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

ABBEY BOURDON AND HOLLY PAIGE CHAOS

Abstract. For a prime number p, we characterize the groups that may arise as torsion subgroups of an elliptic curve with complex multiplication defined over a number field of degree $2p$. In particular, our work shows that a classification in the strongest sense is tied to determining whether there exist infinitely many Sophie Germain primes.

1. Introduction

In 1922, Mordell proved that the set of $\mathbb{Q}$-rational points of an elliptic curve E defined over $\mathbb{Q}$ is a finitely generated abelian group [23]. That is, $E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r$, where $E(\mathbb{Q})_{\text{tors}}$ denotes the finite collection of torsion points and $r \in \mathbb{Z}^{\geq 0}$ is the rank of $E/\mathbb{Q}$. It is natural to ask what groups arise as $E(\mathbb{Q})_{\text{tors}}$ as E ranges over all elliptic curves over $\mathbb{Q}$, and the answer is known due to work of Mazur.

Theorem 1.1 (Mazur, [21]). *Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q})_{\text{tors}}$ is isomorphic to one of the following groups:*

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

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

More generally, if E is an elliptic curve defined over a number field F, then the collection of F-rational points of E is again a finitely generated abelian group by Weil [31], so one may seek to classify the groups occurring as $E(F)_{\text{tors}}$. In fact, by Merel's Uniform Boundedness Theorem [22], there are only finitely many groups that arise as $E(F)_{\text{tors}}$, even as E ranges over all elliptic curves defined over all number fields F of a fixed degree. Thus the fundamental question which motivates our work is the following:

Question 1. *For a fixed $d \in \mathbb{Z}^+$, what groups arise as torsion subgroups of an elliptic curve defined over a number field of degree d?*

Now 100 years after Mordell's proof, the answer to Question 1 is known only for $d \leq 3$; see [21, 18, 20, 19, 11]. A fundamental obstruction to extending the classification to $d > 3$ is the existence of so-called **sporadic** or **isolated** points on modular curves which can give rise to torsion subgroups occurring on only finitely many elliptic curves (up to isomorphism) defined over all number fields of a fixed degree. To date, we lack adequate tools for detecting such points, and hence the problem of classifying torsion subgroups of elliptic curves over higher degree number fields remains largely open.

One way to obtain classification results beyond cubic fields is to restrict the elliptic curves under consideration. One common family of elliptic curves to study in this context is elliptic curves $E/\mathbb{Q}$ under base extension, where the classification of torsion subgroups is known for degrees $d \leq 5$, $d = 7$, or d not divisible by a prime ≤ 7; see [24, 13, 12]. If we require only that the j-invariant of E lie in $\mathbb{Q}$, then analogous classification results exist [14, 10]. Another common family is elliptic curves with

2020 *Mathematics Subject Classification.* Primary 11G05, 11G15.

complex multiplication (CM), which are elliptic curves with unusually large endomorphism rings. Whereas most elliptic curves have endomorphism ring isomorphic to $\mathbb{Z}$, we say E/F is a CM elliptic curve if $\mathrm{End}_{\overline{F}}(E) \cong \mathcal{O}$, an order in an imaginary quadratic field K. Each order is uniquely determined by its discriminant $\Delta \coloneqq [\mathcal{O}_K : \mathcal{O}]^2 \cdot \Delta_K$, where Δ_K is the discriminant of K and $\mathcal{O}_K$ is its ring of integers. For the collection of all CM elliptic curves, the classification of torsion subgroups is known for any $d \leq 13$ or for any odd $d > 13$; see [6, 25, 5, 4]. We note that CM elliptic curves produce many examples of sporadic points on modular curves (see, for example, [7]), so this provides further motivation for studying this class in particular.

In the present work, we extend the classification of torsion subgroups of CM elliptic curves to those defined over any number field of degree twice a prime, building on work of the first author and Clark [1, 2]. In fact, since the classification is known for $d = 4, 6$, and 10 by [6], we need only consider fields of degree $2p$ for primes $p > 5$. Our classification is most clearly stated in the context of new subgroups. By Theorem 2.1 in [4], if a torsion subgroup arises in degree d', then it arises in any degree d for which $d' \mid d$. We say a CM torsion subgroup is **new** if it occurs in degree d and not in any degree $d' < d$ such that $d' \mid d$. Since torsion subgroups of CM elliptic curves in degrees 1 and 2 are known [25, 6], and there are no new CM torsion subgroups in degree $p > 5$ for p prime [4], it suffices to classify only the new subgroups arising in degree $2p$.

Theorem 1.2. *Let F be a number field of degree $2p$ for $p > 5$ prime and let E/F be an elliptic curve with CM by the order of discriminant Δ. Then $E(F)_{\mathrm{tors}}$ is new if and only if one of the following occurs:*

(1) $\Delta = -115$, $p = 11$, *and* $E(F)_{\mathrm{tors}} \cong \mathbb{Z}/23\mathbb{Z}$.
(2) $\Delta = -235$, $p = 23$, *and* $E(F)_{\mathrm{tors}} \cong \mathbb{Z}/47\mathbb{Z}$.
(3) $\Delta \in \{-11, -19, -27, -43, -67, -163\}$, $2p + 1$ *is prime with* $\left(\frac{\Delta}{2p+1}\right) = 1$, *and* $E(F)_{\mathrm{tors}} \cong \mathbb{Z}/(2p + 1)\mathbb{Z}$.
(4) $\Delta \in \{-8, -12, -16, -28\}$, $2p + 1$ *is prime with* $\left(\frac{\Delta}{2p+1}\right) = 1$, *and* $E(F)_{\mathrm{tors}} \cong \mathbb{Z}/2(2p + 1)\mathbb{Z}$.
(5) $\Delta = -7$, $2p + 1$ *is prime with* $\left(\frac{\Delta}{2p+1}\right) = 1$, *and* $E(F)_{\mathrm{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2(2p + 1)\mathbb{Z}$.
(6) $\Delta = -3$, $p = 7$, *and* $E(F)_{\mathrm{tors}} \cong \mathbb{Z}/49\mathbb{Z}$.
(7) $\Delta = -3$, $6p + 1$ *is prime, and* $E(F)_{\mathrm{tors}} \cong \mathbb{Z}/(6p + 1)\mathbb{Z}$.
(8) $\Delta = -4$, $4p + 1$ *is prime, and* $E(F)_{\mathrm{tors}} \cong \mathbb{Z}/2(4p + 1)\mathbb{Z}$.

In particular, any new torsion subgroup arises on one of only finitely many CM elliptic curves, and all but $\Delta = -115$ and -235 correspond to imaginary quadratic orders of class number 1.

Remark 1.3. In [15], the authors classify torsion subgroups of Mordell curves defined over $\mathbb{Q}$ under base extension to number fields of degree $2p$ and $3p$, where $p \geq 5$ is prime. Every Mordell curve E has $j(E) = 0$ and CM by the order of discriminant $\Delta = -3$. Our classification result includes additional groups since we are not requiring elliptic curves with $j(E) = 0$ to be defined over $\mathbb{Q}$.

Theorem 1.2 tells us that if $\Delta \neq -3, -4$, then the only Δ-CM torsion subgroups that can arise in degree $2p$ for $p > 5$ that did not occur over a number field of degree 2 or degree p must have exponent $2p + 1$ or $2(2p + 1)$, where p is a Sophie Germain prime. It is conjectured that there are infinitely many Sophie Germain primes, though this remains unproven. These primes were a vital piece of Sophie Germain's investigations concerning Fermat's Last Theorem.

From Theorem 1.2, we can quickly deduce the torsion subgroups that arise for CM elliptic curves defined over number fields of degree $2p$ where $p > 5$ is prime, including for the first previously unknown degree $d = 14$. For example, 7 is not a Sophie Germain prime, but $6 \cdot 7 + 1$ and $4 \cdot 7 + 1$ are both prime. Thus, by Theorem 1.2, the new torsion subgroups in degree 14 are precisely $\mathbb{Z}/43\mathbb{Z}$, $\mathbb{Z}/49\mathbb{Z}$, and $\mathbb{Z}/58\mathbb{Z}$. We record this and other small degrees in the following result.

Corollary 1.4. *Let F be a number field of degree $2p$ for $p \in \{7, 11, 13, 17, 19\}$, and let E/F be a CM elliptic curve. The group $E(F)_{\mathrm{tors}}$ is isomorphic to one of the following groups which arises over quadratic fields*

$$\begin{array}{ll} \mathbb{Z}/m\mathbb{Z} & \textit{for } m = 1, 2, 3, 4, 6, 7, \textit{ or } 10 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z} & \textit{for } m = 1, 2, \textit{ or } 3 \\ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} & \end{array}$$

or else

(1) $p = 7$ and $E(F)_{\mathrm{tors}} \cong \mathbb{Z}/m\mathbb{Z}$ for $m = 43, 49,$ or 58,
(2) $p = 11$ and $E(F)_{\mathrm{tors}} \cong \mathbb{Z}/m\mathbb{Z}$ for $m = 23, 46, 67$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/46\mathbb{Z}$,
(3) $p = 13$ and $E(F)_{\mathrm{tors}} \cong \mathbb{Z}/m\mathbb{Z}$ for $m = 79$ or 106, or
(4) $p = 17$ and $E(F)_{\mathrm{tors}} \cong \mathbb{Z}/m\mathbb{Z}$ for $m = 103$.

Moreover, each group occurs.

Remark 1.5. Since there are only finitely many CM j-invariants contained in all number fields of a fixed degree (see §2), each of these groups necessarily arises on only finitely many CM elliptic curves.

In particular, by Corollary 1.4, we see that *no* new torsion subgroups arise on CM elliptic curves defined over number fields of degree $d = 2 \cdot 19$. Thus, another consequence of Theorem 1.2 is a description of degrees of the form $2p$ such that no new torsion subgroups occur.

Corollary 1.6. *Let F be a number field of degree $2p$, for $p > 5$, and suppose none of the following hold:*

(1) $2p + 1$ is prime and split in an imaginary quadratic order of class number 1 with $\Delta < -4$.
(2) $4p + 1$ is prime.
(3) $6p + 1$ is prime.

Then for any CM elliptic curve E/F, the torsion subgroup $E(F)_{\mathrm{tors}}$ is isomorphic to one of the groups that arise for CM elliptic curves defined over quadratic fields.

This finding is significant in the context of "stratification of torsion," a phenomenon first explored in [3, 5] for CM torsion subgroups in odd degree. For any positive integer d, let $\mathscr{G}_{\mathrm{CM}}(d)$ denote the set of isomorphism classes of groups which arise as $E(F)_{\mathrm{tors}}$ for some CM elliptic curve E over some degree d number field F. For any positive integer d, we define the set of d-Olson degrees to be those positive integers d' for which $\mathscr{G}_{\mathrm{CM}}(d') = \mathscr{G}_{\mathrm{CM}}(d)$. In the case of odd d, we find that the set of d-Olson degrees possesses a positive asymptotic density [5], but whether the same holds true for any even d is still an open problem. See [5, Questions 1.6].

Remark 1.7. In fact, as noted by Clark, Corollary 1.6 implies there exist infinitely many 2-Olson degrees. Recall the Prime Number Theorem states that the number of primes $p \leq X$ is asymptotic to $\frac{X}{\log X}$. On the other hand, for any even $a \in \mathbb{Z}^+$, as $X \to \infty$ the number of primes $p \leq X$ such that $ap + 1$ is also prime is $O(\frac{X}{\log^2 X})$; see [16, Thm. 3.12]. By applying this with $a = 2, 4$ and 6, we see that there are infinitely many primes $p \leq X$ such that $2p$ is a 2-Olson degree.

Acknowledgements

We thank Frank Moore, Jeremy Rouse, and the anonymous referees for helpful comments on an earlier draft, and we thank Pete L. Clark for Remark 1.7 and other helpful comments. The first author was partially supported by an A.J. Sterge Faculty Fellowship and NSF grant DMS-2137659.

2. Background and Notation

For most elliptic curves E over a number field F, the ring of endomorphisms of E defined over $\overline{F}$ is isomorphic to $\mathbb{Z}$, where $n \in \mathbb{Z}$ corresponds to the multiplication-by-n map on E. We say an elliptic curve has **complex multiplication**, or CM, if its endomorphism ring is strictly larger than $\mathbb{Z}$. For a CM elliptic curve E/F, there is an imaginary quadratic field K and positive integer f such that $\mathrm{End}_{\bar{F}}(E) \cong \mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$, the order in K of **conductor** f. Here $\mathcal{O}_K$ denotes the full ring of integers in K. In particular, we note that $\mathcal{O} \subseteq \mathcal{O}_K$ and $[\mathcal{O}_K : \mathcal{O}] = f$. The order is largest when $f = 1$, and so we call $\mathcal{O}_K$ the **maximal order**. Any order $\mathcal{O}$ in an imaginary quadratic field K can be uniquely identified using its **discriminant**,

$$\Delta = \Delta(\mathcal{O}) = f^2 \cdot \Delta_K,$$

where Δ_K is the discriminant of K. We let ω denote the number of units in $\mathcal{O}$, so

$$\omega = \begin{cases} 6 & \text{if } \Delta = -3, \\ 4 & \text{if } \Delta = -4, \\ 2 & \text{if } \Delta < -4. \end{cases}$$

For an elliptic curve E with CM by the order of discriminant Δ, we have $\Delta = -3$ if and only if $j(E) = 0$ and $\Delta = -4$ if and only if $j(E) = 1728$. We use w_K to denote $\#\mathcal{O}_K^\times$.

CM elliptic curves have a well-known and beautiful connection with class field theory. For example, if E has CM by the maximal order in K, then $K(j(E), \mathfrak{h}(E_{\mathrm{tors}}))$ is the maximal abelian extension of K, where $\mathfrak{h} : E \to E/\operatorname{Aut}(E) \cong \mathbb{P}^1$ denotes a Weber function on E. If one adjoins the values of a Weber function only on points of order dividing N, we obtain the ray class field of K modulo N; see, for example Theorem II.5.6 and Corollary II.5.7 of [30]. Of particular relevance to the present work is the fact that if E has CM by the order in K of conductor f, then $K(j(E))$ is the ring class field of K of conductor f and $[K(j(E)) : K] = [\mathbb{Q}(j(E)) : \mathbb{Q}] = h(\mathcal{O})$, the class number of $\mathcal{O}$. For an elliptic curve E with CM by the order of discriminant $f^2\Delta_K$ with $f \geq 2$, we have [9, Cor. 7.24]

$$[K(j(E)) : K] = h_K \frac{2}{w_K} f \prod_{p \mid f} \left(1 - \left(\frac{\Delta_K}{p}\right) \frac{1}{p}\right), \tag{1}$$

where h_K denotes the class number of K and $\left(\frac{\Delta_K}{p}\right)$ is the Kronecker symbol. As there are only finitely many imaginary quadratic fields of a given class number [17, Theorem III], there are only finitely many imaginary quadratic orders of a given class number by (1). For each imaginary quadratic order $\mathcal{O}$, there are precisely $h(\mathcal{O})$ non-isomorphic $\mathcal{O}$-CM elliptic curves.

A crucial ingredient in the proof of our main result is the following theorem. Recall $\omega = \#\mathcal{O}^\times$.

Theorem 2.1 (Bourdon, Clark, [2, Theorem 4.1])**.** *Let K be an imaginary quadratic field, and let $\mathcal{O}$ 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 $T(\mathcal{O}, M, N) \in \mathbb{Z}^+$ 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 $\mathcal{O}$-CM elliptic curve E/F such that $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow E(F)$ if and only if $T(\mathcal{O}, M, N) \mid d$.

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

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

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

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

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

(3) Suppose $N \geq 4$. Then we have

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

where the definition of $\widetilde{T}(\mathcal{O}, \ell^a, \ell^b)$ appears below. Put $c := \operatorname{ord}_\ell(f)$.

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

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

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

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

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

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

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

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

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

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

From this, we deduce the following corollary, which also appears as Theorem 6.2 in [1]. It refines earlier results of Silverberg [28, 29].

Corollary 2.2. *Let $\mathcal{O}$ be an order in an imaginary quadratic field K, and let $N \in \mathbb{Z}^+$. Then*

$$\varphi(N) \mid \omega \cdot T(\mathcal{O}, 1, N).$$

Suppose E/F is an $\mathcal{O}$-CM elliptic curve with $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow E(F)$. Since $[K(j(E)) : K] = [\mathbb{Q}(j(E)) : \mathbb{Q}] = h(\mathcal{O})$, we can actually consider the divisibility conditions in Theorem 2.1 over $\mathbb{Q}(j(E))$, as illustrated in the field diagram below.

$$\begin{tikzcd}
 & FK \arrow[dd, dash, "\text{divisible by } T(\mathcal{O},M,N)"] \\
F \arrow[ur, dash, "1 \text{ or } 2"] \arrow[dd, dash, "\text{divisible by } T(\mathcal{O},M,N)"'] & \\
 & K(j(E)) \arrow[dd, dash, "h(\mathcal{O})"] \\
\mathbb{Q}(j(E)) \arrow[ur, dash, "2"] \arrow[dd, dash, "h(\mathcal{O})"'] & \\
 & K \\
\mathbb{Q} \arrow[ur, dash, "2"] &
\end{tikzcd}$$

Corollary 2.3. *Let $\mathcal{O}$ be an order in an imaginary quadratic field K, and let E/F be an $\mathcal{O}$-CM elliptic curve with an F-rational point of order $N \in \mathbb{Z}^+$. Then $T(\mathcal{O}, 1, N) \mid [F : \mathbb{Q}(j(E))]$ and*

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

Proof. This follows from Corollary 2.2 and the diagram above. □

Following [2], for any imaginary quadratic order $\mathcal{O}$ and integers $M \mid N$, we let $T^\circ(\mathcal{O}, M, N)$ denote the least degree of an extension $F/\mathbb{Q}(j(E))$ in which an $\mathcal{O}$-CM elliptic curve E/F has $\mathbb{Z}/M\mathbb{Z}\times\mathbb{Z}/N\mathbb{Z} \hookrightarrow E(F)$. In particular, F need not contain the CM field K. We note $T^\circ(\mathcal{O}, M, N) = 2^\epsilon \cdot T(\mathcal{O}, M, N)$, where $\epsilon \in \{0, 1\}$. Explicit formulas for $T^\circ(\mathcal{O}, M, N)$ for fixed $\mathcal{O}$ are computed in [2, §8].

In the case where $M = 1$, we use the streamlined notation $T(\mathcal{O}, N) := T(\mathcal{O}, 1, N)$ and $T^\circ(\mathcal{O}, N) := T^\circ(\mathcal{O}, 1, N)$. We have the following description of $T^\circ(\mathcal{O}, N)$, which follows from Theorems 1.3, 6.1, 6.2, and 6.6 in [2].

Theorem 2.4 (Bourdon, Clark [2])**.** *Let $\mathcal{O}$ be an imaginary quadratic order of conductor f in K. Let $N \in \mathbb{Z}^+$ have prime power decomposition $\ell_1^{a_1} \cdots \ell_r^{a_r}$ with $\ell_1 < \ldots < \ell_r$. The least degree over $\mathbb{Q}(j(E))$ in which there is an $\mathcal{O}$-CM elliptic curve E with a rational point of order N is $T(\mathcal{O}, N)$ if and only if $T^\circ(\mathcal{O}, \ell_i^{a_i}) = T(\mathcal{O}, \ell_i^{a_i})$ for all $1 \leq i \leq r$. Otherwise the least degree is $2 \cdot T(\mathcal{O}, N)$. Moreover, $T^\circ(\mathcal{O}, \ell_i^{a_i}) = T(\mathcal{O}, \ell_i^{a_i})$ if and only if one of the following holds, where $c_i := \operatorname{ord}_{\ell_i}(f)$:*

(1) ℓ_i is inert in $\mathcal{O}$
(2) $\ell_i^{a_i} = 2$ and is split or ramified in $\mathcal{O}$
(3) $\ell_i^{a_i} = 2^{a_i}$ where 2 is ramified in $\mathcal{O}$ but not in K, $c_i \geq 2$, and $a_i \leq 2c_i - 2$
(4) $\ell_i^{a_i} = 2^{a_i}$ where 2 is ramified in K and $c_i = 0$
(5) $\ell_i^{a_i} = 2^{a_i}$ where $\operatorname{ord}_2(\Delta_K) = 2$, $c_i \geq 1$, and $a_i \leq 2c_i$
(6) $\ell_i^{a_i} = 2^{a_i}$ where $\operatorname{ord}_2(\Delta_K) = 3$, $c_i \geq 1$
(7) $\ell_i > 2$ is ramified in $\mathcal{O}$ but split in K and $a_i \leq 2c_i$
(8) $\ell_i > 2$ is ramified in $\mathcal{O}$ and not split in K

Let E/F be an $\mathcal{O}$-CM elliptic curve and $P \in E$ a point of order N. If $[F : \mathbb{Q}] = T^\circ(\mathcal{O}, N) \cdot h(\mathcal{O})$, then $F = \mathbb{Q}(j(E), \mathfrak{h}(P))$, where $\mathfrak{h} : E \to E/\operatorname{Aut}(E) \cong \mathbb{P}^1$ is a Weber function on E. Moreover, if $\psi : E \to E'$ is an isomorphism, then $\mathfrak{h}(P) = \mathfrak{h}(\psi(P))$ by [27, p.107]. It follows that for any $P \in E$, the fields $K(j(E), \mathfrak{h}(P))$ and $\mathbb{Q}(j(E), \mathfrak{h}(P))$ do not depend on the chosen Weierstrass equation for E. See [2, §2.4] and [1, §7A] for additional details.

3. Determining the Exponent of New Subgroups

Let $p > 5$ be a prime number, and suppose F is a number field of degree $2p$. Let E/F be a CM elliptic curve with $E(F)_{\text{tors}} \cong \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ for $M \mid N$. By definition, this torsion subgroup is **new** if it does not occur as the torsion subgroup of a CM elliptic curve defined over a number field of degree 1, 2, or p. However, every CM torsion subgroup arising in degree 1 also arises in degree 2, and there are *no* new torsion subgroups of CM elliptic curves in prime degree $p > 5$ by [4, Theorem 1.4]. Thus $E(F)_{\text{tors}}$ is new if and only if it does not occur in degree 2.

In this section, we will determine the possible exponents of a new CM torsion subgroup in degree $2p$. If $E(F)_{\text{tors}} \cong \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ is a new torsion subgroup, then either N appears already as the exponent of a CM torsion subgroup in degree 2 and $N \in \{1, 2, 3, 4, 6, 7, 10\}$ by [6, §4.2], or else it has exponent outside this list. We say $E(F)_{\text{tors}}$ has a **new exponent** N if $E(F)_{\text{tors}}$ is new and $N \notin \{1, 2, 3, 4, 6, 7, 10\}$.

3.1. Two Preliminary Lemmas.

By Corollary 2.2, if $\mathcal{O}$ is an order in an imaginary quadratic field and $N \in \mathbb{Z}^+$, then

$$\varphi(N) \mid \omega \cdot T(\mathcal{O}, N).$$

Since $T^\circ(\mathcal{O}, N) \in \{T(\mathcal{O}, N), 2 \cdot T(\mathcal{O}, N)\}$, this implies $\varphi(N) \mid \omega \cdot T^\circ(\mathcal{O}, N)$. The following lemma shows equality can hold under only very specific conditions.

Lemma 3.1. *Let $N \in \mathbb{Z}^{\geq 4}$ have prime power decomposition $\ell_1^{a_1} \cdots \ell_r^{a_r}$ with $\ell_1 < \cdots < \ell_r$, and let $\mathcal{O}$ be an imaginary quadratic order of discriminant Δ. If $\varphi(N) = \omega \cdot T^\circ(\mathcal{O}, N)$, then every ℓ_i with $\ell_i^{a_i} \geq 3$ is ramified in $\mathcal{O}$. If $\ell_i^{a_i} = 2$, then 2 is split or ramified in $\mathcal{O}$.*

Proof. Suppose $\ell \mid N$ is prime and $\operatorname{ord}_\ell(N) = a$ with $\ell^a \geq 3$, and suppose $\varphi(N) = \omega \cdot T^\circ(\mathcal{O}, N)$. In particular, this implies $T(\mathcal{O}, N) = T^\circ(\mathcal{O}, N)$ by Corollary 2.2, and so by Theorem 2.4, we have $T(\mathcal{O}, \ell^a) = T^\circ(\mathcal{O}, \ell^a)$. Then $\left(\frac{\Delta}{\ell}\right) \neq 1$ by Theorem 2.4. Suppose $\left(\frac{\Delta}{\ell}\right) = -1$. Recall from Theorem 2.1 that since $N \geq 4$,

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

If $\varphi(N) = \omega \cdot T(\mathcal{O}, N)$, we must have $\varphi(N) = \prod_{i=1}^{r} \widetilde{T}(\mathcal{O}, \ell_i^{a_i})$. Moreover, since $\varphi(\ell_i^{a_i}) \mid \widetilde{T}(\mathcal{O}, \ell_i^{a_i})$ for all i, we must have $\varphi(\ell^a) = \widetilde{T}(\mathcal{O}, \ell^a)$. By Theorem 2.1 we have

$$\widetilde{T}(\mathcal{O}, \ell^a) = \ell^{2a-2}(\ell^2 - 1) = (\ell^{a-1})(\ell^{a-1})(\ell - 1)(\ell + 1) > \varphi(\ell^a).$$

We have reached a contradiction. The same kind of calculation shows 2 cannot be inert in $\mathcal{O}$. □

Lemma 3.2. *Let E/F be an $\mathcal{O}$-CM elliptic curve with an F-rational point of order N for $N \in \mathbb{Z}^+$. If $\omega \cdot [F : \mathbb{Q}(j(E))] = \varphi(N)$, then*

$$T(\mathcal{O}, N) = T^\circ(\mathcal{O}, N) = [F : \mathbb{Q}(j(E))].$$

Proof. By Corollaries 2.2 and 2.3 we have

$$\varphi(N) \mid \omega \cdot T(\mathcal{O}, N) \mid \omega \cdot [F : \mathbb{Q}(j(E))] = \varphi(N),$$

from which we conclude equality holds throughout. Thus $T(\mathcal{O}, N) = T^\circ(\mathcal{O}, N) = [F : \mathbb{Q}(j(E))]$. □

3.2. **Determining new exponents.** Let F be a number field of degree $2p$, for $p > 5$ prime. If E/F is an $\mathcal{O}$-CM elliptic curve with a point of order N, then $h(\mathcal{O}) = [\mathbb{Q}(j(E)) : \mathbb{Q}] \in \{1, 2, p, 2p\}$. We will consider each case separately in a series of lemmas. One important ingredient is the following theorem of Parish.

Theorem 3.3 (Parish, [26, §6])**.** *Let E be a CM elliptic curve defined over $F = \mathbb{Q}(j(E))$. Then $E(F)_{\text{tors}}$ is isomorphic to one of the following groups: the trivial group $\{\cdot\}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}$, or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

All other cases build upon Theorems 2.1 and 2.4 in combination with Lemma 3.1.

Lemma 3.4. *Let F be a number field of degree $2p$. Suppose E/F is an $\mathcal{O}$-CM elliptic curve, where $h(\mathcal{O}) = 2p$. Then $E(F)_{\text{tors}}$ is not new.*

Proof. Here, $F = \mathbb{Q}(j(E))$ and $E(F)_{\text{tors}}$ is one of the groups arising over $\mathbb{Q}$ by Theorem 3.3. □

Lemma 3.5. *Let F be a number field of degree $2p$ for $p > 5$. Suppose E/F is an $\mathcal{O}$-CM elliptic curve, where $h(\mathcal{O}) = p$. Then $E(F)_{\text{tors}} \cong \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ for $M \mid N$ and $N \in \{1, 2, 3, 4, 6\}$.*

Proof. Note in this case $[F : \mathbb{Q}(j(E))] = 2$, which means $\varphi(N) \mid \omega \cdot 2$ by Corollary 2.3. As $h(\mathcal{O}) = p$, we have $\omega = 2$, and so $N \in \{1, 2, 3, 4, 5, 6, 8, 10, 12\}$. If N is a new exponent, then $N \in \{5, 8, 12\}$. We will show these do not occur, and we will also rule out $N = 10$.

Suppose $N \in \{5, 8, 12\}$. Then $\varphi(N) = 4 = 2 \cdot [F : \mathbb{Q}(j(E))]$, and by Lemma 3.2 we have $T(\mathcal{O}, N) = T^{\circ}(\mathcal{O}, N) = 2$. Thus by Lemma 3.1 each prime dividing N is ramified in $\mathcal{O}$. Since $h(\mathcal{O}) = p > 5$, in particular the class number is odd, and so $\Delta(\mathcal{O}) = -2^{\epsilon} \cdot \ell^{2a+1}$ for $\epsilon \in \{0, 2\}$ and $\ell \equiv 3 \pmod 4$ prime; see, for example, Lemma 3.5 of [4]. This shows immediately that $N \neq 5$. So suppose $N = 8$. Then $\epsilon = 2$, and $\mathcal{O}$ is an order of conductor $2\ell^a$, where 2 is split or inert in the corresponding imaginary quadratic field $K = \mathbb{Q}(\sqrt{-\ell})$. Then $T(\mathcal{O}, 2^3) < T^{\circ}(\mathcal{O}, 2^3)$ by Theorem 2.4, which gives a contradiction. Similarly, if $N = 12$, we find $T(\mathcal{O}, 2^2) < T^{\circ}(\mathcal{O}, 2^2)$, and so $T(\mathcal{O}, 12) < T^{\circ}(\mathcal{O}, 12)$ by Theorem 2.4.

Finally, we note $N \neq 10$, since E cannot have a point of order 5 by the argument above. □

Lemma 3.6. *Let F be a number field of degree $2p$ for $p > 5$. Suppose E/F is an $\mathcal{O}$-CM elliptic curve, where $\mathcal{O}$ has class number 2. Then $E(F)_{\text{tors}}$ has new exponent N if and only if one of the following occurs:*

(1) $N = 23$, $p = 11$, and $\Delta(\mathcal{O}) = -115$.
(2) $N = 47$, $p = 23$, and $\Delta(\mathcal{O}) = -235$.

Proof. Suppose $E(F)_{\text{tors}} \cong \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ for $M \mid N$. Note in this case $[F : \mathbb{Q}(j(E))] = p$, which means $\varphi(N) \mid \omega \cdot p$ by Corollary 2.3. As $h(\mathcal{O}) = 2$, we have $\omega = 2$. If $\varphi(N) \mid 2p$, then $N = 2^a \cdot q^b$ where q is an odd prime and $a \leq 2$, for otherwise $\text{ord}_2(\varphi(N)) > \text{ord}_2(2p) = 1$. If $b = 0$, then $N \in \{1, 2, 4\}$, so suppose $b > 0$. It follows that $a \leq 1$, for otherwise $\text{ord}_2(\varphi(N)) > 1$. Thus

$$\varphi(N) = 2^{a-1} \cdot q^{b-1}(q-1) \mid 2p.$$

If $q = 3$, then the assumption that $p > 5$ implies $N = 3$ or $N = 6$, so suppose $q \neq 3$. Then $q - 1 \mid 2p$ implies $q - 1 = 2p$, since both p, q are odd and $q \neq 3$. That is, if $E(F)$ has a point of order N, then $N \in \{1, 2, 3, 4, 6, 2p + 1, 2 \cdot (2p + 1)\}$ where $2p + 1$ is prime. If N is a new exponent, then $N \notin \{1, 2, 3, 4, 6\}$ by definition, and so $N \in \{2p + 1, 2 \cdot (2p + 1)\}$.

Now, suppose E/F has a point P of order $N = 2p + 1$, where $2p + 1$ is prime. Then $\varphi(N) = 2p$, and by Lemma 3.2, we have $p = T(\mathcal{O}, N) = T^{\circ}(\mathcal{O}, N)$. Thus by Lemma 3.1, N is ramified in $\mathcal{O}$. That is, $N \mid f^2 \Delta_K$. Based on the formula for $h(\mathcal{O})$ (see equation 1 in §2) and the classification of imaginary quadratic fields of class numbers 1 and 2 (see, for example, [8, p.229]), this can happen only if $N = 23$ and $\Delta(\mathcal{O}) = -115$ or $N = 47$ and $\Delta(\mathcal{O}) = -235$. Conversely, if $\Delta(\mathcal{O}) = -115$, then there exists a point of order 23 in degree $11 \cdot [\mathbb{Q}(j(E)) : \mathbb{Q}] = 2 \cdot 11$ by Theorem 2.4. Similarly, if $\Delta(\mathcal{O}) = -235$, then there exists a point of order 47 in degree $23 \cdot [\mathbb{Q}(j(E)) : \mathbb{Q}] = 2 \cdot 23$.

Finally, suppose E/F has a point P of order $2 \cdot (2p+1)$, where $2p+1$ is prime. Then in particular E has a point of order $2p+1$, and so by the previous paragraph either $2p+1 = 23$ and $\Delta(\mathcal{O}) = -115$ or else $2p+1 = 47$ and $\Delta(\mathcal{O}) = -235$. In each case, 2 is inert in $\mathcal{O}$, and so by Theorem 2.1 $T(\mathcal{O}, 2 \cdot (2p+1)) = 3p$, and we have a contradiction by Corollary 2.3. □

Lemma 3.7. *Let F be a number field of degree $2p$ for $p > 5$. Suppose E/F is an $\mathcal{O}$-CM elliptic curve, where $\mathcal{O}$ has class number 1 and $\Delta(\mathcal{O}) < -4$. Then $E(F)_{\text{tors}}$ has new exponent N if and only if we are in one of the following cases:*

(1) $N = 2p+1$ where $2p+1$ is a prime split in $\mathcal{O}$ and $\left(\frac{\Delta}{2}\right) = -1$.

(2) $N = 2 \cdot (2p+1)$ where $2p+1$ is a prime split in $\mathcal{O}$ and $\left(\frac{\Delta}{2}\right) \neq -1$.

Proof. Suppose $E(F)_{\text{tors}} \cong \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ for $M \mid N$. Note in this case $[F : \mathbb{Q}(j(E))] = [F : \mathbb{Q}] = 2p$, which means $\varphi(N) \mid \omega \cdot 2p$ by Corollary 2.3. Since $\Delta < -4$, it follows that $\omega = 2$. Thus $\varphi(N) \mid 4p$. If $\varphi(N) \mid 4$, then $N \in \{1, 2, 3, 4, 5, 6, 8, 10, 12\}$. If $\varphi(N) \mid 2p$, then the proof of the previous lemma shows $N \in \{1, 2, 3, 4, 6, 2p+1, 2 \cdot (2p+1)\}$ where $2p+1$ is prime. Thus the only remaining case is when $\varphi(N) = 4p$. But in this case Lemma 3.2 implies $T(\mathcal{O}, N) = T^{\circ}(\mathcal{O}, N) = 2p$. By Lemma 3.1, if $N \geq 4$, then $N = \prod \ell_i^{a_i}$ where ℓ_i is a prime ramified in $\mathcal{O}$ or $N = 2 \cdot \prod \ell_i^{a_i}$ where 2 is split in $\mathcal{O}$ and ℓ_i is an odd prime ramified in $\mathcal{O}$. As the discriminant of $\mathcal{O}$ is in

$$\{-7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163\},$$

there are no possibilities such that $\varphi(N) = 4p$ for $p > 5$. We note that if N is new, then $N \notin \{1, 2, 3, 4, 6, 10\}$ by definition. Furthermore, $N \notin \{5, 8, 12\}$, for otherwise $4 \mid [F : \mathbb{Q}]$; see, for example, the table in the appendix of [4].

Now, suppose $N = 2p+1$, where $2p+1$ is prime. Since $p > 5$, we see immediately from the list of imaginary quadratic discriminants of class number 1 that N is not ramified in $\mathcal{O}$, and N is not inert, for otherwise $T(\mathcal{O}, N) = 2p(p+1) \nmid [F : \mathbb{Q}]$ by Theorem 2.1. Now, suppose N is split in $\mathcal{O}$. Then $T^{\circ}(\mathcal{O}, N) = 2p$ by Theorem 2.4. By Theorem 2.1, $N = 2 \cdot (2p+1)$ is possible only if 2 is split or ramified in $\mathcal{O}$. Conversely, suppose 2 is split or ramified in $\mathcal{O}$. Then $\Delta \in \{-7, -8, -12, -16, -28\}$. In each case, such an $\mathcal{O}$-CM elliptic curve E/F will always have an F-rational point of order 2; this can be seen, for example, by the fact that any model of such an elliptic curve over $\mathbb{Q}$ will have a rational point of order 2, and points of order 2 are invariant under quadratic twist. □

Lemma 3.8. *Let F be a number field of degree $2p$ for $p > 5$. Suppose E/F is an $\mathcal{O}$-CM elliptic curve, where $\Delta(\mathcal{O}) = -4$. Then $E(F)_{\text{tors}}$ has new exponent N if and only if $N = 2 \cdot (4p+1)$ where $4p+1$ is prime.*

Proof. Suppose $E(F)_{\text{tors}} \cong \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ for $M \mid N$. If $\Delta = -4$, then $\omega = 4$ and $\varphi(N) \mid 8p$ by Corollary 2.3. If $\varphi(N) \mid 8$, then

$$N \in \{1, 2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 20, 24, 30\}.$$

If $\varphi(N) \mid 4p$, then $\operatorname{ord}_2(\varphi(N)) \leq \operatorname{ord}_2(4p) = 2$ implies $N = 2^a \cdot q_1^b \cdot q_2^c$ where q_1, q_2 are odd primes and $a \leq 3$. If $a = 3$, then $N = 8$, so suppose $a = 2$. Then $N = 2^2 \cdot q_1^b$. If $b > 0$, then the assumption that $\varphi(N) = 2 \cdot q_1^{b-1}(q_1 - 1) \mid 4p$ implies $q_1 = 3$ or $2p+1$ as above, and $b = 1$. If $a \leq 1$, then $N = 2^a \cdot q_1^b \cdot q_2^c$, and we have

$$\varphi(N) = q_1^{b-1}(q_1 - 1) \cdot q_2^{c-1}(q_2 - 1) \mid 4p.$$

In particular, $q_i - 1 \mid 4p$ implies $q_i \in \{3, 5, 2p+1, 4p+1\}$, since it is an odd prime. Thus if $\varphi(N) \mid 4p$, the only possibilities are

$$N \in \{1, 2, 3, 4, 5, 6, 8, 10, 12, 2p+1, 2 \cdot (2p+1), 3 \cdot (2p+1), 4 \cdot (2p+1), 6 \cdot (2p+1), 4p+1, 2 \cdot (4p+1)\},$$

where $2p+1$ and $4p+1$ can arise only if they are prime. Finally, suppose $\varphi(N) = 8p$. But Lemma 3.2 implies $2p = T(\mathcal{O}, N) = T^{\circ}(\mathcal{O}, N)$. By Lemma 3.1, $N \in \{1, 3, 2^a\}$ since $\Delta = -4$, but none of these satisfy $\varphi(N) = 8p$.

We note that if N is a new exponent, then $N \notin \{1, 2, 3, 4, 6, 10\}$ by definition, so we may remove these values from consideration. By Theorem 2.1, $T(\mathcal{O}, N) \nmid 2p$ if $N \in \{8, 12, 15, 20\}$, which implies N cannot be any of these values, along with 16, 24, or 30. Though there can exist a point of order 5 on an $\mathcal{O}$-CM elliptic curve defined over a number field F of degree $2p$, such an elliptic curve corresponds to an equation of the form $y^2 = x^3 + Ax$ and so has an F-rational point of order 2. Thus an exponent of 5 is not possible. Now, consider a prime $N = 2p+1$, which cannot be ramified since $\Delta = -4$. If N is inert, then $T(\mathcal{O}, N) = p(p+1) \nmid 2p$. In addition, N cannot be split, since then $T(\mathcal{O}, N) = p/2$ would not be an integer. Thus if $E(F)_{\text{tors}}$ has new exponent N, then $N \in \{4p+1, 2\cdot(4p+1)\}$ where $4p+1$ is prime. Since $\left(\frac{-4}{4p+1}\right) = 1$, there is a point of order $4p+1$ in degree $2p$ by Theorem 2.4 and Theorem 2.1. As E has the form $y^2 = x^3 + Ax$, there is a point of order 2 as well, so $N = 2\cdot(4p+1)$. □

Lemma 3.9. *Let F be a number field of degree $2p$ for $p > 5$. Suppose E/F is an $\mathcal{O}$-CM elliptic curve, where $\Delta(\mathcal{O}) = -3$. Then $E(F)_{\text{tors}}$ has new exponent N if and only if we are in one of the following cases:*

(1) $N = 49$ and $p = 7$.

(2) $N = 6p+1$ where $6p+1$ is prime.

Proof. Suppose $E(F)_{\text{tors}} \cong \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ for $M \mid N$. If $\Delta = -3$, then $\omega = 6$ and $\varphi(N) \mid 12p$ by Corollary 2.3. If $\varphi(N) \mid 12$, then

$$N \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 14, 18, 21, 26, 28, 36, 42\}.$$

If $\varphi(N) \mid 6p$, then $\text{ord}_2(\varphi(N)) \le \text{ord}_2(6p) = 1$ implies $N = 2^a \cdot q^b$ for an odd prime q and $a \le 2$. Suppose $b > 0$. Then $a \le 1$ and $q - 1 \mid 6p$ implies $q \in \{3, 7, 2p+1, 6p+1\}$ since q is an odd prime. If $\varphi(N) \mid 4p$, then as shown in the proof of Lemma 3.8,

$$N \in \{1, 2, 3, 4, 5, 6, 8, 10, 12, 2p+1, 2\cdot(2p+1), 3\cdot(2p+1), 4\cdot(2p+1), 6\cdot(2p+1), 4p+1, 2\cdot(4p+1)\},$$

where $2p+1$ and $4p+1$ can arise only if they are prime. Finally, suppose $\varphi(N) = 12p$. But then Lemma 3.2 implies $T(\mathcal{O}, N) = T^{\circ}(\mathcal{O}, N) = 2p$. Since $\Delta = -3$, Lemma 3.1 implies $N \in \{1, 2, 3^a\}$, but none of these satisfy $\varphi(N) = 12p$.

If N is a new exponent, then $N \notin \{1, 2, 3, 4, 6, 7, 10\}$ by definition. By Theorem 2.1, $N \notin \{5, 8, 9, 12, 14, 18, 26, 28, 36, 42, 98\}$ since $T(\mathcal{O}, N) \nmid 2p$. Next, we will show $2p+1 \nmid N$ when $2p+1$ is prime. Since $\Delta = -3$, $2p+1$ is not ramified, and it cannot be split because then $T(\mathcal{O}, 2p+1) \notin \mathbb{Z}$. Thus $2p+1$ is inert in $\mathcal{O}$, and $T(\mathcal{O}, N) > 2p$; contradiction. Similarly, we cannot have $4p+1 \mid N$ when $4p+1$ is prime.

The remaining options are $N \in \{13, 21, 49, 6p+1, 2\cdot(6p+1)\}$ where $6p+1$ is prime. To see $N \ne 13$, note that by Lemma 7.6 and Theorem 7.8 in [1], if $P \in E$ has order 13 and $K = \mathbb{Q}(\sqrt{-3})$, then $[K(\mathfrak{h}(P)) : K] = 2$ or 24, where $\mathfrak{h}$ denotes a Weber function on E. Since P is defined over a number field of degree $2p$, it must be that $[K(\mathfrak{h}(P)) : K] = 2$. Then $[\mathbb{Q}(\mathfrak{h}(P)) : \mathbb{Q}] = 2$, since its degree must also divide $2p$. However, then there is a twist of E defined over $\mathbb{Q}(\mathfrak{h}(P))$ such that P becomes rational, and $T(\mathcal{O}, 13) = T^{\circ}(\mathcal{O}, 13) = 2$. This contradicts Theorem 2.4. Similarly, $N \ne 21$: by Lemma 7.6, Proposition 7.7, and Theorem 7.8 in [1], $[K(\mathfrak{h}(P)) : K] = [\mathbb{Q}(\mathfrak{h}(P)) : \mathbb{Q}] = 2$ since this quantity must divide $2p$. But then $T(\mathcal{O}, 21) = T^{\circ}(\mathcal{O}, 21) = 2$, which contradicts Theorem 2.4.

We note $N = 49$ does occur as a new exponent in degree $2\cdot 7$ by Theorem 2.4, and this is the only possible degree since $\varphi(49) \mid 12p$ only if $p = 7$. If $N = 6p+1$ is prime, then $\left(\frac{-3}{6p+1}\right) = 1$, and there exists a point of order N in degree $2p$ by Theorem 2.4. However, $T(\mathcal{O}, 2\cdot(6p+1)) = 3p$, and so we cannot have an $\mathcal{O}$-CM elliptic curve with a point of order $2\cdot(6p+1)$ in degree $2p$. □

4. Determining New Torsion Subgroups

Suppose F is a number field of degree $2p$, where $p > 5$ is prime, and E/F is an $\mathcal{O}$-CM elliptic curve. If $E(F)_{\text{tors}} \cong \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ for $M \mid N$ is new, then either N occurs already as an exponent of a CM torsion subgroup in degree 1 or 2 and

$$N \in \{1, 2, 3, 4, 6, 7, 10\}$$

by [6, §4.1, 4.2], or else by the previous section we are in one of the following cases:

(1) $\Delta(\mathcal{O}) = -115$, $p = 11$, and $N = 23$,
(2) $\Delta(\mathcal{O}) = -235$, $p = 23$, and $N = 47$,
(3) $\Delta(\mathcal{O}) \in \{-11, -19, -27, -43, -67, -163\}$ and $N = 2p+1$ is prime with $\left(\frac{\Delta}{2p+1}\right) = 1$,
(4) $\Delta(\mathcal{O}) \in \{-7, -8, -12, -16, -28\}$ and $N = 2\cdot(2p+1)$ where $2p+1$ is prime with $\left(\frac{\Delta}{2p+1}\right) = 1$,
(5) $\Delta(\mathcal{O}) = -4$ and $N = 2 \cdot (4p+1)$ where $4p+1$ is prime,
(6) $\Delta(\mathcal{O}) = -3$, $p = 7$, and $N = 49$,
(7) $\Delta(\mathcal{O}) = -3$ and $N = 6p+1$ where $6p+1$ is prime.

Lemma 4.1. *Suppose F is a number field of degree $2p$, where $p > 5$ is prime, and E/F is an $\mathcal{O}$-CM elliptic curve. If $E(F)_{\text{tors}} \cong \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ for $M \mid N$ is new, then $M = 1$ or 2.*

Proof. Suppose $\ell \mid M$ is prime. If $\ell = \omega \cdot p + 1 > 4$, then by Theorem 2.1 we have $T(\mathcal{O}, \ell, \ell) > 2p$. This is a contradiction. By §3 as summarized above, it remains to consider

$$M \in \{3, 4, 5, 6, 7, 10, 49\}.$$

Note that for any $M \geq 3$, the CM field K is contained in $F(E[M])$ by Lemma 3.15 of [4], and so $2 \cdot T(\mathcal{O}, M, N) \mid [F : \mathbb{Q}]$ by Theorem 2.1. We reach a contradiction for

$$(M, N) \in \{(3, 6), (4, 4), (5, 10), (6, 6), (7, 7), (7, 49), (10, 10), (49, 49)\}.$$

This leaves only $(M, N) = (3, 3)$, but $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ occurs already in degree 2 by [6, §4.2]. □

By the classification of CM torsion subgroups in degree 2 [6, §4.2] and the previous lemma, the only possible new subgroup with an old exponent is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$. Any other new torsion subgroup will be of the form $\mathbb{Z}/N\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ for a new exponent N. In particular, if N is odd, then the new torsion subgroup is precisely $\mathbb{Z}/N\mathbb{Z}$. It remains to check whether one can have full 2-torsion in each of the following cases:

(1) $N = 10$
(2) $N = 2 \cdot (2p+1)$ where $2p+1$ is prime, $\Delta(\mathcal{O}) \in \{-7, -8, -12, -16, -28\}$ and $\left(\frac{\Delta}{2p+1}\right) = 1$
(3) $N = 2 \cdot (4p+1)$ where $4p+1$ is prime and $\Delta(\mathcal{O}) = -4$

Lemma 4.2. *$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ does not occur as a new torsion subgroup of a CM elliptic curve defined over a number field of degree $2p$ for $p > 5$.*

Proof. Suppose E/F is an $\mathcal{O}$-CM elliptic curve with $E(F)_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$, and let $P \in E(F)$ be a point of order 10. By Corollary 2.2, we have $2 \mid T(\mathcal{O}, 10)$ unless $\Delta = -4$. Thus $2 \nmid h(\mathcal{O})$, for otherwise $4 \mid [F : \mathbb{Q}]$ by Corollary 2.3. In addition, $h(\mathcal{O}) \neq p$ by Lemma 3.5. Since $h(\mathcal{O}) \mid 2p$, it follows that $h(\mathcal{O}) = 1$. Moreover, $\Delta(\mathcal{O}) = -4$ by the table in the appendix of [4] since otherwise $[\mathbb{Q}(\mathfrak{h}(P)) : \mathbb{Q}] \nmid 2p$. Also, this table shows that $\mathbb{Q}(\mathfrak{h}(P))$ has degree 2, as neither 4 nor 8 divide $2p$. Since $T(\mathcal{O}, 10) = 1$ by Theorem 2.1, it follows that $K = \mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(\mathfrak{h}(P))$. In particular, $K \subseteq F$. Moreover, $T(\mathcal{O}, 2, 10) = 2$. Since $T(\mathcal{O}, 2, 10) \mid [F : K]$, it follows that $4 \mid [F : \mathbb{Q}]$; contradiction. □

Lemma 4.3. *$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2(2p+1)\mathbb{Z}$ where $2p+1$ is prime and $p > 5$ is prime occurs as a new torsion subgroup of an $\mathcal{O}$-CM elliptic curve in degree $2p$ if and only if $\Delta(\mathcal{O}) = -7$ and $\left(\frac{\Delta}{2p+1}\right) = 1$.*

Proof. Suppose E/F is an $\mathcal{O}$-CM elliptic curve with $E(F)_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2(2p+1)\mathbb{Z}$. Then $\Delta(\mathcal{O}) \in \{-7,-8,-12,-16,-28\}$ and $\left(\frac{\Delta}{2p+1}\right) = 1$ by Lemma 3.7. We consider two cases. First, suppose 2 is ramified in $\mathcal{O}$. Then $T(\mathcal{O},2,2(2p+1)) = 2p$ by Theorem 2.1, yet by Theorem 2.4, $T^{\circ}(\mathcal{O},2,2(2p+1)) = 2 \cdot 2p$ since $2p+1$ is split. So we must have 2 split in $\mathcal{O}$, which occurs if and only if $\Delta = -7$. Then $T(\mathcal{O},2,2(2p+1)) = p$, and $T^{\circ}(\mathcal{O},2,2(2p+1)) = 2p$, as desired.

Finally, we must show that if $\Delta(\mathcal{O}) = -7$ and $\mathbb{Z}/2(2p+1)\mathbb{Z} \hookrightarrow E(F)_{\text{tors}}$, then in fact E has full 2-torsion over F. By Lemma 7.6 and Theorem 7.8 in [1], if $P \in E(F)$ has order $2p+1$ and $K = \mathbb{Q}(\sqrt{-7})$, then $[K(\mathfrak{h}(P)) : K] = p$ or $2p^2$. Since P is defined over a number field of degree $2p$, it must be that $[K(\mathfrak{h}(P)) : K] = p$. By Theorem 2.4, $[\mathbb{Q}(\mathfrak{h}(P) : \mathbb{Q}] = 2p$, and so $K \subseteq \mathbb{Q}(\mathfrak{h}(P)) \subseteq F$. Thus E has full 2-torsion over F by Theorem 4.2 of [4], as we recall that 2-torsion is model-independent. □

Lemma 4.4. *$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2(4p+1)\mathbb{Z}$ where $4p+1$ is prime and $p > 5$ is prime does not occur as a new torsion subgroup of a CM elliptic curve in degree $2p$.*

Proof. Suppose F is a number field of degree $2p$ for $p > 5$ prime, and suppose E/F is an $\mathcal{O}$-CM elliptic curve with a point of order $4p+1$, where $4p+1$ is prime. Then by the lemmas of §3.2, $\Delta(\mathcal{O}) = -4$. Since $4p+1$ is split in $\mathcal{O}$, Theorem 2.1 implies $T(\mathcal{O},2,2(2p+1)) = 2p$. However, by Theorem 2.4, $T^{\circ}(\mathcal{O},2,2(4p+1)) = 2 \cdot 2p$, and we have a contradiction. □

References

1. Abbey Bourdon and Pete L. Clark, *Torsion points and Galois representations on CM elliptic curves*, Pacific J. Math. **305** (2020), no. 1, 43–88. MR 4077686
2. ______, *Torsion points and isogenies on CM elliptic curves*, J. Lond. Math. Soc. (2) **102** (2020), no. 2, 580–622. MR 4171427
3. Abbey Bourdon, Pete L. Clark, and Paul Pollack, *Anatomy of torsion in the CM case*, Math. Z. **285** (2017), no. 3-4, 795–820.
4. 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.
5. Abbey Bourdon and Paul Pollack, *Torsion subgroups of CM elliptic curves over odd degree number fields*, Int. Math. Res. Not. IMRN (2017), no. 16, 4923–4961.
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.
7. Pete L. Clark, Tyler Genao, Paul Pollack, and Frederick Saia, *The least degree of a CM point on a modular curve*, to appear in J. Lond. Math. Soc., available at: http://alpha.math.uga.edu/∼pete/least_CM_degree-1226.pdf.
8. Henri Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993.
9. 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.
10. John Cremona and Filip Najman, *$\mathbb{Q}$-curves over odd degree number fields*, Res. Number Theory **7** (2021), no. 4, Paper No. 62, 30. MR 4314224
11. Maarten Derickx, Anastassia Etropolski, Mark van Hoeij, Jackson S. Morrow, and David Zureick-Brown, *Sporadic cubic torsion*, Algebra Number Theory **15** (2021), no. 7, 1837–1864. MR 4333666
12. Enrique González-Jiménez, *Complete classification of the torsion structures of rational elliptic curves over quintic number fields*, J. Algebra **478** (2017), 484–505. MR 3621686
13. Enrique González-Jiménez and Filip Najman, *Growth of torsion groups of elliptic curves upon base change*, Math. Comput. **89** (2020), no. 323, 1457–1485.
14. Tomislav Gužvić, *Torsion of elliptic curves with rational j-invariant defined over number fields of prime degree*, Proc. Am. Math. Soc. **149** (2021), no. 8, 3261–3275 (English).
15. Tomislav Gužvić and Bidisha Roy, *Torsion groups of Mordell curves over number fields of higher degree*, available at: arxiv:2105.04954.
16. Heini Halberstam and Hans-Egon Richert, *Sieve methods*, London Mathematical Society Monographs, No. 4, Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], London-New York, 1974. MR 0424730
17. Hans Heilbronn, *On the class-number in imaginary quadratic fields*, The Quarterly Journal of Mathematics **os-5** (1934), no. 1, 150–160.

18. Sheldon Kamienny, *Torsion points on elliptic curves over all quadratic fields*, Duke Math. J. **53** (1986), no. 1, 157–162.
19. ______, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. **109** (1992), no. 2, 221–229.
20. Monsur Kenku and Fumiyuki Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149.
21. Barry Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186 (1978).
22. Loïc Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), no. 1-3, 437–449.
23. Louis Mordell, *On the rational solutions of the indeterminate equations of the third and fourth degrees.*, Proc. Camb. Philos. Soc. **21** (1922), 179–192.
24. Filip Najman, *Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$*, Math. Res. Lett. **23** (2016), no. 1, 245–272.
25. Loren D. Olson, *Points of finite order on elliptic curves with complex multiplication*, Manuscripta Math. **14** (1974), 195–205.
26. James L. Parish, *Rational torsion in complex-multiplication elliptic curves*, J. Number Theory **33** (1989), no. 2, 257–265.
27. Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, vol. 11, Princeton University Press, Princeton, NJ, 1994, Reprint of the 1971 original, Kanô Memorial Lectures, 1. MR 1291394
28. Alice Silverberg, *Torsion points on abelian varieties of CM-type*, Compositio Math. **68** (1988), no. 3, 241–249.
29. ______, *Points of finite order on abelian varieties*, p-adic methods in number theory and algebraic geometry, Contemp. Math., vol. 133, Amer. Math. Soc., Providence, RI, 1992, pp. 175–193.
30. Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.
31. André Weil, *L'arithmétique sur les courbes algébriques*, Acta Math. **52** (1929), no. 1, 281–315.