TORSION SUBGROUPS OF CM ELLIPTIC CURVES OVER ODD DEGREE NUMBER FIELDS

ABBEY BOURDON AND PAUL POLLACK

ABSTRACT. Let $\mathscr{G}_{\mathrm{CM}}(d)$ denote the collection of groups (up to isomorphism) that appear as the torsion subgroup of a CM elliptic curve over a degree d number field. We completely determine $\mathscr{G}_{\mathrm{CM}}(d)$ for odd integers d and deduce a number of statistical theorems about the behavior of torsion subgroups of CM elliptic curves. Here are three examples: (1) For each odd d, the set of natural numbers d' with $\mathscr{G}_{\mathrm{CM}}(d') = \mathscr{G}_{\mathrm{CM}}(d)$ possesses a well-defined, positive asymptotic density. (2) Let $T_{\mathrm{CM}}(d) = \max_{G \in \mathscr{G}_{\mathrm{CM}}(d)} \#G$; under the Generalized Riemann Hypothesis,

$$\Big(\frac{12e^\gamma}{\pi}\Big)^{2/3} \le \limsup_{\substack{d\to\infty \\ d \text{ odd}}} \frac{T_{\mathrm{CM}}(d)}{(d\log\log d)^{2/3}} \le \Big(\frac{24e^\gamma}{\pi}\Big)^{2/3}.$$

(3) For each $\epsilon > 0$, we have $\#\mathscr{G}_{\mathrm{CM}}(d) \ll_\epsilon d^\epsilon$ for all odd d; on the other hand, for each $A > 0$, we have $\#\mathscr{G}_{\mathrm{CM}}(d) > (\log d)^A$ for infinitely many odd d.

1. INTRODUCTION

For a given positive integer d, let $\mathscr{G}(d)$ denote the set of (isomorphism classes) of abelian groups that appear as $E(F)[\mathrm{tors}]$ for some elliptic curve E defined over some degree d number field F, and let $T(d)$ denote the supremum of the orders of all such groups. Celebrated work of Merel [23] shows that $T(d) < \infty$ for every d. However, the nature of the finite sets $\mathscr{G}(d)$ remains largely mysterious. The only d for which $\mathscr{G}(d)$ has been completely determined are $d = 1$ (Mazur [22], 1977) and $d = 2$ (work of Kamienny, Kenku, and Momose, completed in 1992 [17, 16]). And while there are completely explicit upper bounds on $T(d)$, the known bounds grow superexponentially, whereas it is widely believed that $T(d)$ is bounded polynomially in d.

More can be said if we restrict the class of elliptic curves under consideration. In particular, elliptic curves with complex multiplication (CM) are of interest since they are known to provide examples of rational points of large order appearing in unusually low degree [8]. Let $\mathscr{G}_{\mathrm{CM}}(d)$ and $T_{\mathrm{CM}}(d)$ be defined as above, but with the added restriction that E has CM. Whereas $\mathscr{G}(d)$ is known only for $d = 1$ and $d = 2$, the set $\mathscr{G}_{\mathrm{CM}}(d)$ has been computed for all $d \le 13$ [9]. And in contrast to the situation for $T(d)$ where the known upper bounds are (presumably) far from sharp, the upper order of $T_{\mathrm{CM}}(d)$ has recently been determined. In [10], it is shown that

$$\limsup_{d\to\infty} \frac{T_{\mathrm{CM}}(d)}{d\log\log d} < \infty.$$

From earlier work of Breuer [6], this lim sup is positive. Hence, $T_{\mathrm{CM}}(d)$ has upper order $d\log\log d$. Several other statistics concerning $T_{\mathrm{CM}}(d)$ are investigated in [4]; e.g., it is shown there that the average of $T_{\mathrm{CM}}(d)$ for $d \le x$ is $x/(\log x)^{1+o(1)}$, as $x \to \infty$.

In [5], the authors study torsion of CM elliptic curves over *real* number fields, meaning number fields admitting at least one real embedding. Observe that all number fields of odd degree are real. One of the central results of [5] is a complete classification of which groups arise as torsion subgroups of CM elliptic curves defined over number fields of odd degree, i.e., a classification of the elements of $\bigcup_{d \text{ odd}} \mathscr{G}_{\mathrm{CM}}(d)$. This strengthens earlier work of Aoki [2].

Date: July 1, 2016.

Theorem 1.1 (Odd Degree Theorem, [5], cf. [2, Corollary 9.4]). *Let F be a number field of odd degree, let $E_{/F}$ be a K-CM elliptic curve, and let $T = E(F)[\text{tors}]$. Then:*

a) One of the following occurs:
  (1) T is isomorphic to the trivial group $\{\bullet\}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$;
  (2) $T \cong \mathbb{Z}/\ell^n\mathbb{Z}$ for a prime $\ell \equiv 3 \pmod 8$ and $n \in \mathbb{Z}^+$ and $K = \mathbb{Q}(\sqrt{-\ell})$;
  (3) $T \cong \mathbb{Z}/2\ell^n\mathbb{Z}$ for a prime $\ell \equiv 3 \pmod 4$ and $n \in \mathbb{Z}^+$ and $K = \mathbb{Q}(\sqrt{-\ell})$.
b) If $E(F)[\text{tors}] \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, then $\operatorname{End} E$ has discriminant $\Delta = -4$.
c) If $E(F)[\text{tors}] \cong \mathbb{Z}/4\mathbb{Z}$, then $\operatorname{End} E$ has discriminant $\Delta \in \{-4, -16\}$.
d) Each of the groups listed in part a) arises up to isomorphism as the torsion subgroup $E(F)$ of a CM elliptic curve E defined over an odd degree number field F.

However, given a particular subgroup that does arise, the argument of [5] does not identify the degrees d in which it occurs. The main theorem of this paper is precisely such a result. Here, $h_{\mathbb{Q}(\sqrt{-\ell})}$ denotes the class number of $\mathbb{Q}(\sqrt{-\ell})$.

Theorem 1.2 (Strong Odd Degree Theorem). *Let $\ell \equiv 3 \pmod 4$ and $n \in \mathbb{Z}^+$. Define δ as follows:*

$$\delta = \begin{cases} \left\lfloor \frac{3n}{2} \right\rfloor - 1, & \ell > 3, \\ 0, & \ell = 3 \text{ and } n = 1, \\ \left\lfloor \frac{3n}{2} \right\rfloor - 2, & \ell = 3 \text{ and } n \geq 2. \end{cases}$$

Then:

(1) For any odd positive integer d, the groups $\{\bullet\}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ appear as the torsion subgroup of a CM elliptic curve defined over a number field of degree d.
(2) $\mathbb{Z}/\ell^n\mathbb{Z}$ appears as the torsion subgroup of a CM elliptic curve defined over a number field of odd degree d if and only if $\ell \equiv 3 \pmod 8$ and d is a multiple of $h_{\mathbb{Q}(\sqrt{-\ell})} \cdot \frac{\ell-1}{2} \cdot \ell^\delta$.
(3) $\mathbb{Z}/2\ell^n\mathbb{Z}$ appears as the torsion subgroup of a CM elliptic curve defined over a number field of odd degree d if and only if one of the following holds:
  a. $\ell \equiv 3 \pmod 8$, where $n \geq 2$ if $\ell = 3$, and d is a multiple of $3 \cdot h_{\mathbb{Q}(\sqrt{-\ell})} \cdot \frac{\ell-1}{2} \cdot \ell^\delta$, or
  b. $\ell = 3$ and $n = 1$ and d is any odd positive integer, or
  c. $\ell \equiv 7 \pmod 8$ and d is a multiple of $h_{\mathbb{Q}(\sqrt{-\ell})} \cdot \frac{\ell-1}{2} \cdot \ell^\delta$.

This theorem can be used to algorithmically determine $\mathscr{G}_{\text{CM}}(d)$ for any odd degree d. See section 7 for a table of the groups which arise for odd $d \leq 99$.

The CM elliptic curves with a point of order ℓ^n in lowest possible odd degree are unexpectedly varied. In the case of even degrees, points of order ℓ often appear for the first time on a CM elliptic curve with a rational j-invariant. For example, any prime $\ell \equiv 1 \pmod 3$ appears for the first time in even degree $\frac{\ell-1}{3}$ on an elliptic curve E with $j(E) = 0$ by [8, Theorem 1]. However, we see already from the Odd Degree Theorem that a CM elliptic curve with a rational point of order ℓ in odd degree will not have a rational j-invariant once $\ell > 163$. Moreover, through the proof of the Strong Odd Degree Theorem, we find that the algebraic structure of these optimal examples is surprisingly complex. Specifically, we find that if $n \geq 3$, an elliptic curve with a point of order ℓ^n in lowest possible odd degree necessarily has CM by a *non-maximal* order, and the size of the conductor increases with n. See Remark 2.7 for a precise statement along these lines. Non-maximal orders provide considerable technical complications, due in part to the fact that ideals do not necessarily factor uniquely into prime ideals, and so many results in the literature are formulated only to address the case of CM by the full ring of integers. However, we know now that non-maximal orders play a crucial role in the extremal behavior of rational torsion points of elliptic curves.

Theorem 1.2 opens the door to establishing new statistical properties of $\mathscr{G}_{\text{CM}}(d)$ and $T_{\text{CM}}(d)$, as d ranges over odd integers. The mean of $T_{\text{CM}}(d)$ for odd $d \leq x$ is studied already in [4], where it is

shown to be $x^{1/3+o(1)}$, as $x \to \infty$. This should be compared with the unrestricted average, which we recalled above was $x/(\log x)^{1+o(1)}$. In the next theorem, we study the upper order of $T_{\mathrm{CM}}(d)$ for odd d. Again, we find that it is much smaller than the corresponding unrestricted statistic.

Theorem 1.3 (Upper order of $T_{\mathrm{CM}}(d)$ for odd d)**.**

(1) There is an infinite sequence of odd d, with $d \to \infty$, where

$$T_{\mathrm{CM}}(d) \geq \left(\left(\frac{12e^{\gamma}}{\pi} + o(1)\right) d \log\log d\right)^{2/3}.$$

(2) Assume the Riemann Hypothesis for Dirichlet L-functions. Then as $d \to \infty$ through all odd integers,

$$T_{\mathrm{CM}}(d) \leq \left(\left(\frac{24e^{\gamma}}{\pi} + o(1)\right) d \log\log d\right)^{2/3}.$$

Unconditionally, $T_{\mathrm{CM}}(d) \ll_{\epsilon} d^{2/3+\epsilon}$ for each fixed $\epsilon > 0$ and all odd d.

We turn next to understanding the "stratification" of torsion by degree.

In 1974, Olson showed that $\mathscr{G}_{\mathrm{CM}}(1) = \{\{\bullet\}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}\}$ [26]. Computations carried out in [9] revealed that this same list reoccurs as $\mathscr{G}_{\mathrm{CM}}(d)$ for several other small values of d. This was one of the phenomena investigated in [5], where it was shown that $\mathscr{G}_{\mathrm{CM}}(d) = \mathscr{G}_{\mathrm{CM}}(1)$ if $d = p$ or p^2 for some prime $p \geq 7$.

Call d an *Olson degree* if $\mathscr{G}_{\mathrm{CM}}(d) = \mathscr{G}_{\mathrm{CM}}(1)$. The following complete classification of Olson degrees was proved in [4]. To state the result, we need one more piece of notation. Given a set $\mathcal{G}$ of positive integers, we write $\mathscr{M}(\mathcal{G})$ for the *set of multiples of* $\mathcal{G}$, meaning the collection of all positive integers divisible by some element of $\mathcal{G}$.

Proposition 1.4 ([4])**.** *The complement of the set of Olson degrees can be written as $\mathscr{M}(\mathcal{G})$, where*

$$\mathcal{G} = \{2\} \cup \left\{\frac{\ell - 1}{2} \cdot h_{\mathbb{Q}(\sqrt{-\ell})} : \ell \text{ prime}, \ell \equiv 3 \pmod 4, \ell > 3\right\}.$$

As a corollary of Proposition 1.4, it was proved in [5] that the set of Olson degrees possesses a positive density. It is easy, for reasons recalled at the start of §4.1, to rigorously bound this density from above by $4/15 = 0.26666\ldots$. However, no explicit lower bound is proved in [4]. We take the opportunity here to address this lacuna, estimating the density of Olson degrees to within 0.1%.

Theorem 1.5. *The density of Olson degrees lies in the open interval* $(0.264, 0.265)$.

Thus, a little more than half of the odd numbers d are Olson degrees.

It is natural to wonder if our results on Olson degrees are the tip of a larger iceberg. Generalizing the above, we say that d and d' are *CM-torsion-equivalent* if $\mathscr{G}_{\mathrm{CM}}(d) = \mathscr{G}_{\mathrm{CM}}(d')$. In this case, we call d a d'-Olson degree. The following questions were suggested by Pete L. Clark:

Questions 1.6. *Is it true that for every d, the set of d-Olson degrees possesses an asymptotic density? If so, is the sum of the densities of d-Olson degrees, taken over inequivalent d, equal to 1?*

To avoid a possible source of confusion, we remind the reader that asymptotic density is finitely additive but not countably additive. Thus, an affirmative answer to the first question does not immediately imply an affirmative answer to the second.

Note that if d and d' are CM-torsion equivalent, then d and d' share the same parity. Indeed, if d' is even, then $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ is realizable in degree d' (see [5, Theorems 1.4, 2.1]), whereas the Odd Degree Theorem guarantees that such a group is never realizable in any odd degree d, so that $\mathscr{G}_{\mathrm{CM}}(d) \neq \mathscr{G}_{\mathrm{CM}}(d')$. Consequently, each equivalence class consists entirely of even integers or entirely of odd integers.

Using Theorem 1.2, we are able to answer affirmatively the odd degree variants of Questions 1.6.

Theorem 1.7 (Stratification of torsion in odd degrees)**.** *For each odd positive integer d, the set of d-Olson degrees possesses a positive asymptotic density. Moreover, using $\mathbf{d}(\cdot)$ for asymptotic density,*

$$\sum_d \mathbf{d}(\{d\text{-Olson degrees}\}) = \frac{1}{2},$$

where the sum on the left is taken over any complete set of inequivalent odd integers.

Remark 1.8. *One can use the method of proof of Theorem 1.5 to study the density of d-Olson degrees for other odd d. For instance, we have calculated in this way that the 3-Olson degrees have density between 6.2% and 6.4%.*

We conclude with a result about the number of groups realizable in a given odd degree, i.e., the number $\#\mathscr{G}_{\mathrm{CM}}(d)$ for odd d. There is no mystery about how small $\#\mathscr{G}_{\mathrm{CM}}(d)$ can be; the Strong Odd Degree Theorem implies that $\mathscr{G}_{\mathrm{CM}}(1)$ is always a subset of $\mathscr{G}_{\mathrm{CM}}(d)$, so that $\#\mathscr{G}_{\mathrm{CM}}(d) \geq 6$, with equality if and only d is an Olson degree. But how large can $\#\mathscr{G}_{\mathrm{CM}}(d)$ be? This is the subject of our final theorem, proved in §6.

Theorem 1.9. *For each fixed $\epsilon > 0$, we have $\#\mathscr{G}_{\mathrm{CM}}(d) \ll_\epsilon d^\epsilon$ for all positive odd integers d. On the other hand, for each fixed $A > 0$, there are infinitely many odd d with $\#\mathscr{G}_{\mathrm{CM}}(d) > (\log d)^A$.*

Theorem 1.9 provides another point of contrast between the even and odd degree cases. Indeed, at the end of §6 we will adapt methods of Erdős [13] and Pomerance [28, 29] to show that for some constant $\eta > 0$ and all large x, we have $\max_{d \leq x} \#\mathscr{G}_{\mathrm{CM}}(d) > x^\eta$.

2. Complete determination of torsion in odd degrees: Proof of Theorem 1.2

2.1. **Background.** Let $\ell > 2$ be prime, and let F be a number field of odd degree. If $E_{/F}$ is a CM elliptic curve with an F-rational point of order ℓ^n, then the Odd Degree Theorem gives that $\ell \equiv 3 \pmod 4$. Moreover, we also have the following additional results of [5]. Here, ζ_{ℓ^n} denotes a primitive ℓ^nth root of unity, and $h(\Delta)$ denotes the class number of the order of discriminant Δ.

Theorem 2.1 ([5])**.** *Let F be a number field of odd degree, and let $E_{/F}$ be a CM elliptic curve with a point of order ℓ^n in $E(F)$ for some prime $\ell \equiv 3 \pmod 4$. Then:*

(1) E has CM by an order of discriminant $\Delta = -(2^\epsilon \ell^a)^2 \cdot \ell$ for $\epsilon \in \{0, 1\}$ and $a \in \mathbb{Z}_{\geq 0}$.
(2) $\mathbb{Q}(\zeta_{\ell^n}) \subset FK$.
(3) $\dfrac{\varphi(\ell^n)}{2} h(\Delta) \mid [F : \mathbb{Q}]$.
(4) If E has CM by an order of discriminant $\Delta = -\ell^{2a+1}$, there is a basis of $E[\ell^n]$ such that if $\sigma \in \mathrm{Gal}(\bar{F}/FK)$, then the image of σ under the mod-ℓ^n Galois representation associated to E is of the following form:

$$\rho_{\ell^n}(\sigma) = \begin{bmatrix} 1 & \beta\left(\frac{\Delta - t^2}{4t}\right) \\ 0 & 1 \end{bmatrix}, \quad 4t \mid t^2 - \Delta,\ \beta t \equiv 0 \pmod{\ell^n}.$$

Proof. Since $h(\Delta) = [\mathbb{Q}(j(E)) : \mathbb{Q}]$ and $\mathbb{Q}(j(E))$ is a subfield of F, it follows that $h(\Delta)$ is odd. Then part (1) is a consequence of the Odd Degree Theorem and [5, Lemma 3.5]. Parts (2) and (3) may be deduced from [5, Theorem 4.12]. Part (4) follows from the proof of [5, Theorem 4.12(a)]. □

As indicated in the introduction, elliptic curves with CM by a non-maximal order play a significant role in determining $\mathscr{G}_{\mathrm{CM}}(d)$ for odd d. One approach to analyzing rational torsion points on an elliptic curve with CM by a non-maximal order is to consider the rational torsion points on an elliptic curve with smaller conductor induced by the following natural isogeny. We thank Pete L. Clark for the idea of the next proof.

Proposition 2.2. *Let $E_{/F}$ be an elliptic curve with CM by the order $\mathcal{O}$ in K of conductor f. If $f' \mid f$, there exists an F-rational isogeny $\iota_{f'} \colon E \to E'$, where $E'_{/F}$ is an elliptic curve with CM by the order in K of conductor f'. Moreover, $\iota_{f'}$ is cyclic of degree $d = \frac{f}{f'}$.*

Proof. Let $\mathcal{O}'$ be the order of K of conductor f', and let $I = d\mathcal{O}'$. Then I is an ideal of $\mathcal{O}$, and we may form the I-torsion kernel,

$$E[I] = \{x \in E(\bar{F}) : \forall \alpha \in I,\, \alpha x = 0\}.$$

Since I is fixed by complex conjugation, $E[I]$ is defined over F. (See the discussion in Section 3.3 of [5].) Thus we have an F-rational isogeny $E \to E/E[I]$. It remains to show $E/E[I]$ has CM by $\mathcal{O}'$ and that $E[I]$ is cyclic of order d.

Choose an embedding $F \hookrightarrow \mathbb{C}$ so that $E \cong_{\mathbb{C}} E_{\mathcal{O}}$, where $E_{\mathcal{O}}$ is the $\mathcal{O}$-CM elliptic curve corresponding to $\mathbb{C}/\mathcal{O}$ under uniformization. Since $\mathcal{O} \subset \mathcal{O}'$, we have a natural map $\mathbb{C}/\mathcal{O} \to \mathbb{C}/\mathcal{O}'$, and hence a map from $E_{\mathcal{O}} \to E_{\mathcal{O}'}$. Then as in Proposition 1.4 of [34],

$$\begin{aligned}\ker(E_{\mathcal{O}} \to E_{\mathcal{O}'}) &\cong \ker(\mathbb{C}/\mathcal{O} \to \mathbb{C}/\mathcal{O}') \\ &= \mathcal{O}'/\mathcal{O} \\ &= \{z \in \mathbb{C} : z\mathcal{O}' \subset \mathcal{O}'\}/\mathcal{O}\end{aligned}$$

We will show $\{z \in \mathbb{C} : z\mathcal{O}' \subset \mathcal{O}'\} = \{z \in \mathbb{C} : zd\mathcal{O}' \subset \mathcal{O}\}$. Indeed, if $z\mathcal{O}' \subset \mathcal{O}'$, then in particular $z = a + f'k$ for some $a \in \mathbb{Z}$ and $k \in \mathcal{O}_K$. Then $(a + f'k)d\mathcal{O}' \subset \mathcal{O}$, as desired. Conversely, if $zd\mathcal{O}' \subset \mathcal{O}$, then $z = (a/d) + f'k$, for some $a \in \mathbb{Z}$ and $k \in \mathcal{O}_K$. Note that if d divides a, then $z\mathcal{O}' \subset \mathcal{O}'$, as desired. But d must divide a, for otherwise $zd\mathcal{O}'$ would not be contained in $\mathcal{O}$. Thus:

$$\begin{aligned}\ker(\mathbb{C}/\mathcal{O} \to \mathbb{C}/\mathcal{O}') &= \{z \in \mathbb{C} : zd\mathcal{O}' \subset \mathcal{O}\}/\mathcal{O} \\ &= \{z \in \mathbb{C} : \alpha z \in \mathcal{O} \,\forall\, \alpha \in I\}/\mathcal{O} \\ &= \{z \in \mathbb{C}/\mathcal{O} : \alpha z = 0 \,\forall\, \alpha \in I\} \\ &= \mathbb{C}/\mathcal{O}[I] \\ &\cong E_{\mathcal{O}}[I].\end{aligned}$$

Composing with the isomorphism $E \cong_{\mathbb{C}} E_{\mathcal{O}}$ gives an isogeny $E \to E_{\mathcal{O}'}$ with kernel $E[I]$. It follows that $E/E[I] \cong_{\mathbb{C}} E_{\mathcal{O}'}$, and so $E/E[I]$ has CM by $\mathcal{O}'$. Moreover, $E[I] \cong \mathcal{O}'/\mathcal{O}$, which is cyclic of order d. □

Remark 2.3. *If $f' = 1$, we recover the classical statement which appears, for example, as Proposition 25 in* [8].

Finally, we will make use of the connection between CM elliptic curves and class field theory, as stated in the following result. For a positive integer N and an imaginary quadratic field K, we let $K^{(N\mathcal{O}_K)}$ denote the N-ray class field of K.

Proposition 2.4. *Let F be a number field, and let $E_{/F}$ be an elliptic curve with CM by an order in K. If $(\mathbb{Z}/N\mathbb{Z})^2 \hookrightarrow E(F)$ for some $N \in \mathbb{Z}^+$, then $K^{(N\mathcal{O}_K)} \subset FK$.*

Proof. For CM by the maximal order, see [34, Theorem II.5.6]. For the general case, see [10, Theorem 5]. □

Lemma 2.5. *Let $\ell \equiv 3 \pmod 4$ be prime and $K = \mathbb{Q}(\sqrt{-\ell})$. If $n \in \mathbb{Z}^+$, then for any $a \geq n$,*

$$\mathbb{Q}(\zeta_{\ell^a}) \cap K^{\ell^n \mathcal{O}_K} = \mathbb{Q}(\zeta_{\ell^n}).$$

Proof. Let $\mathcal{O}$ be the order in K of discriminant $\Delta = -\ell^{2n+1}$, and let $K_{\mathcal{O}}$ denote the ring class field of K of conductor ℓ^n. Then by Corollary 8.7 of Cox [12], $K_{\mathcal{O}} \subset K^{\ell^n \mathcal{O}_K}$. The field $\mathbb{Q}(\zeta_{\ell^a}) \cap K_{\mathcal{O}}$ is generalized dihedral over $\mathbb{Q}$ by Theorem 9.18 of Cox [12], and since it is also abelian over $\mathbb{Q}$ we have

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{\ell^a}) \cap K_{\mathcal{O}}/K) \cong (\mathbb{Z}/2\mathbb{Z})^{\nu}.$$

However, $[K_{\mathcal{O}} : K] = h(\Delta)$ is odd by [5, Lemma 3.5]. Hence $\mathbb{Q}(\zeta_{\ell^a}) \cap K_{\mathcal{O}} = K$.

Since $\mathbb{Q}(\zeta_{\ell^n}) \subset K^{\ell^n \mathcal{O}_K}$, we have $\mathbb{Q}(\zeta_{\ell^n}) \subset \mathbb{Q}(\zeta_{\ell^a}) \cap K^{\ell^n \mathcal{O}_K}$. Let $\delta = [\mathbb{Q}(\zeta_{\ell^a}) \cap K^{\ell^n \mathcal{O}_K} : \mathbb{Q}(\zeta_{\ell^n})]$. Then the compositum of $K_{\mathcal{O}}$ and $\mathbb{Q}(\zeta_{\ell^a}) \cap K^{\ell^n \mathcal{O}_K}$ has degree

$$\frac{1}{w_K} h_K \ell^{2n-1}(\ell - 1)\delta$$

over K, where w_K denotes the number of roots of unity in K. Since

$$[K^{\ell^n \mathcal{O}_K} : K] = \frac{1}{w_K} h_K \ell^{2n-1}(\ell - 1)$$

(see [11, Corollary 3.2.5]), we find $\delta = 1$ and $\mathbb{Q}(\zeta_{\ell^a}) \cap K^{\ell^n \mathcal{O}_K} = \mathbb{Q}(\zeta_{\ell^n})$. □

2.2. **Identifying torsion in lowest degree.** We will use part (4) of Theorem 2.1 to deduce a relationship between the discriminant Δ and the rational torsion of the elliptic curve. Since $t \mid \Delta$, we find a connection between $\mathrm{ord}_\ell(\Delta)$ and the full torsion over FK forced by the existence of an F-rational point of order ℓ^n. For example, suppose F is a number field of odd degree and $E_{/F}$ is an elliptic curve with CM by an order of discriminant $\Delta = -\ell$, where $\ell \equiv 3 \pmod 4$ is prime. If $E(F)$ contains a point of order ℓ^n, then E has full ℓ^{n-1} torsion over FK by Theorem 2.1(4). This kind of argument is key to ruling out points of order ℓ^n appearing in low degree on elliptic curves with small conductor. Instead, we find that elliptic curves E defined over $F = \mathbb{Q}(j(E))$ which possess a cyclic F-rational isogeny of degree ℓ^n give examples of rational points of order ℓ^n appearing in lowest possible odd degree. Such isogenies have been classified by Kwon [19].

Theorem 2.6. *Let F be a number field of odd degree, let $\ell \equiv 3 \pmod 4$ be prime, and let $n \in \mathbb{Z}^+$. If $E_{/F}$ is a CM elliptic curve with a point of order ℓ^n in $E(F)$, then*

$$h_{\mathbb{Q}(\sqrt{-\ell})} \cdot \frac{\ell - 1}{2} \cdot \ell^{\delta} \mid [F : \mathbb{Q}],$$

where

$$\delta = \begin{cases} \left\lfloor \frac{3n}{2} \right\rfloor - 1, & \ell > 3, \\ 0, & \ell = 3 \text{ and } n = 1, \\ \left\lfloor \frac{3n}{2} \right\rfloor - 2, & \ell = 3 \text{ and } n \geq 2. \end{cases}$$

Moreover, for any such ℓ and n, there exists a CM elliptic curve defined over a number field of degree $h_{\mathbb{Q}(\sqrt{-\ell})} \cdot \frac{\ell-1}{2} \cdot \ell^{\delta}$ with a rational point of order ℓ^n.

Proof. Let F be a number field of odd degree, and suppose $E_{/F}$ is a CM elliptic curve with a point P of order ℓ^n in $E(F)$, where $\ell \equiv 3 \pmod 4$ is prime. For now suppose $\ell \neq 3$. It follows from Theorem 2.1 that E has CM by an order in $K = \mathbb{Q}(\sqrt{-\ell})$ of discriminant $\Delta = -(2^\epsilon \ell^a)^2 \cdot \ell$ for $\epsilon \in \{0, 1\}$ and $a \in \mathbb{Z}_{\geq 0}$, and

$$\frac{\varphi(\ell^n)}{2} \cdot h(\Delta) = h_K \frac{\ell - 1}{2} \ell^{a+n-1} \left(2 - \left(\frac{-\ell}{2}\right)\right)^{\epsilon} \mid [F : \mathbb{Q}]. \tag{1}$$

(The formula for $h(\Delta)$ appears in [12, Theorem 7.24].) If $a \geq \lfloor \frac{n}{2} \rfloor$, then this quantity is divisible by $h_K \frac{\ell-1}{2} \ell^{\delta}$, as desired. So we may assume $a < \lfloor \frac{n}{2} \rfloor$.

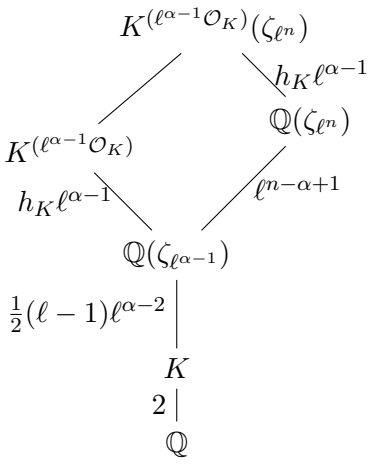
Let $\varphi \colon E \to E'$ be the F-rational isogeny of degree $2^\epsilon \ell^a$ whose existence is guaranteed by Proposition 2.2, where E' is an elliptic curve with CM by $\mathcal{O}_K$. Then $\varphi(P)$ has order ℓ^α, where

$\alpha \geq n - a \geq 2$. Indeed, $n - a < 2$ contradicts $a < \lfloor \frac{n}{2} \rfloor$. By Theorem 2.1, there is a basis of $E'[\ell^\alpha]$ such that if $\sigma \in \mathrm{Gal}(\bar{F}/FK)$, then $\rho_{\ell^\alpha}(\sigma)$ is of the following form:

$$\begin{bmatrix} 1 & \beta\left(\frac{-\ell - t^2}{4t}\right) \\ 0 & 1 \end{bmatrix}, \quad 4t \mid t^2 + \ell, \quad \beta t \equiv 0 \pmod{\ell^\alpha}.$$

In particular, $t \mid \ell$, so $\beta t \equiv 0 \pmod{\ell^\alpha}$ implies $\beta \equiv 0 \pmod{\ell^{\alpha-1}}$. Thus E' has full $\ell^{\alpha-1}$-torsion over FK. Since FK contains $\mathbb{Q}(\zeta_{\ell^n})$ by Theorem 2.1 and $K^{\ell^{\alpha-1}\mathcal{O}_K}$ by Proposition 2.4, it follows from Lemma 2.5 that $h_K(\ell-1)\ell^{n+\alpha-2} \mid [FK : \mathbb{Q}]$. Hence

$$h_K \frac{(\ell-1)}{2} \ell^{n+\alpha-2} \mid [F : \mathbb{Q}]. \tag{2}$$



Since $a < \lfloor \frac{n}{2} \rfloor$, we have $n + \alpha - 2 \geq 2n - a - 2 \geq \delta$. It follows that $h_K \frac{(\ell-1)}{2} \ell^\delta \mid [F : \mathbb{Q}]$.

If $\ell = 3$, then by Theorem 2.1 E has CM by an order $\mathcal{O}$ in $K = \mathbb{Q}(\sqrt{-3})$ of discriminant $\Delta = -(2^\epsilon 3^a)^2 \cdot 3$ for $\epsilon \in \{0, 1\}$ and $a \in \mathbb{Z}_{\geq 0}$. In addition, Theorem 2.1 implies

$$\frac{\varphi(3^n)}{2} \cdot h(\Delta) = \frac{3^{a+n+\epsilon-1}}{[\mathcal{O}_K^\times : \mathcal{O}^\times]} \mid [F : \mathbb{Q}]. \tag{3}$$

If $a \geq \lfloor \frac{n}{2} \rfloor$, then this quantity is divisible by $h_K \frac{3-1}{2} 3^\delta = 3^\delta$, as desired. So we may assume $a < \lfloor \frac{n}{2} \rfloor$. Arguing as above, we find that FK contains both $K^{3^{\alpha-1}\mathcal{O}_K}$ and $\mathbb{Q}(\zeta_{3^n})$ for some $\alpha \geq n - a \geq 2$. By Lemma 2.5, these fields are linearly disjoint over $\mathbb{Q}(\zeta_{3^{\alpha-1}})$; hence,

$$3^{n+\alpha-3} \mid [F : \mathbb{Q}]. \tag{4}$$

Since $a < \lfloor \frac{n}{2} \rfloor$, we have $n + \alpha - 3 \geq 2n - a - 3 \geq \delta$. It follows that $3^\delta \mid [F : \mathbb{Q}]$.

It remains to show these divisibility conditions are best possible. Set $a = \lfloor \frac{n}{2} \rfloor$. Then $\ell^n \mid \Delta = -(\ell^a)^2\ell$. Let E be an $\mathcal{O}(\Delta)$-CM elliptic curve defined over $F = \mathbb{Q}(j(E))$. By work of Kwon [19, Corollary 4.2], E admits an F-rational isogeny which is cyclic of degree ℓ^n. It follows from [5, Theorem 5.6] that there is a twist E_1 of $E_{/F}$ and an extension L/F of degree $\varphi(\ell^n)/2$ such that $E_1(L)$ has a point of order ℓ^n. We have $[L : \mathbb{Q}] = \frac{\varphi(\ell^n)}{2} h(\Delta) = h_K \frac{\ell-1}{2} \ell^\delta$, as desired. □

Remark 2.7. *Let $n \in \mathbb{Z}^+$ and $\ell \equiv 3 \pmod 4$ be prime. Suppose F is a number field of degree $h_{\mathbb{Q}(\sqrt{-\ell})} \cdot \frac{\ell-1}{2} \cdot \ell^\delta$ and $E_{/F}$ is a CM elliptic curve with an F-rational point of order ℓ^n. It follows from the proof of Theorem 2.6 that E has CM by an order of discriminant $\Delta = -(2^\epsilon \ell^a)^2 \ell$ where $a = \lfloor \frac{n}{2} \rfloor$, $\lfloor \frac{n}{2} \rfloor - 1$, or $\lfloor \frac{n}{2} \rfloor + 1$. The latter two cases are only possible if n is even or if $n = 1$ (and*

$\ell = 3$), respectively. In particular, we see that E necessarily has CM by a non-maximal order if $n \geq 3$.

Corollary 2.8. *Let $\ell \equiv 3 \pmod 4$ be prime, and let $n \in \mathbb{Z}^+$. Let F be a number field of odd degree. If $E_{/F}$ is a CM elliptic curve with a point of order ℓ^n in $E(F)$, then E has CM by $K = \mathbb{Q}(\sqrt{-\ell})$ and FK contains $K^{\ell^{\lfloor \frac{n}{2} \rfloor}\mathcal{O}_K}(\zeta_{\ell^n})$.*

Proof. By Theorem 2.1, E has CM by the order $\mathcal{O}$ in $K = \mathbb{Q}(\sqrt{-\ell})$ of discriminant $\Delta = -(2^\epsilon \ell^a)^2 \cdot \ell$ for $\epsilon \in \{0, 1\}$ and $a \in \mathbb{Z}_{\geq 0}$. We consider two cases.

If $a \geq \lfloor \frac{n}{2} \rfloor$, then $\mathcal{O}$ is contained in the order $\mathcal{O}'$ of conductor $\ell^{\lfloor \frac{n}{2} \rfloor}$. Thus the ring class field of K with conductor $\ell^{\lfloor \frac{n}{2} \rfloor}$, $K_{\mathcal{O}'}$, is contained in $K_{\mathcal{O}} = K(j(E)) \subset FK$. (See exercise 9.19 of Cox [12].) Since $\mathbb{Q}(\zeta_{\ell^n}) \subset FK$ by Theorem 2.1 and $\mathbb{Q}(\zeta_{\ell^n}) \cap K_{\mathcal{O}'} = K$ by the proof of Lemma 2.5, $K_{\mathcal{O}'}(\zeta_{\ell^n})$ is a subfield of FK of degree $h_{\mathbb{Q}(\sqrt{-\ell})} \cdot (\ell - 1) \cdot \ell^\delta$. By Corollary 8.7 of Cox [12], $K_{\mathcal{O}'} \subset K^{\ell^{\lfloor \frac{n}{2} \rfloor}\mathcal{O}_K}$, so $K_{\mathcal{O}'}(\zeta_{\ell^n}) \subset K^{\ell^{\lfloor \frac{n}{2} \rfloor}\mathcal{O}_K}(\zeta_{\ell^n})$. Since they have the same degree, equality holds.

If $a < \lfloor \frac{n}{2} \rfloor$, then FK contains $K^{\ell^{\alpha-1}\mathcal{O}_K}$ and $\mathbb{Q}(\zeta_{\ell^n})$, where $\alpha \geq n - a \geq \lfloor \frac{n}{2} \rfloor + 1$. Thus FK contains $K^{\ell^{\lfloor \frac{n}{2} \rfloor}\mathcal{O}_K}(\zeta_{\ell^n})$. □

Corollary 2.9. *Let $\ell \equiv 3 \pmod 4$ be prime, and let $n \in \mathbb{Z}^+$. Suppose $E_{/F}$ is a CM elliptic curve with a point of order ℓ^n in $E(F)$. If $[F : \mathbb{Q}] = h_{\mathbb{Q}(\sqrt{-\ell})} \cdot \frac{\ell-1}{2} \cdot \ell^\delta$, for δ defined as above, then E has CM by an order in $K = \mathbb{Q}(\sqrt{-\ell})$ and $FK = K^{\ell^{\lfloor \frac{n}{2} \rfloor}\mathcal{O}_K}(\zeta_{\ell^n})$. In particular, ℓ is the only prime which ramifies in F.*

Proof. This follows from Corollary 2.8. □

2.3. **Proof of the Strong Odd Degree Theorem.** Let T be a group which appears as the torsion subgroup of a CM elliptic curve defined over a number field of odd degree. We will identify an odd positive integer d_T such that $d_T \mid [F : \mathbb{Q}]$ whenever $E_{/F}$ is a CM elliptic curve with $E(F)[\text{tors}] \cong T$ and F is of odd degree. Once we exhibit a number field F of degree d_T and a CM elliptic curve $E_{/F}$ with $E(F)[\text{tors}] \cong T$, the Strong Odd Degree Theorem will follow by a result of [5]:

Theorem 2.10. *Let $A_{/F}$ be an abelian variety over a number field, and let $d \geq 2$. There are infinitely many L/F such that $[L : F] = d$ and $A(L)[\text{tors}] = A(F)[\text{tors}]$.*

Proof. See Theorem 2.1 of [5]. □

We isolate the more involved case in the following lemma. Here, δ is as defined in the statement of the Strong Odd Degree Theorem.

Lemma 2.11. *Let F be a number field of odd degree. If $E_{/F}$ is a CM elliptic curve with $E(F)[\text{tors}] \cong \mathbb{Z}/2\ell^n\mathbb{Z}$ for $\ell \equiv 3 \pmod 8$, where $n \geq 2$ if $\ell = 3$, then $3 \cdot h_{\mathbb{Q}(\sqrt{-\ell})} \cdot \frac{\ell-1}{2} \cdot \ell^\delta \mid [F : \mathbb{Q}]$.*

Proof. We will first consider the case where $\ell \equiv 3 \pmod 8$, $\ell \neq 3$. Suppose $E_{/F}$ is an elliptic curve with CM by an order $\mathcal{O}$ of discriminant Δ in K, and suppose $E(F)[\text{tors}] \cong \mathbb{Z}/2\ell^n\mathbb{Z}$. By Theorem 2.1, $\Delta = -(2^\epsilon \ell^a)^2 \cdot \ell$ for $\epsilon \in \{0, 1\}$ and $a \in \mathbb{Z}_{\geq 0}$. If $\epsilon = 0$, then $K^{2\mathcal{O}_K} \subset F(\sqrt{d}) = FK$ by [5, Lemma 3.15] and Proposition 2.4. By Corollary 2.8, $K^{\ell^{\lfloor \frac{n}{2} \rfloor}\mathcal{O}_K}(\zeta_{\ell^n}) \subset FK$. Since 2 ramifies in $K^{2\mathcal{O}_K}$ and $K^{\ell^{\lfloor \frac{n}{2} \rfloor}\mathcal{O}_K}(\zeta_{\ell^n})$ is unramified away from ℓ, these fields are linearly disjoint over $K^{\mathcal{O}_K}$. Thus $3 \cdot h_K(\ell - 1)\ell^\delta \mid [FK : \mathbb{Q}]$, and $3 \cdot h_K \cdot \frac{\ell-1}{2} \cdot \ell^\delta \mid [F : \mathbb{Q}]$. If $\epsilon = 1$, then the ring class field of K of conductor 2 is contained in $K_{\mathcal{O}} = K(j(E)) = FK$ (see exercise 9.19 of Cox [12]). Since this ring class field and $K^{\ell^{\lfloor \frac{n}{2} \rfloor}\mathcal{O}_K}(\zeta_{\ell^n})$ are linearly disjoint over $K^{\mathcal{O}_K}$, it follows that $3 \cdot h_{\mathbb{Q}(\sqrt{-\ell})} \cdot \frac{\ell-1}{2} \cdot \ell^\delta \mid [F : \mathbb{Q}]$.

Suppose $\ell = 3$, and suppose $E_{/F}$ has CM by an order $\mathcal{O}$ of discriminant Δ in K and $E(F)[\text{tors}] \cong \mathbb{Z}/2 \cdot 3^n\mathbb{Z}$. As in the lemma statement, we assume $n \geq 2$. We first consider the case where $2 \mid \Delta$, i.e., $\Delta = -(2 \cdot 3^a)^2 \cdot 3$ for $a \in \mathbb{Z}_{\geq 0}$. If $a \geq \lfloor \frac{n}{2} \rfloor$, then $3^{\delta+1} \mid [F : \mathbb{Q}]$ by equation (3). If $a < \lfloor \frac{n}{2} \rfloor$, then we must consider several sub-cases:

- $a \geq 1$: Since 6 divides the conductor of $\mathcal{O}$, the ring class field of conductor 6, $K_{\mathcal{O}'}$, is contained in $K_{\mathcal{O}} = K(j(E)) \subset FK$ (see exercise 9.19 of Cox [12]). The prime 2 ramifies in $K_{\mathcal{O}'}$, so $K^{3^{\lfloor \frac{n}{2} \rfloor}\mathcal{O}_K}(\zeta_{3^n})$ and $K_{\mathcal{O}'}$ are linearly disjoint over K. Since $[K_{\mathcal{O}'} : K] = 3$, we have $3^{\delta+1} \mid [F : \mathbb{Q}]$.
- $a = 0$, $n \geq 3$: The proof of Theorem 2.6 shows that a rational point of order $2 \cdot 3^n$ forces $K^{3^{\alpha-1}\mathcal{O}_K}(\zeta_{3^n}) \subset FK$, where $\alpha \geq n$. Thus $K^{3^{n-1}\mathcal{O}_K}(\zeta_{3^n}) \subset FK$, which means $3^{2n-3} \mid [F : \mathbb{Q}]$. Since $n \geq 3$, we have $3^{\delta+1} \mid [F : \mathbb{Q}]$.
- $a = 0$, $n = 2$: Let P be the point of order 18 in $E(F)[\text{tors}]$, where E is an elliptic curve with CM by an order of discriminant $\Delta = -2^2 \cdot 3$. Note $j(E) = 2^4 3^3 5^3$. Work of [18] implies E has an equation of the form
$$y^2 + (1-c)xy - by = x^3 - bx^2$$
for some $b, c \in F$ and $P = (0, 0)$. We let $j(b, c)$ denote the j-invariant of E. As in [9], we may obtain a polynomial $f_{18} \in \mathbb{Q}[b, c]$ that vanishes when $(0, 0)$ has order 18. A computation shows that if
$$\begin{cases} f_{18}(b, c) = 0 \\ j(b, c) = 2^4 3^3 5^3 \end{cases},$$
then $9 \mid [\mathbb{Q}(b, c) : \mathbb{Q}]$ (see the research website of the first author for the `Magma` scripts used). Hence $9 \mid [F : \mathbb{Q}]$, as desired.

Next, suppose $2 \nmid \Delta$, i.e., $\Delta = -(3^a)^2 \cdot 3$ for $a \in \mathbb{Z}_{\geq 0}$. If $a \geq 1$, then by Proposition 2.2, there exists an F-rational isogeny $\iota_3 \colon E \to E'$, where E' has CM by the order in $K = \mathbb{Q}(\sqrt{-3})$ of conductor 3. Since the kernel of this isogeny has size 3^{a-1}, a point of order 2 in $E(F)$ induces a point of order 2 in $E'(F)$. But E' is a quadratic twist of the elliptic curve $E_0 : y^2 = x^3 - 480x + 4048$, and points of order 2 are invariant under quadratic twists. Thus $E_0(F)$ contains a point of order 2, and F contains a root α of $x^3 - 480x + 4080$. Since 2 ramifies in $K(\alpha)$, the fields $K(\alpha)$ and $K^{3^{\lfloor \frac{n}{2} \rfloor}\mathcal{O}_K}(\zeta_{3^n})$ are linearly disjoint over K; hence $3^{\delta+1} \mid [F : \mathbb{Q}]$.

If $a = 0$ and $n \geq 3$, $K^{3^{n-1}\mathcal{O}_K}(\zeta_{3^n}) \subset FK$ and $3^{\delta+1} \mid [F : \mathbb{Q}]$ as above. Finally, if $a = 0$ and $n = 2$, then $j(E) = 0$. As in the case where $2 \mid \Delta$, a computation shows that $9 \mid [F : \mathbb{Q}]$. Again, see the research website of the first author for the `Magma` scripts used. □

Theorem 2.12 (Strong Odd Degree Theorem)**.** *Let $\ell \equiv 3 \pmod 4$ and $n \in \mathbb{Z}^+$. Define δ as follows:*
$$\delta = \begin{cases} \lfloor \frac{3n}{2} \rfloor - 1, & \ell > 3, \\ 0, & \ell = 3 \text{ and } n = 1, \\ \lfloor \frac{3n}{2} \rfloor - 2, & \ell = 3 \text{ and } n \geq 2. \end{cases}$$
Then:

(1) For any odd positive integer d, the groups $\{\bullet\}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ appear as the torsion subgroup of a CM elliptic curve defined over a number field of degree d.

(2) $\mathbb{Z}/\ell^n\mathbb{Z}$ appears as the torsion subgroup of a CM elliptic curve defined over a number field of odd degree d if and only if $\ell \equiv 3 \pmod 8$ and d is a multiple of $h_{\mathbb{Q}(\sqrt{-\ell})} \cdot \frac{\ell-1}{2} \cdot \ell^\delta$.

(3) $\mathbb{Z}/2\ell^n\mathbb{Z}$ appears as the torsion subgroup of a CM elliptic curve defined over a number field of odd degree d if and only if one of the following holds:

a. $\ell \equiv 3 \pmod 8$*, where* $n \geq 2$ *if* $\ell = 3$*, and* d *is a multiple of* $3 \cdot h_{\mathbb{Q}(\sqrt{-\ell})} \cdot \frac{\ell-1}{2} \cdot \ell^\delta$*, or*
b. $\ell = 3$ *and* $n = 1$ *and* d *is any odd positive integer, or*
c. $\ell \equiv 7 \pmod 8$ *and* d *is a multiple of* $h_{\mathbb{Q}(\sqrt{-\ell})} \cdot \frac{\ell-1}{2} \cdot \ell^\delta$*.*

Proof. The groups $\{\bullet\}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ appear as torsion subgroups of CM elliptic curves defined over $\mathbb{Q}$ by work of Olson [26], so part (1) is an immediate consequence of Theorem 2.10. For part (2), suppose $E_{/F}$ is a CM elliptic curve with $E(F)[\text{tors}] \cong \mathbb{Z}/\ell^n\mathbb{Z}$. Then $\ell \equiv 3 \pmod 8$ by the Odd Degree Theorem, and $[F : \mathbb{Q}]$ is a multiple of $h_{\mathbb{Q}(\sqrt{-\ell})} \cdot \frac{\ell-1}{2} \cdot \ell^\delta$ by Theorem 2.6. Conversely, if for each $\ell \equiv 3 \pmod 8$ there exists a number field F of degree $h_{\mathbb{Q}(\sqrt{-\ell})} \cdot \frac{\ell-1}{2} \cdot \ell^\delta$ and a CM elliptic curve $E_{/F}$ with $E(F)[\text{tors}] \cong \mathbb{Z}/\ell^n\mathbb{Z}$, part (2) will follow from Theorem 2.10.

First suppose $\ell \equiv 3 \pmod 8$, $\ell \neq 3$. By Theorem 2.6 there exists a CM elliptic curve E defined over a number field F of degree $h_{\mathbb{Q}(\sqrt{-\ell})} \cdot \frac{\ell-1}{2} \cdot \ell^\delta$ with $\ell^n \parallel E(F)[\text{tors}]$. By the Odd Degree Theorem, E has CM by $K = \mathbb{Q}(\sqrt{-\ell})$ and $E(F)[\text{tors}] \cong \mathbb{Z}/\ell^n\mathbb{Z}$ or $\mathbb{Z}/2\ell^n\mathbb{Z}$. But if $E(F)[\text{tors}] \cong \mathbb{Z}/2\ell^n\mathbb{Z}$, then $3 \cdot h_K \cdot \frac{\ell-1}{2} \cdot \ell^\delta \mid [F : \mathbb{Q}]$ by Lemma 2.11, which is a contradiction. Thus $E(F)[\text{tors}] \cong \mathbb{Z}/\ell^n\mathbb{Z}$, as desired. If $\ell = 3$, we know that $\mathbb{Z}/3\mathbb{Z}$ occurs in degree 1 by work of Olson [26], and $\mathbb{Z}/9\mathbb{Z}$ occurs in degree 3 by work of Clark, Corn, Rice, and Stankewicz [9]. If $n \geq 3$, we know there is an elliptic curve E defined over a number field of F degree 3^δ with $3^n \parallel E(F)[\text{tors}]$ by Theorem 2.6. If $E(F)[\text{tors}] \cong \mathbb{Z}/2 \cdot 3^n\mathbb{Z}$, then $3^{\delta+1} \mid [F : \mathbb{Q}]$ by Lemma 2.11. Thus the Odd Degree Theorem guarantees $E(F)[\text{tors}] \cong \mathbb{Z}/3^n\mathbb{Z}$, as desired. This completes the proof of part 2.

Let F be a number field of odd degree, and suppose $E_{/F}$ is a CM elliptic curve with $E(F)[\text{tors}] \cong \mathbb{Z}/2\ell^n\mathbb{Z}$ for some prime $\ell \equiv 3 \pmod 4$. If $\ell \equiv 3 \pmod 8$, where $n \geq 2$ if $\ell = 3$, then $3 \cdot h_{\mathbb{Q}(\sqrt{-\ell})} \cdot \frac{\ell-1}{2} \cdot \ell^\delta \mid [F : \mathbb{Q}]$ by Lemma 2.11. If $\ell \equiv 7 \pmod 8$, then $h_{\mathbb{Q}(\sqrt{-\ell})} \cdot \frac{\ell-1}{2} \cdot \ell^\delta \mid [F : \mathbb{Q}]$ by Theorem 2.6. Thus part 3 will follow from Theorem 2.10 if we can demonstrate that there is a CM elliptic curve E defined over a number field F of smallest possible odd degree with $E(F)[\text{tors}] \cong \mathbb{Z}/2\ell^n\mathbb{Z}$.

Suppose $\ell \equiv 3 \pmod 8$, where $n \geq 2$ if $\ell = 3$. By the proof of part 2, there is a number field F of degree $h_K \cdot \frac{\ell-1}{2} \cdot \ell^\delta$ and a CM elliptic curve $E_{/F}$ with $E(F)[\text{tors}] \cong \mathbb{Z}/\ell^n\mathbb{Z}$. Since points of order 2 correspond to the roots of a cubic polynomial, E gains a rational 2-torsion point over a cubic extension of F, say $F(\alpha)$. By the Odd Degree Theorem and Lemma 2.11, $E(F(\alpha))[\text{tors}] \cong \mathbb{Z}/2\ell^n\mathbb{Z}$. Since $[F : \mathbb{Q}] = 3 \cdot h_{\mathbb{Q}(\sqrt{-\ell})} \cdot \frac{\ell-1}{2} \cdot \ell^\delta$, we may conclude part 3(a).

If $\ell = 3$ and $n = 1$, then $\mathbb{Z}/2\ell\mathbb{Z}$ does occur in degree 1 by Olson [26]. Thus 3(b) holds. For 3(c), let $\ell \equiv 7 \pmod 8$. By Theorem 2.6 there exists a CM elliptic curve E defined over a number field F of degree $h_{\mathbb{Q}(\sqrt{-\ell})} \cdot \frac{\ell-1}{2} \cdot \ell^\delta$ with $\ell^n \parallel E(F)[\text{tors}]$. The Odd Degree Theorem shows $E(F)[\text{tors}] \cong \mathbb{Z}/2\ell^n\mathbb{Z}$, as desired. □

3. The upper order of $T_{\text{CM}}(d)$ for odd degrees d: Proof of Theorem 1.3

Here we exploit the fact that while $h_{\mathbb{Q}(\sqrt{-\ell})}$ is typically of size $\asymp \ell^{1/2}$, it can be smaller by a factor of size $1/\log\log\ell$, but (assuming GRH) no more. The precise statements we need correspond via Dirichlet's class number formula to the following two estimates.

Proposition 3.1 (Joshi)**.** *There is a sequence of primes* $\ell \equiv 3 \pmod 4$*,* $\ell \to \infty$*, with*

$$L(1, (\tfrac{-\ell}{\cdot})) \leq \frac{\pi^2}{6e^\gamma} \frac{1}{\log\log\ell}.$$

Proof. This is part of [15, Theorem 1]. □

Proposition 3.2 (Littlewood)**.** *Assume the Riemann Hypothesis for Dirichlet L-functions. Then as $|D| \to \infty$, with D ranging through fundamental discriminants,*

$$L(1, (\tfrac{D}{\cdot})) \geq \left(\frac{\pi^2}{12e^\gamma} + o(1)\right) \frac{1}{\log\log|D|}.$$

For D satisfying $(\frac{D}{2}) = 1$, this lower bound can be strengthened to

$$L(1, (\tfrac{D}{\cdot})) \geq \left(\frac{\pi^2}{4e^\gamma} + o(1)\right) \frac{1}{\log\log|D|}.$$

Proof. The first assertion is explicitly contained in [21, Theorem 1]. The second can be proved by the same method. For the sake of completeness, we sketch an argument for the second claim taking as a starting point the the modern approach to Littlewood's work presented in [20, §5.2]. From [20, eq. (5.2)], we see that with $X = \frac{1}{4}(\log|D|)^2$,

$$\log L(1, (\tfrac{D}{\cdot})) \geq \sum_{n \leq X} \Lambda(n)(\tfrac{D}{n}) \left(\frac{1}{n\log n} - \frac{1}{X\log X}\right) + o(1),$$

as $|D| \to \infty$. (We have dropped lower order terms from [20], since we are only interested in asymptotics, not in an explicit bound.) For each prime p, the contribution to the right-hand sum from n that are powers of p is at least

$$\sum_{p^k \leq X} \Lambda(p^k)(-1)^k \left(\frac{1}{p^k \log p^k} - \frac{1}{X\log X}\right);$$

moreover, since $(\frac{D}{2}) = 1$, the factor $(-1)^k$ appearing here can be replaced with 1 when $p = 2$. Now summing over p,

$$\log L(1, (\tfrac{D}{\cdot})) \geq \sum_{p^k \leq X} \Lambda(p^k)(-1)^k \left(\frac{1}{p^k \log p^k} - \frac{1}{X\log X}\right) + 2 \sum_{\substack{2^k \leq X \\ k \text{ odd}}} \Lambda(2^k) \left(\frac{1}{2^k \log 2^k} - \frac{1}{X\log X}\right) + o(1).$$

As on p. 2408 of [20],

$$\sum_{p^k \leq X} \Lambda(p^k)(-1)^k \left(\frac{1}{p^k \log p^k} - \frac{1}{X\log X}\right) \geq -\log\log X - \gamma + \log\frac{\pi^2}{6} + o(1).$$

Moreover,

$$\begin{aligned} 2 \sum_{\substack{2^k \leq X \\ k \text{ odd}}} \Lambda(2^k) \left(\frac{1}{2^k \log 2^k} - \frac{1}{X\log X}\right) &= 2 \sum_{\substack{2^k \leq X \\ k \text{ odd}}} \frac{1}{k \cdot 2^k} + o(1) \\ &= 2 \sum_{k \geq 1} \frac{1}{k \cdot 2^k} - \sum_{j \geq 1} \frac{1}{j \cdot 2^{2j}} + o(1) = 2\ln\left(\frac{1}{1 - \frac{1}{2}}\right) + \ln\left(1 - \frac{1}{4}\right) + o(1) = \ln(3) + o(1). \end{aligned}$$

Collecting the estimates and exponentiating (and noting that $\log X \sim 2\log\log|D|$), we obtain the claim. □

We can now prove the unconditional lower-bound half of Theorem 1.3.

Proof of Theorem 1.3(i). We fix a sequence of primes ℓ as in Proposition 3.1. To each such ℓ, we associate the odd positive integer $d = h_{\mathbb{Q}(\sqrt{-\ell})} \cdot \frac{\ell-1}{2}$. Clearly, $d \to \infty$ as $\ell \to \infty$. By Dirichlet's class number formula,

$$d = \frac{\sqrt{\ell}}{\pi} L(1, (\tfrac{-\ell}{\cdot})) \cdot \frac{\ell - 1}{2} \leq \left(\frac{\pi}{12e^\gamma} + o(1)\right) \ell^{3/2} / \log\log\ell,$$

as $\ell \to \infty$. It is straightforward to deduce that $\ell^{3/2} \geq (\frac{12e^\gamma}{\pi} + o(1))d \log\log d$. From the Strong Odd Degree Theorem, either $\mathbb{Z}/\ell\mathbb{Z}$ or $\mathbb{Z}/2\ell\mathbb{Z}$ is realizable in degree d, and so $T_{\mathrm{CM}}(d) \geq \ell$. Theorem 1.3(i) follows. □

The proof of the upper bound is more intricate.

Proof of Theorem 1.3(ii). We will assume to start with that the Riemann Hypothesis for L-functions holds, and we will prove that under this assumption,

$$T_{\mathrm{CM}}(d) \leq \left(\left(\frac{24e^\gamma}{\pi} + o(1)\right) d \log\log d\right)^{2/3} \tag{5}$$

as $d \to \infty$ through odd values. We say a few words at the end about how to modify the proof to obtain the unconditional upper bound $T_{\mathrm{CM}}(d) \ll_\epsilon d^{2/3+\epsilon}$.

From the Odd Degree Theorem, the largest torsion subgroup realizable in degree d has the form $\mathbb{Z}/\ell^n\mathbb{Z}$ or $\mathbb{Z}/2\ell^n\mathbb{Z}$ for a prime $\ell \equiv 3 \pmod 4$ and a positive integer n. Here the prime ℓ and the positive integer n are uniquely determined by d.

Case 1: n is even. From Theorem 1.2 along with the bounds $\frac{\ell-1}{2} \geq \frac{\ell}{3}$ and $h_{\mathbb{Q}(\sqrt{-\ell})} \geq 1$,

$$d \geq \frac{\ell-1}{2} \cdot \ell^\delta \cdot h_{\mathbb{Q}(\sqrt{-\ell})} \geq \frac{1}{3}\ell^{\delta+1} \geq \frac{1}{9}\ell^{3n/2}.$$

To see the last estimate, notice that $\ell^{\delta+1} = \ell^{3n/2}$ unless $\ell = 3$, in which case it is $\frac{1}{3}\ell^{3n/2}$. Hence, $\ell^n \leq (9d)^{2/3}$ and $T_{\mathrm{CM}}(d) \leq 2\ell^n \leq 2 \cdot (9d)^{2/3}$. This certainly implies (5) for these d.

Case 2: $\ell < \log\log d$. Here Theorem 1.2 implies that

$$d \geq \frac{1}{3}\ell^{\delta+\frac{3}{2}} \cdot \frac{h_{\mathbb{Q}(\sqrt{-\ell})}}{\ell^{1/2}} \geq \frac{1}{9}\ell^{3n/2} \cdot \frac{h_{\mathbb{Q}(\sqrt{-\ell})}}{\ell^{1/2}} \geq \frac{1}{9(\log\log d)^{1/2}}\ell^{3n/2}.$$

Thus, $T_{\mathrm{CM}}(d) \leq 2\ell^n \ll d^{2/3}(\log\log d)^{1/3}$ in these cases, so (5) again holds.

Case 3: n odd and $\ell \geq \log\log d$. Taking $D = -\ell$ in Proposition 3.2 and invoking the class number formula, we deduce from Proposition 3.2 that as $d \to \infty$,

$$d \geq h_{\mathbb{Q}(\sqrt{-\ell})} \cdot \frac{\ell-1}{2} \cdot \ell^\delta = \frac{\sqrt{\ell}}{\pi} L(1, (\tfrac{-\ell}{\cdot})) \cdot \frac{\ell-1}{2}\ell^\delta \tag{6}$$

$$\geq \left(\frac{\pi}{24e^\gamma} + o(1)\right) \frac{\ell^{\delta+3/2}}{\log\log \ell} = \left(\frac{\pi}{24e^\gamma} + o(1)\right) \frac{\ell^{3n/2}}{\log\log \ell}. \tag{7}$$

This certainly implies that $d \geq \ell$ for large d, and hence $\log\log d \geq \log\log \ell$. Feeding this back into the above estimate gives

$$d \geq \left(\frac{\pi}{24e^\gamma} + o(1)\right) \frac{\ell^{3n/2}}{\log\log d}, \quad \text{whence} \quad \ell^n \leq \left(\left(\frac{24e^\gamma}{\pi} + o(1)\right) d \log\log d\right)^{2/3}.$$

As a consequence, if the largest torsion subgroup in degree d has the form $\mathbb{Z}/\ell^n\mathbb{Z}$, rather than $\mathbb{Z}/2\ell^n\mathbb{Z}$, then we again obtain (5). It remains to treat the subcase when the largest torsion subgroup has the form $\mathbb{Z}/2\ell^n\mathbb{Z}$. Recall that $d \to \infty$ and $\ell \geq \log\log d$, so certainly we can assume $\ell > 3$. If $\ell \equiv 3 \pmod 8$, Theorem 1.2 shows that the first inequality in (6) can be strengthened by a factor of 3. If $\ell \equiv 7 \pmod 8$, then $(\frac{-\ell}{2}) = 1$, and Proposition 3.2 shows that the inequality in (7) can be strengthened by a factor of 3. Following the argument through shows that in either case,

$$\ell^n \leq \left(\left(\frac{8e^\gamma}{\pi} + o(1)\right) d \log\log d\right)^{2/3},$$

and hence

$$T_{\mathrm{CM}}(d) \leq 2\left(\left(\frac{8e^{\gamma}}{\pi} + o(1)\right) d \log\log d\right)^{2/3}.$$

Since $8 \cdot 2^{3/2} < 24$, (5) holds in this case as well.

The proof of the unconditional bound is similar but simpler. The key difference is that in the treatment of odd n, we are forced to use Siegel's lower bound $L(1, (\frac{D}{\cdot})) \gg_\epsilon |D|^{-\epsilon}$ instead of the much stronger results of Proposition 3.2. □

4. The density of Olson degrees: Proof of Theorem 1.5

4.1. **Upper bound.** To bound the density of Olson degrees from above, we must bound from below the density of $\mathscr{M}(\mathcal{G})$ for the set $\mathcal{G}$ appearing in Proposition 1.4. There is an obvious plan of attack: Bound $\mathscr{M}(\mathcal{G})$ from below by $\mathscr{M}(\mathcal{H})$ for a large finite subset $\mathcal{H} \subset \mathcal{G}$. For example, since $\frac{7-1}{2} \cdot h_{\mathbb{Q}(\sqrt{-7})} = 3$ and $\frac{11-1}{2} \cdot h_{\mathbb{Q}(\sqrt{-11})} = 5$, we have $\{2,3,5\} \subset \mathcal{G}$, and so

$$\mathbf{d}(\mathscr{M}(\mathcal{G})) \geq \mathbf{d}(\mathscr{M}(\{2,3,5\})) = \frac{11}{15}.$$

This implies the upper bound of $\frac{4}{15}$ — mentioned in the introduction — for the density of Olson degrees. In this section, we implement the same strategy with a much larger set $\mathcal{H}$.

It requires some finesse to make this method computationally feasible. For any finite set $\mathcal{H}$ of positive integers, inclusion-exclusion immediately yields a formula for $\mathscr{M}(\mathcal{H})$, namely

$$\mathbf{d}(\mathscr{M}(\mathcal{H})) = \sum_{j=1}^{\#\mathcal{H}} (-1)^{j-1} \sum_{\substack{\mathcal{A} \subset \mathcal{H} \\ \#\mathcal{A}=j}} \frac{1}{\mathrm{lcm}(\mathcal{A})}.$$

Unfortunately, the above formula involves $2^{\#\mathcal{H}} - 1$ terms and so a direct implementation of this idea quickly becomes prohibitively time-consuming. To work around this we make two observations, encoded in the following lemmas.

Lemma 4.1. *For a finite collection $\mathcal{H}$ of positive integers, let*

$$\mathcal{H}_{\mathrm{rel}} = \{h \in \mathcal{H} : h \text{ is relatively prime to all other elements of } \mathcal{H}\}.$$

Then

$$1 - \mathbf{d}(\mathscr{M}(\mathcal{H})) = (1 - \mathbf{d}(\mathscr{M}(\mathcal{H} \setminus \mathcal{H}_{\mathrm{rel}}))) \prod_{h \in \mathcal{H}_{\mathrm{rel}}} \left(1 - \frac{1}{h}\right).$$

If $\mathcal{H}$ is a finite set of natural numbers and p is a prime, we define *the p-scaled set* $\mathcal{H}_{(p)}$ by

$$\mathcal{H}_{(p)} = \{h/\gcd(h,p) : h \in \mathcal{H}\},$$

and we define the *p-sieved set* $\mathcal{H}^{(p)}$ by

$$\mathcal{H}^{(p)} = \{h \in \mathcal{H} : p \nmid h\}.$$

Lemma 4.2. *Let $\mathcal{H}$ be a finite collection of positive integers. For any prime number p,*

$$\mathbf{d}(\mathscr{M}(\mathcal{H})) = \frac{1}{p}\mathbf{d}(\mathscr{M}(\mathcal{H}_{(p)})) + \left(1 - \frac{1}{p}\right)\mathbf{d}(\mathscr{M}(\mathcal{H}^{(p)})).$$

Lemmas 4.1 and 4.2 make pleasant elementary exercises, and we omit the proofs. The more difficult of the two, Lemma 4.2, appears in more general form in work of Behrend [3, Lemma, p. 681].

Proof of the upper bound in Theorem 1.5. We begin by computing a large list of elements of $\mathcal{G}$ which eventually will be truncated to form our $\mathcal{H}$. Specifically, we start with the singleton set $\{2\}$. We then successively go through the primes $3 < \ell \leq 100000$ from the congruence class 3 mod 4, throwing $g_\ell := \frac{\ell-1}{2} \cdot h_{\mathbb{Q}(\sqrt{-\ell})}$ into our set whenever g_ℓ is not divisible by a preexisting element. (If g_ℓ is divisible by such an element, then there is no need to throw it in, as this would not lead to a larger set of multiples.) At the end of this process, we sort the resulting list; this leaves us with a set the first several elements of which are

$$2, 3, 5, 913, 1631, 1703, 2051, 2891, 3247, 3401, 3619, 4067, 5327, 6251, 6617, 7051, 7183, 7429, 9737,$$
$$10829, 11129, 11143, 12389, 12463, 12673, 12847, 17611, 18403, 19253, 19931, 20033, 22211, 22747,$$
$$23351, 27491, 28237, 30173, 32927, 33541, 38171, 38641, 39311, 39689, 40687, 42601, 45103, \ldots.$$

We let $\mathcal{H}$ consist of the first 38 elements of this list, so that

$$\mathcal{H} = \{2, 3, 5, 913, \ldots, 32927\}.$$

We will show that

$$1 - \mathbf{d}(\mathscr{M}(\mathcal{H})) < 0.265.$$

This implies the same upper bound 0.265 for the density of Olson degrees.

Apply Lemma 4.1 to $\mathcal{H}$. In this case, one computes that $\mathcal{H}_{\text{rel}} = \{2, 3, 5, 11129, 27491\}$. Thus, puting $\mathcal{H}' = \mathcal{H} \setminus \mathcal{H}_{\text{rel}}$,

$$1 - \mathbf{d}(\mathscr{M}(\mathcal{H})) = (1 - \mathbf{d}(\mathscr{M}(\mathcal{H}')))\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{11129}\right)\left(1 - \frac{1}{27491}\right).$$

To estimate $\mathbf{d}(\mathscr{M}(\mathcal{H}'))$, we apply Lemma 4.2 with $p = 11$:

$$\mathbf{d}(\mathscr{M}(\mathcal{H}')) = \frac{1}{11}\mathbf{d}(\mathscr{M}(\mathcal{H}'_{(11)})) + \left(1 - \frac{1}{11}\right)\mathbf{d}(\mathscr{M}(\mathcal{H}'^{(11)})).$$

The set $\mathcal{H}'^{(11)}$ has only 23 elements, and so $\mathbf{d}(\mathscr{M}(\mathcal{H}'^{(11)}))$ can be computed without fuss by inclusion-exclusion. We find that

$$\mathbf{d}(\mathscr{M}(\mathcal{H}'^{(11)})) = 0.004217267361708\ldots.$$

Let $\mathcal{H}'' = \mathcal{H}'_{(11)}$. Then $\mathcal{H}''$ has 33 elements; 33 is large enough that a direct inclusion-exclusion computation is best avoided. So we make another application of Lemma 4.1, this time to $\mathcal{H}''$. We compute that $\mathcal{H}''_{\text{rel}} = \{641, 653, 1013, 1133, 1601\}$. So with $\mathcal{H}''' = \mathcal{H}'' \setminus \mathcal{H}''_{\text{rel}}$,

$$1 - \mathbf{d}(\mathscr{M}(\mathcal{H}'')) = (1 - \mathbf{d}(\mathscr{M}(\mathcal{H}'''))\left(1 - \frac{1}{641}\right)\left(1 - \frac{1}{653}\right)\left(1 - \frac{1}{1013}\right)\left(1 - \frac{1}{1133}\right)\left(1 - \frac{1}{1601}\right).$$

The set $\mathcal{H}'''$ has 28 elements. However, it contains both 83 and $4067 = 83 \cdot 49$. So we may remove 4067 from $\mathcal{H}'''$ without changing the corresponding set of multiples. Similarly, $\mathcal{H}'''$ contains both 329 and $6251 = 19 \cdot 329$, and so 6251 can also be removed. This brings $\#\mathcal{H}'''$ down to 26, which is small enough that the inclusion-exclusion computation is manageable. We find that

$$1 - \mathbf{d}(\mathscr{M}(\mathcal{H}''')) = 0.979914305743609\ldots.$$

Working back through the chain of equalities,

$$1 - \mathbf{d}(\mathscr{M}(\mathcal{H}'')) = 0.974452539520107\ldots,$$
$$\mathbf{d}(\mathscr{M}(\mathcal{H}')) = 0.006156375826997\ldots,$$

and finally

$$1 - \mathbf{d}(\mathscr{M}(\mathcal{H})) = 0.264991512979231\ldots.$$

This completes the proof of the upper bound half of Theorem 1.5. □

4.2. **Lower bound.** For the rest of this section, ℓ always denotes a prime with $\ell > 3$ and $\ell \equiv 3 \bmod 4$. To establish the lower bound in Theorem 1.5, we require a lower bound on the numbers g_ℓ that holds "most of the time". Via Dirichlet's class number formula, this comes down to bounding below $L(1, (\frac{-\ell}{\cdot}))$. We will deduce what we need from the following variant of the Siegel–Tatuzawa theorem, due to Chen [7].

Proposition 4.3. *Let $0 < \epsilon < \frac{1}{\log(10^6)}$. For all real primitive characters χ of conductor $q > \exp(1/\epsilon)$, with at most one exception,*

$$L(1, \chi) > \min\left\{\frac{1}{7.732 \log q}, \frac{1.5 \cdot 10^6 \cdot \epsilon}{q^\epsilon}\right\}. \tag{8}$$

Let $\epsilon_0 = \frac{0.999}{\log(10^6)}$, and apply Proposition 4.3 with $\epsilon = \epsilon_0$. The minimum in (8) corresponds to the first term when $q \lessapprox 2.82 \cdot 10^{115}$, and to the second term past this point. Moreover, for $q > 10^{115}$, one checks that the right-hand side of (8) is bounded below by $10^5 \cdot q^{-\epsilon_0}$. We use these observations in the proof of the next result.

Corollary 4.4. *For all negative fundamental discriminants D with $|D| > 10^6$, except for a single possible exception, we have*

$$h_{\mathbb{Q}(\sqrt{D})} > 0.041\sqrt{|D|}/\log|D| \quad \textit{when} \quad |D| \le 10^{115},$$

and, with $\epsilon_0 = 0.999/\log(10^6)$,

$$h_{\mathbb{Q}(\sqrt{D})} > 3 \cdot 10^4 \cdot |D|^{\frac{1}{2}-\epsilon_0} \quad \textit{when} \quad |D| > 10^{115}.$$

Proof. Recall that when D is negative and $|D| > 4$, we have $h_{\mathbb{Q}(\sqrt{D})} = \frac{\sqrt{|D|}}{\pi} L(1, (\frac{D}{\cdot}))$. Since $\frac{1}{7.732\pi} = 0.0411\ldots$ and $\frac{10^5}{\pi} > 3 \cdot 10^4$, the result follows. □

Proof of the lower bound in Theorem 1.5. We have already noted that $\mathcal{G} \supset \{2, 3, 5\}$ and that

$$\mathbf{d}(\mathscr{M}(\{2, 3, 5\})) = \frac{11}{15} = 0.7333\ldots.$$

The lower bound claimed in Theorem 1.5 is equivalent to the assertion that $\mathscr{M}(\mathcal{G})$ has density < 0.736. So it is enough to show that, with $\overline{\mathbf{d}}(\cdot)$ denoting upper density,

$$\overline{\mathbf{d}}(\mathscr{M}(\mathcal{G}) \setminus \mathscr{M}(\{2, 3, 5\})) < 0.0026. \tag{9}$$

Suppose that $m \in \mathscr{M}(\mathcal{G})$ and $m \notin \mathscr{M}(\{2, 3, 5\})$. Then m has the form $g_\ell r$, where $\gcd(g_\ell, 30) = \gcd(r, 30) = 1$. Fixing ℓ with $\gcd(g_\ell, 30) = 1$, the number of corresponding $m \le x$ is $\frac{4}{15}\frac{x}{g_\ell} + O(1)$. (The $O(1)$ error term comes from the application of inclusion-exclusion to enforce the condition $\gcd(r, 30) = 1$.) Hence, the total number of such $m \le x$ is at most

$$\frac{4}{15}x \sum_{\substack{\ell:\ g_\ell \le x \\ \gcd(g_\ell, 30) = 1}} \frac{1}{g_\ell} + O(x/\log x).$$

Dividing by x and letting $x \to \infty$ shows that

$$\overline{\mathbf{d}}(\mathscr{M}(\mathcal{G}) \setminus \mathscr{M}(\{2, 3, 5\})) \le \frac{4}{15} \sum_{\ell:\ \gcd(g_\ell, 30) = 1} \frac{1}{g_\ell}.$$

We write

$$\sum_{\ell:\ \gcd(g_\ell, 30) = 1} \frac{1}{g_\ell} = \sum\nolimits_1 + \sum\nolimits_2 + \sum\nolimits_3,$$

where $\sum_1$, $\sum_2$, and $\sum_3$ indicate a restriction to the ranges $\ell \le 10^9$, $10^9 < \ell \le 2.8 \cdot 10^9$, and $\ell > 2.8 \cdot 10^9$, respectively.

We treat these three sums in turn. The first sum can be calculated directly in `PARI`, using the routine `quadclassunit` to compute the class numbers of the fields $\mathbb{Q}(\sqrt{-\ell})$. We find that

$$\sum\nolimits_1 < 0.00788.$$

We remark that, in general, `PARI`'s function `quadclassunit` is only guaranteed to produce correct output assuming the truth of GRH. However, in our range of ℓ, the GRH-conditional result employed here has been verified by extensive computations of Jacobson, Ramachandran, and Williams. (See the discussion in [14, §3.4].) So our estimation of $\sum_1$ is in fact unconditional. To treat $\sum_2$, we recall that Watkins [35] has shown that $h_{\mathbb{Q}(\sqrt{D})} > 100$ for all negative fundamental discriminants with $|D| > 2383747$. Thus, replacing the condition $\gcd(g_\ell, 30) = 1$ by the weaker hypothesis that $\gcd(\frac{\ell-1}{2}, 30) = 1$,

$$\sum\nolimits_2 < \sum_{\substack{10^9 < \ell \le 2.8 \cdot 10^9 \\ \gcd(\frac{\ell-1}{2}, 30) = 1}} \frac{1}{\frac{\ell-1}{2} \cdot 100} < 0.0001819,$$

where again the final estimate comes from an explicit computation in `PARI`.

It remains to treat $\sum_3$. We write $\sum_3 = \sum_3' + \sum_3''$, where $'$ is the contribution of the possible exceptional $D = -\ell$ described in Corollary 4.4, and $''$ is the contribution from all other ℓ. Using that $h_{\mathbb{Q}(\sqrt{-\ell})} > 100$ for this exceptional ℓ (if it exists),

$$\sum\nolimits_3' < \frac{1}{\frac{2.8 \cdot 10^9 - 1}{2} \cdot 100} < 10^{-11}.$$

We turn next to $\sum_3''$. Let $\Pi(t)$ be the number of $\ell \in (3, t]$ with $\gcd(\frac{\ell-1}{2}, 30) = 1$. Each ℓ counted here satisfies $\ell \equiv 3 \pmod 4$, $\ell \equiv 2 \pmod 3$, and $\ell \equiv 2, 3$, or $4 \pmod 5$. So ℓ is forced into 3 of the $\varphi(60) = 16$ reduced residue classes modulo 60. By the Brun–Titchmarsh theorem in the explicit form of Montgomery–Vaughan [24],

$$\Pi(t) \le 2 \frac{3}{16} \frac{t}{\log(t/60)} = \frac{3}{8} \frac{t}{\log(t/60)}$$

for every $t > 60$.

Applying Corollary 4.4, we find that

$$\begin{aligned}
\sum\nolimits_3'' &< \sum_{\substack{2.8 \cdot 10^9 < \ell \le 10^{115} \\ \gcd(\frac{\ell-1}{2}, 30) = 1}} \frac{1}{\frac{\ell-1}{2} \cdot \frac{0.041\sqrt{\ell}}{\log \ell}} + \sum_{\substack{\ell > 10^{115} \\ \gcd(\frac{\ell-1}{2}, 30) = 1}} \frac{1}{\frac{\ell-1}{2} \cdot 3 \cdot 10^4 \cdot \ell^{1/2-\epsilon_0}} \\
&= \frac{2}{0.041} \int_{2.8 \cdot 10^9}^{10^{115}} \frac{\log t}{(t-1)\sqrt{t}} \, d\Pi(t) + \frac{2}{3 \cdot 10^4} \int_{10^{115}}^{\infty} \frac{1}{(t-1) \cdot t^{1/2-\epsilon_0}} \, d\Pi(t) \\
&< \frac{2}{0.041} \int_{2.8 \cdot 10^9}^{\infty} \Pi(t) \left(-\frac{\log t}{(t-1)\sqrt{t}} \right)' dt + \frac{2}{3 \cdot 10^4} \int_{10^{115}}^{\infty} \Pi(t) \left(-\frac{1}{(t-1)t^{1/2-\epsilon_0}} \right)' dt.
\end{aligned}$$

Inserting the above upper bound for $\Pi(t)$ and using `Mathematica` to bound the resulting integrals from above, we find that

$$\sum\nolimits_3'' < 0.001220.$$

Putting everything together,

$$\overline{\mathbf{d}}(\mathscr{M}(\mathcal{G}) \setminus \mathscr{M}(\{2,3,5\})) \le \frac{4}{15} \left(\sum\nolimits_1 + \sum\nolimits_2 + \sum\nolimits_3 \right)$$

$$< \frac{4}{15}\left(0.00788 + 0.0001819 + 10^{-11} + 0.001220\right) < 0.00248.$$

This establishes (9) and so completes the proof of the lower bound in Theorem 1.5. □

5. Stratification of torsion in odd degrees: Proof of Theorem 1.7

We begin with an analytic lemma concerning integers with prescribed sets of divisors. Let $\mathcal{G}$ be a set of positive integers. For each positive integer n, put $\mathcal{D}(n, \mathcal{G}) = \{g \in \mathcal{G} : g \mid n\}$.

Lemma 5.1. *Let $\mathcal{G}$ be a set of odd positive integers, and suppose that the sum of the reciprocals of the elements of $\mathcal{G}$ converges. Let $\mathcal{H}$ be any finite subset of $\mathcal{G}$. The set of odd n with $\mathcal{D}(n, \mathcal{G}) = \mathcal{H}$ possesses a well-defined asymptotic density; this density is positive as long as there is at least one such n.*

Proof. We prove the lemma in two steps. First, we show that the density exists, and then we show positivity. Let $\mathcal{A}$ be the set of odd n with $\mathcal{D}(n, \mathcal{G}) = \mathcal{H}$. For each real $z > \max \mathcal{H}$, put

$$\mathcal{A}_z = \{n : \mathcal{D}(n, \mathcal{G} \cap [1, z]) = \mathcal{H}\}.$$

Notice that whenever $z' > z > \max \mathcal{H}$,

$$\mathcal{A} \subset \mathcal{A}_{z'} \subset \mathcal{A}_z. \tag{10}$$

Now whether or not n belongs to $\mathcal{A}_z$ depends only on n modulo $2\prod_{g \in \mathcal{G} \cap [1,z]} g$. Thus, $\mathcal{A}_z$ is a finite union of congruence classes, and so $\mathbf{d}(\mathcal{A}_z)$ exists. From (10), $\mathbf{d}(\mathcal{A}_z)$ is a nonincreasing function of z, and so we we may define

$$\delta = \lim_{z \to \infty} \mathbf{d}(\mathcal{A}_z).$$

We will show that $\mathcal{A}$ has asymptotic density δ.

In what follows, we continue to use $\overline{\mathbf{d}}(\cdot)$ for upper density, and we use $\underline{\mathbf{d}}(\cdot)$ for lower density.

From the first inclusion in (10), $\overline{\mathbf{d}}(\mathcal{A}) \le \mathbf{d}(\mathcal{A}_z)$ for all z; now letting $z \to \infty$ shows that $\mathcal{A}$ has upper density at most δ. Now consider the lower density of $\mathcal{A}$. If $n \in \mathcal{A}_z$ but $n \notin \mathcal{A}$, then n is divisible by some $g \in \mathcal{G}$ with $g > z$; the number of these $n \le x$ is at most $x \sum_{g \in \mathcal{G},\ g > z} 1/g$. Dividing by x and letting $x \to \infty$, it follows that

$$\underline{\mathbf{d}}(\mathcal{A}) \ge \mathbf{d}(\mathcal{A}_z) - \sum_{g \in \mathcal{G},\ g > z} \frac{1}{g}.$$

Letting $z \to \infty$, and recalling our assumption that the reciprocal sum of the elements of $\mathcal{G}$ converges, we find that $\underline{\mathbf{d}}(\mathcal{A}) \ge \delta$. Thus, $\mathbf{d}(\mathcal{A}) = \delta$.

It remains to show the positivity of δ under the assumption that $\mathcal{A}$ is nonempty. We prove this by exhibiting a subset of $\mathcal{A}$ of positive lower density. Fix $n_0 \in \mathcal{A}$. For each real $z > \max \mathcal{H}$, put

$$M_z := 2 \prod_{g \in \mathcal{G},\ g \le z} g.$$

We consider n of the form $n_0 m$, where $m \equiv 1 \pmod{M_z}$. Clearly, the set of $m \equiv 1 \pmod{M_z}$ has density $\frac{1}{M_z}$. Moreover, each number of the form $n_0 m$ is odd and satisfies $\mathcal{D}(n_0 m, \mathcal{G} \cap [1, z]) = \mathcal{H}$. So if $m \le x$ and $n_0 m \notin \mathcal{A}$, then $g \mid n_0 m$ for some $g \in \mathcal{G}$ with $g \in (z, n_0 x]$; hence,

$$g / \gcd(g, n_0) \mid m.$$

Since $m \equiv 1 \pmod{M_z}$, we must have $g/\gcd(g, n_0)$ coprime to M_z. Hence, the above divisibility forces m into a uniquely determined residue class modulo $gM_z/\gcd(g, n_0)$. The number of these

$m \le x$ is at most

$$\sum_{\substack{z<g\le n_0 x\\ g\in\mathcal{G},\ (g/\gcd(g,n_0),M_z)=1}} \left(\frac{x\gcd(g,n_0)}{gM_z}+1\right) \le \frac{x}{M_z}\cdot\left(n_0\sum_{\substack{g>z\\ g\in\mathcal{G}}}\frac{1}{g}\right)+\sum_{\substack{g\le n_0 x\\ g\in\mathcal{G}}} 1.$$

Observe that

$$\sum_{\substack{g\le n_0 x\\ g\in\mathcal{G}}} 1 \le x^{1/2}+\sum_{\substack{x^{1/2}<g\le n_0 x\\ g\in\mathcal{G}}} 1 \le x^{1/2}+\sum_{\substack{x^{1/2}<g\le n_0 x\\ g\in\mathcal{G}}}\frac{n_0 x}{g} \le x^{1/2}+x\left(n_0\sum_{\substack{g>x^{1/2}\\ g\in\mathcal{G}}}\frac{1}{g}\right).$$

Thus, the number of $m \le x$ with $m \equiv 1 \pmod{M_z}$ and $n_0 m \notin \mathcal{A}$ is at most

$$\frac{x}{M_z}\cdot\left(n_0\sum_{\substack{g>z\\ g\in\mathcal{G}}}\frac{1}{g}\right)+x\left(n_0\sum_{\substack{g>x^{1/2}\\ g\in\mathcal{G}}}\frac{1}{g}\right)+x^{1/2}.$$

Dividing by x and letting $x\to\infty$, we find that the upper density of $m \equiv 1 \pmod{M_z}$ with $n_0 m \notin \mathcal{A}$ is at most

$$\frac{1}{M_z}\left(n_0\sum_{g>z}\frac{1}{g}\right).$$

We now fix z large enough that the parenthesized term is smaller than $1/2$. Then the lower density of m with $n_0 m \in \mathcal{A}$ is at least $\frac{1}{2M_z}$, and so the lower density of $\mathcal{A}$ is at least $\frac{1}{2n_0 M_z}$. □

We can now prove the first assertion of Theorem 1.7.

Proof that the density of the d-Olson degrees exists and is positive, for odd d. Let G run over the groups realizable as torsion subgroups in odd degree, as specified by the Odd Degree Theorem. For each such G, Theorem 1.2 shows that G is realizable in a particular odd degree d precisely when a certain explicitly described positive odd integer g_G (say) divides d. So with $\mathcal{G} = \{g_G : G \text{ realizable in odd degree}\}$, the d-Olson degrees are precisely the odd positive integers d' with

$$\mathcal{D}(d',\mathcal{G}) = \mathcal{D}(d,\mathcal{G}).$$

The existence of the density of d-Olson degrees, together with its positivity, now follows from Lemma 5.1 once it is checked that $\sum_{g\in\mathcal{G}} 1/g$ converges. From Theorem 1.2, every $g \in \mathcal{G}$ has the form $h_{\mathbb{Q}(\sqrt{-\ell})}\cdot\frac{\ell-1}{2}\cdot\ell^\delta$ or $3h_{\mathbb{Q}(\sqrt{-\ell})}\cdot\frac{\ell-1}{2}\cdot\ell^\delta$ for some prime $\ell \equiv 3 \pmod 4$ and some nonnegative integer δ. Hence,

$$\sum_{g\in\mathcal{G}}\frac{1}{g} \le \frac{4}{3}\sum_{\ell}\frac{1}{h_{\mathbb{Q}(\sqrt{-\ell})}\cdot\frac{\ell-1}{2}}\sum_{\delta}\frac{1}{\ell^\delta} < \frac{8}{3}\sum_{\ell}\frac{1}{h_{\mathbb{Q}(\sqrt{-\ell})}\cdot\frac{\ell-1}{2}}.$$

As already observed in [4], this final sum on ℓ converges; for example, this follows from Siegel's lower bound $h_{\mathbb{Q}(\sqrt{-\ell})} \gg_\epsilon \ell^{1/2-\epsilon}$. □

It remains to prove that the densities of the sets of d-Olson degrees, for inequivalent odd d, sum to $1/2$. For this we need the following result from [4].

Proposition 5.2 ("Typical boundedness" of torsion in the CM case)**.** *For each $\epsilon > 0$, there is a positive real number z such that the set of (odd or even) d with $T_{\mathrm{CM}}(d) > z$ has upper density smaller than ϵ.*

Proof of the final assertion of Theorem 1.7. We must show that for any complete set $\mathcal{D}$ of inequivalent odd degrees, $\sum_{d\in\mathcal{D}} \mathbf{d}(\{d\text{-Olson degrees}\}) = 1/2$. To begin, fix $\epsilon > 0$ and choose z so that the integers d with $T_{\mathrm{CM}}(d) > z$ comprise a set of upper density smaller than ϵ.

Since equivalent integers d share the same value of $T_{\mathrm{CM}}(d)$, the set of odd d with $T_{\mathrm{CM}}(d) \le z$ is a union of equivalence classes. Moreover, since there are only finitely many abelian groups of order at most z, this union is necessarily a finite one. So we can pick $d_1, \dots, d_k \in \mathcal{D}$ with

$$\{\text{odd d} : T_{\mathrm{CM}}(d) \le z\} = \bigcup_{i=1}^{k} \{d_i\text{-Olson degrees}\},$$

where the union on the right is disjoint. Exploiting finite additivity,

$$\begin{aligned}\sum_{d\in\mathcal{D}} \mathbf{d}(\{d\text{-Olson degrees}\}) &\ge \sum_{i=1}^{k} \mathbf{d}(\{d_i\text{-Olson degrees}\}) \\ &= \mathbf{d}(\{\text{odd d} : T_{\mathrm{CM}}(d) \le z\}) = \frac{1}{2} - \mathbf{d}(\{\text{odd d} : T_{\mathrm{CM}}(d) > z\}) > \frac{1}{2} - \epsilon.\end{aligned}$$

On the other hand, we also have that for each positive Z,

$$\sum_{d\in\mathcal{D},\ d\le Z} \mathbf{d}(\{d\text{-Olson degrees}\}) = \mathbf{d}\Big(\bigcup_{d\in\mathcal{D},\ d\le Z} \{d\text{-Olson degrees}\}\Big) \le \mathbf{d}(\{\text{odd d}\}) = \frac{1}{2}.$$

Letting $Z \to \infty$,

$$\sum_{d\in\mathcal{D}} \mathbf{d}(\{d\text{-Olson degrees}\}) \le \frac{1}{2}.$$

Since $\epsilon > 0$ is arbitrary, we conclude that $\sum_{d\in\mathcal{D}} \mathbf{d}(\{d\text{-Olson degrees}\}) = 1/2$. □

6. The number of groups that can appear in a given degree

6.1. **Odd degrees: Proof of Theorem 1.9.** The proof of the lower bound in Theorem 1.9 will depend on the following "Brun–Titchmarsh theorem on average", which gives nontrivial information about primes in $[2, X]$ in arithmetic progressions with moduli slightly larger than $X^{1/2}$ (i.e., slightly beyond the range of applicability of the Bombieri–Vinogradov Theorem or the GRH). For the rest of this section, we fix the constant

$$\delta_0 = 10^{-100}.$$

As usual, $\pi(x; q, a)$ denotes the count of primes $p \le x$ with $p \equiv a \pmod q$.

Proposition 6.1. *Let $A > 0$. If $X > X_0(A)$ and $Q \in [X^{1/2}, X^{1/2+\delta_0}]$, then*

$$0.85\frac{X}{\varphi(q)\log X} \le \pi(X; q, 1) \le 1.48\frac{X}{\varphi(q)\log X}$$

for all $q \in [Q, 2Q]$ except those belonging to an exceptional set $\mathscr{E}_A(X, Q)$ of cardinality not exceeding $Q(\log X)^{-A}$.

Proof. This is a theorem of Rousselet [32]. □

Proof of Theorem 1.9. The upper bound is relatively straightforward. The Odd Degree Theorem implies that apart from $\{\bullet\}$, $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, the elements of $\mathscr{G}(d)$ are of the form $\mathbb{Z}/\ell^n\mathbb{Z}$ or $\mathbb{Z}/2\ell^n\mathbb{Z}$, where $\ell \equiv 3 \pmod 4$ is prime. From Theorem 1.2, for $\mathbb{Z}/\ell^n\mathbb{Z}$ or $\mathbb{Z}/2\ell^n\mathbb{Z}$ to appear, it is necessary that $\frac{\ell-1}{2}$ divide d. Thus, the number of possible ℓ is at most $\tau(d)$. Theorem 1.2 also implies that $n \le \frac{2}{3}v_\ell(d) + O(1)$, where $v_\ell(\cdot)$ is the ℓ-adic valuation. Since $v_\ell(d) \ll \log(d)$, given ℓ there are only $O(\log(3d))$ possibilities for n. Hence,

$$\#\mathscr{G}_{\mathrm{CM}}(d) \ll 1 + \tau(d)\log(3d) \ll_\epsilon d^\epsilon,$$

where we use in the last step the well-known upper estimate for the maximal order of $\tau(d)$.

The lower bound requires significantly more effort. Recall from Theorem 1.2 that if $\ell \equiv 3 \pmod 4$ is prime and $\frac{\ell-1}{2} h_{\mathbb{Q}(\sqrt{-\ell})} \mid d$, then at least one of $\mathbb{Z}/\ell\mathbb{Z}$ or $\mathbb{Z}/2\ell\mathbb{Z}$ belongs to $\mathscr{G}(d)$. So if $r(d)$ denotes the number of divisors of d of the form $\frac{\ell-1}{2} h_{\mathbb{Q}(\sqrt{-\ell})}$, with ℓ as above, then

$$\#\mathscr{G}(d) \geq r(d).$$

Now let A be any large, fixed positive real number. We will show that there are infinitely many odd d with

$$r(d) > (\log d)^{\frac{1}{4} A \delta_0}.$$

The lower bound in Theorem 1.9 is then immediate.

In what follows, we allow implied constants to depend on A, and ℓ is understood to run only over primes from the residue class 3 mod 4.

For each real number $x \geq 3$, put

$$M := \prod_{2 < p \leq \frac{1}{2} \log x} p.$$

By the prime number theorem, $M \leq x^{2/3}$ for large x. Our plan is to show that the average of $r(d)$ is large when taken over those $d \leq x$ that are multiples of M. (This strategy is inspired by a similar argument of Prachar [30]. Cf. the proof of [1, Proposition 10].) Hence, some individual term $r(d)$ must also be large. Now

$$\begin{aligned} \sum_{\substack{d \leq x \\ M \mid d}} r(d) &= \sum_{\substack{d \leq x \\ M \mid d}} \#\{(m,\ell) : m \left(\frac{\ell-1}{2}\right) h_{\mathbb{Q}(\sqrt{-\ell})} = d\} \\ &= \#\{(m,\ell) : M \mid m \left(\frac{\ell-1}{2}\right) h_{\mathbb{Q}(\sqrt{-\ell})}, \text{ and } m \left(\frac{\ell-1}{2}\right) h_{\mathbb{Q}(\sqrt{-\ell})} \leq x\}. \end{aligned}$$

We partition the pairs (m,ℓ) counted above according to the value of $\gcd(2M, m)$. Since we seek only a lower bound on the partial sums of $r(d)$, it is enough to consider pairs with $\gcd(2M, m)$ highly restricted. Let

$$T = (\log x)^A.$$

Given $g \mid 2M$ with $g \in (T, 2T]$, we construct pairs (m,ℓ) with $\gcd(2M, m) = 2M/g$ as follows: First, fix $\ell \leq T^{2-\delta_0}$ with $g/\gcd(g,2) \mid \ell - 1$. Choose any $m \leq \frac{x}{h_{\mathbb{Q}(\sqrt{-\ell})} \cdot (\ell-1)/2}$ with $\gcd(2M, m) = 2M/g$. Then the pair (m,ℓ) is counted above. Given ℓ, inclusion-exclusion shows that the number of corresponding m is (as $x \to \infty$)

$$\sim \frac{x}{\frac{\ell-1}{2} h_{\mathbb{Q}(\sqrt{-\ell})}} \frac{1}{2M/g} \frac{\varphi(g)}{g}.$$

Using $h_{\mathbb{Q}(\sqrt{-\ell})} \ll \ell^{1/2} \log \ell$ and $\varphi(g) \gg g/\log\log g$, the preceding expression is

$$\gg \frac{x}{M(\log\log x)^2} \cdot \frac{g}{\ell^{3/2}}.$$

Summing on ℓ, and recalling that $\ell \leq T^{2-\delta_0}$, the number of pairs we construct for our given g is

$$\gg \frac{x}{M(\log\log x)^2} \frac{T}{T^{\frac{3}{2}(2-\delta_0)}} \sum_{\substack{\ell \leq T^{2-\delta_0} \\ \ell \equiv 3 \pmod 4 \\ \ell \equiv 1 \pmod{g/\gcd(g,2)}}} 1.$$

Now

$$\sum_{\substack{\ell\le T^{2-\delta_0}\\ \ell\equiv 3 \pmod 4\\ \ell\equiv 1 \pmod{g/\gcd(g,2)}}} 1 = \pi(T^{2-\delta_0}; g/\gcd(g,2), 1) - \pi(T^{2-\delta_0}; 4g/\gcd(g,2), 1).$$

In the notation of Proposition 6.1,

$$\pi(T^{2-\delta_0}; g/\gcd(g,2), 1) \ge 0.85 \cdot \frac{T^{2-\delta_0}}{\varphi(g/\gcd(g,2))\log(T^{2-\delta_0})}$$

unless g is even and $g/2 \in \mathscr{E}_1(T^{2-\delta_0}, T/2)$ or g is odd and $g \in \mathscr{E}_1(T^{2-\delta_0}, T)$; from Proposition 6.1, the number of g involved in these exceptional sets is $O(T/\log\log x)$. Similarly, as long as g avoids a certain set of size $O(T/\log\log x)$, we have

$$\pi(T^{2-\delta_0}; 4g/\gcd(g,2), 1) \le 1.48 \cdot \frac{T^{2-\delta_0}}{2\varphi(g/\gcd(g,2))\log(T^{2-\delta_0})}.$$

Inserting these prime counting estimates above (noting that $1.48/2 < 0.85$) we find that as long as g avoids a set of size $O(T/\log\log x)$, we construct

$$\gg \frac{x}{M(\log\log x)^2}\frac{T}{T^{\frac12(2-\delta_0)}}\frac{1}{g\log T} \gg \frac{x}{M(\log\log x)^3}\frac{1}{T^{1-\frac12\delta_0}}$$

pairs for a given g.

We now wish to sum over allowable values of g. Recall that our $g \in (T, 2T]$ must satisfy $g \mid 2M$, i.e., g must be a squarefree, $\frac12\log x$-smooth number. Without the squarefree restriction, the number of these $g \le 2T$ is $\sim 2\rho(A)T$, where $\rho(\cdot)$ is Dickman's function; insisting that g is squarefree cuts this down to $\sim \frac{12}{\pi^2}\rho(A)T$ (see, e.g., [25]). Similarly, the number of $\frac12\log x$-smooth $g \le T$ is $\sim \frac{6}{\pi^2}\rho(A)T$. Thus, there are $\gg T$ values of $g \in (T, 2T]$ that divide $2M$. (This could also be established by more elementary methods.) Excluding the $O(T/\log\log x)$ bad values of g coming from the application of Proposition 6.1, we are still left with $\gg T$ allowable values of g (for large x). It follows that

$$\sum_{\substack{d\le x\\ M\mid d}} r(d) \gg \frac{x}{M(\log\log x)^3}\frac{1}{T^{1-\frac12\delta_0}}\cdot T = \frac{x}{M}\cdot\frac{(\log x)^{\frac12 A\delta_0}}{(\log\log x)^3},$$

and hence

$$\sum_{\substack{d\le x\\ M\mid d}} r(d) > \frac{x}{M}(\log x)^{\frac14 A\delta_0}$$

for large enough x.

Since there are no more than x/M multiples of M in $[1, x]$, there is some $d \le x$ satisfying $r(d) > (\log x)^{\frac14 A\delta_0}$, and hence also $r(d) > (\log d)^{\frac14 A\delta_0}$. Letting $x \to \infty$, we obtain infinitely many distinct d of this kind. □

6.2. **Even degrees.** In this section we explain why the upper bound in Theorem 1.9 fails if we do not restrict to odd values of d. The key ingredient in our argument is a variant of the following 1935 theorem of Erdős [13] asserting the existence of "popular" values of Euler's φ-function.

Proposition 6.2. *For some constant $\delta > 0$ and all sufficiently large x,*

$$\max_{m\le x} \#\{n \text{ squarefree} : \varphi(n) = m\} > x^{\delta}.$$

An easy modification of Erdős's proof yields the following more general result.

Proposition 6.3. *Let $\mathscr{P}$ be any subset of the primes with positive relative lower density. There are constants $\delta = \delta(\mathscr{P}) > 0$ and $x_0 = x_0(\mathscr{P})$ such that for all $x > x_0$,*

$$\max_{m \le x} \#\{n : n \text{ is a squarefree product of primes in } \mathscr{P}, \text{ and } \varphi(n) = m\} > x^{\delta}.$$

Proof (sketch). We refer the reader to the proof of Proposition 6.2 appearing in the survey article [29] (see that paper's Theorem 4.6). It is clear from that exposition that the proposition will follow if it is shown that, for some fixed $\alpha > 0$ and all large T,

$$\#\{p \le T : p \in \mathscr{P}, \text{ all prime factors of } p-1 \text{ are at most } T^{1-\alpha}\} \gg T/\log T. \tag{11}$$

By hypothesis, there is a constant $c > 0$ such that for all large T,

$$\#\{p \le T : p \in \mathscr{P}\} \ge cT/\log T.$$

From Brun's sieve, if α is fixed sufficiently close to 1 and T is large, then

$$\#\{\text{primes } p \le T : q \mid p-1 \text{ for some prime } q > T^{1-\alpha}\} < \frac{c}{2} T/\log T;$$

up to changes in notation, this assertion is contained in Erdős's proof of [13, Lemma 4]. Combining the last two estimates yields (11). □

Theorem 6.4. *For some constant $\eta > 0$ and all sufficiently large x,*

$$\max_{d \le x} \#\mathscr{G}_{\mathrm{CM}}(d) > x^{\eta}.$$

Proof. Let E be an elliptic curve with $j(E) = 0$, and choose a model of E defined over $\mathbb{Q}$. Since E has CM by the full ring of integers in $K = \mathbb{Q}(\sqrt{-3})$, the image of $\mathrm{Gal}(\bar{\mathbb{Q}}/K)$ under the mod-ℓ Galois representation associated to E lands in a split Cartan subgroup for each prime $\ell \equiv 1 \pmod 3$. (See [8, p. 12-13].) Thus we have a K-rational cyclic subgroup of order ℓ. Let $n = \ell_1 \ell_2 \cdots \ell_r$, where $\ell_i \equiv 1 \pmod 3$ are distinct primes, and let P_i be a generator of the K-rational subgroup of order ℓ_i. Then $P_1 + \cdots + P_r$ generates a K-rational subgroup of order n. By [5, Theorem 5.5], there is a number field F_n of degree dividing $\varphi(n)$ and a quadratic twist E' of $E_{/F_n}$ such that $E'(F_n)$ has a point of order n. Below we write $E' = E'_n$ to indicate the dependence on n. By enlarging F_n if necessary, we can (and will) assume that $[F_n : \mathbb{Q}] = \varphi(n)$.

Let $\mathscr{P}$ be the set of primes congruent to 1 modulo 3, so that $\mathscr{P}$ has relative density 1/2. Let $\delta = \delta(\mathscr{P})$ be the positive constant whose existence is specified in Proposition 6.3. Thus, for all large x, there is an integer $d \le x$ for which the set

$$\mathscr{N} := \{\text{squarefree numbers } n \text{ composed of primes } \ell \equiv 1 \pmod 3 : \varphi(n) = d\}$$

satisfies $\#\mathscr{N} > x^{\delta}$. For each $n \in \mathscr{N}$, let F_n be the number field specified in the previous paragraph, so that $[F_n : \mathbb{Q}] = d$. We will bound $\#\mathscr{G}_{\mathrm{CM}}(d)$ from below by showing that there is not too much repetition among the groups $E'_n(F_n)[\mathrm{tors}]$, for $n \in \mathscr{N}$.

Suppose that n and n' both belong to $\mathscr{N}$ and that $E'_n(F_n)[\mathrm{tors}] \cong E'_{n'}(F_{n'})[\mathrm{tors}] \cong G$ (say). Then both n and n' divide the exponent of G. The exponent of G is bounded by $\#G$, and from [10], $\#G \le T_{\mathrm{CM}}(d) \ll x \log\log x$. (We could avoid appealing to [10] by referencing earlier results of Silverberg [33] or Prasad–Yogananda [31].) Hence (for large x) the number of integers that divide the exponent of G is no more than $x^{\delta/2}$. So no more than $x^{\delta/2}$ numbers $n \in \mathscr{N}$ share the same value of $E'_n(F_n)[\mathrm{tors}]$. Thus,

$$\#\mathscr{G}_{\mathrm{CM}}(d) \ge \frac{\#\mathscr{N}}{x^{\delta/2}} > x^{\delta/2}.$$

Since $d \le x$, this establishes Theorem 6.4 with $\eta = \delta/2$. □

We can go a bit further. The arguments presented by Pomerance in [29, §4] suggest the following conjecture on the upper order of $\#\mathscr{G}_{\mathrm{CM}}(d)$.

Conjecture 6.5. *As $x \to \infty$,*

$$\max_{d \le x} \#\mathscr{G}_{\mathrm{CM}}(d) = x/L(x)^{1+o(1)},$$

where $L(x) = \exp(\log x \frac{\log\log\log x}{\log\log x})$.

Indeed, the proof of [29, Theorem 4.4] shows that under a reasonable conjecture on the distribution of smooth shifted primes (appearing there as Hypothesis 4.3), there are numbers $m \le x$ with at least $x/L(x)^{1+o(1)}$ representations in the form $\varphi(n)$, with n squarefree. We expect Hypothesis 4.3 to remain true even when restricted to primes from the residue class 1 mod 3. Combining the argument for [29, Theorem 4.4] with the above proof of Theorem 6.4 then shows that

$$\max_{d \le x} \#\mathscr{G}_{\mathrm{CM}}(d) \ge x/L(x)^{1+o(1)}.$$

The upper bound half of Conjecture 6.5 can be proved unconditionally. We start from [29, Theorem 4.1], which asserts that

$$\max_{m \le x} \#\{n : \varphi(n) = m\} \le x/L(x)^{1+o(1)}. \tag{12}$$

Now take any positive integer $d \le x$. From [4, Theorem 2.4], if $G \cong E(F)[\mathrm{tors}]$ for some CM elliptic curve E over some degree d number field F, then, writing $\mathrm{rad}(\cdot)$ for the product-of-distinct-prime-factors function,

$$\varphi(\mathrm{rad}(\#G)) = \prod_{\ell \mid \#G} (\ell - 1) \mid 12d.$$

From the maximal order of the divisor function, $\tau(12d) \le \exp(O(\log x/\log\log x))$, and this last expresion is $L(x)^{o(1)}$. So given d, the integer $\varphi(\mathrm{rad}(\#G))$ is restricted to a set of at most $L(x)^{o(1)}$ possible values. It now follows from (12) that, given d, there are at most $x/L(x)^{1+o(1)}$ possible values of $\mathrm{rad}(\#G)$. From [10], we have $\#G = O(x\log\log x)$. As a consequence, given a value of $\mathrm{rad}(\#G)$, there are at most $\exp(O(\log x/\log\log x))$ possibilities for $\#G$ (see, e.g., [27, Lemma 4.2]). Hence, there are no more than $x/L(x)^{1+o(1)}$ possibilities for $\#G$. But the structure of G is determined by its two invariant factors; hence, given $\#G$, the number of possible choices for G is crudely bounded by $\tau(\#G)$, which is at most $\exp(O(\log x/\log\log x))$. We conclude that $\#\mathscr{G}_{\mathrm{CM}}(d) \le x/L(x)^{1+o(1)}$, as claimed.

7. CM Torsion Subgroups in Odd Degree $d \le 99$

We have written `PARI/GP` code which, given an odd positive integer d, returns the list of groups which appear the torsion subgroup of a CM elliptic curve defined over a number field of degree d. This code is available at the research website of either author.

On a modern desktop computer, one can process all odd $d \le 2 \cdot 10^8$ in about 12 hours. The output in the more modest range $d \le 99$ is included below.

Degree	Torsion Subgroups Appearing
1	$\mathbb{Z}/m\mathbb{Z}$ for $m = 1, 2, 3, 4, 6$ and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
3	$\mathbb{Z}/m\mathbb{Z}$ for $m = 1, 2, 3, 4, 6, 9, 14$ and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
5	$\mathbb{Z}/m\mathbb{Z}$ for $m = 1, 2, 3, 4, 6, 11$ and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
7	Olson
9	$\mathbb{Z}/m\mathbb{Z}$ for $m = 1, 2, 3, 4, 6, 9, 14, 18, 19, 27$ and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
11	Olson
13	Olson
15	$\mathbb{Z}/m\mathbb{Z}$ for $m = 1, 2, 3, 4, 6, 9, 11, 14, 22$ and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

Degree	Torsion Subgroups Appearing
17	Olson
19	Olson
21	$\mathbb{Z}/m\mathbb{Z}$ for $m = 1, 2, 3, 4, 6, 9, 14, 43$ and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
23	Olson
25	5-Olson
27	$\mathbb{Z}/m\mathbb{Z}$ for $m = 1, 2, 3, 4, 6, 9, 14, 18, 19, 27, 38, 54$ and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
29	Olson
31	Olson
33	$\mathbb{Z}/m\mathbb{Z}$ for $m = 1, 2, 3, 4, 6, 9, 14, 46, 67$ and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
35	5-Olson
37	Olson
39	3-Olson
41	Olson
43	Olson
45	$\mathbb{Z}/m\mathbb{Z}$ for $m = 1, 2, 3, 4, 6, 9, 11, 14, 18, 19, 22, 27, 62$ and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
47	Olson
49	Olson
51	3-Olson
53	Olson
55	5-Olson
57	3-Olson
59	Olson
61	Olson
63	$\mathbb{Z}/m\mathbb{Z}$ for $m = 1, 2, 3, 4, 6, 9, 14, 18, 19, 27, 43, 86$ and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
65	5-Olson
67	Olson
69	3-Olson
71	Olson
73	Olson
75	15-Olson
77	Olson
79	Olson
81	$\mathbb{Z}/m\mathbb{Z}$ for $m = 1, 2, 3, 4, 6, 9, 14, 18, 19, 27, 38, 54, 81, 163$ and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
83	Olson
85	5-Olson
87	$\mathbb{Z}/m\mathbb{Z}$ for $m = 1, 2, 3, 4, 6, 9, 14, 59$ and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$
89	Olson
91	Olson
93	3-Olson
95	5-Olson
97	Olson
99	$\mathbb{Z}/m\mathbb{Z}$ for $m = 1, 2, 3, 4, 6, 9, 14, 18, 19, 27, 46, 67, 134$ and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

Acknowledgements. We thank Kenneth Jacobs for suggesting we study large values of $\#\mathscr{G}_{\mathrm{CM}}(d)$ and Anton Mosunov for helpful pointers to the literature on unconditional class number computations. We thank Pete L. Clark for useful conversations and for suggesting we consider the stratification of torsion subgroups. We are also grateful to Mits Kobayashi for enlightening discussions about densities of sets of multiples. The research of the first author is supported in part by NSF grant DMS-1344994 (RTG in Algebra, Algebraic Geometry, and Number Theory at the University of Georgia). Work of the second author is supported by NSF award DMS-1402268.

References

1. Leonard M. Adleman, Carl Pomerance, and Robert S. Rumely, *On distinguishing prime numbers from composite numbers*, Ann. of Math. (2) **117** (1983), no. 1, 173–206.
2. Noboru Aoki, *Torsion points on abelian varieties with complex multiplication*, Algebraic cycles and related topics (Kitasakado, 1994), World Sci. Publ., River Edge, NJ, 1995, pp. 1–22. MR 1414432 (98e:11073)
3. Felix A. Behrend, *Generalization of an inequality of Heilbronn and Rohrbach*, Bull. Amer. Math. Soc. **54** (1948), 681–684.
4. Abbey Bourdon, Pete L. Clark, and Paul Pollack, *Anatomy of torsion in the CM case*, preprint, submitted (http://arxiv.org/abs/1506.00565).
5. Abbey Bourdon, Pete L. Clark, and James Stankewicz, *Torsion points on CM elliptic curves over real number fields*, preprint, submitted (http://arxiv.org/abs/1411.2742).
6. Florian Breuer, *Torsion bounds for elliptic curves and Drinfeld modules*, J. Number Theory **130** (2010), no. 5, 1241–1250.
7. Yong-Gao Chen, *On the Siegel-Tatuzawa-Hoffstein theorem*, Acta Arith. **130** (2007), 361–367.
8. Pete L. Clark, Brian Cook, and James Stankewicz, *Torsion points on elliptic curves with complex multiplication*, Int. J. Number Theory **9** (2013), 447–479.
9. 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.
10. Pete L. Clark and Paul Pollack, *The truth about torsion in the CM case*, C. R. Math. Acad. Sci. Paris **353** (2015), no. 8, 683–688.
11. Henri Cohen, *Advanced topics in computational number theory*, Graduate Texts in Mathematics, vol. 193, Springer-Verlag, New York, 2000.
12. David A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory and complex multiplication*, A Wiley-Interscience Publication, John Wiley & Sons Inc., New York, 1989.
13. Paul Erdős, *On the normal number of prime factors of $p-1$ and some related problems concerning Euler's φ-function*, Quart. J. Math. **6** (1935), 205–213.
14. Michael J. Jacobson, Jr., Shantha Ramachandran, and Hugh C. Williams, *Numerical results on class groups of imaginary quadratic fields*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 4076, Springer, Berlin, 2006, pp. 87–101.
15. Padmini T. Joshi, *The size of $L(1,\chi)$ for real nonprincipal residue characters χ with prime modulus*, J. Number Theory **2** (1970), 58–73.
16. Sheldon Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. **109** (1992), no. 2, 221–229.
17. Monsur A. Kenku and Fumiyuki Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149.
18. Daniel Sion Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc. (3) **33** (1976), no. 2, 193–237.
19. Soonhak Kwon, *Degree of isogenies of elliptic curves with complex multiplication*, J. Korean Math. Soc. **36** (1999), no. 5, 945–958.
20. Youness Lamzouri, Xiannan Li, and Kannan Soundararajan, *Conditional bounds for the least quadratic non-residue and related problems*, Math. Comp. **84** (2015), 2391–2412.
21. John E. Littlewood, *On the class number of the corpus $P(\sqrt{-k})$*, Proc. London Math. Soc. **27** (1928), 358–372.
22. Barry Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186 (1978).
23. Loïc Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), no. 1-3, 437–449.
24. Hugh L. Montgomery and Robert C. Vaughan, *The large sieve*, Mathematika **20** (1973), 119–134.

25. Mongi Naimi, *Les entiers sans facteurs carré $\leq x$ dont leurs facteurs premiers $\leq y$*, Groupe de travail en théorie analytique et élémentaire des nombres, 1986–1987, Publ. Math. Orsay, vol. 88, Univ. Paris XI, Orsay, 1988, pp. 69–76.
26. Loren D. Olson, *Points of finite order on elliptic curves with complex multiplication*, Manuscripta Math. **14** (1974), 195–205.
27. Paul Pollack, *On the greatest common divisor of a number and its sum of divisors*, Michigan Math. J. **60** (2011), 199–214.
28. Carl Pomerance, *Popular values of Euler's function*, Mathematika **27** (1980), 84–89.
29. ———, *Two methods in elementary analytic number theory*, Number theory and applications (Banff, AB, 1988), NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., vol. 265, Kluwer Acad. Publ., Dordrecht, 1989, pp. 135–161.
30. Karl Prachar, *Über die Anzahl der Teiler einer natürlichen Zahl, welche die Form $p-1$ haben*, Monatsh. Math. **59** (1955).
31. Dipendra Prasad and Chalya S. Yogananda, *Bounding the torsion in CM elliptic curves*, C. R. Math. Acad. Sci. Soc. R. Can. **23** (2001), no. 1, 1–5.
32. Bruno Rousselet, *Inégalités de type Brun-Titchmarsh en moyenne*, Groupe de travail en théorie analytique et élémentaire des nombres, 1986–1987, Publ. Math. Orsay, vol. 88, Univ. Paris XI, Orsay, 1988, pp. 91–123.
33. Alice Silverberg, *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.
34. Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.
35. Mark Watkins, *Class numbers of imaginary quadratic fields*, Math. Comp. **73** (2004), 907–938 (electronic).

E-mail address: abourdon@uga.edu

E-mail address: pollack@uga.edu

Department of Mathematics, Boyd Graduate Studies Building, University of Georgia, Athens, Georgia 30602, USA