ON THE STRATIFICATION CONJECTURE FOR CM TORSION SUBGROUPS

PETE L. CLARK

ABSTRACT. Work of Bourdon-Clark-Pollack shows that the set of degrees $d \in \mathbb{Z}^+$ for which the classification of torsion subgroups of CM elliptic curves over all number fields of degree d is the same as the classification of CM torsion of elliptic curves over $\mathbb{Q}$ has positive asymptotic density. Based on this, I conjectured that for every $d_0 \in \mathbb{Z}^+$, the set of $d \in \mathbb{Z}^+$ such that the classification of CM torsion in degree d as the same as in degree d_0 has positive density. This was proven for all odd d_0 by Bourdon-Pollack in 2017. Here we give the first results on even d_0: the conjecture holds for $d_0 = 2$ and for $d_0 = 2p_0$ for a set of primes p_0 of relative density one. However, we will also explain why the conjecture seems likely to be false for $d_0 = 2p_0$ where p_0 lies in an infinite set of prime numbers, including $p_0 = 3$.

1. Introduction

For groups G and H, we write $G \hookrightarrow H$ to mean that there is an injective group homomorphism from G to H; we also say that G **embeds in** H.

For a subset $S \subseteq \mathbb{Z}^+$, if $\lim_{N\to\infty} \frac{\#(S\cap[1,N])}{N}$ exists, we call it the **density** of S and denote it by $\delta(S)$. We define the **upper density** $\overline{\delta}(S)$ (resp. the **lower density** $\underline{\delta}(S)$) by replacing the limit by a limit superior (resp. by a limit inferior); thus for all $S \subseteq \mathbb{Z}^+$ we have $0 \leq \underline{\delta}(S) \leq \overline{\delta}(S) \leq 1$, and the existence of $\delta(S)$ is equivalent to the equality $\underline{\delta}(S) = \overline{\delta}(S)$.

For $d \in \mathbb{Z}^+$, let $\mathcal{G}(d)$ denote the set of isomorphism classes of groups of the form $E(F)[\mathrm{tors}]$ with F a number field of degree d and $E_{/F}$ an elliptic curve. For every such elliptic curve $E_{/F}$, there are positive integers $M \mid N$ such that $E(F) \cong \mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$, so we may and shall regard $\mathcal{G}(d)$ as a set of such groups $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$. Let $\mathcal{G}_{\mathbf{CM}}(d)$ be the subset of $\mathcal{G}(d)$ obtained by imposing the condition that the elliptic curves $E_{/F}$ have **complex multiplication**: that is, the geometric endomorphism ring of E is strictly larger than $\mathbb{Z}$ and thus is an order in an imaginary quadratic field [Si86, Cor. III.9.4].

Remark 1.1.

a) *Work of Merel* [Me96] *implies that for all $d \in \mathbb{Z}^+$, the set $\mathcal{G}(d)$ is finite. By* [BCS17, Thm. 2.1a)]*, if $d_1 \mid d_2$ then $\mathcal{G}(d_1) \subseteq \mathcal{G}(d_2)$ Work of Mazur* [Ma77] *then gives*

$$\forall d \in \mathbb{Z}^+,\ \mathcal{G}(d) \supseteq \mathcal{G}(1) = \{\mathbb{Z}/N\mathbb{Z} \text{ for } N \in \{[1,10],12\} \cup \{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \text{ for } n \text{ in } \{[1,4]\}\}.$$

b) *Earlier work of Silverberg* [Si88], [Si92] *implies that for all $d \in \mathbb{Z}^+$, the set $\mathcal{G}_{\mathbf{CM}}(d)$ is finite. Once again* [BCS17, Thm. 2.1a)] *implies that if $d_1 \mid d_2$ then $\mathcal{G}_{\mathbf{CM}}(d_1) \subseteq \mathcal{G}_{\mathbf{CM}}(d_2)$. Work of Olson* [Ol74] *then gives*

$$\forall d \in \mathbb{Z}^+,\ \mathcal{G}_{\mathbf{CM}}(d) \supseteq \mathcal{G}_{\mathbf{CM}}(1) = \{\mathbb{Z}/N\mathbb{Z} \text{ for } N \in [1,4] \cup \{6\}\} \cup \{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\}.$$

This paper continues the study of arithmetical statistical phenomena on torsion subgroups of elliptic curves over number fields that are particular to the CM case. For $d \in \mathbb{Z}^+$ we define $T_{\mathbf{CM}}(d)$ (resp. $T_{\neg\mathbf{CM}}(d)$) to be the maximum size of $\#E(F)[\mathrm{tors}]$ as F ranges over number fields of degree d and $E_{/F}$ ranges over elliptic curves with complex multiplication (resp. *without* complex multiplication). These functions have very different growth behaviors. We know [CP17, Thm. 1.1]

$$\limsup_d \frac{T_{\mathbf{CM}}(d)}{d \log\log d} = \frac{e^\gamma \pi}{\sqrt{3}}, \tag{1}$$

so the "upper order" of $T_{\mathbf{CM}}(d)$ is $\log\log d$. For the non-CM case, we know [CP17, Thm. 6.4]

$$\limsup_d \frac{T_{\neg\mathbf{CM}}(d)}{\sqrt{d \log\log d}} \geq \sqrt{\frac{\pi^2 e^\gamma}{3}}.$$

It is a folk conjecture that $T(d)$ (or, equivalently in view of (1), $T_{\neg\mathbf{CM}}(d)$) should grow no faster than some power of d, but the best known bounds (due to Merel, Parent and Oesterlé [Pa99]) are more than an exponential way from this. For the lower order, we know [BCS17, Thm. 1.4]

$$\liminf_d T_{\mathbf{CM}}(d) = 6 = T_{\mathbf{CM}}(1), \tag{2}$$

while [CMP18, §2.1]

$$\liminf_d \frac{T_{\neg\mathbf{CM}}(d)}{\sqrt{d}} > 0.$$

In particular, we have $\lim_{d\to\infty} T_{\neg\mathbf{CM}}(d) = \infty$, and it follows that for all $d_1 \in \mathbb{Z}^+$, the set of $d_2 \in \mathbb{Z}^+$ such that $\mathcal{G}(d_1) = \mathcal{G}(d_2)$ is finite.[1] In this regard also, the CM case is quite different. Bourdon-Clark-Stankewicz showed [BCS17, Thm. 1.4]

$$\text{for all primes } p \geq 7,\ T_{\mathbf{CM}}(p) = T_{\mathbf{CM}}(1)$$

– notice that this implies (2) above – and then Bourdon-Clark-Pollack showed [BCP17, Thm. 1.3] that the set of $d \in \mathbb{Z}^+$ such that $T_{\mathbf{CM}}(1) = T_{\mathbf{CM}}(d)$ has positive density. Thus whereas the mapping $d \mapsto \mathcal{G}(d)$ has finite fibers (and may be injective), the mapping $d \mapsto \mathcal{G}_{\mathbf{CM}}(d)$ has at least one fiber that is not only infinite but of positive density. This suggests a more refined study in the CM case.

For $d_1, d_2 \in \mathbb{Z}^+$, we write $d_1 \sim d_2$ if $\mathcal{G}_{\mathbf{CM}}(d_1) = \mathcal{G}_{\mathbf{CM}}(d_2)$.[2] This is an equivalence relation, and we denote the $\sim$-equivalence class of $d \in \mathbb{Z}^+$ by $[d]_\sim$. For $d, d_0 \in \mathbb{Z}^+$, if $d \sim d_0$ we say that d is a **d_0-Olson degree**; if moreover $d_0 \mid d$, then we say that d is a **strongly d_0-Olson degree**. For $d_0 \in \mathbb{Z}^+$, let $[d_0]_S$ denote the set of all strongly d_0-Olson degrees.

About ten years ago, I made the following conjecture:

Conjecture 1.2 (Stratification of Torsion in the CM Case)**.**

a) *For all $d_0 \in \mathbb{Z}^+$, the set $[d_0]_S$ of strongly d-Olson degrees has positive lower density.*

[1] Since $\mathcal{G}(d)$ is only known for $d \in \{1, 2, 3\}$, it is not surprising that there are no known examples of $d_1 < d_2$ with $\mathcal{G}(d_1) = \mathcal{G}(d_2)$. However when $\mathcal{G}(d_1)$ is known, one can often show computationally that $\mathcal{G}(d_1) \neq \mathcal{G}(d_2)$: e.g. from Mazur's Theorem and the table on [vH14, p. 4] it follows that for all $d \geq 2$ we have $\mathcal{G}(1) \subsetneq \mathcal{G}(d)$.

[2] This notation signals our exclusive focus on the CM case; otherwise we would write $\sim_{\mathbf{CM}}$.

b) *For all $d \in \mathbb{Z}^+$, the set $[d_0]_\sim$ has a density. Moreover, let $d_1 < d_2 < \ldots < d_n < \ldots$ be a set of representatives for the distinct $\sim$-equivalence classes of $\mathbb{Z}^+$ (so every positive integer is d_n-Olson for exactly one n). Then*

$$\sum_{n=1}^{\infty} \delta([d_n]_\sim) = 1.$$

In [BP17], Bourdon-Pollack showed that for every **odd** $d_0 \in \mathbb{Z}^+$, the set $[d_0]_\sim$ of d_0-Olson degrees has positive density. They also proved "the odd degree part" of Conjecture 1.2b): namely, if $e_1 < \ldots < e_n < \ldots$ is a set of representatives for the distinct odd $\sim$-equivalence classes of $\mathbb{Z}^+$ (so that every odd positive integer is e_n-Olson for exactly one n), then

$$\sum_{n=1}^{\infty} \delta([e_n]_\sim) = \frac{1}{2}.$$

Very little is known about d_0-Olson degrees and strongly d_0-Olson degrees when d_0 is even. An early work [CCRS14] computes $\mathcal{G}_{\mathbf{CM}}(d)$ for $d \leq 13$ and thereby shows there is no $2 < d < 14$ with $2 \sim d$. The existence of a 2-Olson degree $d > 2$ was shown only recently by Bourdon-Chaos [BC23], who showed that 38 is 2-Olson.[3] The work of Bourdon-Chaos does much more than this: [BC23, Thm. 1.2] computes $\mathcal{G}_{\mathbf{CM}}(2p)$ for all primes $p \geq 7$ and thus gives a characterization of 2-Olson degrees of the form $2p$. We will be making use of the precise result, so let us record it here:

Theorem 1.3. *(Bourdon-Chaos* [BC23, Thm. 1.2]*) Let $p \geq 7$ be a prime number.*

a) *The set $\mathcal{G}_{\mathbf{CM}}(2p)$ consists of the following groups $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$:*
- $\mathbb{Z}/N\mathbb{Z} \mid N \in \{1, 2, 3, 4, 6, 7, 10\}$*, in all cases.*
- $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$*, in all cases.*
- $\mathbb{Z}/49\mathbb{Z}$*, if $p = 7$.*
- $\mathbb{Z}/(2p+1)\mathbb{Z}$*, if $2p+1$ is prime and $\left(\frac{\Delta}{2p+1}\right) = 1$ for some $\Delta \in \{-11, -19, -43, -67, -163\}$.*
- $\mathbb{Z}/2(2p+1)\mathbb{Z}$*, if $2p+1$ is prime and $\left(\frac{\Delta}{2p+1}\right) = 1$ for some $\Delta \in \{-7, -8\}$.*
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2(2p+1)\mathbb{Z}$*, if $2p+1$ is prime and $\left(\frac{-7}{2p+1}\right) = 1$.*
- $\mathbb{Z}/2(4p+1)$*, if $4p+1$ is prime.*
- $\mathbb{Z}/(6p+1)$*, if $6p+1$ is prime.*

b) *We have $[2p]_\sim \neq [2]_\sim$ if and only if at least one of the following occurs:*
- (i) *$2p+1$ is prime, and $\left(\frac{\Delta}{2p+1}\right) = 1$ for some $\Delta \in \{-7, -8, -11, -19, -43, -67, -163\}$.*
- (ii) *$4p+1$ is prime.*
- (iii) *$6p+1$ is prime.*

Theorem 1.3 implies that asymptotically 100% of the degrees of the form $2p$ for a prime number p are 2-Olson [BC23, Remark 1.7], so by the Prime Number Theorem, the number of 2-Olson degrees $d \leq X$ is at least $\frac{X}{2\log X}(1+o(1))$. In her 2024 PhD thesis [Bi24], I. Bildik determined $\mathcal{G}_{\mathbf{CM}}(2pq)$ for primes $2 < p < q$. She finds that $2pq$ is 2-Olson unless there is $a \in \{2, 4, 6\}$ such that at least one of $ap+1$,$aq+1$,$apq+1$ is prime, which she shows is asymptotically 0% of the degrees of the form $2pq$. By Landau's asymptotics for 2-almost primes [La09], it follows that the number of 2-Olson degrees $d \leq X$ is at least $\frac{X \log\log X}{2\log X}(1+o(1))$. These results show that the set of 2-Olson degrees is infinite and not too sparse, though they leave open the question of whether a positive proportion

[3]It turns out that 38 is the smallest $d > 2$ such that $d \sim 2$: cf. Proposition 1.9b).

of positive integers are 2-Olson.

Our first result in this paper is to answer this question in the affirmative:

Theorem 1.4. *Let $\mathcal{D}$ be the set of $d \in \mathbb{Z}^+$ such that:*

(i) $d \equiv 2 \pmod 4$ *and* $3 \nmid d$*; and*

(ii) *For a prime number ℓ, if $\ell - 1 \mid 12d$, then $\ell \in \{2, 3, 5, 7, 13, 19, 37, 73\}$.*

Then:

a) *We have $\mathcal{D} \subseteq [2]_S$: that is, every $d \in \mathcal{D}$ is strongly 2-Olson.*

b) *The set $\mathcal{D}$ has positive lower density.*

Remark 1.5. *The intersection of $\mathcal{D}$ with the set $2\mathcal{P} := \{2p \mid p \text{ is prime}\}$ is*

$$\{2p \mid p \text{ is prime and for all } a \in \{2, 4, 6, 8, 12, 24\},\ ap + 1 \text{ is not prime}\}.$$

Comparing to Theorem 1.3 we see that indeed $\mathcal{D} \cap 2\mathcal{P}$ is a proper subset of $[2]_\sim \cap 2\mathcal{P}$, but both sets have the same asymptotic behavior as does $2\mathcal{P}$, i.e., have $\frac{X}{2 \log X}(1 + o(1))$ elements up to X.

Fix $k \in \mathbb{Z}^+$, and let $2\mathcal{P}_k := \{2p_1 \cdots p_k \mid p_1, \ldots, p_k \text{ are all prime}\}$. Then the intersection of $\mathcal{D}$ with $2\mathcal{P}_k$ contains the set of $2p_1 \cdots p_k \in 2\mathcal{P}_k$ with $2 < p_1 < \ldots < p_k$ such that for every nonempty subset $\mathfrak{s} \subseteq \{1, \ldots, k\}$, for no $a \in \{2, 4, 6, 8, 12, 24\}$ is $a \prod_{i \in \mathfrak{s}} p_i$ prime. When $k = 2$, the same arguments of [Bi24, §3.2] *can also be used to show that $\mathcal{D} \cap 2\mathcal{P}_2$ has the same asymptotic behavior as $2\mathcal{P}_2$. I believe the same should hold for all k, in which case we would have*

$$\#\big(\mathcal{D} \cap 2\mathcal{P}_k \cap [1, X]\big) = \frac{X (\log \log X)^{k-1}}{2(k-1)! \log X}(1 + o(1)),$$

but I have not tried to prove this for $k \geq 3$.

The proof of Theorem 1.4a) is an algebraic argument that relies on recent work of Bourdon-Clark and Clark-Saia [BC20a], [BC20b], [CS] on degrees of CM points on certain elliptic modular curves. In §2 we recall some of this work and use it to show many results of the form: if d, M, N are positive integers such that $M \mid N$ and there is a CM elliptic curve defined over a degree d number field such that $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow E(F)$, then this forces a certain divisibility on d – often that $3 \mid d$ or $4 \mid d$ – which gives a contradiction for d lying in the set $\mathcal{D}$ appearing in the statement of Theorem 1.4. The proof of Theorem 1.4b) is of an entirely different character, relying (only) on the work of on Erdős-Wagstaff on shifted prime divisors [EW80], as we will recall in §3.

The method of proof of Theorem 1.4 is rather flexible: one may *try* to use it to show that $[d_0]_S$ has positive lower density for any fixed d_0. Each of the following conditions is auspicious for the success of this method: (i) $4 \nmid d_0$; (ii) $3 \nmid d_0$; (iii) we know $\mathcal{G}_{\mathbf{CM}}(d_0)$ explicitly. Thus it is natural to explore the cases in which d_0 is odd and $d_0 = 2p$ for a prime $p > 3$.

We will show that $[d_0]_S$ has positive lower density for all odd d_0 (Theorem 5.2). When d_0 is *minimal* – there is no $d < d_1$ with $d \sim d_1$ – this follows from the work of Bourdon-Pollack [BP17], while in the general case we deduce it from one of their results using work of Pomerance-Wagstaff [PW23].

Let $p > 2$ be prime. In view of Theorem 1.3, we treat separately the case in which $2p + 1$ is prime and the case in which it is not, the latter being the case of relative density one. We will show: for all $p > 2$ for which $2p+1$ is *not* prime, the set $[2p]_S$ has positive lower density (Corollary 5.4). In fact we prove a stronger result (Theorem 5.3) implying that Conjecture 1.2a) holds for a

set of even integers of positive density. This and Theorem 5.2 imply that the lower density of the set of integers for which Conjecture 1.2a) holds exceeds $\frac{1}{2}$.

When $2p+1$ s prime, things are more complicated: now the set $\mathcal{G}_{\mathbf{CM}}(2p)$ varies depending on the set of class number one imaginary quadratic fields in which $2p+1$ splits. If enough of these splitting conditions hold, we can still prove that $[2p]_S$ has positive lower density (Theorem 5.6). In the absence of such splitting conditions, our method fails. But in fact, for some of these values of p the failure of the method uncovers a phenomenon that casts serious doubt on the truth of Conjecture 1.2 for $d_0 = 2p$. To be precise, Propositions 5.8 and 5.9 imply:

Theorem 1.6.

a) *Suppose that every sufficiently large odd positive integer D is the class number of an imaginary quadratic field $\mathbb{Q}(\sqrt{-\ell})$ for a prime $\ell \equiv 23 \pmod 4$. Then $[6]_\sim$ is finite.*

b) *Let $p > 3$ be a prime such that $p \equiv 1, 2, 6 \pmod 7$ and $2p+1$ is prime. Suppose that every sufficiently large odd positive integer D is the class number of an imaginary quadratic field $\mathbb{Q}(\sqrt{-\ell})$ for a prime $\ell \equiv 7 \pmod 8$ such that $2p+1$ splits in $\mathbb{Q}(\sqrt{-\ell})$. Then $[2p]_S$ is finite.*

It is a standard conjecture – very much out of current reach – that every positive integer is the class number of some imaginary quadratic field. More precisely, for $h \in \mathbb{Z}^+$ let $\mathcal{F}(h)$ denote the set of discriminants of imaginary quadratic fields of class number h. Then K. Soundararajan has made the more precise conjecture [So07, p. 14, (C1)]

$$\frac{h}{\log h} \ll \#\mathcal{F}(h) \ll h \log h.$$

Since for odd $h > 1$, imaginary quadratic fields of class number h must have discriminant $-p$ or $-4p$ for a prime $p \equiv 3 \pmod 4$, if Soundararajan's conjecture holds, then the failure of the hypotheses in Theorem 1.6 would imply a dramatic lack of equidistribution of elements of $\mathcal{F}(h)$ into congruence classes modulo 24 or modulo $4(2p+1)$. Moreover the hypothesis of part a) is supported by some computations that we will mention soon.

One way of trying to repair Conjecture 1.2a) was suggested to me by P. Pollack: namely, we may conjecture that for all $d_0 \in \mathbb{Z}^+$, the set $[d_0]_S$ is either finite or of positive lower density. Although likely to be true, it seems to me that there ought to be a more "optimistic" reformulation. Let me now prove a small piece of optimism. We will need the following result [BCP17, Thm. 1.1(i)] that also made use of the work of Erdős-Wagstaff on shifted prime divisors.

Theorem 1.7 (Bourdon-Clark-Pollack)**.** *For all $\epsilon > 0$, there is $B_\epsilon \in \mathbb{Z}^+$ with the following property: the set of all $d \in \mathbb{Z}^+$ such that that there is a degree d number field F and a CM elliptic curve $E_{/F}$ with $\#E(F)[\mathrm{tors}] > B_\epsilon$ has upper density less ϵ.*

This has the following consequence:

Corollary 1.8. *Let $d_0 \in \mathbb{Z}^+$. Then there is $d_1 \in \mathbb{Z}^+$ such that $d_0 \mid d_1$ and the set $[d_1]_\sim$ of d_1-Olson degrees has positive upper density.*

Proof. Applying Theorem 1.7 with $\epsilon = \frac{1}{2d_0}$, we get that the set of S of degrees $d \in d_0\mathbb{Z}^+$ such that every torsion subgroup of a CM elliptic curve defined over a number field of degree d has size at most B_ϵ has lower density at least $\frac{1}{2d_0}$, hence also upper density at least $\frac{1}{2d_0}$. Therefore as d ranges over elements of S, only finitely many diferent sets $\mathcal{G}_{\mathbf{CM}}(d)$ can arise; because the limsup of a finite sum is at most the sum of the limsups, at least one $\mathcal{G}_{\mathbf{CM}}(d)$ must have positive upper density. □

For instance, Corollary 1.8 does not imply that a positive proportion of degrees are 4-Olson – it is not currently known whether any $d > 4$ is 4-Olson – but it does imply that there is some d_0 divisible by 4 such that the d_0-Olson degrees have positive upper density. I wonder whether Corollary 1.8 holds with "lower density" in place of "positive density." If so, this would be one optimistic salvaging of Conjecture 1.2a). The method we introduce here would allow us to prove this for $d_0 = 6$ with an explicit value of d_1. Alas, we have to stop somewhere, so we leave this to a future work.

In §6 we prove some further computational results. If $d_0 \in \mathbb{Z}^+$ is minimal in its $\sim$-equivalence class, it is natural to ask whether every element of $[d_0]_\sim$ must be a multiple of d_0. We prove that this is true for several small values of d_0 and for all odd d_0. We also establish the following result.

Proposition 1.9.

a) *We have*

$$\overline{\delta}([2]_\sim) \leq 0.036891,\ \overline{\delta}([10]_\sim) \leq 0.009227,\ \overline{\delta}([14]_\sim) \leq 0.006149,\ \overline{\delta}([22]_\sim) \leq 0.0036891.$$

b) *The set of* 2*-Olson degrees* $d \leq 1000$ *is*

$$\{2, 38, 62, 118, 142, 218, 298, 314, 334, 394, 422, 466, 454, 458, 538, 634, 674, 698\}$$
$$\cup \{706, 722, 758, 766, 778, 802, 842, 878, 898, 914, 926, 958\}.$$

c) *The set of* 10*-Olson degrees* $d \leq 2000$ *is* $\{2, 1490, 1970\}$.

d) *The set of* 14*-Olson degrees* $d \leq 2000$ *is* $\{14, 266, 994, 1526\}$.

e) *The set of* 22*-Olson degrees* $d \leq 2000$ *is* $\{22, 1298, 1562\}$.

f) *The set of* 6*-Olson degrees* $d < 45762$ *is* $\{6\}$.

2. Preliminaries

Given an elliptic curve E defined over a number field F and an embedding $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow E(F)$ with $M \mid N$ and $N \geq 3$, there is an induced closed point P_1 on the modular curve $X_1(M, N)$. We have maps of modular curves

$$X_1(M, N) \stackrel{\pi}{\to} X_0(M, N) \stackrel{J}{\to} X(1) \cong \mathbb{P}^1$$

cf. [CS, §0.1], and we put $P_0 \coloneqq \pi(P_1) \in X_0(M, N)$ and $P = J(P_0) \in X(1)$. The field $\mathbb{Q}(P)$ is (by definition) $\mathbb{Q}(j(E))$. If E has CM by the order of discriminant $\Delta = \mathfrak{f}^2\Delta_K$ and conductor $\mathfrak{f}$ in the imaginary quadratic field K, then we denote the field $\mathbb{Q}(j(E))$ by $\mathbb{Q}(\mathfrak{f})$ and call it the rational ring class field of conductor $\mathfrak{f}$. Up to isomorphism, $\mathbb{Q}(\mathfrak{f})$ depends only on Δ and thus only on K and $\mathfrak{f}$ [CS, §1.2]. We denote by $K(\mathfrak{f})$ the field $K(j(E))$; this is the ring class field of conductor $\mathfrak{f}$. We have

$$[\mathbb{Q}(\mathfrak{f}) : \mathbb{Q}] = h_\Delta,$$

the class number of the order Δ. Thus we have that d is divisible by

$$[\mathbb{Q}(P_1) : \mathbb{Q}] = [\mathbb{Q}(P_1) : \mathbb{Q}(P_0)][\mathbb{Q}(P_0) : \mathbb{Q}(\mathfrak{f})]h_\Delta,$$

which gives us three sources for divisibility. In this work we will only make use of the parity of h_Δ, which comes from Gauss's genus theory: h_Δ is odd if and only if $\Delta \in \{-4, -8, -12, -16\}$ or $\Delta = -2^\epsilon \ell^{2L+1}$ where $\epsilon \in \{0, 2\}$, $\ell \equiv 3 \pmod 4$ is a prime, and $L \in \mathbb{Z}^+$ [CS, §1.10.1].

The work [CS] determines the possible values for $[\mathbb{Q}(P_1) : \mathbb{Q}(P_0)]$ and $[\mathbb{Q}(P_0) : \mathbb{Q}(\mathfrak{f})]$ in every case. For brevity, we call $[\mathbb{Q}(P_1) : \mathbb{Q}(P_0)]$ the **first factor** of d. The first factor divides $\frac{\varphi(N)}{2}$ and is always divisible by $\frac{\varphi(N)}{w_\Delta}$, where w_Δ is the cardinality of the unit group of the order $\mathcal{O}$ of discriminant Δ. Thus the first factor is $\frac{\varphi(N)}{2}$ whenever $\Delta \notin \{-3, -4\}$; it is also $\frac{\varphi(N)}{2}$ whenever

$M \geq 2$. When $M = 1$ and $\Delta = -3$, the first factor is $\frac{\varphi(N)}{2}$ unless N is of **Type I**: that is, divisible neither by 9 nor by any prime $p \equiv 2 \pmod 3$. (In the remaining case – namely $\Delta = -3$, $M = 1$ and N of Type I – the elliptic curve $E_{/F}$ can be chosen so that the first factor is $\frac{\varphi(N)}{6}$.) When $M = 1$ and $\Delta = -4$, the first factor is $\frac{\varphi(N)}{2}$ unless N is of **Type II**: that is, divisible neither by 4 nor by any prime $p \equiv 3 \pmod 4$. (In the remaining case – namely $\Delta = -4$, $M = 1$ and N of Type II – the elliptic curve $E_{/F}$ can be chosen so that the first factor is $\frac{\varphi(N)}{4}$.)

The following result shows that in most cases the **complementary factor** $[\mathbb{Q}(P_0) : \mathbb{Q}]$ is even:

Theorem 2.1. *Let $P_0 \in X_0(M, N)$ be a closed CM point of odd degree. If $M \geq 2$, then $(M, N) = (2, 2)$. If $M = 1$, then $N \in \{1, 2, 4\}$ or $N \in \{\ell^a, 2\ell^a\}$ for a prime $\ell \equiv 3 \pmod 4$ and $a \in \mathbb{Z}^+$.*

Proof. See [CS, (1.12)]. □

Proposition 2.2. *Let $d \in \mathbb{Z}^+$ and let $\ell > 2$ be a prime number such that $\mathbb{Z}/\ell\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(d)$.*

a) *If $\ell \equiv 1 \pmod 9$, then $3 \mid d$.*
b) *If $\ell \equiv 1 \pmod 3$, then $3 \mid d$ or $\Delta = -3$.*
c) *If $\ell \equiv 1 \pmod 8$, then $4 \mid d$.*
d) *If $\ell \equiv 1 \pmod 4$, then $4 \mid d$ or $\Delta = -4$.*
e) *If $\ell \equiv 1 \pmod{12}$, then $3 \mid d$ or $4 \mid d$.*

Proof. a) If $\ell \equiv 1 \pmod 9$, then the first factor of d is $\frac{\ell-1}{m}$ for $m \in \{2, 4, 6\}$, hence is divisible by 3.
b) If $\ell \equiv 1 \pmod 3$ and $\Delta \neq -3$, then the first factor of d is divisible by $\frac{\ell-1}{m}$ for $m \in \{2, 4\}$, hence is divisible by 3.
c),d) If $\ell \equiv 1 \pmod 8$, then the first factor of d is divisible by $\frac{\ell-1}{m}$ for $m \in \{2, 4, 6\}$, hence is even. Similarly, if $\ell \equiv 1 \pmod 4$ and $\Delta \neq -4$, then the first factor of d is divisible by $\frac{\ell-1}{m}$ for $m \in \{2, 6\}$, hence is even. By Theorem 2.1, the complementary factor is also even. So $4 \mid d$.
e) This is immediate from parts b) and d). □

We have $\mathbb{Z}/7\mathbb{Z}, \mathbb{Z}/10\mathbb{Z} \in \mathcal{G}_{\mathbf{CM}}(2)$ [CCRS14, §4.2], so the hypotheses on Δ in parts b) and d) of Proposition 2.2 are necessary.

Corollary 2.3. *Let F be a number field of degree d, let $\ell \equiv 1 \pmod 4$ be a prime, and let $E_{/F}$ be a CM elliptic curve. If $\mathbb{Z}/\ell\mathbb{Z} \hookrightarrow E(F)[\mathrm{tors}]$ and $\#E(F)[\mathrm{tors}]$ is odd, then $4 \mid d$.*

Proof. Suppose that F is a number field of degree d with $4 \nmid d$ and that $E_{/F}$ is a Δ-CM elliptic curve such that $\mathbb{Z}/\ell\mathbb{Z} \hookrightarrow E(F)$. By Proposition 2.2d), we have $\Delta = -4$. But for any -4-CM elliptic curve $E_{/F}$ we have $\mathbb{Z}/2\mathbb{Z} \hookrightarrow E(F)$, so $\#E(F)[\mathrm{tors}]$ cannot be odd. □

Theorem 2.4.

a) *Let $N \in \mathbb{Z}^{\geq 5}$ and $d \in \mathbb{Z}^+$ be such that $\mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(d)$. Then:*
   (i) *Either $\frac{\varphi(N)}{2} \mid d$ or $\frac{\varphi(N)}{3} \mid d$.*
   (ii) *If N is* not *of Type I, then $\frac{\varphi(N)}{2} \mid d$.*
   (iii) *If N is neither of Type I nor of Type II and is not of the form ℓ^a or $2\ell^a$ for a prime $\ell \equiv 3 \pmod 4$ and $a \in \mathbb{Z}^+$, then $\varphi(N) \mid d$.*
   (iv) *If N is of Type I and* not *of Type II and is not of the form ℓ^a or $2\ell^a$ for a prime $\ell \equiv 3 \pmod 4$ and $a \in \mathbb{Z}^+$, then $\frac{\varphi(N)}{3} \mid d$.*
   b) Let $\ell > 2$ be a prime such that $\mathbb{Z}/2\ell\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(d)$. Then $\frac{\ell-1}{2} \mid d$.

Proof. a) (i), (ii) We may work throughout with Δ-CM elliptic curves with $\Delta \in \{-3, -4\}$, since for all other Δ's the first factor of d is $\frac{\varphi(N)}{2}$.

First suppose that N is *not* of Type I. If N is also not of Type II, then the first factor of d is $\frac{\varphi(N)}{2}$ and we're done, so suppose that N is of Type II, in which case the first factor of d is divisible by $\frac{\varphi(N)}{4}$. Since $N > 2$ is of Type II, there is a prime $\ell \equiv 1 \pmod 4$ such that $\ell \mid N$, and then Theorem 2.1 implies that the complementary factor is also even, so $\frac{\varphi(N)}{2} \mid d$.

Next suppose that N is of Type II. Then as above the complementary factor is even, so overall d is divisible by $\frac{\varphi(N)}{2}$ or $\frac{\varphi(N)}{3}$, as desired.

Thus we may assume that N is of Type I and not of Type II. If $\Delta = -4$ then since N is not of Type II the first factor of d is $\frac{\varphi(N)}{2}$, so we may assume that $\Delta = -3$. Since N is of Type I it is divisible by a prime $\ell \equiv 1 \pmod 3$. By Theorem 2.1, the complementary factor of d is even unless $N = \ell^a$ or $2\ell^a$ for some $a \in \mathbb{Z}^+$, so we may assume that N is of this form. Since $\varphi(2\ell^a) = \varphi(\ell^a)$, we may assume that $N = \ell^a$. In this case, by [CS, §1.8.1, Case 1.2 and §2.7.1], the unique primitive degree of a -3-CM point on $X_1(\ell^a)$ is $\frac{\varphi(\ell^a)}{3}$, completing the proof.

(iii) The first factor of d is $\frac{\varphi(N)}{2}$ and by Theorem 2.1 the complementary factor is even.

(iv) the first factor of d is divisible by $\frac{\varphi(N)}{6}$ and by Theorem 2.1 the complementary factor is even.

b) We may apply a)(ii) with $N = 2\ell$. □

Proposition 2.5. *Let $d, N \in \mathbb{Z}^+$, and suppose that $\mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(d)$.*

a) *If $4 \mid N$ and $N > 4$, then $4 \mid \varphi(N) \mid d$.*
b) *If $2^a \mid N$ for some $a \geq 3$, then $2^{a-1} \mid d$.*
c) *If $\ell^a \mid N$ for some prime $\ell > 2$ and some $a \geq 2$, then $\ell^{a-1} \mid d$.*

Proof. a) Theorem 2.4a)(iii) gives $\varphi(N) \mid d$. By hypothesis N is either divisible by 8 or by 4ℓ for some prime $\ell > 2$; either way we find $4 \mid \varphi(N)$.

b) This is immediate from part a).

c) If $\ell = 3$, then N is not of Type I, so the first factor of d is $\frac{\varphi(N)}{m}$ for $m \in \{2, 4\}$, which is divisible by ℓ^{a-1}. If $\ell > 3$, then the first factor of d is $\frac{\varphi(N)}{m}$ for $m \in \{2, 4, 6\}$, which is divisible by ℓ^{a-1}. □

For future use, we record some specifics. In the following result, the reader may check that all statements follow immediately from Theorem 2.4 or Proposition 2.5.

Corollary 2.6. *Let $N \in \mathbb{Z}^{\geq 3}$, let F be a number field of degree d, and let $E_{/F}$ be a Δ-CM elliptic curve such that $\mathbb{Z}/N\mathbb{Z} \hookrightarrow E(F)$.*

a) *If $N = 8$, then $e_8 := 4 \mid d$.*
b) *If $N = 9$, then $e_9 := 3 \mid d$.*
c) *If $N = 11$, then $e_{11} := 5 \mid d$.*
d) *If $N = 12$, then $e_{12} := 4 \mid d$.*
e) *If $N = 14$, then $e_{14} := 3 \mid d$.*
f) *If $N = 15$, then $e_{15} := 8 \mid d$.*
g) *If $N = 20$, then $e_{20} := 8 \mid d$.*
h) *If $N = 21$, then $e_{21} := 4 \mid d$.*
i) *If $N = 22$, then $e_{22} := 10 \mid d$.*
j) *If $N = 24$, then $e_{24} := 16 \mid d$.*
k) *If $N = 25$, then $e_{25} := 10 \mid d$.*
l) *If $N = 26$, then $e_{26} := 6 \mid d$.*

m) *If* $N = 27$, *then* $e_{27} \coloneqq 9 \mid d$.
n) *If* $N = 28$, *then* $e_{28} \coloneqq 12 \mid d$.
o) *If* $N = 33$, *then* $e_{33} \coloneqq 20 \mid d$.
p) *If* $N = 35$, *then* $e_{35} \coloneqq 24 \mid d$.
q) *If* $N = 58$, *then* $e_{58} \coloneqq 14 \mid d$.
r) *If* $N = 74$, *then* $e_{74} \coloneqq 18 \mid d$.

Remark 2.7. *Theorem 2.6 is best possible in the sense that for all* 18 *values of* N *treated there, the number* e_d *is the greatest common divisor of all degrees of number fields* F *such that there is a CM elliptic curve* $E_{/F}$ *with* $\mathbb{Z}/N\mathbb{Z} \hookrightarrow E(F)$. *Indeed:*

a) *For* $N \in \{8, 9, 11, 12, 14, 15, 20, 21, 25, 26, 27, 28, 35, 58, 74\}$, *the number* e_d *is the least degree of a CM point on* $X_1(N)$, *as follows from* [Sgit].
b) *The data of* [Sgit] *also shows that the least degree of a CM point on* $X_1(49)$ *is* 14. *However, by* [BP17, Thm. 1.2], *there is a CM point on* $X_1(49)$ *of degree* $147 = 3 \cdot 7^2$. *Thus in this case there is more than one primitive degree of CM points on* $X_1(N)$, *but the gcd of all such primitive degrees is* $e_{49} \coloneqq 7$.

Proposition 2.8. *Let* $M \in \mathbb{Z}^{\geq 3}$. *Let* F *be a number field of degree* d, *and let* $E_{/F}$ *be an elliptic curve such that* $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/MZ \hookrightarrow E(F)$. *Then* $\varphi(M) \mid [F : \mathbb{Q}]$.

Proof. The hypotheses imply that each geometric M-torsion point on E is F-rational. By the Galois equivariance of the Weil e_M pairing, this implies that F contains a primitive Mth root of unity ζ_M, so $\varphi(M) = [\mathbb{Q}(\zeta_M) : \mathbb{Q}] \mid d$. □

Proposition 2.9. *Let* F *be a number field of degree* d, *and let* $E_{/F}$ *be a* Δ*-CM elliptic curve.*

a) *If* $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \hookrightarrow E(F)$, *then* $4 \mid d$.
b) *Suppose* $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \hookrightarrow E(F)$.
   (i) *If* $3 \nmid \Delta$, *then* $4 \mid d$.
   (ii) *If* $\Delta < -3$ *and* $3 \mid \Delta$, *then* $6 \mid d$.
c) *If* $\Delta = -3$ *and* $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \hookrightarrow E(F)$, *then* $6 \mid d$.

Proof. Suppose that $E_{/F}$ has complex multiplication by the imaginary quadratic order $\mathcal{O} = \mathcal{O}_\Delta$ of discriminant $\Delta = \mathfrak{f}^2\Delta_K$ in the imaginary quadratic field K. Let w_Δ be the number of roots of unity in $\mathcal{O}$. Suppose that for some $M \geq 3$ we have $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/M\mathbb{Z} \hookrightarrow E(F)$. By CITE, F contains the ring class field $K(\mathfrak{f})$ of $\mathcal{O}$. Let

$$C_M \coloneqq (\mathcal{O}/M\mathcal{O})^\times$$

be the modulo M Cartan subgroup. By [BC20a, Cor. 1.5 and Lemma 2.2b)], we have

$$M^2 \prod_{p \mid M} \left(1 - \left(\frac{\Delta}{p}\right)\frac{1}{p}\right)\left(1 - \frac{1}{p}\right) = \#C_M(\mathcal{O}) \mid w_\Delta[F : K(\mathfrak{f})]. \tag{3}$$

a) Suppose $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \hookrightarrow E(F)$. Because $F \supseteq K(\mathfrak{f})$ and $[K(\mathfrak{f}) : \mathbb{Q}]$ is even, it suffices to show that $[F : K(\mathfrak{f})]$ is even.
• If $\Delta \neq -4$, then $4 \mid \#C_4(\mathcal{O})$, so (3) gives $4 \mid 6[F : K(\mathfrak{f})]$, so $2 \mid [F : K(\mathfrak{f})]$.
• If $\Delta = -4$, then $\#C_4(\mathcal{O}) = 8$, so (3 gives $8 \mid 4[F : K(\mathfrak{f})]$, so $2 \mid [F : K(\mathfrak{f})]$. b) Suppose $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3Z \hookrightarrow E(F)$.
(i) Suppose that $3 \nmid \Delta$. First suppose that $\Delta \neq -4$. Then (3) gives: $4 \mid \#C_4(\mathcal{O}) \mid 2[F : K(\mathfrak{f})]$, so $[F : K(\mathfrak{f})]$ is even. Now suppose that $\Delta = -4$: then $\#C_3(\mathcal{O}) = 8$, so (3) gives: $8 \mid 4[F : K(\mathfrak{f})]$, so again $[F : K(\mathfrak{f})]$ is even.

(ii) If $3 \mid \Delta$ and $\Delta \neq -3$, then $3 \mid \#C_3(\mathcal{O}) \mid 4[F : K(\mathfrak{f})]$, so $3 \mid d$.
Before moving on, we remark that $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \in \mathcal{G}_{\mathbf{CM}}(2)$. It follows from our proof so far that $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \hookrightarrow E(F)$ for a Δ-CM elliptic curve defined over a quadratic field F, then $\Delta = -3$, as was already established in [BCS17, Thm. 1.4].[4]
c) If $E_{/F}$ is a -3-CM elliptic curve and $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \hookrightarrow E(F)$, then [BC20b, Thm. 4.1] implies that $3 \mid [F : \mathbb{Q}(\sqrt{-3}]$, so $6 \mid d$. □

Proposition 2.10. *Let $\ell \equiv 1 \pmod 4$, let F be a number field of degree d, and let $E_{/F}$ be a CM elliptic curve such that $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\ell\mathbb{Z} \hookrightarrow E(F)$. Then $4 \mid d$.*

Proof. Because $M > 1$ and $\ell \equiv 1 \pmod 4$, the first factor of d is $\frac{\varphi(2\ell)}{2} = \frac{\ell-1}{2}$ is even, and by Theorem 2.1, the complementary factor is also even, so $4 \mid d$. □

Theorem 2.11. *Let $N, d \in \mathbb{Z}^+$ with $N \geq 3$. Suppose there is a degree d number field F and a Δ-CM elliptic curve $E_{/F}$ such that $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow E(F)$.*

a) *If N is divisible by a prime $\ell \equiv 1 \pmod 4$, then $4 \mid d$.*
b) *If N is divisible by a prime $\ell \equiv 3 \pmod 4$ with $\ell > 3$, then either $4 \mid d$ or $2\ell \mid d$.*
c) *If N is divisible by a prime power $\ell^a \geq 3$, then $\ell^{2a-2}(\ell - 1) \mid d$.*

Proof. In all cases we are assuming that there is a prime ℓ such that $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z} \hookrightarrow E(F)$, so Proposition 2.8 implies $\ell - 1 = \varphi(\ell) \mid d$. When $\ell \equiv 1 \pmod 4$ this means $4 \mid d$, proving part a).

Write $\Delta = \mathfrak{f}^2 \Delta_K$. For the next parts, we will use a result of Bourdon-Clark [BC20a, Thm. 1.4]: because $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \times \hookrightarrow E(F)$, we have that

$$\frac{2h_\Delta}{w_\Delta} N^2 \prod_{p \mid N} \left(1 - \left(\frac{\Delta}{p}\right)\frac{1}{p}\right)\left(1 - \frac{1}{p}\right) \mid d. \tag{4}$$

b) Let $K = \mathbb{Q}(\sqrt{\Delta})$ be the CM field. By [BCS17, Lemma 3.15], since $\ell > 2$ we have $K \subseteq F$, while by Proposition 2.8 we have $\mathbb{Q}(\zeta_\ell) \subseteq F$. The unique quadratic subfield of $\mathbb{Q}(\zeta_\ell)$ is $\mathbb{Q}(\sqrt{-\ell})$, so if $K \neq \mathbb{Q}(\sqrt{-\ell})$, then F contains two different quadratic fields and thus $4 \mid d$. So we may assume that $K = \mathbb{Q}(\sqrt{-\ell})$, in which case (4) shows that $\ell \mid d$ (the hypothesis $\ell > 3$ is used to ensure that $\ell \nmid w_\Delta$). Since $F \supseteq \mathbb{Q}(\sqrt{-\ell})$ we have that d is even and thus $2\ell \mid d$.
c) The left hand side of (4) is a positive integer. If we start with N that is divisble by ℓ and not by ℓ^2 and then replace N by $\ell^{a-1}N$, we see that the left hand side is divisible by ℓ^{2a-2}. Again, Proposition 2.8 implies $\ell - 1 \mid d$, so $\ell^{2a-2} \mid d$. Thus $\ell^{2a-2}(\ell - 1) \mid d$. □

Corollary 2.12. *Let $d \in \mathbb{Z}^+$ be such that neither 3 nor 4 divides d, and let $M, N \in \mathbb{Z}^+$ be such that $2 \leq M \leq N \leq 10$ and $M \mid N$. If $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(d)$, then*

$$(M, N) \in \{(2,2), (2,4), (2,6), (3,3)\}.$$

Proof. Parts a) and b) of Theorem 2.6 rule out $N \in \{8.9\}$. It now suffices to rule out

$$(M, N) \in \{(4,4), (5,5), (3,6), (7,7), (4,8), (3,9), (2,10)\}.$$

The case $(M, N) = (4, 4)$ is ruled out by Proposition 2.9. Because $\varphi(5) = 4$ and $\varphi(7) = 6$, the cases $(M, N) \in \{(5,5), (7,7)\}$ are ruled out by Proposition 2.8. The case $(M, N) = (3, 6)$ is ruled out by Proposition 2.9. The case $(M, N) = (2, 10)$ is ruled out by Proposition 2.10. □

[4]Notice that Proposition 2.8 implies that the CM field must be $\mathbb{Q}(\sqrt{-3})$ but does not give that the order must be the maximal order rather than either of the two nonmaximal orders of class number 1.

3. Proof of Theorem 1.4

3.1. **Proof of Theorem 1.4a.** By [CCRS14, §4.2], we have

$$\mathcal{G}_{\mathbf{CM}}(2) = \begin{cases} \{\mathbb{Z}/N\mathbb{Z} \mid N = 1,2,3,4,6,7,10\} \cup \\ \{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \mid n = 1,2,3\} \cup \\ \{\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}\} \end{cases}.$$

For positive integers d, M, N with $M \mid N$, we write $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(d)$ if there is a degree d number field F and a CM elliptic curve $E_{/F}$ such that $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow E(F)$; if this holds, we say that $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ embeds in $\mathcal{G}_{\mathbf{CM}}(d)$.

We observe that for $M \mid N$, if $\mathbb{Z}/MZ \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(2)$ but $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \notin \mathcal{G}_{\mathbf{CM}}(2)$, then $M = 1$ and $N = 5$. By Corollary 2.3, if for $d \in \mathbb{Z}^+$ we have $\mathbb{Z}/5\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(d)$, then $4 \mid d$. So:

Remark 3.1. *Let $d \in \mathbb{Z}^+$ with $d \equiv 2 \pmod 4$. Then $\mathcal{G}_{\mathbf{CM}}(d) \supsetneq \mathcal{G}_{\mathbf{CM}}(2)$ if and only if any of the following hold:*

a) *There is a group $T \in \mathcal{G}_{\mathbf{CM}}(d)$ with an element of order ℓ for some prime $\ell \geq 11$.*
b) *There is a group $T \in \mathcal{G}_{\mathbf{CM}}(d)$ with an element of order N for some*

$$N \in \{9, 12, 14, 15, 20, 21, 25, 35, 49\}.$$

c) *One of the following groups embeds in $\mathcal{G}_{\mathbf{CM}}(d)$:*

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z},\ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z},\ \mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}.$$

We will prove Theorem 1.4a) by showing that for $d \in \mathcal{D}$, none of the conditions of Remark 3.1 hold.

• Let $d \in \mathcal{D}$, and let ℓ be a prime number such that $\mathbb{Z}/\ell\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(d)$. Thus there is a degree d number field F and a CM elliptic curve $E_{/F}$ such that $\mathbb{Z}/\ell\mathbb{Z} \hookrightarrow E(F)$. This induces a closed CM point P on $X_1(\mathbb{Z}/\ell\mathbb{Z})$ such that $[\mathbb{Q}(P) : \mathbb{Q}] \mid d$. In the terminology of §2, the first factor of d is divisible by $\frac{\varphi(\ell)}{m} = \frac{\ell-1}{m}$ for some $m \in \{2, 4, 6\}$. Thus $\ell - 1 \mid 12d$, so by definition of d we have $\ell \in \{2, 3, 5, 7, 13, 19, 37, 73\}$. Because d is divisible neither by 3 nor by 4, Proposition 2.2 rules out $\ell \in \{13, 19, 37, 73\}$, and it follows that $\ell \leq 7$ as desired.

• Let $d \in \mathbb{Z}^+$, let $N \in \{9, 12, 14, 15, 20, 21, 25, 35, 49\}$ and suppose $\mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(d)$. Theorem 2.6 shows that if $N \neq 49$, then d is divisible either by 3 or 4, so $d \notin \mathcal{D}$. If $\mathbb{Z}/49\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(d)$, then d is divisible by $\frac{\varphi(49)}{m}$ for some $m \in 2, 4, 6$, hence $7 \mid 12d$. But since 29 is prime, by definition of $\mathcal{D}$ we have $29 - 1 = 2^2 \cdot 7 \nmid 12d$, so $7 \nmid d$. This rules out $N = 49$.

The groups in Remark 3.1c) are ruled out by Corollary 2.12.

3.2. **Proof of Theorem 1.4b).** For $d \in \mathbb{Z}^+$, a **shifted prime divisor** of d is a divisor of the form $p - 1$ for a prime number p. Theorem 1.4b) will be a quick consequence of the following striking analytic result [EW80, Thm. 3]:

Theorem 3.2 (Erdős-Wagstaff)**.** *For $d \in 2\mathbb{Z}^+$, let $\mathcal{S}_d$ be the set of all $n \in \mathbb{Z}^+$ such that n has the same shifted prime divisors as d. Then $\mathcal{S}_d$ has positive density.*

Proof of Theorem 1.4b): We start with the set $\mathcal{S}_{72}$ of all positive integers having the same shifted prime divisors as 72. Thus for $n \in \mathcal{S}_{72}$ and a prime ℓ, we have $\ell - 1 \mid n$ if and only if $\ell \in \{2, 3, 5, 7, 13, 19, 37, 73\}$. So every element of $\mathcal{S}_{72}$ is divisible by 72. By Theorem 3.2 the set

$$\mathcal{A} := \frac{1}{36}\mathcal{S}_{72} = \left\{ \frac{n}{36} \;\middle|\; n \in \mathcal{S}_{72} \right\}$$

is a subset of $2\mathbb{Z}^+$ of positive density. For $d \in \mathcal{A}$ and a prime ℓ, if $\ell - 1 \mid 12d$, then $\ell - 1 \mid 36d \in \mathcal{S}_{72}$, so $\ell \in \{2, 3, 5, 7, 13, 19, 37, 73\}$. Because 17 is prime, no element of $\mathcal{S}_{72}$ is divisible by $2^4 = 17 - 1$, so no element of $\mathcal{A}$ is divisible by 4. Because 109 is prime, no element of $\mathcal{S}_{72}$ is divisible by $2^2 \cdot 3^3 = 109 - 1$, hence no element of $\mathcal{S}_{72}$ is divisible by 27, hence no element of $\mathcal{A}$ is divisible by 3. Thus $\mathcal{A} \subseteq \mathcal{D}$, so $\mathcal{D}$ has positive lower density: indeed $\underline{\delta}(\mathcal{D}) \geq 36\delta(\mathcal{S}_{72})$.

4. Positive Lower Density of $[10]_S$, $[14]_S$ and $[22]_S$

4.1. **Statement of the Results.** Here are the main results of this section, which immediately imply that that the sets of strongly 10-Olson, strongly 14-Olson and strongly 22-Olson degrees each have positive lower density.

Theorem 4.1. *Let $\mathcal{D}_5$ be the set of positive integers d satisfying both of the following conditions:*

(i) $d \equiv 2 \pmod 4$, $\gcd(3 \cdot 7 \cdot 11 \cdot 31, d) = 1$, $5 \mid d$ *and* $25 \nmid d$.
(ii) *For a prime ℓ, we have* $\ell - 1 \mid 36d \iff \ell \in \{2, 3, 5, 7, 11, 13, 19, 31, 37, 41, 61, 73, 181\}$.

Then:

a) *We have $\mathcal{D}_5 \subseteq [10]_S$.*
b) *The set $\mathcal{D}_5$ has positive density.*

Theorem 4.2. *Let $\mathcal{D}_7$ be the set of positive integers d satisfying both of the following conditions:*

(i) $d \equiv 2 \pmod 4$, $\gcd(3 \cdot 5 \cdot 29 \cdot 43, d) = 1$, $7 \mid d$ *and* $49 \nmid d$.
(ii) *For a prime ℓ, we have* $\ell - 1 \mid 36d \iff \ell \in \{2, 3, 5, 7, 13, 29, 37, 43, 73, 127\}$.

Then:

a) *We have $\mathcal{D}_7 \subseteq [14]_S$.*
b) *The set $\mathcal{D}_7$ has positive density.*

Theorem 4.3. *Let $\mathcal{D}_{11}$ be the set of positive integers d satisfying both of the following conditions:*

(i) $d \equiv 2 \pmod 4$, $\gcd(3 \cdot 5 \cdot 7 \cdot 23 \cdot 67, d) = 1$ *and* $11 \mid d$.
(ii) *For a prime ℓ, we have* $\ell - 1 \mid 36d \iff \ell \in \{2, 3, 5, 7, 13, 19, 23, 37, 67, 73, 89, 199, 397\}$.

Then:

a) *We have $\mathcal{D}_{11} \subseteq [22]_S$.*
b) *The set $\mathcal{D}_{11}$ has positive density.*

4.2. **Proof of Theorem 4.1a), 4.2a) and 4.3a).** For $M, N, d \in \mathbb{Z}^+$ with $M \mid N$, we write $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(d)$ to mean there is a degree d number field F and a CM elliptic curve $E_{/F}$ such that $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow E(F)$.

The proofs of Theorem 4.1a), Theorem 4.2a) and Theorem 4.3a) have the same structure, so we will run the steps in parallel.

Step 0: • By [CCRS14, §4.10] we have

$$\mathcal{G}_{\mathbf{CM}}(10) = \begin{cases} \{\mathbb{Z}/N\mathbb{Z} \mid N = 1,2,3,4,6,7,10,11,22,31,50\} \cup \\ \{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \mid n = 1,2,3,11\} \cup \\ \{\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}\} \end{cases}.$$

Thus the only groups $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ that embed in $\mathcal{G}_{\mathbf{CM}}(10)$ but are not elements of $\mathcal{G}_{\mathbf{CM}}(10)$ are $\mathbb{Z}/5\mathbb{Z}$ and $\mathbb{Z}/25\mathbb{Z}$. Let $d \in \mathcal{D}_5$. Since $4 \nmid d$, Corollary 2.3 implies that neither $\mathbb{Z}/5\mathbb{Z}$ nor $\mathbb{Z}/25\mathbb{Z}$ is an element of $\mathcal{G}_{\mathbf{CM}}(d)$. So to prove Theorem 4.1a) it suffices to show: for $d \in \mathcal{D}_5$ and $M, N \in \mathbb{Z}^+$ with $M \mid N$, if $\mathbb{Z}/MZ \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(d)$, then $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(10)$.

• By Theorem 1.3, we have

$$\mathcal{G}_{\mathbf{CM}}(14) = \begin{cases} \{\mathbb{Z}/N\mathbb{Z} \mid N = 1,2,3,4,6,7,10,43,49,58\} \cup \\ \{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \mid n = 1,2,3\} \cup \\ \{\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}\} \end{cases}.$$

Thus the only groups $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ that embed in $\mathcal{G}_{\mathbf{CM}}(14)$ but are not elements of $\mathcal{G}_{\mathbf{CM}}(14)$ are $\mathbb{Z}/5\mathbb{Z}$ and $\mathbb{Z}/29\mathbb{Z}$. For the same reasons as the previous paragaph, to prove Theorem 4.2a) it suffices to show: for $d \in \mathcal{D}_7$ and $M, N \in \mathbb{Z}^+$ with $M \mid N$, if $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(d)$, then $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(14)$.

• By Theorem 1.3 we have

$$\mathcal{G}_{\mathbf{CM}}(22) = \begin{cases} \{\mathbb{Z}/N\mathbb{Z} \mid N = 1,2,3,4,6,7,10,23,46,67\} \cup \\ \{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \mid n = 1,2,3,23\} \cup \\ \{\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}\} \end{cases}.$$

Thus the only group $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ that embeds in $\mathcal{G}_{\mathbf{CM}}(22)$ but is not an element of $\mathcal{G}_{\mathbf{CM}}(22)$ is $\mathbb{Z}/5\mathbb{Z}$. For the same reasons as above, to Prove Theorem 4.3a) it suffices to show: for $d \in \mathcal{D}_{11}$ and for $M, N \in \mathbb{Z}^+$ with $M \mid N$, if $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(d)$, then $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(22)$.

Step 1: • Let $d \in \mathcal{D}_5$, and let ℓ be a prime number such that $\mathbb{Z}/\ell\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(d)$. The first factor of d is divisible by $\frac{\varphi(\ell)}{m} = \frac{\ell-1}{m}$ for some $m \in \{2,4,6\}$, so $\ell - 1 \mid 36d$ and thus

$$\ell \in \{2,3,5,7,11,13,19,31,37,41,61,73,181\}$$

by definition of $\mathcal{D}_5$. Because d is divisible by neither 3 nor 4, Proposition 2.2 shows that ℓ is not congruent to 1 modulo 8, 9 or 12, so we find that $\ell \in \{2,3,5,7,11,31\}$ and thus $\mathbb{Z}/\ell\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(10)$.

• Let $d \in \mathcal{D}_7$, and let ℓ be a prime number such that $\mathbb{Z}/\ell\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(d)$. As above we have $\ell - 1 \mid 36d$, so by definition of $\mathcal{D}_7$ we have

$$\ell \in \{2,3,5,7,13,29,37,43,73,127\},$$

and Proposition 2.2 shows $\ell \in \{2,3,5,7,29,43\}$ and thus $\mathbb{Z}/\ell\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(14)$.

• Let $d \in \mathcal{D}_{11}$, and let ℓ be a prime number such that $\mathbb{Z}/\ell\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(d)$. As above we have

$\ell - 1 \mid 36d$, so by definition of $\mathcal{D}_{11}$ we have

$$\ell \in \{2, 3, 5, 7, 13, 19, 23, 37, 67, 73, 89, 199, 397\},$$

and Proposition 2.2 shows $\ell \in \{2, 3, 5, 7, 23, 67\}$ and thus $\mathbb{Z}/\ell\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(22)$.

Step 2: • Let $d \in \mathcal{D}_5$, and let $N \in \mathbb{Z}^+$ be such that $\mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(10)$.
Step 2a): Suppose N is not divisible by 11, 25 or 31.
∘ Suppose $7 \mid N$. If $7^2 \mid N$, then the first factor of d is divisible by $\frac{\varphi(49)}{m} = \frac{42}{m}$ for some $m \in \{2, 4, 6\}$ hence is divisible by 7, contradicting the definition of $\mathcal{D}_5$. By Theorem 2.6, since d is divisible by neither 3 nor 4, N is not divisible by 14, 21 or 35. So $N = 7$ and $\mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(10)$.
∘ Suppose $7 \nmid N$ and $5 \mid N$. Theorem 2.6 implies that N is not divisible by 15 or by 20. So $N \in \{5, 10\}$ and $\mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(10)$.
∘ Suppose $7 \nmid N$, $5 \nmid N$ and $3 \mid N$. Theorem 2.6 implies that N is not divisible by 9 or by 12. So $N \in \{3, 6\}$ and $\mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(10)$.
∘ Suppose $7 \nmid N$, $5 \nmid N$, $3 \nmid N$ and $2 \mid N$. Theorem 2.6 implies that N is not divisible by 8, so $N \in \{2, 4\}$ and $\mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(10)$.
Step 2b): Suppose $11 \mid N$ and write $N = 11a$ for $a \in \mathbb{Z}^+$. If $11 \mid a$ then the first factor of d would be divisible by 11, which is not the case. If $4 \mid a$, then the first factor of d would be divisible by $\frac{\varphi(44)}{2} = 20$. If a is divisible by an odd prime ell, then the first factor of d and the complementary factor of d would both be even, so $4 \mid d$. So $N \in \{11, 22\}$ and $\mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(10)$.
Step 2c): Suppose $25 \mid N$. If $125 \mid N$, then the first factor of d would be divisible by $\frac{\varphi(125)}{4}$ hence by 25, contradicting the definition of $\mathcal{D}_5$. If N is divisible either by 100 or by 25ℓ for a prime $\ell \notin \{2, 5\}$, then the first factor and the complementary factor of d are both even so $4 \mid d$. Thus $N = 25$ or 50 and $\mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(10)$.
Step 2d): Suppose $31 \mid N$. If $31^2 \mid N$, then the first factor of d would be divisible by 31, which is not the case. If N is divisible by 31ℓ for some prime $\ell \notin \{2, 31\}$, then the first factor and the complementary factor of d are both even so $4 \mid d$. Thus $N = 31$ and $\mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(10)$.

• Let $d \in \mathcal{D}_7$, and let $N \in \mathbb{Z}^+$ be such that $\mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(14)$.
Step 2a): Suppose N is not divisible by 29, 43 or 49. Identical arguments to the those made above show that $N \in \{1, 2, 3, 4, 5, 6, 7, 10\}$, so $\mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(14)$.
Step 2b): Suppose $29 \mid N$ and write $N = 29a$. If $29 \mid a$ then $29 \mid d$, which is not the case. If $4 \mid a$ then the first factor of d would be divisible by $\frac{\varphi(4 \cdot 29)}{2} = 28$. If a is divisible by a prime $\ell \notin \{2, 29\}$, then as above $4 \mid d$. Thus $N \in \{29, 58\}$ and $\mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(14)$.
Step 2c): Suppose $43 \mid N$ and write $N = 43a$ for $a \in \mathbb{Z}^+$. If $43 \mid a$ then $43 \mid d$, which is not the case. If $2 \mid a$ then $2 \cdot 43 \mid N$ and the first factor of d is divisible by $\frac{\varphi(2 \cdot 43)}{2} = 21$. If a is divisible by a prime $\ell \notin \{2, 43\}$,then both the first factor of d and the complementary factor are even, so $4 \mid d$. Thus $N = 43$ and $\mathbb{Z}/NZ \hookrightarrow \mathcal{G}_{\mathbf{CM}}(14)$.
Step 2d): Suppose $49 \mid N$ and write $N = 49a$ for $a \in \mathbb{Z}^+$. If $7 \mid a$ then $7^2 \mid d$, which is not the case. If $2 \mid a$ then the first factor of d is divisible by $\frac{\varphi(98)}{2} = 42$. If for a prime $\ell \notin \{2, 7\}$ we have that $7 \mid a$ then as above $4 \mid d$.

• Let $d \in \mathcal{D}_{11}$, and let $N \in \mathbb{Z}^+$ be such that $\mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(22)$.
Step 2a): Suppose N is not divisible by 23 or 67. Identical arguments to those made above show that $N \in \{1, 2, 3, 4, 5, 6, 7, 10\}$, so $\mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(22)$.
Step 2b): Suppose $23 \mid N$ and write $N = 23a$ for $a \in \mathbb{Z}^+$. If $23 \mid a$, then $23 \mid d$, which is not the

case. If $4 \mid a$, then the first factor of d is $\frac{\varphi(4\cdot 23)}{2} = 22$ and the complementary factor is even, so $4 \mid d$. If $\ell \mid a$ for some prime $\ell \notin \{2, 23\}$, then the first factor and the complementary factor of d are both even, so $4 \mid d$. So $N \in \{23, 46\}$ and $\mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(22)$.
Step 3b): Suppose $67 \mid a$ and write $N = 67a$ for $a \in \mathbb{Z}^+$. If $67 \mid a$ then $67 \mid d$ which is not the case. If $2 \mid a$ then the first factor of d is $\frac{\varphi(2\cdot 67)}{2} = 33$. If $\ell \mid a$ for some prime $\ell \notin \{2, 67\}$, then the first factor and the complementary factor of d are both even, so $4 \mid d$. Thus $N = 67$ and $\mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(22)$.

Step 3: • Let $d \in \mathcal{D}_5$, let $M, N \in \mathbb{Z}^+$ with $M \geq 2$ and $M \mid N$, and suppose $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(d)$, so by Step 2 we have $N \in \{1, 2, 3, 4, 6, 7, 10, 11, 22, 31, 50\}$.
• If $N \leq 10$, then Corollary 2.12 shows $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(2) \subseteq \mathcal{G}_{\mathbf{CM}}(10)$.
◦ By Proposition 2.8, if $5 \mid M$ then $4 \mid d$, and if $31 \mid M$ then $3 \mid d$.
◦ Suppose $11 \mid M$, so $\mathbb{Z}/11\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(d)$. Theorem 2.11b) implies that d is divisible by 4 or 11, a contradiction either way.
◦ Now let us address the cases of $N \geq 11$. If $N = 11$ then as just seen, we cannot have $M = 11$. Similarly, if $N = 22$, we cannot have $M = 11$, while we have $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/22\mathbb{Z} \in \mathcal{G}_{\mathbf{CM}}(10)$. If $N = 31$ then we cannot have $M = 31$ as above. If $N = 50$ then as above we cannot have $5 \mid N$, while by Proposition 2.10 we cannot have $2 \mid N$. Thus in all cases we find that $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(d)$ implies $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(10)$, completing the proof of Theorem 4.1a).

• Let $d \in \mathcal{D}_7$, let $M, N \in \mathbb{Z}^+$ with $M \geq 2$ and $M \mid N$, and suppose $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(d)$, so by Step 2 we have $N \in \{1, 2, 3, 4, 5, 6, 7, 10, 29, 43, 49, 58\}$.
◦ The case of $N \leq 10$ is again handled by Corollary 2.12.
◦ If $N \in \{29, 43\}$ then $M = N$ and Proposition 2.8 shows that d is divisible by $\varphi(29) = 28$ or by $\varphi(43) = 42$. If $N = 49$, then $7 \mid M$ so $\mathbb{Z}/7\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(d)$, and Proposition 2.8 shows $\varphi(7) = 6 \mid d$. If $N = 58$ then $29 \mid M$, so $\mathbb{Z}/29\mathbb{Z} \times \mathbb{Z}/29\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(d)$, and Proposition 2.8 shows $\varphi(29) = 28 \mid d$. Thus in all cases we find that $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(d)$ implies $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(14)$, completing the proof of Theorem 4.2a).

• Let $d \in \mathcal{D}_{11}$, let $M, N \in \mathbb{Z}^+$ with $M \geq 2$ and $M \mid N$, and suppose $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(d)$, so by Step 2 we have $N \in \{1, 2, 3, 4, 5, 6, 7, 10, 23, 46, 67\}$.
◦ The case of $N \leq 10$ is again handled by Corollary 2.12.
◦ If $N = 23$ then $M = 23$, and Theorem 2.11b) implies that d is divisible by 4 or by 23, which is not the case. Similarly, if $N = 67$ then $M = 67$ and Theorem 2.11b) implies that d is divisible by 4 or by 67, which is no the case. Thus in all cases we find that $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(d)$ implies $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(22)$, completing the proof of Theorem 4.3a).

4.3. **Proof of Theorems 4.1b), 4.2b) and 4.3b).** For an even positive integer d_0, recall that $\mathcal{S}_{d_0}$ denotes the set of positive integers having the same shifted prime divisors as does d_0: for all primes ℓ, we have $\ell - 1 \mid d_0 \iff \ell - 1 \mid d$ and that by Theorem 3.2, the set $\mathcal{S}_{d_0}$ has positive density.

Let n be a positive integer such that $\gcd(6, n) = 1$, and consider the set $\mathcal{S}_{72n}$. Since 73 is prime and $73 - 1 = 72 \mid 72n$, every $d \in \mathcal{S}_{72n}$ is a multiple of $72 = 2^3 \cdot 3^2$. Thus

$$\mathbb{D}_n := \frac{1}{36}\mathcal{S}_{72n}$$

is a subset of $2\mathbb{Z}^+$ of positive density. We claim: for $n \in \{5, 7, 11\}$, the set $\mathbb{D}_n$ is the set $\mathcal{D}_n$ defined in the statements of Theorems 4.1, 4.2 and 4.3. This will prove Theorems 4.1b), 4.2b) and 4.3b).

For $d \in \mathbb{Z}^+$, condition (ii) of Theorem 4.1 is that $36d$ has the same shifted prime divisors as does $72 \cdot 5$, so this condition means $d \in \mathbb{D}_n$ and thus $\mathcal{D}_n \subseteq \mathbb{D}_n$. Conversely, we will show that every $d \in \mathbb{D}_n$ satisfies the divisibilities and nondivisibilities asserted in condition (i) of Theorem 4.1, so $\mathcal{D}_n = \mathbb{D}_n$. Similarly, condition (ii) of Theorem 4.1 is that $36d$ has the same shifted prime divisors as does $72 \cdot 7$ and condition Theorem 4.3 is that $36d$ has the same shifted prime divisors as does $72 \cdot 11$, and again we will show that the divisibilities and nondivisibilities asserted in condition (i) of Theorem 4.2 (resp. Theorem 4.3) are satisfied by every $d \in \mathcal{D}_7$ (resp. by every $d \in \mathcal{D}_{11}$).

Since 17 is prime and $17 - 1 = 2^4 \nmid 72n$, no element of $\mathcal{D}_n$ is divisible by 4. Since 109 is prime and $109 - 1 = 2^2 \cdot 3^3 \nmid 72n$, no element of $\mathcal{S}_{72}$ is divisible by $2^3 \cdot 3^3$, so no element of $\mathcal{D}_n$ is divisible by 3. If $5 \nmid n$, then since 11 is prime and $11 - 1 = 2 \cdot 5 \nmid 72n$, no element of $\mathcal{D}_n$ is divisible by 5. If $7 \nmid n$, then since 29 is prime and $29 - 1 = 2^2 \cdot 7 \nmid 72n$, no element of $\mathcal{D}_n$ is divisible by 7. If $11 \nmid n$, then since 23 is prime and $23 - 1 = 2 \cdot 11 \nmid 72$, no element of $\mathcal{D}_n$ is divisible by 11. If $23 \nmid n$, then since 139 is prime and $139 - 1 = 2 \cdot 3 \cdot 23 \nmid 72n$, no element of $\mathcal{D}_n$ is divisible by 23. If $5^2 \nmid n$, then since 101 is prime and $101 - 1 = 2^2 \cdot 5^2 \nmid 72n$, no element of $\mathcal{D}_n$ is divisible by 25. If $29 \nmid n$, then since 59 is prime and $59 - 1 = 2 \cdot 29 \nmid 72m$, no element of $\mathcal{D}_n$ is divisible by 29. If $31 \nmid n$, then since 373 is prime and $373 - 1 = 2^2 \cdot 3 \cdot 31 \nmid 72n$, no element of $\mathcal{D}_n$ is divisible by 31. If $43 \nmid n$, then since 173 is prime and $173 - 1 - 2^2 \cdot 43 \nmid 72n$, no element of $\mathcal{D}_n$ is divisible by 43. If $7^2 \nmid n$, then since 197 is prime and $197 - 1 = 2^2 \cdot 7^2 \nmid 72n$, no element of $\mathcal{D}_n$ is divisible by 49. If $67 \nmid d$, then since 269 is prime and $269 - 1 = 2^2 \cdot 67 \nmid 72n$, no element of $\mathcal{D}_n$ is divisible by 67.

5. On $[d_0]_S$ when d_0 is odd or $d_0 = 2p$

Now we turn to proving results of the form that $[d_0]_S$ has positive density for d_0 lying in a certain infinite set of positive integers. For this, there is one aspect of our method that needs to be changed. Previously, for a fixed and rather small $n \in \mathbb{Z}^+$, in order to establish various statements of the form "No element of $\frac{1}{36}\mathcal{S}_{72n}$ is divisible by m," we found some positive integer $c \mid 36$ and a prime number ℓ such that $\ell - 1 \nmid 72n$ and $\ell - 1 = cm$. This worked because since n was rather small, so was m, and small numbers are much more likely to be prime. However, the density of $m \in \mathbb{Z}^+$ such that $cm + 1$ is prime for some $c \mid 36$ is 0. So when working with arbitrarily large values of n we need another ingredient in order to impose nondivisibility conditions on elements of $\frac{1}{36}\mathcal{S}_{72n}$. Fortunately, the result we need appears in recent work of Pomerance-Wagstaff [PW23] that we describe next.

5.1. **A result of Pomerance-Wagstaff.**

Theorem 5.1 (Pomerance-Wagstaff)**.** *Let $n \in \mathbb{Z}^+$ be even, and let $R \in \mathbb{Z}^+$. Let $\mathcal{M}_{n,R}$ be the set of posititve integers d satisfying all of the following conditions:*

(i) *d has the same shifted prime divisors as n.*
(ii) *$n \mid d$.*
(iii) *$\gcd(\frac{d}{n}, R) = 1$.*

Then the set $\mathcal{M}_{n,R}$ has positive density.

Proof. Condition (iii) is equivalent to requiring that $\frac{d}{n}$ not be divisible by any ℓ lying in a fixed finite set $\mathfrak{L}$ of prime numbers. When $\mathfrak{L} = \{\ell\}$, this is [PW23, Lemma 1]. The proof for any finite $\mathfrak{L}$ is identical: instead of applying the main argument of the proof to $\mathcal{A} := \mathcal{A}_n \cup \{\ell\}$, one applies to it $\mathcal{A} := \mathcal{A}_n \cup \mathfrak{L}$. □

5.2. **Positive lower density of $[d_0]_S$ for all odd d_0.**

Theorem 5.2. *Let $d_0 \in \mathbb{Z}^+$ be odd. Then the set $[d_0]_S$ of strongly d_0-Olson degrees has positive lower density.*

Proof. Let

$$R \coloneqq \prod_{\text{primes } \ell \text{ such that } \ell-1 \mid 2d_0} \ell(\ell-1)h_{-\ell}.$$

Let $n \in \mathcal{M}_{2d_0,R}$. Then $n \equiv 2 \pmod 4$, so every element $d \in \frac{1}{2}\mathcal{M}_{2d_0,R}$ is of the form $d = ed_0$ with $\gcd(e, R) = 1$. Let $\ell \equiv 3 \pmod 4$ be a prime such that $h_{-\ell}\frac{\ell-1}{2} \mid d = ed_0$. Then $\ell - 1$ is a shifted prime divisor of $2d$ hence also a shifted prime divisor of $2d_0$, so $\gcd(h_{-\ell}\frac{\ell-1}{2}, e) = 1$ and thus $h_{-\ell}\frac{\ell-1}{2} \mid d_0$. Moreover, for such a prime ℓ we have $\mathrm{ord}_\ell(d_0) = \mathrm{ord}_\ell(d)$. It follows from [BP17, Thm. 1.2] that for any odd $d \in \mathbb{Z}^+$, the set $\mathcal{G}_{\mathbf{CM}}(d)$ depends only on the set of primes $\ell \equiv 3 \pmod 4$ such that $h_{-\ell}\frac{\ell-1}{2} \mid d$ and the ℓ-adic valuations $\mathrm{ord}_\ell(d)$ of these primes, and thus:

$$\mathcal{G}_{\mathbf{CM}}(d_0) = \mathcal{G}_{\mathbf{CM}}(d).$$

That is, every $d \in \frac{1}{2}\mathcal{M}_{2d_0,R}$ is strongly d_0-Olson. By Theorem 5.1, this set of strongly d_0-Olson degrees has positive density, so the set of all strongly d_0-Olson degrees has positive lower density. □

5.3. **Positive lower density of $[2p]_S$ when $2p+1$ is not prime.** Let p be a prime number such that $2p + 1$ is *not* prime (as is the case for asymptotically 100% of primes). In this section we will prove that the set $[2p]_S$ of strongly $2p$-Olson degrees has positive lower density. The least p for which $2p + 1$ is not prime is $p = 7$, is handled by Theorem 4.2, so we may assume that $p > 7$.

Theorem 5.3. *Let $p > 7$ be a prime number such that $2p + 1$ is* not *prime. Let $d_0 \in \mathbb{Z}^+$ be such that $2p \mid d_0$ and $36d_0$ has the same shifted prime divisors as does $72p$. If $4p + 1$ is prime (resp. if $6p + 1$ is prime), we assume that $4p + 1 \nmid d_0$ (resp. that $6p + 1 \nmid d_0$). Then the set $[d_0]_S$ of strongly d_0-Olson degrees has positive lower density.*

Proof. By Theorem 1.3, we have

$$\mathcal{G}_{\mathbf{CM}}(d_0) = \begin{cases} \{\mathbb{Z}/N\mathbb{Z} \mid N = 1, 2, 3, 4, 6, 7, 10\} \cup \\ \{\mathbb{Z}/2(4p + 1)\mathbb{Z}\} \text{ if } 4p + 1 \text{ is prime} \cup \\ \{\mathbb{Z}/(6p + 1)\mathbb{Z}\} \text{ if } 6p + 1 \text{ is prime} \cup \\ \{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \mid n = 1, 2, 3\} \cup \\ \{\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}\} \end{cases}.$$

In other words $\mathcal{G}_{\mathbf{CM}}(d_0) \backslash \mathcal{G}_{\mathbf{CM}}(2)$ is contained in $\{\mathbb{Z}/2(4p+1)\mathbb{Z}, \mathbb{Z}/(6p+1)\mathbb{Z}\}$; the group $\mathbb{Z}/2(4p+1)\mathbb{Z}$ actually occurs if and only if $4p + 1$ is prime and the group $\mathbb{Z}/(6p + 1)\mathbb{Z}$ actually occurs if and only if $6p + 1$ is prime. Since 73 is prime and $73 - 1 = 2^3 \cdot 3^2 \mid 72p$, also $72 \mid 36d_0$, so d_0 is even. Since 17 is prime and $17 - 1 = 2^4 \nmid 72p$, also $2^4 \nmid 36d_0$, so $d_0 \equiv 2 \pmod 4$. Because 109 is prime and $109 - 1 = 2^2 \cdot 3^3 \nmid 72p$, $3 \nmid d_0$. Since 31 is prime and $31 - 1 = 2 \cdot 3 \cdot 5 \nmid 72p$, we have $5 \nmid d_0$. Because 29 is prime and $29 - 1 = 2^2 \cdot 7$, we have $7 \nmid d_0$.

With notation as in Theorem 5.1, we consider the set

$$\mathcal{M} \coloneqq \mathcal{M}_{36d_0,(4p+1)\cdot(6p+1)}$$

of multiples of $36d$ of $36d_0$ such that $\gcd((4p + 1)(6p + 1), \frac{d}{d_0}) = 1$ and $36d$ has the same shifted prime divisors as does $36d_0$. Thus each $36d \in \mathcal{M}$ has the same shifted prime divisors as does $72p$,

so $d \equiv 2 \pmod 4$ and $\gcd(3 \cdot 5 \cdot 7, d) = 1$. We put

$$\mathcal{D} := \frac{1}{36}\mathcal{M},$$

so by Theorem 5.1 the set $\mathcal{D}$ has positive density. We claim that for all $d \in \mathcal{D}$ we have $\mathcal{G}_{\mathbf{CM}}(d) = \mathcal{G}_{\mathbf{CM}}(2p)$, which will complete the proof.
Step 0: Let $d \in \mathcal{D}$, so $2p \mid d_0 \mid d$. Since $d \equiv 2 \pmod 4$, Corollary 2.3 now implies that neither $\mathbb{Z}/5\mathbb{Z}$ nor $\mathbb{Z}/(4p+1)\mathbb{Z}$ is an element of $\mathcal{G}_{\mathbf{CM}}(d)$. So, as usual, it suffices to show that for $d \in \mathcal{D}$ and positive integers $M \mid N$, if $\mathbb{Z}/MZ \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(d)$, then $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \in \mathcal{G}_{\mathbf{CM}}(2p)$.
Step 1: Let $\ell > 7$ be a prime number such that $\mathbb{Z}/\ell\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(d)$. Then $\ell - 1 \mid 36d$, so $\ell - 1 \mid 72p$ and thus – using here that $2p+1$ is not prime – we get $\ell \in \mathcal{P}_p$, where:

$$\mathcal{P}_p := \{13, 37, 73, 4p+1, 6p+1, 8p+1, 12p+1, 18p+1, 24p+1, 36p+1, 72p+1\}. \tag{5}$$

Proposition 2.2 now implies that $\ell \in \{4p+1, 6p+1\}$.

Step 2: Let $d \in \mathcal{D}$ and let $N \in \mathbb{Z}^+$ be such that $\mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(d)$.
Step 2a): Suppose N is not divisible by any prime $\ell > 7$. As we've now seen several times, since $\gcd(3 \cdot 5 \cdot 7, d) = 1$, it follows that $N \in \{1, 2, 3, 4, 6, 7, 10\}$ so $\mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(2p)$.
Step 2b): Suppose $4p+1$ is prime and N is divisible by $4p+1$. If N is divisible by $(4p+1)^2$, then d would be divisible by $4p+1$. But our assumptions rule this out $4p+1$ divides neither d_0 nor $\frac{d}{d_0}$. If N is divisible by $4(4p+1)$, then since $4(4p+1)$ is not of Type II, the first factor of d is divisible by $\frac{\varphi(4(4p+1))}{2} = 4p$. If N is divisible by $\ell(4p+1)$ for some prime $\ell \notin \{2, 4p+1\}$ then the first factor and the complementary factor of d are both even, so $4 \mid d$. Thus $N \in \{4p+1, 2(4p+1)\}$ and $\mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(2p)$.
Step 2c): Suppose $6p+1$ is prime and N is divisible by $6p+1$. For the same reasons as in Step 3b), N is not divisble by $(6p+1)^2$. If N is divisible by $2(6p+1)$, then since $2(6p+1)$ is neither of Type I nor Type II, we have $3 \mid \frac{\varphi(2(6p+1))}{2} \mid d$. If N is divisible by $\ell(6p+1)$ for some prime $\ell \notin \{2, 6p+1\}$, then as above we get $4 \mid d$.

Step 3: Let $d \in \mathcal{D}$, let $M, N \in \mathbb{Z}^+$ with $M \geq 2$ and $M \mid N$, and suppose $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(d)$, so by Step 2 we have $N \in \{1, 2, 3, 4, 6, 7, 10, 4p+1, 2(4p+1), 6p+1\}$. As above, if $N \leq 10$, then $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/NZ \hookrightarrow \mathcal{G}_{\mathbf{CM}}(2) \subseteq \mathcal{G}_{\mathbf{CM}}(2p)$. If $N = 4p+1$ then $4p+1$ is prime; if so, then $M = 4p+1$ and Proposition 2.8 implies that $4p = \varphi(4p+1) \mid d$. The case $N = 2(4p+1)$ can only occur if $4p+1$ is prime; the previous sentence rules out the case $4p+1 \mid M$ and Proposition 2.10 rules out $M = 2$. If $N = 6p+1$ then $6p+1$ is prime; if so, then $M = 6p+1$ and Proposition 2.8 implies that $6p = \varphi(6p+1) \mid d$. Thus $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(2p)$, completing the proof. □

Regarding the somewhat complicated hypothesis of Theorem 5.3: first of all, we may certainly take $d_0 = 2p$, which together with Theorem 4.2 yields the aforementioned result:

Corollary 5.4. *Let p be a prime number such that $2p+1$ is not prime. Then the set $[2p]_S$ of strongly $2p$-Olson degrees has positive lower density.*

The point though is that by Theorem 5.1, for each prime $p > 7$ such that $2p+1$ is prime, the set of positive integers d_0 that satisfy the hypotheses of Theorem 5.3 has positive density. Thus even applying Theorem 5.3 with $p = 13$, for instance, we get:

Corollary 5.5. *Let $\mathcal{E}$ be the set of even positive integers d_0 such that $[d_0]_S$ has positive lower density. Then $\mathcal{E}$ itself has positive lower density.*

5.4. **Analysis of $[2p]_S$ for $p > 2$ such that $2p+1$ is prime.** We now consider the set $[2p]_S$ of strongly $2p$-Olson degrees for a prime p such that $2p+1$ is also prime. Actually we only consider the case $p > 2$: the case of $p = 2$ involves a discussion of $\mathcal{G}_{\mathbf{CM}}(d)$ when d is divisible by 4, in which many of the tools we've developed here do not apply. As mentioned above, we *will* consider $p = 3$, but let us save it until the end.

Let $p > 3$ be a prime such that $2p+1$ is also prime. Let $d_0 \in \mathbb{Z}^+$ satisfy: • $2p \mid d_0$;
• $36d_0$ has the same shifted prime divisors as does $72p$; and
• $\gcd((2p+1), (4p+1)(6p+1), d_0) = 1$.

Put

$$\mathcal{M} \coloneqq \mathcal{M}_{36d_0,(2p+1)(4p+1)(6p+1)},$$

and put

$$\mathcal{D} \coloneqq \frac{1}{36}\mathcal{M}.$$

This is very similar to the setting of the proof of Theorem 5.3; the main change is that now, if $d \in \mathcal{D}$ and $\ell > 7$ is a prime such that $\mathbb{Z}/\ell\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(d)$, then with $\mathcal{P}_p$ as in (5) we find that $\ell \in \mathcal{P}_p \cup \{2p+1\}$. Let us see for which additional positive integers $M \mid N$ this allows $\mathbb{Z}/MZ \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(d)$:

• Suppose $2p+1 \mid N$. If $(2p+1)^2 \mid N$, then $2p+1 \mid d$, which is not the case. If $4(2p+1) \mid N$, then the first factor and complementary factors of d are even, so $4 \mid d$. If for a prime $\ell \notin \{2, 2p+1\}$ we have $\ell(2p+1) \mid N$, then as above we get $4 \mid d$. So $N \in \{2p+1, 2(2p+1)\}$.

• Let $d \in \mathcal{D}$, let $M, N \in \mathbb{Z}^+$ with $M \geq 2$ and $M \mid N$, and suppose $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(d)$. If $N = 2p+1$ then $M = 2p+1$ and Theorem 2.11b) implies that d is divisible either by 4 or by $2p+1$. It follows that if $N = 4(2p+1)$ then M cannot be divisible by $2p+1$. It follows that $\mathcal{G}_{\mathbf{CM}}(d) \subseteq \mathcal{T}(p)$, where

$$\mathcal{T}(p) \coloneqq \begin{cases} \{\mathbb{Z}/N\mathbb{Z} \mid N = 1,2,3,4,6,7,10\} \cup \\ \{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \mid n = 1,2,3\} \cup \\ \{\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}\} \cup \\ \{\mathbb{Z}/2(4p+1)\mathbb{Z}\} \textbf{ if } 4p+1 \textbf{ is prime} \cup \\ \{\mathbb{Z}/(6p+1)\mathbb{Z}\} \textbf{ if } 6p+1 \textbf{ is prime} \cup \\ \{\mathbb{Z}/(2p+1)\mathbb{Z}, \mathbb{Z}/2(2p+1)\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2(2p+1)\mathbb{Z}.\} \end{cases}.$$

Now we compare to $\mathcal{G}_{\mathbf{CM}}(d_0) = \mathcal{G}_{\mathbf{CM}}(2p)$. By Theorem 1.3, we find that $\mathcal{T}(p) = \mathcal{G}_{\mathbf{CM}}(2p)$ if and only if $p \equiv 4, 5 \pmod 7$ (equivalently, $\left(\frac{-7}{2p+1}\right) = 1$) and $\left(\frac{\Delta}{2p+1}\right) = 1$ for some $\Delta \in \{-11, -19, -43, -67, -163\}$. Thus we have proved:

Theorem 5.6. *Let $p > 7$ be a prime number such that $2p+1$ is prime, $p \equiv 4, 5 \pmod 7$ and $\left(\frac{\Delta}{2p+1}\right) = 1$ for some $\Delta \in \{-11, -19, -43, -67, -163\}$. Let $d_0 \in \mathbb{Z}^+$ be such that $2p \mid d_0$, $\gcd((2p+1)(4p+1)(6p+1), d_0) = 1$ and $36d_0$ has the same shifted prime divisors as does $72p$. Then the set $[d_0]_S$ of strongly d_0-Olson degrees has positive lower density.*

Because $11 \equiv 4 \pmod 7$ and $\left(\frac{-11}{23}\right) = 1$, Theorem 5.6 implies that $[22]_S$ has positive lower density, as already follows from Theorem 4.2. However Theorem 4.2 produces a more explicit positive density subset $\mathcal{D}_{11}$ of $[22]_S$.

The least prime $p > 3$ to which neither Corollary 5.4 nor Theorem 5.6 applies is $p = 23$. In this case, because $\left(\frac{-11}{47}\right) = 1$, by [BC23, Thm. 1.2] we have $\mathbb{Z}/47\mathbb{Z} \in \mathcal{G}_{\mathbf{CM}}(46)$. However, because

$$\left(\frac{-3}{47}\right) = \left(\frac{-4}{47}\right) = \left(\frac{-7}{47}\right) = \left(\frac{-8}{47}\right) = -1,$$

by [BC23, Thm. 1.2], neither $\mathbb{Z}/2 \cdot 47\mathbb{Z}$ nor $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2 \cdot 47\mathbb{Z}$ lies in $\mathcal{G}_{\mathbf{CM}}(46)$. This turns out to not only to be an obstruction to our method of proving that $[46]_S$ has positive lower density: in fact, it casts serious doubt on whether $[46]_S$ is even infinite, as we will now explain. Let K be an imaginary quadratic field with fundamental discriminant $\Delta_K \equiv 1 \pmod 8$ and such that $\left(\frac{\Delta_K}{47}\right) = 1$. Then 2 splits in K, so the 2-ray class field $K^{(2)}$ of K and the Hilbert class field $K^{(1)}$ of K coincide. It follows (already from the classical Main Theorem of Complex Multiplication) that if $E_{/K^{(1)}}$ is any Δ_K-CM elliptic curve, then $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \hookrightarrow E(K^{(1)})$. Moreover, since 47 splits in K, there is an invertible ideal I in $\mathbb{Z}_K$ of norm 47, so that $E[I]$ is a cyclic $K^{(1)}$-rational subgroup scheme of E [BC20a, Lemma 2.4] and thus E has a $K^{(1)}$-rational 47-isogeny. Thus we have a $K^{(1)}$-rational Δ-CM point on the modular curve $X_0(2, 2 \cdot 47)$. The natural modular covering $\pi : X_1(2, 2 \cdot 47) \to X_0(2, 2 \cdot 47)$ of degree $\frac{\varphi(47)}{2}$ then shows that there is a closed Δ-CM point on $X_1(2, 2 \cdot 47)$ of degree dividing $2h_{\Delta_K} \cdot \frac{\varphi(47)}{2} = 46h_{\Delta_K}$. (In fact, using [CS, Thm. 0.4.1], one finds that the residue field of this point has degree precisely $46h_{\Delta_K}$.) We have proved:

Lemma 5.7. *For every imaginary quadratic field K with discriminant Δ_K such that $\Delta_K \equiv 1 \pmod 8$ and $\left(\frac{\Delta_K}{47}\right) = 1$, we have $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2 \cdot 47\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(46h_{\Delta_K})$. In particular we have*

$$46h_{\Delta_K} \notin [46]_S.$$

Because 46 is a minimal degree, every $d \in \mathbb{Z}^+$ such that $d \sim 46$ is a multiple of 46; by Remark 6.1c) d must be of the form $46D$ with D odd. The class number h_K will be odd if $\Delta = -\ell$ for a prime $\ell \equiv 3 \pmod 4$. Thus for every prime $\ell \equiv 7 \pmod 8$ such that $\left(\frac{-\ell}{47}\right) = 1$, the degree $46h_{-\ell}$ is *not* 46-Olson. However, we expect that every sufficiently large odd number D is of the form $h_{-\ell}$ for a prime $\ell \equiv 7 \pmod 8$ such that $\left(\frac{-\ell}{47}\right) = 1$. If so, $[46]_\sim$ is finite.

In the above discussion, it was not crucial that $\left(\frac{-3}{47}\right) = \left(\frac{-4}{47}\right) = \left(\frac{-8}{47}\right) = -1$; if one of these symbols had been 1, then we would have $\mathbb{Z}/2 \cdot 46\mathbb{Z} \in \mathcal{G}_{\mathbf{CM}}(46)$ but still $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2 \cdot 46\mathbb{Z}$ would not embed in $\mathcal{G}_{\mathbf{CM}}(46)$, so the outcome would have been the same.

Exactly the same arguments establish the following result:

Proposition 5.8. *Let $p > 3$ be a prime such that $2p+1$ is prime. Suppose that $p \equiv 1, 2, 6 \pmod 7$. If $d \sim 2p$, then $d = 2pD$ for an odd $D \in \mathbb{Z}^+$ that is* not *of the form $h_{-\ell}$ for any prime $\ell \equiv 7 \pmod 8$ such that $\left(\frac{-\ell}{2p+1}\right) = 1$.*

Again Proposition 5.8 leads us to believe that Conjecture 1.2a) is false for $d = 2p$ and a prime p staisfying the conditions of Proposition 5.8 and that on, the contrary, in this case $[2p]_\sim$ is finite.

Suppose that $p > 5$ is a prime such that $2p + 1$ is prime, $p \equiv 4, 5 \pmod 7$ but $\left(\frac{\Delta}{2p+1}\right) = -1$ for all $\Delta \in \{-11, -19, -43, -67, -163\}$. Then

$$\mathbb{Z}/(2p+1)\mathbb{Z} \notin \mathcal{G}_{\mathbf{CM}}(2p), \text{ but } \mathbb{Z}/2(2p+1)\mathbb{Z}, \mathbb{Z}/\mathbb{Z} \times \mathbb{Z}/2(2p+1)\mathbb{Z} \in \mathcal{G}_{\mathbf{CM}}(2p).$$

In this case if $\ell \equiv 3 \pmod 4$ is a prime such that $\left(\frac{-\ell}{2p+1}\right) = 1$, then $\mathbb{Z}/(2p+1)\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(2ph_{-\ell})$, but since also $\mathbb{Z}/(2p+1)\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(2p)$, this is not enough to conclude that $2ph_{-\ell}$ is not a $2p$-Olson degree. For such primes p, our method of proof fails but not in a way that directly points to the falsity of Conjecture 1.2a) for $d = 2p$. We leave this case unresolved for now.

Finally, we consider $p = 3$. From [CCRS14, §4.6] we have that $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2 \cdot 9\mathbb{Z}$ does not embed in $\mathcal{G}_{\mathbf{CM}}(6)$. However, let $\ell \equiv 23 \pmod{24}$ be a prime number, and let $K := \mathbb{Q}(\sqrt{-\ell})$. Then again $K^{(2)} = K^{(1)}$ and 3 splits in K, so for all $a \in \mathbb{Z}^+$ there is an invertible ideal I in $\mathbb{Z}_K$ such that $\mathbb{Z}_K/I$ is isomorphic as a $\mathbb{Z}$-module to $\mathbb{Z}/3^a\mathbb{Z}$. Thus any $-\ell$-CM elliptic curve $E_{/K^{(1)}}$ has $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z} \hookrightarrow E(K^{(1)})$ and a $K^{(1)}$-rational cyclic 3^a-isogeny, which yields a $-\ell$-CM closed point on $X_0(2, 2\cdot 9)$ of degree $2h_{-\ell}$ and thus a $-\ell$-CM closed point on $X_1(2, 2\cdot 9)$ of degree $2h_{-\ell} \cdot \frac{\varphi(9)}{2} = 6h_{-\ell}$. We have shown:

Proposition 5.9. *Let $d \in \mathbb{Z}^+$. Suppose $d \sim 6$. Then $d = 6D$ for an odd $D \in \mathbb{Z}^+$ that is* not *of the form $h_{-\ell}$ for any prime $\ell \equiv 23 \pmod{24}$.*

We find it very plausible that every sufficiently large odd number D is of the form $h_{-\ell}$ for such a prime $\ell \equiv 23 \pmod{24}$. In fact, computations suggest that every odd $D \notin \{1, 9\}$ is of this form. By Remark 6.1h), if $d \sim 6$ then $9 \nmid d$. So it seems likely that $[6]_\sim$ is finite, and it may well be the case that $[6]_\sim = \{6\}$.

6. Some Complements

6.1. **d_0-Olson vs. Strongly d_0-Olson.** We say that $d_0 \in \mathbb{Z}^+$ is **minimal** if d_0 is the least element of $[d_0]_\sim$: that is, there is no positive integer $d_1 < d_0$ such that $\mathcal{G}_{\mathbf{CM}}(d_1) = \mathcal{G}_{\mathbf{CM}}(d_0)$. If every d_0-Olson degree is a strongly d_0-Olson degree, then d_0 must be minimal. We do not know whether the converse is true in general, but in this section we will establish it for certain values of d_0. Trivially this holds for $d_0 = 1$.

For $M, N, d_0 \in \mathbb{Z}^+$, we say that $(\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}, d_0)$ is an **S-pair** if for all $d \in \mathbb{Z}^+$, the group $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ is an element of $\mathcal{G}_{\mathbf{CM}}(d)$ if and only if $d_0 \mid d$. Whenever there is an S-pair with second coordinate d_0, a degree is d_0-Olson if and only if it is strongly d_0-Olson.

Remark 6.1. *For all minimal $d_0 \leq 20$ we can find an S-pair with second coordinate d_0, and thus for all $d_0 \leq 20$, we have that $[d_0]_\sim = [d_0]_S$ if and only if d_0 is minimal. Indeed:*

a) *By Proposition 2.8 and* [CCRS14, §4.2]*, $(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, 2)$ is an S-pair, so 2-Olson degrees are strongly 2-Olson. Moreover Olson degrees are odd.*
b) *By Theorem 2.6b) and* [CCRS14, §4.3]*, $(\mathbb{Z}/9\mathbb{Z}, 3)$ is an S-pair.*
c) *By Proposition 2.9a) and* [CCRS14, §4.4]*, $(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, 4)$ is an S-pair. Moreover, if d is 2-Olson, then $d \equiv 2 \pmod 4$.*
d) *By Proposition 2.6c) and* [CCRS14, §4.5]*, $(\mathbb{Z}/11\mathbb{Z}, 5)$ is an S-pair.*
e) *By Proposition 2.6l) and* [CCRS14, §4.6]*, $(\mathbb{Z}/26\mathbb{Z}, 6)$ is an S-pair.*
f) *7 is 1-Olson hence not minimal.*
g) *By Proposition 2.6f) and* [CCRS14, §4.8]*, $(\mathbb{Z}/15\mathbb{Z}, 8)$ is an S-pair.*
h) *By Proposition 2.6k) and* [CCRS14, §4.9]*, $(\mathbb{Z}/27\mathbb{Z}, 9)$ is an S-pair.*
i) *By Proposition 2.6i) and* [CCRS14, §4.10]*, $(\mathbb{Z}/50\mathbb{Z}, 10)$ is an S-pair.*
j) *11 is 1-Olson hence not minimal.*
k) *By Proposition 2.6l) and* [CCRS14, §4.12]*, $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/28\mathbb{Z}, 12)$ is an S-pair.*

l) 13 *is* 1*-Olson hence not minimal.*
m) *By Proposition 2.6n) and* [BC23, Thm. 1.2(8)]*,* $(\mathbb{Z}/58\mathbb{Z}, 14)$ *is an* S*-pair.*
n) *There is no strong* S*-pair with second coordinate* 15*: by* [BP17, §7] *we have*

$$\mathcal{G}_{\mathbf{CM}}(15) \setminus (\mathcal{G}_{\mathbf{CM}}(3) \cup \mathcal{G}_{\mathbf{CM}}(5)) = \{\mathbb{Z}/22\mathbb{Z}\},$$

while by [CCRS14, §4.10] *we have* $\mathbb{Z}/22\mathbb{Z} \in \mathcal{G}_{\mathbf{CM}}(10)$*. Nevertheless, if for* $d \in \mathbb{Z}^+$ *we have* $\mathcal{G}_{\mathbf{CM}}(d) \supseteq \mathcal{G}_{\mathbf{CM}}(15)$*, then* $\mathcal{G}_{\mathbf{CM}}(d)$ *contains both* $\mathcal{G}_{\mathbf{CM}}(3)$ *and* $\mathcal{G}_{\mathbf{CM}}(5)$*, so by parts b) and d) we have* $15 \mid d$*.*
o) *By Corollary 2.6 and Remark 2.7,* $(\mathbb{Z}/24\mathbb{Z}, 16)$ *is an* S*-pair.*
p) 17 *is* 14*-Olson hence not minimal.*
q) *By Corollary 2.6 and Remark 2.7,* $(\mathbb{Z}/74\mathbb{Z}, 18)$ *is an* S*-pair.*
r) 19 *is* 1*-Olson hence not minimal.*
s) *By Corollary 2.6 and Remark 2.7,* $(\mathbb{Z}/33\mathbb{Z}, 20)$ *is an* S*-pair.*

Theorem 6.2. *Let* p *be a prime number such that* $2p$ *is minimal – equivalently,* $2p$ *is* not *a* 2*-Olson degree. Then every* $2p$*-Olson degree is strongly* $2p$*-Olson.*

Proof. By Remark 6.1, for every prime $p \leq 7$, the every $2p$-Olson degree is strongly $2p$-Olson, so we may (and shall) assume that $p > 7$. By Theorem 1.3, $2p$ is minimal if and only if at least one of the following occurs: (i) $2p+1$ is prime and splits in an imaginary quadratic field of class number 1; (ii) $4p+1$ is prime; or (iii) $6p+1$ is prime.
Case 1: Suppose that $2p+1$ is prime and splits in an imaginary quadratic field of class number 1. By [BC23, Thm. 1.2], there is a number field F of degree $2p$ and a Δ-CM elliptic curve $E_{/F}$ such that $\mathbb{Z}/(2p+1)\mathbb{Z} \hookrightarrow E(F)$. So if $d \in \mathbb{Z}^+$ is such that $\mathcal{G}_{\mathbf{CM}}(2p) \subseteq \mathcal{G}_{\mathbf{CM}}(d)$ then there is a number field F of degree $2p$ and a CM elliptic curve $E_{/F}$ such that $\mathbb{Z}/(2p+1)\mathbb{Z} \hookrightarrow E(F)$. Since $2p+1$ is neither of Type I nor of Type II, the first factor of d is divisible by $\frac{\varphi(2p+1)}{2} = p$, so $p \mid d$. Since $\mathcal{G}_{\mathbf{CM}}(d) \supseteq \mathcal{G}_{\mathbf{CM}}(2p) \subseteq \mathcal{G}_{\mathbf{CM}}(2)$, by Remark 6.1a) we have $2 \mid d$, so $2p \mid d$.
Case 2: Suppose $4p+1$ is prime. By [BC23, Thm. 1.2(8)], we have $\mathbb{Z}/2(4p+1)\mathbb{Z} \in \mathcal{G}_{\mathbf{CM}}(2p)$. Suppose that F is a number field of degree d and $E_{/F}$ is a CM elliptic curve with $\mathbb{Z}/2(4p+1)\mathbb{Z} \hookrightarrow E(F)$. Since $2(4p+1)$ is not of Type II, the first factor of d is divisible by $\frac{\varphi(2(4p+1))}{4} = p$, and by Theorem 2.1 the complementary factor of d is even, so $2p \mid d$.
Case 3: Suppose $6p+1$ is prime. Let $d \in \mathbb{Z}^+$ be such that $\mathcal{G}_{\mathbf{CM}}(2p) \subseteq \mathcal{G}_{\mathbf{CM}}(d)$. In particular we have $\mathcal{G}_{\mathbf{CM}}(d) \supseteq \mathcal{G}_{\mathbf{CM}}(2)$, so d is even by Remark 6.1a). By [BC23, Thm. 1.2(7)], we have $\mathbb{Z}/(6p+1)\mathbb{Z} \in \mathcal{G}_{\mathbf{CM}}(2p) \subseteq \mathcal{G}_{\mathbf{CM}}(d)$. Suppose that F is a number field of degree d and $E_{/F}$ is a CM elliptic curve with $\mathbb{Z}/(6p+1)\mathbb{Z} \hookrightarrow E(F)$. Since $p > 2$, we have $6p+1 \equiv 3 \pmod 4$, so $6p+1$ is not of Type II, so the first factor of d is $\frac{\varphi(6p+1)}{6} = p > 2$. Thus $2p \mid d$. □

Theorem 6.3. *If* $d_0 \in \mathbb{Z}^+$ *is minimal and odd, then every* d_0*-Olson degree is strongly* d_0*-Olson.*

Proof. Let us call a group $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ **odd** if there is some odd $d \in \mathbb{Z}^+$ such that $G \in \mathcal{G}_{\mathbf{CM}}(d)$. Work of Aoki [Ao95], [Ao06] and Bourdon-Clark-Stankewicz [BCS17, Thm. 5.3] determines which groups $\mathbb{Z}/MZ \times \mathbb{Z}/N\mathbb{Z}$ are odd. Moreover, by [BP17, Thm. 1.2], for each odd $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$, if $d_0(M,N)$ is the least odd degree d such that $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z} \in \mathcal{G}_{\mathbf{CM}}(d)$, then every odd d such that $\mathbb{Z}/MZ \times \mathbb{Z}/N\mathbb{Z} \in \mathcal{G}_{\mathbf{CM}}(d)$ is a multiple of $d_0(M,N)$. Thus for any odd d, $\mathcal{G}_{\mathbf{CM}}(d)$ is determined as the set of odd groups $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ such that $d_0(M,N) \mid d$. From this it follows that if d_0 is odd and minimal and d is odd, then $\mathcal{G}_{\mathbf{CM}}(d_0) \subseteq \mathcal{G}_{\mathbf{CM}}(d)$ if and only if $d_0 \mid d$. □

6.2. **Proof of Proposition 1.9.**
a) First let $d_0 = 2$, and suppose that $d \in [d_0]_\sim$, i.e., d is a strongly 2-Olson degree. By Remark 6.1, we have $d \equiv 2 \pmod 4$. Because $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \in \mathcal{G}_{\mathbf{CM}}(6) \setminus \mathcal{G}_{\mathbf{CM}}(2)$ [CCRS14, §4.6], we have $3 \nmid d$. Because $\mathbb{Z}/22\mathbb{Z} \in \mathcal{G}_{\mathbf{CM}}(10) \setminus \mathcal{G}_{\mathbf{CM}}(2)$ [CCRS14, §4.10], we have $5 \nmid d$. Fix a positive integer X. Usng the aforementioned facts and Theorem 1.3, there is an obvious algorithm to compute the set $S(X)$ (resp., the set $T(X)$) of primes $p \leq X$ such that $d = 2p$ is 2-Olson (resp., is *not* 2-Olson). If d is 2-Olson, then $d \equiv 2 \pmod 4$ and $\gcd(d, p) = 1$ for all $p \in T(X)$, so

$$\overline{\delta}([2]_\sim) \leq \frac{\varphi(\prod_{p \in T(X)} p)}{4 \prod_{p \in T(X)}}.$$

Taking $X := 2 \cdot 10^7$ gives the upper bound of Proposition 1.9a).
Now let $p_0 \in \{5, 7, 11\}$, put $d_0 := 2p_0$ and and let $d \in [d_0]_\sim$, i.e., d is a strongly $2p_0$-Olson degree. The argument here is almost identical to that above: indeed, the only difference is that the condition $\gcd(d, p_0) = 1$ that we got for $d_0 = 2$ is replaced by the condition that $p_0 \mid d$. (By comparing the sets $\mathcal{G}_{\mathbf{CM}}(2p)$ and $\mathcal{G}_{\mathbf{CM}}(2p_0)$, we check that for all other primes $p > 3$, if $\mathcal{G}_{\mathbf{CM}}(2p) \supsetneq \mathcal{G}_{\mathbf{CM}}(2)$ then also $\mathcal{G}_{\mathbf{CM}}(2p)$ is not contained in $\mathcal{G}_{\mathbf{CM}}(2p_0)$.) Thus the upper bound we get on $\overline{\delta}([2p_0]_\sim)$ is $\frac{1}{p_0 - 1}$ times the upper bound we got on $\overline{\delta}([2]_\sim)$, up to rounding up in order to get an inequality.
b) We find that

$$S(500) = \{19, 31, 59, 71, 109, 149, 157, 167, 197\} \cup$$

$$\{211, 223, 227, 229, 317, 337, 349, 353, 379, 383, 389, 401, 421, 439, 463, 479\}.$$

Let $d \leq 1000$ with $d \equiv 2 \pmod 4$. If $p \in S(500)$, then $2p$ is 2-Olson, while if d is divisible by any element of $T(500)$ then d is not 2-Olson. The only d that does not satisfy either of these conditions is $d = 722 = 2 \cdot 19^2$. The set of primes ℓ such that $\ell - 1 \mid 722$ is $\{2, 3, 5, 13, 229, 457\}$. Because of the presence of 229 and 457, we have $722 \notin \mathcal{D}$. However the proof of Theorem 1.4a) will still work to show that $722 \in [2]_\sim$ as long as we can show that neither $\mathbb{Z}/229\mathbb{Z}$ nor $\mathbb{Z}/457\mathbb{Z}$ can embed in $E(F)$ for a Δ-CM elliptic curve E defined over a number field F of degree $d = 722$. Each of these subgroups is ruled out by Proposition 2.2e).
c) Let $d \in \mathbb{Z}^+$. By part a), in order for $d \sim 10$ we need $10 \mid d$, $4 \nmid d$ and $p \nmid d$ for all primes $p \notin \{2, 5\}$ such that $[2p]$ is not 2-Olson. We also need $25 \nmid d$: by [Sgit] we have $\mathbb{Z}/101\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(50)$, while $\mathbb{Z}/101\mathbb{Z}$ does not embed in $\mathcal{G}_{\mathbf{CM}}(10)$. Further we need $31 \nmid d$: otherwise $310 \mid d$ and by [Sgit] we have $\mathbb{Z}/311\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(310) \subseteq \mathcal{G}_{\mathbf{CM}}(d)$, while $\mathbb{Z}/311\mathbb{Z}$ does not embed in $\mathcal{G}_{\mathbf{CM}}(10)$. Let us call the necessary conditions we have imposed on d thus far the non/divisibility conditions.

For each $d \leq 2000$ satisfying the non/divisibility conditions, we compute the shifted prime divisors $\ell - 1$ of $2d$ and $3d$. If every such ℓ lies in $\{2, 3, 7, 11, 31\}$, then Theorem 2.4 shows that for all primes ℓ, we have

$$\mathbb{Z}/\ell\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(d) \implies \mathbb{Z}/\ell\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(10),$$

and then the proof of Theorem 4.1 applies to show that $d \sim 10$. In this we way find that 1490 and 1970 lie in $[10]_\sim = [10]_S$. Every other $d \leq 2000$ that satisfies the non/divisibility conditions, one of $2d$ and $3d$ has at least one shifted prime divisor $\ell - 1$ for $\ell \notin \{2, 3, 7, 11, 31\}$. Comparing with [Sgit], we always at least one such ℓ such that $\mathbb{Z}/\ell\mathbb{Z} \hookrightarrow \mathcal{G}_{\mathbf{CM}}(d')$ for some $d' \mid d$, so d is not 10-Olson.
d), e) The method of proof is identical to that of part c).
f) By Proposition 5.9, if $d \sim 6$, then $d = 6D$ for an odd number D that is *not* the class number of an imaginary quadratic field $\mathbb{Q}(\sqrt{-\ell})$ for any prime $\ell \equiv 23 \pmod{24}$. By recording class numbers of imaginary quadratic fields $\mathbb{Q}(\sqrt{-\ell})$ for such primes $\ell \leq 23 + 24 \cdot 10^6$, we find that for each odd

$D < 7267$ *except* $D \in \{1, 9\}$, there is such an ℓ such that $\mathbb{Q}(\sqrt{-\ell})$ has class number D. By Remark 6.1h), if $d \sim 6$, then $9 \nmid d$. So it follows that if $d \sim 6$ and $d < 7627 \cdot 6 = 45762$, then $d = 6$.

References

[Ao95] N. 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.

[Ao06] N. Aoki, *Torsion points on CM abelian varieties.* Comment. Math. Univ. St. Pauli 55 (2006), 207–229.

[BC20a] A. Bourdon and P.L. Clark, *Torsion points and Galois representations on CM elliptic curves*, Pacific J. Math. 305 (2020), 43–88.

[BC20b] A. Bourdon and P.L. Clark, *Torsion points and rational isogenies on CM elliptic curves.* J. Lond. Math. Soc. (2) 102 (2020), 580–622.

[BC23] A. Bourdon and H.P. Chaos, *Torsion for CM elliptic curves defined over number fields of degree* $2p$. Proc. Amer. Math. Soc. 151 (2023), 1001–1015.

[BCP17] A. Bourdon, P.L. Clark, P. Pollack, *Anatomy of torsion in the CM case.* Math. Z. 285 (2017), 795–820.

[BCS17] A. Bourdon, P.L. Clark and J. Stankewicz, *Torsion points on CM elliptic curves over real number fields.* Trans. Amer. Math. Soc. 369 (2017), 8457-–8496.

[Bi24] I. Bildik, *Torsion subgroups of CM elliptic curves in degree* $2qp$, University of Georgia PhD thesis, 2024.

[BP17] A. Bourdon and P. Pollack, *Torsion subgroups of CM elliptic curves over odd degree number fields.* Int. Math. Res. Not. IMRN 2017, no. 16, 4923–4961.

[CCRS14] P.L. Clark, P. Corn, A. Rice and J. Stankewicz, *Computation on elliptic curves with complex multiplication.* LMS J. Comput. Math. 17 (2014), 509–535.

[CMP18] P.L. CLark, M. Milosevic and P. Pollack, *Typically bounding torsion.* J. Number Theory 192 (2018), 150–167.

[Co89] D. Cox, *Primes of the form* $x^2 + ny^2$*. Fermat, class field theory and complex multiplication.* John Wiley & Sons, New York, 1989.

[CP17] P.L. Clark and P. Pollack, *The truth about torsion in the CM case, II.* Q. J. Math. 68 (2017), 1313–1333.

[CS] P.L. Clark and F. Saia, *CM elliptic curves: volcanoes, reality and applications*, preprint.

[EW80] P. Erdős and S. S. Wagstaff, Jr., *The fractional parts of the Bernoulli numbers.* Illinois J. Math. 24 (1980), 104–112.

[La09] E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen.* Vol. 1. BG Teubner, 1909.

[Ma77] B. Mazur, *Modular curves and the Eisenstein ideal. With an appendix by Mazur and M. Rapoport.* Inst. Hautes Études Sci. Publ. Math. (1977), 33–186.

[Me96] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres.* Invent. Math. 124 (1996), 437–449.

[Ol74] L. Olson, *Points of finite order on elliptic curves with complex multiplication.* Manuscripta math. 14 (1974), 195–205.

[Pa99] P. Parent, *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres.* J. Reine Angew. Math. 506 (1999), 85–116.

[PW23] C. Pomerance and S.S. Wagstaff, Jr., *The denominators of the Bernoulli numbers.* Acta Arith. 209 (2023), 1–15.

[Sgit] `https://raw.githubusercontent.com/fsaia/least-cm-degree/master/Least\%20Degrees/X1/dcm_list_X1_1mil.m`

[Si88] A. Silverberg, *Torsion points on abelian varieties of CM-type.* Compositio Math. 68 (1988), no. 3, 241–249.

[Si92] A. Silverberg, *Points of finite order on abelian varieties.* In *p-adic methods in number theory and algebraic geometry*, 175–193, Contemp. Math. 133, Amer. Math. Soc., Providence, RI, 1992.

[Si86] J. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 106, Springer Verlag, 1986.

[Si94] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 151, Springer-Verlag, 1994.

[So07] K. Soundararajan, *The number of imaginary quadratic fields with a given class number.* Hardy-Ramanujan J. 30 (2007), 13–18.

[vH14] M. van Hoeij, *Low degree places on the modular curve* $X_1(N)$. `https://arxiv.org/abs/1202.4355`