THE TRUTH ABOUT TORSION IN THE CM CASE

PETE L. CLARK AND PAUL POLLACK

Abstract. Let $T_{\text{CM}}(d)$ be the maximum size of the torsion subgroup of an elliptic curve with complex multiplication defined over a degree $d$ number field. We show that there is an absolute, effective constant $C$ such that $T_{\text{CM}}(d) \leq Cd \log \log d$ for all $d \geq 3$.

For a commutative group $G$, we denote by $G[\text{tors}]$ the torsion subgroup of $G$.

1. Introduction

The aim of this note is to prove the following result.

**Theorem 1.** There is an absolute, effective constant $C$ such that for all number fields $F$ of degree $d \geq 3$ and all elliptic curves $E/F$ with complex multiplication,

$$\#E(F)[\text{tors}] \leq Cd \log \log d.$$ 

It is natural to compare this result with the following one.

**Theorem 2** (Hindry–Silverman [HS99]). For all number fields $F$ of degree $d \geq 2$ and all elliptic curves $E/F$ with $j$-invariant $j(E) \in \mathcal{O}_F$, we have

$$\#E(F)[\text{tors}] \leq 1977408d \log d.$$ 

Every CM elliptic curve $E/F$ has $j(E) \in \mathcal{O}_F$, but only finitely many $j \in \mathcal{O}_F$ are $j$-invariants of CM elliptic curves $E/F$. Thus Theorem 1 has a significantly stronger hypothesis and a slightly stronger conclusion than Theorem 2. But the improvement of $\log \log d$ over $\log d$ is interesting in view of the following result.

**Theorem 3** (Breuer [Br10]). Let $E/F$ be an elliptic curve over a number field. There exists a constant $c(E,F) > 0$, integers $3 \leq d_1 < d_2 < \ldots < d_n < \ldots$ and number fields $F_n > F$ with $[F_n : F] = d_n$ such that for all $n \in \mathbb{Z}^+$ we have

$$\#E(F_n)[\text{tors}] \geq \begin{cases} c(E,F)d_n \log \log d_n & \text{if } E \text{ has CM}, \\ c(E,F)\sqrt{d_n \log \log d_n} & \text{otherwise}. \end{cases}$$

Let $T_{\text{CM}}(d)$ be the maximum size of the torsion subgroup of a CM elliptic curve over a degree $d$ number field. Then Theorems 1 and 3 combine to tell us that the upper order of $T_{\text{CM}}(d)$ is $d \log \log d$:

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

To our knowledge, this is the first instance of an upper order result for torsion points on a class of abelian varieties over number fields of varying degree.

Define $T(d)$ as for $T_{\text{CM}}(d)$ but replacing “CM elliptic curve” with “elliptic curve”, and define $T_{-\text{CM}}(d)$ as for $T_{\text{CM}}(d)$ but replacing “CM elliptic curve” with “elliptic curve without CM”. Hindry and Silverman ask whether $T_{-\text{CM}}(d)$ has upper order $\sqrt{d \log \log d}$. If so, the upper order of $T(d)$ would be $d \log \log d$ [CCRS13, Conjecture 1].
2. Proof of the Main Theorem

2.1. Torsion Points and Ray Class Containment

Let $K$ be a number field. Let $O_K$ be the ring of integers of $K$, $\Delta_K$ the discriminant of $K$, $w_K$ the number of roots of unity in $K$ and $h_K$ the class number of $K$. By an “ideal of $O_K$” we shall always mean a nonzero ideal. For an ideal $a$ of $O_K$, we write $K^{(a)}$ for the $a$-ray class field of $K$. We also put $|a| = #O_K/a$ and

$$\varphi_K(a) = #(O_K/a)^\times = |a| \prod_{p|a} \left( 1 - \frac{1}{|p|} \right).$$

An elliptic curve $E$ defined over a field of characteristic 0 has complex multiplication (CM) if $\text{End} E \supseteq \mathbb{Z}$; then $\text{End} E$ is an order in an imaginary quadratic field. We say $E$ has $O$-CM if $\text{End} E \cong O$ and $K$-CM if $\text{End} E$ is an order in $K$.

**Lemma 4.** Let $K$ be an imaginary quadratic field and $a$ an ideal of $O_K$. Then

$$\frac{h_K \varphi_K(a)}{6} \leq \frac{h_K \varphi_K(a)}{w_K} \leq [K^{(a)} : K] \leq h_K \varphi_K(a).$$

**Proof.** This follows from [Co00, Corollary 3.2.4].

**Theorem 5.** Let $K$ be an imaginary quadratic field, $F \supseteq K$ a number field, $E/F$ a $K$-CM elliptic curve and $N \in \mathbb{Z}^+$. If $(\mathbb{Z}/N\mathbb{Z})^2 \hookrightarrow E(F)$, then $F \supseteq K^{(NO_K)}$.

**Proof.** The result is part of classical CM theory when $\text{End} E = O_K$ is the maximal order in $K$ [Si94, II.5.6]. We shall reduce to that case. There is an $O_K$-CM elliptic curve $E'/F$ and a canonical $F$-rational isogeny $\iota: E \rightarrow E'$ [CCRS13, Prop. 25]. There is a field embedding $F \hookrightarrow \mathbb{C}$ such that the base change of $\iota$ to $\mathbb{C}$ is, up to isomorphisms on the source and target, given by $\mathbb{C}/O \rightarrow \mathbb{C}/O_K$. If we put

$$P = 1/N + O \in E[N], \quad P' = 1/N + O_K \in E'[N],$$

then $\iota(P) = P'$ and $P'$ generates $E'[N]$ as an $O_K$-module. By assumption $P \in E(F)$, so $\iota(P) = P' \in E'(F)$. It follows that $(\mathbb{Z}/N\mathbb{Z})^2 \hookrightarrow E'(F)_{\text{tors}}$.

**Remark 6.** In fact one can show — e.g., using adelic methods — that for any $K$-CM elliptic curve $E$ defined over $\mathbb{C}$, the field obtained by adjoining to $K(j(E))$ the values of the Weber function at the $N$-torsion points of $E$ contains $K^{(NO_K)}$.

2.2. Squaring the Torsion Subgroup of a CM Elliptic Curve

**Theorem 7.** Let $K$ be an imaginary quadratic field, let $F \supseteq K$ a field extension, and let $E/F$ be a $K$-CM elliptic curve. Suppose that for positive integers $a$ and $b$ we have an injection $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/ab\mathbb{Z} \hookrightarrow E(F)$. Then $[F(E[ab]) : F] \leq b$.

**Proof.**

**Step 1:** Let $O = \text{End} E$. For $N \in \mathbb{Z}^+$, let $C_N = (O/NO)^\times$. Let $E[N] = E[N](\overline{F})$. As an $O/NO$-module, $E[N]$ is free of rank 1. Let $g_F = \text{Aut}(\overline{F}/F)$, and let $\rho_N: g_F \rightarrow \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be the mod $N$ Galois representation associated to $E/F$. Because $E$ has $O$-CM and $F \supseteq K$, we have

$$\rho_N: g_F \rightarrow \text{Aut}_O E[N] \cong \text{GL}_1(O/NO) \cong (O/NO)^\times = C_N.$$
Let $\Delta$ be the discriminant of $\mathcal{O}$. Then $e_1 = 1$, $e_2 = \frac{\Delta + \sqrt{\Delta}}{2}$ is a $\mathbb{Z}$-basis for $\mathcal{O}$. The induced ring embedding $\mathcal{O} \hookrightarrow M_2(\mathbb{Z})$ is given by $\alpha e_1 + \beta e_2 \mapsto \begin{bmatrix} \alpha & \frac{\beta - \beta \Delta}{\alpha} \\ \beta & \alpha + \beta \Delta \end{bmatrix}$. So

$$C_N = \left\{ \begin{bmatrix} \alpha & \frac{\beta - \beta \Delta}{\alpha} \\ \beta & \alpha + \beta \Delta \end{bmatrix} \mid \alpha, \beta \in \mathbb{Z}/N\mathbb{Z}, \text{ and} \right\} \begin{bmatrix} \alpha^2 + \Delta \alpha \beta + \left(\frac{\Delta^2 - \Delta}{4}\right) \beta^2 \in (\mathbb{Z}/N\mathbb{Z})^2 \end{bmatrix}.$$  

From this we easily deduce the following useful facts:

(i) $C_N$ contains the homotheties $\{[\frac{0}{1}] \mid \alpha \in (\mathbb{Z}/N\mathbb{Z})^\times \}$.

(ii) For all primes $p$ and all $A, B \geq 1$, the natural reduction map $C_{p^A} \to C_{p^B}$ is surjective and its kernel has size $p^{2B}$.

**Step 2:** Primary decomposition reduces us to the case $a = p^A$, $b = p^B$ with $A \geq 0$ and $B \geq 1$. By induction it suffices to treat the case $B = 1$: i.e., we assume $E(F)$ contains full $p^A$-torsion and a point of order $p^{A+1}$ and show $|F(E[p^{A+1}]) : F| \leq p$.

**Case $A = 0$:**

- If $\left(\frac{A}{p}\right) = 1$, then $C_p$ is conjugate to $\{[\begin{bmatrix} \alpha & \beta \\ 0 & \alpha \end{bmatrix} \mid \alpha, \beta \in \mathbb{F}_p^\times \}$. If $\alpha \neq 1$ (resp. $\beta \neq 1$) the only fixed points $(x, y) \in \mathbb{F}_p^2$ of $[\begin{bmatrix} \alpha & \beta \\ 0 & \alpha \end{bmatrix}]$ have $x = 0$ (resp. $y = 0$). Because $E(F)$ contains a point of order $p$ we must either have $\alpha = 1$ for all $[\begin{bmatrix} 0 & \beta \\ 0 & \alpha \end{bmatrix}] \in \rho_p(g_F)$ or $\beta = 1$ for all $[\begin{bmatrix} \alpha & 0 \\ 0 & \beta \end{bmatrix}] \in \rho_p(g_F)$. Either way, $\#\rho_p(g_F) \mid p - 1$.

- If $\left(\frac{A}{p}\right) = -1$, then $C_p$ acts simply transitively on $E[p] \setminus \{0\}$, so if we have one $F$-rational point of order $p$ then $E[p] \subset E(F)$, so $\#\rho_p(g_F) = 1$.

- If $\left(\frac{A}{p}\right) = 0$, then $C_p$ is conjugate to $\{[\begin{bmatrix} \alpha & \beta \\ 0 & \alpha \end{bmatrix} \mid \alpha \in \mathbb{F}_p^\times, \beta \in \mathbb{F}_p\} [BCS15, \S 4.2]$. Since $E(F)$ has a point of order $p$, every element of $\rho_p(g_F)$ has $1$ as an eigenvalue and thus $\rho_p(g_F) \subset \{[\begin{bmatrix} 0 & \beta \\ 0 & 1 \end{bmatrix} \mid \beta \in \mathbb{F}_p]\}$, so has order dividing $p$.

**Case $A \geq 1$:** By (ii), $\mathcal{K} = \ker C_{p^{A+1}} \to C_{p^A}$ has size $p^2$. Since $(\mathbb{Z}/p^A\mathbb{Z})^2 \hookrightarrow E(F)$, we have $\rho_{p^{A+1}}(g_F) \subset \mathcal{K}$. Since $E(F)$ has a point of order $p^{A+1}$, by (i) the homothety $[1+p^A \ 0 \ 0 \ 1+p^A]$ lies in $\mathcal{K} \setminus \rho_{p^{A+1}}(g_F)$. Therefore $\rho_{p^{A+1}}(g_F) \not\subseteq \mathcal{K}$, so $\#\rho_{p^{A+1}}(g_F) \mid p$.  

2.3. Uniform Bound for Euler’s Function in Imaginary Quadratic Fields

Let $a$ be an ideal in an imaginary quadratic field $K$. To apply the results of §2.1, we require a lower bound on $\frac{\varphi_K(a)}{|a|}$. For fixed $K$, it is straightforward to adapt a classical argument of Landau (see the proof of [HW08, Theorem 328, p. 352]). Replacing Landau’s use of Mertens’ Theorem with Rosen’s number field analogue [Ro09], one obtains the following result: let $\gamma$ denote the Euler–Mascheroni constant, and let $\chi(\cdot) = (\Delta \chi)$ be the quadratic Dirichlet character associated to $K$. Then

$$\liminf_{|a| \to \infty} \frac{\varphi_K(a)}{|a|/\log \log |a|} = e^{-\gamma} \cdot L(1, \chi)^{-1}.$$  

Unfortunately, this result is not sufficient for our purposes. There are two sources of difficulty. First, the right-hand side depends on $K$, and can in fact be arbitrarily small (see [BCE50, (4)’]). Second, the statement only addresses limiting behavior as $|a| \to \infty$, and we need a result with no such restriction on $|a|$. However, looking back at Lemma 4 we see that a lower bound on $h_K \frac{\varphi_K(a)}{|a|}$ would suffice. The factor of $h_K$ allows us to prove a totally uniform lower bound.
**Theorem 8.** There is a positive, effective absolute constant $C$ such that for all imaginary quadratic fields $K$ and all nonzero ideals $a$ of $\mathcal{O}_K$ with $|a| \geq 3$, we have

$$\varphi_K(a) \geq \frac{C}{h_K} \cdot \frac{|a|}{\log \log |a|}.$$  

**Lemma 9.** For a fundamental quadratic discriminant $\Delta < 0$ let $K = \mathbb{Q}(\sqrt{\Delta})$, and let $\chi(\cdot) = (\Delta)$. There is an effective constant $C > 0$ such that for all $x \geq 2$,

$$\prod_{p \leq x} \left(1 - \frac{\chi(p)}{p}\right) \geq \frac{C}{h_K}.$$  

**Proof.** By the quadratic class number formula, $h_K \asymp L(1, \chi) \sqrt{|\Delta|}$ [Da00, eq. (15), p. 49]. Writing $L(1, \chi) = \prod_p (1 - \chi(p)/p)^{-1}$ and rearranging, we see (1) holds iff

$$\prod_{p > x} \left(1 - \frac{\chi(p)}{p}\right) \ll \sqrt{|\Delta|},$$

with an effective and absolute implied constant. By Mertens’ Theorem [HW08, Theorem 429, p. 466], the factors on the left-hand side of (2) indexed by $p \leq \exp(\sqrt{|\Delta|})$ make a contribution of $O(\sqrt{|\Delta|})$. Put $y = \max\{x, \exp(\sqrt{|\Delta|})\}$; it suffices to show that $\prod_{p > y} (1 - \chi(p)/p) \ll 1$. Taking logarithms, this will follow if we prove that $\sum_{p > y} \chi(p)/p = O(1)$. For $t \geq \exp(\sqrt{|\Delta|})$, the explicit formula gives $S(t) := \sum_{p \leq t} \chi(p) \log p = -\frac{t^\beta}{\beta} + O(t/\log t)$, where the main term is present only if $L(s, \chi)$ has a Siegel zero $\beta$. (C.f. [Da00, eq. (8), p. 123].) We will assume the Siegel zero exists; otherwise the argument is similar but simpler. By partial summation,

$$\sum_{p > y} \frac{\chi(p)}{p} = -\frac{S(y)}{y \log y} + \int_y^\infty \frac{S(t)}{t^2 \log t} \frac{1}{2} (1 + \log t) \, dt$$

$$\ll 1 + \int_y^\infty \frac{t^\beta}{t^2 \log t} \, dt.$$  

Haneke, Goldfeld–Schinzel, and Pintz have each shown that $\beta \leq 1 - \frac{c}{\sqrt{|\Delta|}}$, where the constant $c > 0$ is absolute and effective [Ha73, GS75, P76]. Using this to bound $t^\beta$, and keeping in mind that $y \geq \exp(\sqrt{|\Delta|})$, we see that the final integral is at most

$$\int_{\exp(\sqrt{|\Delta|})}^\infty \frac{\exp(-c \log t / \sqrt{|\Delta|})}{t \log t} \, dt.$$  

A change of variables transforms the integral into $\int_1^\infty \exp(-cu) u^{-1} \, du$, which converges. Assembling our estimates completes the proof. \hfill \Box

**Proof of Theorem 8.** Write $\varphi_K(a) = |a| \prod_{p | a} (1 - 1/|p|)$, and notice that the factors are increasing in $|p|$. So if $z \geq 2$ is such that $\prod_{|p| \leq z} |p| \geq |a|$, then

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

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 \( |p| \leq z \) according to the splitting behavior of the rational prime \( p \) lying below \( p \).

Noting that \( p \leq |p| \), Mertens’ Theorem and Lemma 9 yield

\[
\prod_{|p| \leq z} \left( 1 - \frac{1}{|p|} \right) \geq \prod_{p \leq z} \left( 1 - \frac{1}{p} \right) \left( 1 - \frac{\phi(p)}{p} \right)
\]

(4)

\[
\gg (\log z)^{-1} \prod_{p \leq z} \left( 1 - \frac{\phi(p)}{p} \right) \gg (\log z)^{-1} : h_K^{-1}.
\]

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

\[
z = (C' \log |a|)^2.
\]

We must check that \( \prod_{|p| \leq z} |p| \geq |a| \). The Prime Number Theorem implies

\[
\prod_{|p| \leq z} |p| \geq \prod_{p \leq z^{1/2}} p \geq \prod_{p \leq C' \log |a|} p \geq |a|;
\]

provided that \( C' \) was chosen appropriately. Combining (3), (4), and (5) gives

\[
\varphi_K(a) \gg |a| \cdot (\log z)^{-1} : h_K^{-1} \gg h_K^{-1} \cdot |a| \cdot (\log(\log(|a|)))^{-1}.
\]

\[\Box\]

2.4. Proof of Theorem 1

Let \( F \) be a number field of degree \( d \geq 3 \), and let \( E/F \) be a \( K \)-CM elliptic curve. We may assume \( \#E(F)[\text{tors}] \geq 3 \). We have \( E(FK)[\text{tors}] \cong \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/ab\mathbb{Z} \) for positive integers \( a \) and \( b \). Theorem 5 gives \( FK \supseteq K(aO_K) \). Along with Lemma 4 we get

\[
2d \geq [FK : \mathbb{Q}] \geq [K(aO_K) : \mathbb{Q}] \geq \frac{h_K\varphi_K(aO_K)}{3}.
\]

By Theorem 7, there is an extension \( L/FK \) with \( (\mathbb{Z}/ab\mathbb{Z}) \rightarrow E(L) \) and \( [L : FK] \leq b \).

Applying Theorem 5 and Lemma 4 as above we get \( L \supseteq K(abO_K) \) and

\[
[L : \mathbb{Q}] \geq [K(abO_K) : \mathbb{Q}] \geq \frac{h_K\varphi_K(abO_K)}{3},
\]

so

\[
d = [F : \mathbb{Q}] \geq \frac{[FK : \mathbb{Q}]}{2} = \frac{[L : \mathbb{Q}]}{2[L : FK]} \geq \frac{[L : \mathbb{Q}]}{2b} \geq \frac{h_K\varphi_K(abO_K)}{6b}.
\]

Multiplying (6) through by \((ab)^2 = |abO_K|\) and rearranging, we get

\[
\#E(FK)[\text{tors}] = a^2b \leq 6 \frac{d}{h_K\varphi_K(abO_K)} |abO_K|.
\]

By Theorem 8 we have

\[
\frac{|abO_K|}{\varphi_K(abO_K)} \ll h_K \log \log |abO_K| \leq h_K \log \log (a^2b)^2 \ll h_K \log \log \#E(FK)[\text{tors}].
\]

Combining (7) and (8) gives

\[
\#E(FK)[\text{tors}] \ll d \log \log \#E(FK)[\text{tors}]
\]

and thus

\[
\#E(F)[\text{tors}] \leq \#E(FK)[\text{tors}] \ll d \log \log d.
\]

Acknowledgments. Thanks to John Voight for his encouragement and to Abbey Bourdon for pointing out an error in a previous draft. We are grateful to the referee for a careful reading of the manuscript.
References

[BCE50] P.T. Bateman, S. Chowla and P. Erdős, Remarks on the size of $L(1, \chi)$. Publ. Math. Debrecen 1 (1950), 165–182.

[BCS15] A. Bourdon, P.L. Clark and J. Stankewicz, Torsion points on CM elliptic curves over real number fields, submitted for publication.

[Br10] F. Breuer, Torsion bounds for elliptic curves and Drinfeld modules. J. Number Theory 130 (2010), 1241–1250.

[CCRS13] 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.

[Co00] H. Cohen, Advanced Topics in Computational Number Theory. Graduate Texts in Mathematics 193, Springer-Verlag, 2000.

[Da00] H. Davenport, Multiplicative Number Theory. Third edition. Graduate Texts in Mathematics, 74. Springer-Verlag, New York, 2000.

[Ha73] W. Haneke, Über die reellen Nullstellen der Dirichletschen L-Reihen. Acta Arith. 22 (1973), 391–421. Corrigendum in 31 (1976), 99–100.

[HS99] M. Hindry and J. Silverman, Sur le nombre de points de torsion rationnels sur une courbe elliptique. C. R. Acad. Sci. Paris Sér. I Math. 329 (1999), no. 2, 97–100.

[HW08] G.H. Hardy and E.M. Wright, An introduction to the theory of numbers. Sixth edition. Oxford University Press, Oxford, 2008.

[GS75] D.M. Goldfeld and A. Schinzel, On Siegel’s zero. Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4) 2 (1975), 571–583.

[Pi76] J. Pintz, Elementary methods in the theory of L-functions. II. On the greatest real zero of a real L-function. Acta Arith. 31 (1976), 273–289.

[Ro99] M. Rosen, A generalization of Mertens’ Theorem. J. Ramanujan Math. Soc. 14 (1999), 1–19.

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