THE TRUTH ABOUT TORSION IN THE CM CASE, II

PETE L. CLARK AND PAUL POLLACK

ABSTRACT. Let $T_{\mathrm{CM}}(d)$ be the largest size of the torsion subgroup of an elliptic curve with complex multiplication (CM) defined over a degree d number field. Work of [5] and [7] showed $\limsup_{d\to\infty} \frac{T_{\mathrm{CM}}(d)}{d \log\log d} \in (0, \infty)$. Here we show that the above limit supremum is precisely $\frac{e^{\gamma}\pi}{\sqrt{3}}$. We also study – in part, out of necessity – the upper order of the size of the torsion subgroup of various restricted classes of CM elliptic curves over number fields.

CONTENTS

1. Introduction 1
1.1. Asymptotics of torsion subgroups of elliptic curves 1
1.2. Refining the truth I 3
1.3. Refining the truth II 3
1.4. Proof of Theorem 1.1 4
1.5. Complements 4
2. Lower bounds on $\varphi_K(\mathfrak{a})$ 5
3. Proof of Theorem 1.2 7
4. Proofs of Theorems 1.3 and 1.4 7
4.1. Proof of Theorem 1.3 8
4.2. Proof of Theorem 1.4 9
5. Proof of Theorem 1.5 10
5.1. Proof of Theorem 1.5a) 10
5.2. Proof of Theorem 1.5b) 10
6. Complements 11
6.1. Comparison to the prime order case 11
6.2. The truth about $T^{\circ}_{\mathrm{CM}}(d)$? 11
6.3. An analogue of Theorem 1.4 in the non-CM case 13
Acknowledgments 16
References 16

1. INTRODUCTION

1.1. **Asymptotics of torsion subgroups of elliptic curves.** Let $E_{/F}$ be an elliptic curve over a number field. Then the torsion subgroup $E(F)[\mathrm{tors}]$ is finite, and it is a problem of fundamental interest to study its size as a function of F and also of $d = [F : \mathbb{Q}]$. For $d \in \mathbb{Z}^+$, we put

$$T(d) = \sup \#E(F)[\mathrm{tors}],$$

the supremum ranging over all elliptic curves defined over all degree d number fields. We know that $T(d) < \infty$ for all $d \in \mathbb{Z}^+$ [12]. Merel's work gives an explicit upper bound on $T(d)$, but it is more than exponential.

In the other direction, it is known that $T(d)$ is *not* bounded above by a linear function of d. This and related bounds can be obtained by the following seemingly naive approach: start with *any* number field F_0 and *any* elliptic curve $E_{/F_0}$. For $n \in \mathbb{Z}^+$, let N_n be the product of the first n prime numbers, and put

$$F_n = F_0(E[N_n]), \quad d_n = [F_n : \mathbb{Q}].$$

An analysis of this "naive approach" was given by F. Breuer [5], who showed

$$\inf_n \frac{\#E(F_n)[\mathrm{tors}]}{\sqrt{d_n \log\log d_n}} > 0. \tag{1}$$

An elliptic curve $E_{/F}$ has **complex multiplication (CM)** if

$$\mathrm{End}(E) := \mathrm{End}_{\overline{F}}(E) \supsetneq \mathbb{Z},$$

in which case $\mathrm{End}(E)$ is an order $\mathcal{O}$ in an imaginary quadratic field K. Moreover, if $F \supset K$ we have $\mathrm{End}_F(E) = \mathcal{O}$, whereas if $F \not\supset K$ we have $\mathrm{End}_F(E) = \mathbb{Z}$. If $E_{/F_0}$ has CM, then Breuer shows by the same "naive approach" that

$$\inf_n \frac{\#E(F_n)[\mathrm{tors}]}{d_n \log\log d_n} > 0, \tag{2}$$

and thus $T(d)$ is not bounded above by a linear function of d. In view of these and other considerations, it is reasonable to define $T_{\mathrm{CM}}(d)$ as for $T(d)$ but restricting to CM elliptic curves only and $T_{\neg\mathrm{CM}}(d)$ as for $T(d)$ but restricting to elliptic curves *without* CM. Then it follows from (1) that

$$\limsup_{d\to\infty} \frac{T_{\neg\mathrm{CM}}(d)}{\sqrt{d \log\log d}} > 0$$

and it follows from (2) that

$$\limsup_{d\to\infty} \frac{T_{\mathrm{CM}}(d)}{d \log\log d} > 0.$$

In a recent work [7, Thm. 1] we showed there is an effective $C > 0$ such that

$$\forall d \geq 3, \quad T_{\mathrm{CM}}(d) \leq C d \log\log d$$

and thus we get an upper order result for $T_{\mathrm{CM}}(d)$:

$$\limsup_{d\to\infty} \frac{T_{\mathrm{CM}}(d)}{d \log\log d} \in (0, \infty). \tag{3}$$

Other statistical behavior of $T_{\mathrm{CM}}(d)$ was studied in [2, 4, 13]; in particular, its average order is $d/(\log d)^{1+o(1)}$ and its normal order (in a slightly nonstandard sense made precise in [2]) is bounded.

In the present work we will improve upon (3), as follows:

Theorem 1.1. $\displaystyle\limsup_{d\to\infty} \frac{T_{\mathrm{CM}}(d)}{d \log\log d} = \frac{e^{\gamma}\pi}{\sqrt{3}}.$

(The easier, lower bound half of Theorem 1.1 was noted in [13, Remark 1.10].) In §1.4 we will deduce Theorem 1.1 from results stated later in the introduction.

1.2. **Refining the truth I.** As mentioned above, it is natural to distinguish between the cases in which the CM is or is not rationally defined over the ground field. In this section we concentrate on the former case: let $T^{\bullet}_{\mathrm{CM}}(d)$ be as for $T_{\mathrm{CM}}(d)$ but restricting to CM elliptic curves $E_{/F}$ for number fields $F \supset K$.

We will also examine the dependence of the bound on the CM field and the CM order. Let $\mathscr{K}$ be a set of imaginary quadratic fields. We define $T_{\mathrm{CM}(\mathscr{K})}(d)$ to be as for $T_{\mathrm{CM}}(d)$ but with the CM field restricted to lie in $\mathscr{K}$. When $\mathscr{K} = \{K\}$ we write $T_{\mathrm{CM}(K)}(d)$ in place of $T_{\mathrm{CM}(\{K\})}(d)$. Once again we denote restriction to number fields $F \supset K$ by a superscripted $\bullet$.

Theorem 1.2. *Let $\epsilon > 0$. There is $\Delta_0 = \Delta_0(\epsilon) < 0$ such that: if $\mathscr{K}$ is the collection of imaginary quadratic fields with $\Delta_K < \Delta_0$, then*
$$\limsup_{d\to\infty} \frac{T^{\bullet}_{\mathrm{CM}(\mathscr{K})}(d)}{d \log\log d} < \epsilon.$$
We will prove Theorem 1.2 in §3. A key ingredient is a lower order result for Euler's totient function across all imaginary quadratic fields which improves upon [7, Thm. 8]. This result is established in §2.

Theorem 1.2 motivates us to concentrate on a fixed imaginary quadratic field as well as a fixed imaginary quadratic order. The next two results address this.

Theorem 1.3. *Fix an imaginary quadratic field K. For $d \in \mathbb{Z}^+$, let $\mathfrak{f}T^{\bullet}_{\mathrm{CM}(K)}(d)$ denote the maximum value of $\mathfrak{f}\#E(F)[\mathrm{tors}]$ as F ranges over all degree d number fields containing K and $E_{/F}$ ranges over all elliptic curves with CM by an order $\mathcal{O}$ of K: here $\mathfrak{f}$ is the conductor of $\mathcal{O}$. Then we have*
$$\limsup_{d\to\infty} \frac{\mathfrak{f}T^{\bullet}_{\mathrm{CM}(K)}(d)}{d \log\log d} \leq \frac{e^{\gamma}\pi}{\sqrt{|\Delta_K|}}.$$
Theorem 1.4. *Let $\mathcal{O}$ be an order in the imaginary quadratic field K, with conductor $\mathfrak{f}$ and discriminant $\Delta = \mathfrak{f}^2\Delta_K$. Let $T^{\bullet}_{\mathcal{O}\text{-CM}}(d)$ be the maximum value of $\#E(F)[\mathrm{tors}]$ as F ranges over all degree d number fields containing K and $E_{/F}$ ranges over all $\mathcal{O}$-CM elliptic curves. Then*
$$\limsup_{d\to\infty} \frac{T^{\bullet}_{\mathcal{O}\text{-CM}}(d)}{d \log\log d} = \frac{e^{\gamma}\pi}{\sqrt{|\Delta|}} = \frac{e^{\gamma}\pi}{\mathfrak{f}\sqrt{|\Delta_K|}}.$$
We will prove Theorems 1.3 and 1.4 in §4.

1.3. **Refining the truth II.** We turn now to upper order results for $\#E(F)[\mathrm{tors}]$ when the CM is *not* defined over the ground field F: define $T^{\circ}_{\mathrm{CM}}(d)$ as for $T_{\mathrm{CM}}(d)$ but restricting to CM elliptic curves $E_{/F}$ for number fields $F \not\supset K$. As above, we will want to impose this restriction along with restrictions on the CM field and CM order, and we denote restriction to number fields $F \not\supset K$ by a superscripted $\circ$.

If $E_{/F}$ is an elliptic curve defined over a number field F not containing K, then $\#E(F)[\mathrm{tors}] \leq \#E(FK)[\mathrm{tors}]$, and thus we have
$$T^{\circ}_{\mathrm{CM}}(d) \leq T^{\bullet}_{\mathrm{CM}}(2d). \tag{4}$$
Although (4) will be of use to us, it is too crude to allow us to deduce Theorem 1.1 from the results of the previous section. To overcome this we establish the following result, which *almost* computes the true upper order of $T^{\circ}_{\mathcal{O}\text{-CM}}(d)$.

Theorem 1.5. *Let $\mathcal{O}$ be an order in an imaginary quadratic field K.*

a) *There is a constant $C(\mathcal{O})$ such that*

$$\forall d \geq 3, \quad T^{\circ}_{\mathcal{O}\text{-CM}}(d) \leq C(\mathcal{O})\sqrt{d \log\log d}.$$

b) *We have* $\limsup_{d\to\infty} \frac{T^{\circ}_{\mathcal{O}\text{-CM}}(d)}{\sqrt{d}} > 0$.

We will prove Theorem 1.5 in §5.

We can now easily deduce:

Theorem 1.6. *We have* $\displaystyle\limsup_{d\to\infty} \frac{T^{\circ}_{\mathrm{CM}}(d)}{d \log\log d} = 0.$

Proof. Step 1: Using (4) we immediately get versions of Theorems 1.2 and 1.3 for $T_{\mathrm{CM}}(d)$: since replacing ϵ by 2ϵ is harmless, Theorem 1.2 holds verbatim with $T_{\mathrm{CM}}(d)$ in place of $T^{\bullet}_{\mathrm{CM}}(d)$, whereas for any imaginary quadratic field K we have

$$\limsup_{d\to\infty} \frac{\mathfrak{f}T_{\mathrm{CM}(K)}(d)}{d \log\log d} \leq \frac{2e^{\gamma}\pi}{\sqrt{|\Delta_K|}}. \tag{5}$$

Step 2: The above strengthened version of Theorem 1.2 reduces us to finitely many quadratic fields, and then the dependence on the conductor in (5) reduces us to finitely many quadratic orders. Thus we may treat one quadratic order at a time, and Theorem 1.5 gives a much better bound than $o(d \log\log d)$ in that case. □

1.4. **Proof of Theorem 1.1.** Theorem 1.1 is a quick consequence of these refined results: by Theorem 1.6 we may restrict to the case in which the number field contains the CM field. Now we argue much as in the proof of Theorem 1.6. By Theorem 1.4, applied with $\mathcal{O}$ the maximal order in $\mathbb{Q}(\sqrt{-3})$,

$$\limsup_{d\to\infty} \frac{T_{\mathrm{CM}}(d)}{d \log\log d} \geq \frac{e^{\gamma}\pi}{\sqrt{3}}.$$

By Theorem 1.2, in any sequence $\{(E_n)_{/F_n}\}$ with $[F_n : \mathbb{Q}] \to \infty$ such that

$$\lim_{n\to\infty} \frac{\#E(F_n)[\mathrm{tors}]}{[F_n : \mathbb{Q}] \log\log[F_n : \mathbb{Q}]} \geq \frac{e^{\gamma}\pi}{\sqrt{3}},$$

only finitely many quadratic fields intervene, and by Theorem 1.3 among orders with the same fraction field the conductors must be bounded. So we have reduced to working with one imaginary quadratic order $\mathcal{O}$ at a time, and Theorem 1.4 tells us that $T^{\bullet}_{\mathcal{O}\text{-CM}}(d)$ is largest when the discriminant of $\mathcal{O}$ is smallest, i.e., when $\mathcal{O}$ is the ring of integers of $\mathbb{Q}(\sqrt{-3})$.

1.5. **Complements.** In §6.1 we compare our results to the asymptotic behavior of prime order torsion studied in [6]. In §6.2 we address – but do not completely resolve – the question of the upper order of $T^{\circ}_{\mathrm{CM}}(d)$. In §6.3 we revisit Breuer's work and give what is in a sense a non-CM analogue of Theorem 1.4: we study the asymptotic behavior of torsion one j-invariant at a time.

2. Lower bounds on $\varphi_K(\mathfrak{a})$

For the classical Euler totient function, it is a well-known consequence of Mertens' Theorem that [11, Thm. 328]

$$\liminf_{n\to\infty} \frac{\varphi(n)}{n/\log\log n} = e^{-\gamma}.$$

Let K be an imaginary quadratic field and $\mathfrak{a}$ a nonzero ideal of $\mathcal{O}_K$. As in [7], we require analogous results for $\varphi_K(\mathfrak{a}) := \#(\mathcal{O}_K/\mathfrak{a})^\times$.

When the field K is fixed, this presents no difficulty. In that case, one can argue precisely as in [11], using the number field analogue of the classical Mertens Theorem: e.g. [14]. For a number field K, let h_K be its class number, let w_K be the number of roots of unity contained in K, and let α_K be the residue of the Dedekind zeta function $\zeta_K(s)$ at $s=1$. Then one finds that

$$\liminf_{|\mathfrak{a}|\to\infty} \frac{\varphi_K(\mathfrak{a})}{|\mathfrak{a}|/\log\log|\mathfrak{a}|} = e^{-\gamma}\alpha_K^{-1}.$$

(Here and below, $|\mathfrak{a}|$ denotes the norm of the ideal $\mathfrak{a}$.) When K is imaginary quadratic, the class number formula (e.g. [9, Theorem 61, p. 284]) gives

$$\alpha_K = \frac{2\pi h_K}{w_K\sqrt{|\Delta_K|}},$$

so that

$$\liminf_{|\mathfrak{a}|\to\infty} \frac{\varphi_K(\mathfrak{a})}{|\mathfrak{a}|/\log\log|\mathfrak{a}|} = \frac{e^{-\gamma}w_K\sqrt{|\Delta_K|}}{2\pi h_K}. \tag{6}$$

When K is allowed to vary, the situation becomes more delicate. In this section we will establish the following result.

Theorem 2.1. *There is a constant $c>0$ such that for all quadratic fields K and all nonzero ideals $\mathfrak{a}$ of $\mathcal{O}_K$ with $|\mathfrak{a}|\geq 3$, we have*

$$\varphi_K(\mathfrak{a}) \geq \frac{c}{\log|\Delta_K|}\cdot\frac{|\mathfrak{a}|}{\log\log|\mathfrak{a}|}.$$

Below, $\star$ denotes Dirichlet convolution, so that $(f\star g)(n) = \sum_{de=n} f(d)g(e)$.

Lemma 2.2. *There is a positive constant C for which the following holds. Let f be a nonnegative multiplicative function. Let χ be a nonprincipal Dirichlet character modulo q. For all $x\geq 2$,*

$$\left|\sum_{n\leq x}\frac{(f\star\chi)(n)}{n}\right| \leq C\log q\cdot\prod_{p\leq x}\left(1+\frac{f(p)}{p}+\frac{f(p^2)}{p^2}+\dots\right). \tag{7}$$

Proof. Write $\sum_{n\leq x}\frac{(f\star\chi)(n)}{n} = \sum_{d\leq x}\frac{f(d)}{d}\sum_{e\leq x/d}\frac{\chi(e)}{e}$. The contribution to the inner sum from values of $e\leq q$ is bounded in absolute value by $1+1/2+\dots+1/q \ll \log q$. Since the partial sums of χ are (crudely) bounded by q, Abel summation shows that the contribution to the inner sum from values of e with $q<e\leq x/d$ is $\ll 1 \ll \log q$. Now the triangle inequality and the nonnegativity of f yield

$$\left|\sum_{n\leq x}\frac{(f\star\chi)(n)}{n}\right| \ll \log q\cdot\sum_{d\leq x}\frac{f(d)}{d}.$$

The sum on d is bounded by the Euler product appearing in (7). $\square$

Lemma 2.3. *There is a constant $c > 0$ for which the following holds. Let χ be a quadratic character modulo q. For all $x \geq 2$,*

$$\prod_{p \leq x} \left(1 - \frac{\chi(p)}{p}\right) \geq \frac{c}{\log q}.$$

Proof. Let f be multiplicative such that $f(p^k) = 1 - \chi(p)$ for every prime power p^k. Since χ is quadratic, f assumes only nonnegative values. Moreover we have $(f \star \chi)(n) = 1$ for all $n \in \mathbb{Z}^+$; indeed, $f \star \chi$ is multiplicative, being a convolution of multiplicative functions, and one sees easily that $(f \star \chi)(p^k) = 1$ for all prime powers p^k. Thus,

$$\sum_{n \leq x} \frac{(f \star \chi)(n)}{n} = \sum_{n \leq x} \frac{1}{n} \gg \log x.$$

Hence, by Lemma 2.2 and Mertens' Theorem [11, Thm. 429],

$$\begin{aligned} \log x \ll (\log q) \cdot \prod_{p \leq x} \left(1 + \frac{1 - \chi(p)}{p - 1}\right) &= (\log q) \cdot \prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1} \cdot \prod_{p \leq x} \left(1 - \frac{\chi(p)}{p}\right) \\ &\ll (\log q)(\log x) \cdot \prod_{p \leq x} \left(1 - \frac{\chi(p)}{p}\right). \end{aligned}$$

Rearranging gives the lemma. $\square$

Proof of Theorem 2.1. We write $\varphi_K(\mathfrak{a}) = |\mathfrak{a}| \cdot \prod_{\mathfrak{p} | \mathfrak{a}} (1 - 1/|\mathfrak{p}|)$ and notice that the factors $1 - 1/|\mathfrak{p}|$ are increasing in $|\mathfrak{p}|$. So if $z \geq 2$ is such that $\prod_{|\mathfrak{p}| \leq z} |\mathfrak{p}| \geq |\mathfrak{a}|$, then

$$\frac{\varphi_K(\mathfrak{a})}{|\mathfrak{a}|} \geq \prod_{|\mathfrak{p}| \leq z} \left(1 - \frac{1}{|\mathfrak{p}|}\right). \tag{8}$$

We first establish a lower bound on the right-hand side, as a function of z, and then we prove the theorem by making a convenient choice of z. We partition the prime ideals with $|\mathfrak{p}| \leq z$ according to the splitting behavior of the rational prime p lying below $\mathfrak{p}$. Noting that $p \leq |\mathfrak{p}|$, Mertens' Theorem and Lemma 2.3 yield

$$\begin{aligned} \prod_{|\mathfrak{p}| \leq z} \left(1 - \frac{1}{|\mathfrak{p}|}\right) \geq \prod_{p \leq z} \prod_{\mathfrak{p} | (p)} \left(1 - \frac{1}{|\mathfrak{p}|}\right) &= \prod_{p \leq z} \left(1 - \frac{1}{p}\right) \left(1 - \frac{\left(\frac{\Delta_K}{p}\right)}{p}\right) \\ &\gg (\log z)^{-1} \prod_{p \leq z} \left(1 - \frac{\left(\frac{\Delta_K}{p}\right)}{p}\right) \gg (\log z)^{-1} \cdot (\log |\Delta_K|)^{-1}. \end{aligned} \tag{9}$$

With C' a large absolute constant to be described momentarily, we set

$$z = (C' \log |\mathfrak{a}|)^2. \tag{10}$$

Let us check that $\prod_{|\mathfrak{p}| \leq z} |\mathfrak{p}| \geq |\mathfrak{a}|$ with this choice of z. In fact, the Prime Number Theorem guarantees that

$$\prod_{|\mathfrak{p}| \leq z} |\mathfrak{p}| \geq \prod_{p \leq z^{1/2}} p \geq \prod_{p \leq C' \log |\mathfrak{a}|} p \geq |\mathfrak{a}|,$$

provided that C' was chosen appropriately. Combining (8), (9), and (10) gives

$$\varphi_K(\mathfrak{a}) \gg |\mathfrak{a}| \cdot (\log z)^{-1} \cdot (\log |\Delta_K|)^{-1} \gg (\log |\Delta_K|)^{-1} \cdot |\mathfrak{a}| \cdot (\log \log |\mathfrak{a}|)^{-1}. \quad \square$$

3. Proof of Theorem 1.2

Let E be an elliptic curve over a degree d number field F. Certainly we may, and shall, assume that $\#E(F)[\mathrm{tors}] \geq 3$. Suppose that E has CM by the imaginary quadratic field K and that $F \supset K$. Let $\mathcal{O} = \operatorname{End} E$, an order in the imaginary quadratic field K. Let $\mathcal{O}_K$ be the ring of integers of K. By [1, Thm. 1.4] there is an elliptic curve $E'_{/F}$ with $\operatorname{End} E' = \mathcal{O}_K$ such that

$$\#E(F)[\mathrm{tors}] \mid \#E'(F)[\mathrm{tors}].$$

Let $\mathfrak{a} \subset \mathcal{O}_K$ be the annihilator ideal of the $\mathcal{O}_K$-module $E'(F)[\mathrm{tors}]$. By [1, Thm. 2.7] we have

$$E'(F)[\mathrm{tors}] \cong \mathcal{O}_K/\mathfrak{a},$$

so

$$\#E'(F)[\mathrm{tors}] = |\mathfrak{a}|.$$

Let $K^{\mathfrak{a}}$ be the ray class field of K of conductor $\mathfrak{a}$. By the First Main Theorem of Complex Multiplication [17, Thm. II.5.6] we have

$$F \supset K^{\mathfrak{a}}, \tag{11}$$

while by [1, Lemma 2.11] we have

$$\frac{2\varphi_K(\mathfrak{a})h_K}{w_K} \mid [K^{\mathfrak{a}} : \mathbb{Q}] \tag{12}$$

with equality in most cases (e.g. unless $\mathfrak{a} \mid 6\mathcal{O}_K$). Combining (11) and (12), we get

$$\varphi_K(\mathfrak{a}) \mid \frac{w_K}{2} \cdot \frac{d}{h_K}.$$

Combining the last inequality with the result of Theorem 2.1, we get

$$|\mathfrak{a}|/\log\log|\mathfrak{a}| \leq \frac{w_K}{2c} \cdot \frac{\log|\Delta_K|}{h_K} \cdot d.$$

Siegel's Theorem (see [8, Chapter 21]) implies that $h_K \gg |\Delta_K|^{1/3}$. So we can choose Δ_0 sufficiently large and negative so that when $\Delta_K < \Delta_0$, we have

$$\frac{\log|\Delta_K|}{h_K} \leq \frac{\epsilon}{6}c.$$

Working under this assumption on Δ_K, we have

$$|\mathfrak{a}|/\log\log|\mathfrak{a}| \leq \frac{\epsilon}{2}d.$$

For all d sufficiently large in terms of ϵ, this implies that

$$\#E(F)[\mathrm{tors}] \leq \#E'(F)[\mathrm{tors}] = |\mathfrak{a}| < \epsilon d \log\log d.$$

Thus,

$$\limsup_{d\to\infty} \frac{T^{\bullet}_{\mathrm{CM}(\mathscr{K})}(d)}{d\log\log d} < \epsilon.$$

4. Proofs of Theorems 1.3 and 1.4

In this section we fix an imaginary quadratic field K.

4.1. **Proof of Theorem 1.3.** Let $F \supset K$ be a number field of degree d, and let $E_{/F}$ be an elliptic curve with CM by an order $\mathcal{O}$, of conductor $\mathfrak{f}$, in K. Put $w = \#\mathcal{O}^\times$. We may and shall assume that $\#E(F)[\mathrm{tors}] \geq 5$. We may write

$$E(F)[\mathrm{tors}] \cong \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/ab\mathbb{Z}$$

for $a, b \in \mathbb{Z}^+$. Since $\#E(F)[\mathrm{tors}] \geq 5$, we have $ab \geq 3$. By [7, Thm. 7] there is a number field $L \supset F$ such that $F(E[ab]) \subset L$ and $[L : F] \leq b$. Let $\mathfrak{h}\colon E \to E/\operatorname{Aut}(E)$ be the Weber function for E, and put

$$W(N, \mathcal{O}) = K(\mathfrak{f})(\mathfrak{h}(E[N])).$$

By [1, Thm. 2.12] we have $L \supset W(ab, \mathcal{O})$ and thus

$$[L : \mathbb{Q}] \geq [W(ab, \mathcal{O}) : K^{(1)}][K^{(1)} : \mathbb{Q}] = 2h_K[W(ab, \mathcal{O}) : K(\mathfrak{f})][K(\mathfrak{f}) : K^{(1)}], \tag{13}$$

where $K(\mathfrak{f})$ is the ring class field of K of conductor $\mathfrak{f}$. We recall some formulas: first, by [18, §4] or [1, Thm. 4.6], we have

$$[W(ab, \mathcal{O}) : K(\mathfrak{f})] = \frac{\#(\mathcal{O}/ab\mathcal{O})^\times}{w}. \tag{14}$$

Moreover, by [1, Lemma 2.3] we have

$$\#(\mathcal{O}/ab\mathcal{O})^\times [K(\mathfrak{f}) : K^{(1)}] = \varphi_K(ab\mathfrak{f}) \left(\frac{\varphi(ab)}{\varphi(ab\mathfrak{f})}\right) \frac{w}{w_K}. \tag{15}$$

Combining (13), (14) and (15) gives

$$[L : \mathbb{Q}] \geq \frac{2h_K}{w_K} \left(\frac{\varphi(ab)}{\varphi(ab\mathfrak{f})}\right) \varphi_K(ab\mathfrak{f}),$$

and thus

$$d = [F : \mathbb{Q}] \geq \frac{[L : \mathbb{Q}]}{b} \geq \frac{2h_K}{bw_K} \left(\frac{\varphi(ab)}{\varphi(ab\mathfrak{f})}\right) \varphi_K(ab\mathfrak{f}).$$

Multiplying by $a^2b^2\mathfrak{f}^2 = |ab\mathfrak{f}\mathcal{O}_K|$ and rearranging, we get

$$\mathfrak{f}^2 \#E(F)[\mathrm{tors}] = \mathfrak{f}^2 a^2 b \leq \frac{w_K}{2} \frac{d}{h_K} \frac{|abf\mathcal{O}_K|}{\varphi_K(ab\mathfrak{f})} \frac{\varphi(ab\mathfrak{f})}{\varphi(ab)}. \tag{16}$$

We have $\frac{\varphi(ab\mathfrak{f})}{\varphi(ab)} \leq \mathfrak{f}$; replacing the factor of $\frac{\varphi(ab\mathfrak{f})}{\varphi(ab)}$ with $\mathfrak{f}$ in the right-hand side of (16) and cancelling the $\mathfrak{f}$'s, we get

$$\mathfrak{f}\#E(F)[\mathrm{tors}] \leq \frac{w_K}{2} \frac{d}{h_K} \frac{|ab\mathfrak{f}\mathcal{O}_K|}{\varphi_K(ab\mathfrak{f})}.$$

Now using (6) we get that, as $\mathfrak{f}\#E(F)[\mathrm{tors}] \to \infty$,

$$\mathfrak{f}\#E(F)[\mathrm{tors}] \leq (1 + o(1)) \frac{e^\gamma \pi}{\sqrt{|\Delta_K|}} d \log\log(a^2b^2\mathfrak{f}^2).$$

Since $\mathfrak{f}\#E(F)[\mathrm{tors}] = \mathfrak{f}a^2b \leq a^2b^2\mathfrak{f}^2 \leq (\mathfrak{f}\#E(F)[\mathrm{tors}])^2$,

$$\log\log(a^2b^2\mathfrak{f}^2) = \log\log(\mathfrak{f}\#E(F)[\mathrm{tors}]) + O(1),$$

so that

$$\mathfrak{f}\#E(F)[\mathrm{tors}] \leq (1 + o(1)) \frac{e^\gamma \pi}{\sqrt{|\Delta_K|}} d \log\log(\mathfrak{f}\#E(F)[\mathrm{tors}]).$$

Thus,

$$\frac{\mathfrak{f}\#E(F)[\mathrm{tors}]}{\log\log \mathfrak{f}\#E(F)[\mathrm{tors}]} \leq (1 + o(1)) \frac{e^\gamma \pi}{\sqrt{|\Delta_K|}} d,$$

which implies that

$$\mathfrak{f}\#E(F)[\text{tors}] \leq (1+o(1))\frac{e^{\gamma}\pi}{\sqrt{|\Delta_K|}} d\log\log d.$$

Thus, for any sequence of K-CM elliptic curves $E_{/F}$ (having $F \supset K$, and $[F:\mathbb{Q}] = d$) with $\mathfrak{f}\#E(F)[\text{tors}] \to \infty$,

$$\limsup \frac{\mathfrak{f}\#E(F)[\text{tors}]}{d\log\log d} \leq \frac{e^{\gamma}\pi}{\sqrt{|\Delta_K|}}.$$

Theorem 1.3 follows immediately.

4.2. **Proof of Theorem 1.4.** Let $\mathcal{O}$ be the order of conductor $\mathfrak{f}$ in the imaginary quadratic field K. Again we put $w = \#\mathcal{O}^{\times}$.

The inequality

$$\limsup_{d\to\infty} \frac{T^{\bullet}_{\mathcal{O}-\mathrm{CM}}(d)}{d\log\log d} \leq \frac{e^{\gamma}\pi}{\mathfrak{f}\sqrt{|\Delta_K|}}$$

is immediate from Theorem 1.3, so it remains to prove the opposite inequality.

Let $n \geq 2$, and let N_n be the product of the primes not exceeding n. We assume that n is large enough so that for all primes ℓ, if $\ell \mid \mathfrak{f}$ then $\ell \mid N_n$. By [1, Thm. 1.1c)] there is a number field $F \supset K$ and an $\mathcal{O}$-CM elliptic curve $E_{/F}$ such that

$$[F:K(j(E))] = \frac{\#(\mathcal{O}/N_n\mathcal{O})^{\times}}{w}$$

and $(\mathbb{Z}/N_n\mathbb{Z})^2 \hookrightarrow E(F)$. Since $K(j(E)) = K(\mathfrak{f})$, using (15) as above shows that

$$[F:\mathbb{Q}] = \frac{2h_K}{w_K}\left(\frac{\varphi(N_n)}{\varphi(N_n\mathfrak{f})}\right)\varphi_K(N_n\mathfrak{f}).$$

Because every prime dividing $\mathfrak{f}$ also divides N_n, we have $\frac{\varphi(N_n)}{\varphi(N_n\mathfrak{f})} = \frac{1}{\mathfrak{f}}$, so

$$d = [F:\mathbb{Q}] = \frac{2h_K}{\mathfrak{f}w_K}\varphi_K(N_n\mathfrak{f}) = \frac{2\mathfrak{f}h_K N_n^2}{w_K}\prod_{p\leq n}\left(1-\frac{1}{p}\right)\left(1-\left(\frac{\Delta_K}{p}\right)\frac{1}{p}\right).$$

It follows that

$$\#E(F)[\text{tors}] \geq N_n^2 = \frac{w_K}{2\mathfrak{f}h_K} d \prod_{p\leq n}\left(1-\frac{1}{p}\right)^{-1}\prod_{p\leq n}\left(1-\left(\frac{\Delta_K}{p}\right)\frac{1}{p}\right)^{-1}.$$

Mertens' Theorem gives $\prod_{p\leq n}(1-1/p)^{-1} \sim e^{\gamma}\log n$, as $n\to\infty$, while

$$\prod_{p\leq n}\left(1-\left(\frac{\Delta_K}{p}\right)\frac{1}{p}\right)^{-1} \to L(1,\left(\frac{\Delta_K}{\cdot}\right)) = \frac{2\pi h_K}{w_K\sqrt{|\Delta_K|}}.$$

Thus we find that as $n\to\infty$ we have

$$\#E(F)[\text{tors}] \geq (1+o(1))\frac{e^{\gamma}\pi}{\mathfrak{f}\sqrt{|\Delta_K|}} d\log n.$$

Moreover, for sufficiently large n we have

$$d = \frac{2h_K}{\mathfrak{f}w_K}\varphi_K(N_n\mathfrak{f}) = \frac{2\mathfrak{f}h_K}{w_K}\varphi_K(N_n) \leq \frac{2\mathfrak{f}h_K}{w_K}N_n^2 \leq N_n^3,$$

so as $n\to\infty$ we have

$$\log\log d \leq \log\log N_n + O(1).$$

By the Prime Number Theorem we have $N_n = e^{(1+o(1))n}$, so

$$\log \log N_n \sim \log n,$$

and thus as $n \to \infty$ we have

$$\log n \geq (1 + o(1)) \log \log d.$$

We conclude that as $n \to \infty$,

$$\#E(F)[\text{tors}] \geq (1 + o(1)) \frac{e^\gamma \pi}{\mathfrak{f}\sqrt{|\Delta_K|}} d \log \log d = (1 + o(1)) \frac{e^\gamma \pi}{\sqrt{|\Delta|}} d \log \log d,$$

completing the proof of Theorem 1.4.

5. Proof of Theorem 1.5

5.1. **Proof of Theorem 1.5a).** Let $\mathcal{O}$ be the order of conductor $\mathfrak{f}$ in the imaginary quadratic field K, let F be a number field not containing K, and let $E_{/F}$ be an $\mathcal{O}$-CM elliptic curve. By [6, Prop. 25] there is a degree $\mathfrak{f}$ cyclic F-rational isogeny $E \to E'$, with $E'_{/F}$ an $\mathcal{O}_K$-CM elliptic curve. It follows that

$$\#E(F)[\text{tors}] \leq \mathfrak{f} \#E'(F)[\text{tors}]. \tag{17}$$

By [3, Lemma 3.15] we have

$$E'(F)[\text{tors}] \cong \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/ab\mathbb{Z}$$

with $a \in \{1, 2\}$. Certainly there are $A, B \in \mathbb{Z}^+$ such that

$$E'(FK)[\text{tors}] \cong \mathbb{Z}/A\mathbb{Z} \times \mathbb{Z}/AB\mathbb{Z}.$$

Write $ab = c_1 c_2$ with c_1 divisible only by primes $p \nmid \Delta_K$ and c_2 divisible only by primes $p \mid \Delta_K$. Then [3, Thm. 4.8] gives $c_1 \mid A$. Let β be the product of the distinct prime divisors of c_2, and let $\mathfrak{b}$ be the product of the distinct prime divisors of Δ_K, so $\beta \mid \mathfrak{b}$. By [1, §6.3] we have $\frac{c_2}{\beta} \mid A$. Since $\gcd(c_1, c_2) = 1$, this implies $\frac{ab}{\beta} \mid A$ and thus

$$\#E'(FK)[\text{tors}] = A^2 B \geq A^2 \geq \frac{a^2 b^2}{\beta^2}. \tag{18}$$

Using (17) and (18) we get

$$\#E(F)[\text{tors}] \leq \mathfrak{f} \#E'(F)[\text{tors}] \leq a \mathfrak{f} \beta \sqrt{\#E'(FK)[\text{tors}]} \leq 2 \mathfrak{f} \mathfrak{b} \sqrt{\#E'(FK)[\text{tors}]}.$$

Note that $\mathfrak{f}$ and $\mathfrak{b}$ depend only on $\mathcal{O}$. Moreover $\#E'(FK)[\text{tors}] \ll_{\mathcal{O}} d \log \log d$, by Theorem 1.4. Thus, as claimed, we have

$$\#E(F)[\text{tors}] \ll_{\mathcal{O}} \sqrt{d \log \log d}.$$

5.2. **Proof of Theorem 1.5b).** First one rather innocuous preliminary result.

Lemma 5.1. *Let F be a subfield of $\mathbb{R}$. Let $E_{/F}$ be an elliptic curve, and let $N \in \mathbb{Z}^+$ have prime power decomposition $N = \prod_{i=1}^r \ell_i^{a_i}$. Then there is a point $P \in E(\mathbb{R})$ of order N such that $[F(P) : F] \leq \prod_{i=1}^r \ell_i^{2a_i - 2}(\ell_i^2 - 1)$.*

Proof. As for every elliptic curve defined over $\mathbb{R}$, we have $E(\mathbb{R}) \cong S^1$ or $E(\mathbb{R}) \cong S^1 \times \mathbb{Z}/2\mathbb{Z}$ (e.g. [17, Cor. V.2.3.1]) . Thus there is $P \in E(\mathbb{R})$ of order N. Let $\overline{F}$ be the algebraic closure of F viewed as a subfield of $\mathbb{C}$. Then $P \in E(\overline{F})$ and the degree $[F(P) : F]$ is the size of the $\mathrm{Aut}(\overline{F}/F)$-orbit on P. For all $\sigma \in \mathrm{Aut}(\overline{F}/F)$, $\sigma(P)$ is also a point of order N, so the size of this orbit is no larger than the number of order $N = \prod_{i=1}^r \ell_i^{a_i}$ points in $E[N](\overline{F}) \cong (\mathbb{Z}/N\mathbb{Z})^2$, which is $\prod_{i=1}^r \ell_i^{2a_i-2}(\ell_i^2 - 1)$. $\square$

We now give the proof of Theorem 1.5b). Let $\mathcal{O}$ be an order in an imaginary quadratic field K. Let $F_0 = \mathbb{Q}(j(\mathbb{C}/\mathcal{O}))$, so that F_0 is a subfield of $\mathbb{R}$ (forcing $F_0 \not\supset K$) and $[F_0 : \mathbb{Q}] = \# \operatorname{Pic} \mathcal{O}$. Let $E_{/F_0}$ be any $\mathcal{O}$-CM elliptic curve. Let $r \in \mathbb{Z}^+$ and let $N_r = p_1 \cdots p_r$ be the product of the first r primes.

Applying Lemma 5.1 to $E_{/F_0}$ we get a number field $F_{N_r} \subset \mathbb{R}$ with

$$d_r := [F_{N_r} : \mathbb{Q}] \leq \# \operatorname{Pic} \mathcal{O} \prod_{i=1}^r (p_i^2 - 1)$$

such that $E(F_{N_r})$ has a point of order N_r. So we have

$$\limsup_{r \to \infty} \frac{d_r}{N_r^2} \leq \frac{\# \operatorname{Pic} \mathcal{O}}{\zeta(2)} = \frac{6 \# \operatorname{Pic} \mathcal{O}}{\pi^2}$$

and thus, as $r \to \infty$,

$$\frac{\# E(F_{N_r})[\text{tors}]}{\sqrt{d_r}} \geq \sqrt{\frac{\pi^2}{6 \# \operatorname{Pic} \mathcal{O}}} + o(1).$$

6. Complements

For a number field F, let $\mathfrak{g}_F = \mathrm{Aut}(\overline{\mathbb{Q}}/F)$ denote the absolute Galois group of F.

6.1. **Comparison to the prime order case.** Fix an imaginary quadratic order $\mathcal{O}$ of discriminant Δ. For all sufficiently large primes p, the least degree of a number field $F \supset K$ such that there is an $\mathcal{O}$-CM elliptic curve $E_{/F}$ with an F-rational point of order p is at least $\left(\frac{2\# \operatorname{Pic} \mathcal{O}}{\# \mathcal{O}^\times}\right)(p-1)$, with equality if p splits in $\mathcal{O}$ [6, Thms. 2 and 3], and thus the upper order of the size of a prime order torsion point divided by the degree of the number field containing K over which it is defined is $\frac{\# \mathcal{O}^\times}{2\# \operatorname{Pic} \mathcal{O}}$. The maximum value of this quantity is 3, occurring iff $\Delta = -3$; the second largest value is 2, occurring iff $\Delta = -4$, and these are indeed the largest two imaginary quadratic discriminants. But the third largest value is 1, occurring iff $\Delta \in \{-7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163\}$. In particular, both the class number h_K and the size of the unit group $\mathcal{O}^\times$ play a role in the asymptotic behavior of prime order torsion but get cancelled out by the special value $L(1, \left(\frac{\Delta_K}{\cdot}\right))$ when we look at the size of the torsion subgroup as a whole.

6.2. The truth about $T_{\mathrm{CM}}^\circ(d)$?

Proposition 6.1. *There is a sequence of $d \to \infty$ along which $T_{\mathrm{CM}}^\circ(d) \geq d^{2/3+o(1)}$.*

Proof. Let ℓ be an odd prime. By [3, Cor. 5.8] applied to the maximal order of $K = \mathbb{Q}(\sqrt{-\ell})$, there is a number field F of degree $d = h_{\mathbb{Q}(\sqrt{-\ell})} \frac{\ell-1}{2}$ and an $\mathcal{O}_K$-CM elliptic curve $E_{/F}$ with an F-rational torsion point of order ℓ. We restrict to $\ell \equiv 3 \pmod 4$ — this has the effect of ensuring that d is odd, and so $F \not\supset K$. Hence, $T_{\mathrm{CM}}^\circ(d) \geq \ell$. By Dirichlet's class number formula together with the elementary bound $L(1, \left(\frac{-\ell}{\cdot}\right)) \ll \log \ell$ (see, e.g., [19, Thm. 8.18]), we have $h_{\mathbb{Q}(\sqrt{-\ell})} \ll \ell^{1/2} \log \ell$. Thus, $d \leq \ell^{3/2+o(1)}$ (as $\ell \to \infty$), and so

$$T^{\circ}_{\mathrm{CM}}(d) \geq \ell \geq d^{2/3+o(1)}.$$

As ℓ tends to infinity, so does d, and the proposition follows. $\square$

Define $T^{\circ}_{\mathrm{CM,max}}(d)$ in the same way as $T^{\circ}_{\mathrm{CM}}(d)$, but with the added restriction that we consider only curves $E_{/F}$ with CM by the maximal order $\mathcal{O}_K$. The preceding proof shows that $T^{\circ}_{\mathrm{CM,max}}(d) \geq d^{2/3+o(1)}$ on a sequence of d tending to infinity.

Theorem 6.2. *For all $\epsilon > 0$, there is $C(\epsilon) > 0$ such that for all $d \in \mathbb{Z}^+$ we have*

$$T^{\circ}_{\mathrm{CM,max}}(d) \leq C(\epsilon) d^{2/3+\epsilon}.$$

Proof. Let $F \not\supset K$ be a number field of degree d, and let $E_{/F}$ be an $\mathcal{O}_K$-CM elliptic curve. There are positive integers a and b with

$$E(F)[\mathrm{tors}] \cong \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/ab\mathbb{Z}.$$

By [3, Lemma 3.15], we have $a \in \{1, 2\}$. The remainder of the proof takes two forms depending on the size of $|\Delta_K|$.

Case I: $|\Delta_K| \geq d^{2/3}$.

Since $E(FK)$ contains a point of order ab, [1, Thm. 5.3] shows that

$$\varphi(ab) \leq \frac{w_K}{2} \frac{2d}{h_K}.$$

By Siegel's Theorem, $h_K \gg_\epsilon |\Delta_K|^{1/2-\epsilon} \geq d^{1/3-2\epsilon/3}$ (as $d \to \infty$), and so

$$\varphi(ab) \ll_\epsilon d^{2/3+2\epsilon/3}.$$

Consequently,

$$\#E(F)[\mathrm{tors}] = a(ab) \leq 2ab \ll_\epsilon d^{2/3+\epsilon}.$$

Case II: $|\Delta_K| < d^{2/3}$.

We can and will assume that $d \geq 3$ and that $\#E(F)[\mathrm{tors}] \geq 3$. Write $ab = c_1 c_2$, where $(c_1, \Delta_K) = 1$ and where every prime dividing c_2 divides Δ_K. By [3, Thm. 4.8], $E(FK)$ has full c_1-torsion, so that

$$c_1^2 \mid \#E(FK)[\mathrm{tors}].$$

Let ℓ^α be a prime power dividing c_2, and let P be a point of $E(FK)$ of order ℓ^α. By [1, §6.3], the $\mathcal{O}_K$-submodule of $E(FK)[\mathrm{tors}]$ generated by P is isomorphic, as a $\mathbb{Z}$-module, to either $\mathbb{Z}/\ell^\alpha\mathbb{Z} \oplus \mathbb{Z}/\ell^\alpha\mathbb{Z}$ or $\mathbb{Z}/\ell^\alpha\mathbb{Z} \oplus \mathbb{Z}/\ell^{\alpha-1}\mathbb{Z}$. It follows that if r is the product of the distinct primes dividing c_2, then

$$c_2^2 \mid r \cdot \#E(FK)[\mathrm{tors}].$$

Since $\gcd(c_1, c_2) = 1$ and $r \mid \Delta_K$, we have

$$c_1^2 c_2^2 \mid \Delta_K \cdot \#E(FK)[\mathrm{tors}]. \tag{19}$$

Applying the proof of Theorem 1.2 to FK, we get that if $\mathfrak{a} \subset \mathcal{O}_K$ is the annihilator ideal of the $\mathcal{O}_K$-module $E(FK)[\mathrm{tors}]$, then we have

$$|\mathfrak{a}| = \#E(FK)[\mathrm{tors}],$$

and

$$\varphi_K(\mathfrak{a}) \leq \frac{w_K}{2} \cdot \frac{2d}{h_K}.$$

Hence, by Theorem 2.1,

$$|\mathfrak{a}|/\log\log|\mathfrak{a}| \leq \frac{w_K}{c} \cdot d\frac{\log|\Delta_K|}{h_K}.$$

Since $\frac{w_K}{c}, \frac{\log|\Delta_K|}{h_K}$ are bounded, this implies $|\mathfrak{a}|/\log\log|\mathfrak{a}| \ll d$, and hence $|\mathfrak{a}| \ll d\log\log d$. Hence, $\log\log|\mathfrak{a}| \ll \log\log d$, and

$$\#E(FK)[\mathrm{tors}] = |\mathfrak{a}| \ll \frac{\log|\Delta_K|}{h_K} \cdot d\log\log d.$$

Now (19) implies that

$$\#E(F)[\mathrm{tors}]^2 = (a^2b)^2 = a^2 \cdot a^2b^2 \leq 4c_1^2c_2^2 \ll \frac{|\Delta_K|\log|\Delta_K|}{h_K} \cdot d\log\log d.$$

By Siegel's Theorem, $h_K \gg_\epsilon |\Delta_K|^{1/2-\epsilon}$. Thus (keeping in mind our upper bound on $|\Delta_K|$ in this case),

$$\frac{|\Delta_K|\log|\Delta_K|}{h_K} \ll_\epsilon |\Delta_K|^{1/2+2\epsilon} \leq d^{1/3+4\epsilon/3},$$

so that

$$\#E(F)[\mathrm{tors}]^2 \ll_\epsilon d^{4/3+2\epsilon}.$$

Hence,

$$\#E(F)[\mathrm{tors}] \ll_\epsilon d^{2/3+\epsilon}.$$

The result follows from combining Cases 1 and 2. □

The above results suggest to us that the upper order of $T^\circ_{\mathrm{CM}}(d)$ is $d^{2/3+o(1)}$, but we cannot yet prove this. When the CM is F-rationally defined, we were able to take advantage of the recent work [1]. The authors of [1] are pursuing analogous algebraic results when the CM is not rationally defined. In view of this, we hope to revisit the upper order of $T^\circ_{\mathrm{CM}}(d)$ later and present more definitive results.

6.3. **An analogue of Theorem 1.4 in the non-CM case.** Our method of showing $\limsup_{d\to\infty} \frac{T^\bullet_{\mathcal{O}\text{-CM}}(d)}{d\log\log d} \geq \frac{e^\gamma\pi}{\sqrt{|\Delta|}}$ is very nearly the "naive approach" of starting with an $\mathcal{O}$-CM elliptic curve defined over $F_0 = K(\mathfrak{f})$ and extending the base to $\tilde{F}_n = F_0(E[N_n])$. Our only departure from this was to pass to the Weber function field $F_n = F_0(\mathfrak{h}(E[N_n]))$ and then twist $E_{/F_n}$ to get full N_n-torsion. We know the degree $[F_n : \mathbb{Q}]$ exactly; the degree $[\tilde{F}_n : \mathbb{Q}]$ depends on the F_0-rational model, but in general is $\#\mathcal{O}^\times$ as large, so the naive approach would give

$$\limsup_{d\to\infty} \frac{T^\bullet_{\mathcal{O}\text{-CM}}(d)}{d\log\log d} \geq \frac{e^\gamma\pi}{\#\mathcal{O}^\times\sqrt{|\Delta|}}.$$

So the naive approach comes within a twist of giving the *true upper order* of $T_{\mathrm{CM}}(d)$.

Observe that in the CM case, fixing the quadratic order $\mathcal{O}$ fixes the $\mathfrak{g}_{\mathbb{Q}}$-conjugacy class of the j-invariant. This motivates the following definition: let $j \in \overline{\mathbb{Q}} \subset \mathbb{C}$ and let $F_0 = \mathbb{Q}(j)$. For positive integers d divisible by $[F_0 : \mathbb{Q}]$, put

$$T_j(d) = \sup \#E(F)[\mathrm{tors}],$$

the supremum ranging over number fields $F \subset \mathbb{C}$ with $[F : \mathbb{Q}] = d$ and elliptic curves $E_{/F}$ such that $j(E) = j$. Note that we could equivalently range over all elliptic curves $E_{/F}$ such that $j(E)$ and j are $\mathfrak{g}_{\mathbb{Q}}$-conjugates.

Theorem 6.3 (Breuer [5]).

a) *If $j \in \overline{\mathbb{Q}}$ is a CM j-invariant, then*

$$\limsup_d \frac{T_j(d)}{d \log\log d} \in (0, \infty).$$

b) *If $j \in \overline{\mathbb{Q}}$ is not a CM j-invariant, then*

$$\limsup_d \frac{T_j(d)}{\sqrt{d \log\log d}} \in (0, \infty).$$

Breuer states his results for a fixed elliptic curve $E_{/F_0}$, but a routine twisting argument gives the result for fixed j.

From this perspective, our Theorem 1.4 can be viewed as sharpening Theorem 6.3a) by computing the value of $\limsup_d \frac{T_j(d)}{d \log\log d}$ for every CM j-invariant. We will now give an analogous sharpening of Theorem 6.3b). For a non-CM elliptic curve E defined over a number field F, we define the **reduced Galois representation**

$$\overline{\rho}_N \colon \mathfrak{g}_F \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$$

as the composite of the mod N Galois representation $\rho_N \colon \mathfrak{g}_F \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ with the quotient map $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$. The point is that if $(E_1)_{/F}$ and $(E_2)_{/F}$ have $j(E_1) = j(E_2)$, then their reduced Galois representations are the same (up to conjugacy in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$). We say that $j \in \overline{\mathbb{Q}}$ is **truly Serre** if for every $E_{/F_0}$ with $j(E) = j$, then $\overline{\rho}_N$ is surjective for all $N \in \mathbb{Z}^+$.

Theorem 6.4. *Let $j \in \overline{\mathbb{Q}} \subset \mathbb{C}$ be a non-CM j-invariant, and let $F_0 = \mathbb{Q}(j)$.*

a) *We have*

$$\limsup_{d \to \infty} \frac{T_j(d)}{\sqrt{d \log\log d}} \geq \sqrt{\frac{\pi^2 e^\gamma}{3[F_0 : \mathbb{Q}]}}. \tag{20}$$

b) *If j is truly Serre, then*

$$\limsup_{d \to \infty} \frac{T_j(d)}{\sqrt{d \log\log d}} = \sqrt{\frac{\pi^2 e^\gamma}{3[F_0 : \mathbb{Q}]}}. \tag{21}$$

Proof. a) Let $(E_0)_{/F_0}$ be an elliptic curve with $j(E_0) = j$. Let $r \geq 2$, let N_r be the product of all primes $p \leq r$, and let $F_{N_r} = F_0(x(E_0[N_r]))$. Then

$$d_r := [F_{N_r} : \mathbb{Q}] \mid [F_0 : \mathbb{Q}] \frac{\# \mathrm{GL}_2(\mathbb{Z}/N_r\mathbb{Z})}{2} = [F_0 : \mathbb{Q}] \frac{\prod_{p \leq r}(p^2 - 1)(p^2 - p)}{2}.$$

The mod N_r-Galois representation on $(E_0)_{/F_{N_r}}$ has image contained in $\{\pm 1\}$ and thus is given by a quadratic character $\chi\colon \mathrm{Aut}(\overline{F_{N_r}}/F_{N_r}) \to \{\pm 1\}$. Let $(E_{N_r})_{/F_{N_r}}$ be the twist of $(E_0)_{/F_{N_r}}$ by χ, so that

$$(\mathbb{Z}/N_r\mathbb{Z})^2 \hookrightarrow E_{N_r}(F_{N_r})$$

and thus

$$\# E_{N_r}(F_{N_r})[\mathrm{tors}] \geq N_r^2.$$

Arguments very similar to those made above – using the Euler product for $\zeta(2)$, Mertens' Theorem and the Prime Number Theorem – give

$$d_r \leq (1+o(1))\frac{3[F_0:\mathbb{Q}]}{\pi^2 e^{\gamma}\log r}N_r^4$$

and

$$\#E(F_{N_r})[\mathrm{tors}]^2 \geq N_r^4 \geq (1+o(1))\frac{\pi^2 e^{\gamma}}{3[F_0:\mathbb{Q}]}d_r \log\log d_r,$$

and thus (20) follows.

b) Let $E_{/F}$ be an elliptic curve with $j(E)=j$ and $[F:\mathbb{Q}]=d$. We may and shall assume that $d \geq 3$ and that $\#E(F)[\mathrm{tors}] \geq 5$. Write

$$E(F)[\mathrm{tors}] \cong \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/ab\mathbb{Z}$$

for $a,b \in \mathbb{Z}^+$, and note that we have $ab \geq 3$.

Step 1: We claim that there is a number field $L \supset F$ such that $F(E[ab]) \subset L$ and $[L:F] \leq b^2$. This is the non-CM analogue of [7, Thm. 7]. As in *loc. cit.* primary decomposition and induction quickly reduce us to the consideration of the case $a=p^A$, $b=p$ for a prime number p and $A \in \mathbb{N}$, and we must show that we have full p^{A+1}-torsion in an extension of degree at most p^2. If $A=0$, then we have an F-rational point P of order p. If $Q \in E[p] \setminus \langle P \rangle$, then the Galois orbit on Q has size at most p^2-p, so we may take $L=F(Q)$ and get $[L:F] \leq p^2-p$. If $A \geq 1$, then E has full p^A-torsion defined over F and an F-rational point P of order p^{A+1}. Let $Q \in E[p^{A+1}]$ be such that $\langle P,Q\rangle = E[p^{A+1}]$. For $\sigma \in \mathfrak{g}_F$, we have $p\sigma(Q)=\sigma(pQ)=pQ$, so there is $R_\sigma \in E[p]$ such that

$$\sigma(Q)=Q+R_\sigma.$$

Thus there are at most p^2 possibilities for $\sigma(Q)$, so again we may take $L=F(Q)$.

Step 2: Let $W(N)=F_0(x(E[N]))$. Then $L \supset W(ab)$, and thus

$$[L:\mathbb{Q}] \geq [W(ab):F_0][F_0:\mathbb{Q}] = [F_0:\mathbb{Q}]\frac{\#\,\mathrm{GL}_2(\mathbb{Z}/ab\mathbb{Z})}{2}.$$

Hence,

$$d=[F:\mathbb{Q}] \geq \frac{[L:\mathbb{Q}]}{b^2} \geq \frac{[F_0:\mathbb{Q}]}{2b^2}\#\,\mathrm{GL}_2(\mathbb{Z}/ab\mathbb{Z}).$$

Multiplying by a^4b^4 and rearranging, we get

$$\#E(F)[\mathrm{tors}]^2 = a^4b^2 \leq \frac{2d}{[F_0:\mathbb{Q}]}\cdot\frac{(ab)^4}{\#\,\mathrm{GL}_2(\mathbb{Z}/ab\mathbb{Z})}.$$

Now

$$\frac{(ab)^4}{\#\,\mathrm{GL}_2(\mathbb{Z}/ab\mathbb{Z})} = \prod_{p\mid ab}\frac{p^4}{(p^2-1)(p^2-p)} = \prod_{p\mid ab}\left(1-\frac{1}{p^2}\right)^{-1}\prod_{p\mid ab}\left(1-\frac{1}{p}\right)^{-1}$$
$$\leq \frac{\pi^2}{6}\prod_{p\mid ab}\left(1-\frac{1}{p}\right)^{-1}.$$

Substituting this above,

$$\#E(F)[\mathrm{tors}]^2 = a^4b^2 \leq \frac{\pi^2}{3[F_0:\mathbb{Q}]}d\prod_{p\mid ab}\left(1-\frac{1}{p}\right)^{-1}. \tag{22}$$

Rearranging,

$$d \geq \frac{3[F_0:\mathbb{Q}]}{\pi^2} \cdot a^4 b^2 \cdot \prod_{p \mid ab} (1-1/p) = \frac{3[F_0:\mathbb{Q}]}{\pi^2} a^3 b \cdot \varphi(ab) > \frac{1}{2} ab.$$

(In the last step, we used the lower bound $\varphi(ab) \geq 2$.) The product in (22) is only increased if p is taken to run over the first ω primes, where ω is the number of distinct primes dividing ab. For large d, the first ω primes all belong to the interval $[1, 2\log d]$; otherwise, their product would exceed $2d$ (by the prime number theorem), forcing $ab > 2d$, and contradicting the last displayed inequality. Hence, as $d \to \infty$,

$$\prod_{p \mid ab} \left(1 - \frac{1}{p}\right)^{-1} \leq \prod_{p \leq 2 \log d} \left(1 - \frac{1}{p}\right)^{-1} = (1 + o(1)) e^{\gamma} \log\log d.$$

Plugging this back into (22) and taking square roots yields the upper bound

$$T_j(d) \leq \left(\sqrt{\frac{\pi^2 e^{\gamma}}{3[F_0:\mathbb{Q}]}} + o(1) \right) \sqrt{d \log\log d}.$$

Combining this with the lower bound from part a), the result follows. □

Remark 1.

a) If $E_{/F_0}$ is an elliptic curve over a number field with surjective adelic Galois representation $\hat{\rho}\colon \mathfrak{g}_{F_0} \to \mathrm{GL}_2(\widehat{\mathbb{Z}})$, then $j(E_0)$ is truly Serre. The converse also holds. Indeed, suppose j is truly Serre, and let $E_{/F_0}$ be any elliptic curve with $j(E) = j$, let $N \in \mathbb{Z}^+$, and let $\rho_N\colon \mathfrak{g}_{F_0} \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be the mod N Galois representation. By definition of truly Serre, we have $\langle \rho_N(\mathfrak{g}_{F_0}), -1 \rangle = \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. It follows [16, p. 145] that $\rho_N(\mathfrak{g}_{F_0}) = \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Since this holds for all $N \in \mathbb{Z}^+$, it follows that $\hat{\rho}$ is surjective.

b) Greicius showed [10, Thm. 1.2] that if $E_{/F_0}$ is an elliptic curve over a number field with surjective adelic Galois representation, then $F_0 \cap \mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}$ and $\sqrt{\Delta} \notin F_0\mathbb{Q}^{\mathrm{ab}}$, where Δ is the discriminant of any Weierstrass model of E. Thus if $[F_0:\mathbb{Q}] \leq 2$ the adelic Galois representation cannot be surjective. Greicius also exhibited an elliptic curve over a non-Galois cubic field with surjective adelic Galois representation [10, Thm. 1.5]. Zywina showed [20] that if $F_0 \supsetneq \mathbb{Q}$ is a number field such that $F_0 \cap \mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}$ then there is an elliptic curve $E_{/F_0}$ with surjective adelic Galois representation. In fact he shows that "most Weierstrass equations over F_0" define an elliptic curve with surjective adelic Galois representation. His work makes it plausible that when measured by height, "most $j \in F_0$" are truly Serre.

Acknowledgments

We thank Abbey Bourdon and Drew Sutherland for helpful and stimulating conversations on the subject matter of this paper. The second author is supported by the National Science Foundation [DMS-1402268].

References

[1] A. Bourdon and P.L. Clark. *Torsion points and Galois representations on CM elliptic curves.* https://arxiv.org/abs/1612.03229

[2] A. Bourdon, P.L. Clark and P. Pollack, *Anatomy of torsion in the CM case.* To appear in Math. Z.

[3] A. Bourdon, P.L. Clark and J. Stankewicz, *Torsion points on CM elliptic curves over real number fields.* To appear in Transactions of the AMS.

[4] A. Bourdon and P. Pollack. *Torsion subgroups of CM elliptic curves over odd degree number fields.* To appear in Int. Math. Res. Notices.

[5] F. Breuer, *Torsion bounds for elliptic curves and Drinfeld modules.* J. Number Theory 130 (2010), 1241-1250.

[6] P.L. Clark, B. Cook and J. Stankewicz, *Torsion points on elliptic curves with complex multiplication (with an appendix by Alex Rice).* International Journal of Number Theory 9 (2013), 447–479.

[7] P.L. Clark and P. Pollack. *The truth about torsion in the CM case.* C. R. Math. Acad. Sci. Paris **353** (2015), 683–688.

[8] H. Davenport. *Multiplicative number theory.* 3rd edition. Graduate Texts in Mathematics, no. 74. Springer-Verlag, New York, 2000.

[9] A. Fröhlich and M.J. Taylor, *Algebraic number theory.* Cambridge Studies in Advanced Mathematics, no. 27. Cambridge University Press, Cambridge, 1993.

[10] A. Greicius, *Elliptic curves with surjective adelic Galois representations.* Experiment. Math. 19 (2010), 495-507.

[11] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers.* Sixth edition. Oxford University Press, Oxford, 2008.

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

[13] N. McNew, P. Pollack, and C. Pomerance. *Numbers divisible by a large shifted prime and large torsion subgroups of CM elliptic curves.* To appear in Int. Math. Res. Notices.

[14] M. Rosen, *A generalization of Mertens' Theorem.* J. Ramanujan Math. Soc. **14** (1999), 1-19.

[15] J.-P. Serre, *Propriétés galoisiennes des points elliptiques.* Invent. Math. 15 (1972), no. 4, 259–331.

[16] J.-P. Serre, *Lectures on the Mordell-Weil theorem.* 3rd edition. Aspects of Mathematics. Friedr. Vieweg & Sohn, Braunschweig, 1997.

[17] J. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, no. 151. Springer-Verlag, 1994.

[18] P. Stevenhagen, *Hilbert's 12th problem, complex multiplication and Shimura reciprocity.* Class field theory – its centenary and prospect (Tokyo, 1998), 161-176, Adv. Stud. Pure Math., 30, Math. Soc. Japan, Tokyo, 2001.

[19] G. Tenenbaum, *Introduction to analytic and probabilistic number theory.* 3rd edition. Graduate Studies in Mathematics, no. 163. American Mathematical Society, Providence, RI, 2015.

[20] D. Zywina, *Elliptic curves with maximal Galois action on their torsion points.* Bull. Lond. Math. Soc. 42 (2010), 811-826.

Department of Mathematics, Boyd Graduate Studies Research Center, University of Georgia, Athens, GA 30602, USA

E-mail address: pete@math.uga.edu

E-mail address: pollack@uga.edu