentor

Computer Skills

LaTex, Magma, Sage, Python, R

Graduate Coursework

Abstract Algebra I, Abstract Algebra II, Commutative Algebra, Advanced Linear Algebra, Algebraic Number Theory, Algebraic Combinatorics, Intro Real Analysis, Real Analysis II, Topology, Theory of Computation (Computer Science)